República Federativa do Brasil
Ministério da Indústria, Comércio Exterior
e Serviços
Instituto Nacional da Propriedade Industrial

(11) PI 0509577-8 B1

(22) Data do Depósito: 24/03/2005

(45) Data de Concessão: 12/12/2017

(54) Título: "DISPOSITIVO DE PROCESSAMENTO DE DADOS, MEIO DE GRAVAÇÃO E PROGRAMA DE PROCESSAMENTO DE DADOS".

(51) Int.Cl.: G06F 1/00

(30) Prioridade Unionista: 01/06/2004 JP 2004-163734, 02/04/2004 JP 2004-110069, 02/07/2004 JP 2004-196531, 07/07/2004 JP 2004-201009, 13/07/2004 JP 2004-206335, 17/05/2004 JP 2004-146963, 21/05/2004 JP 2004-151621

(73) Titular(es): PANASONIC INTELLECTUAL PROPERTY MANAGEMENT CO., LTD.

(72) Inventor(es): YUICHI FUTA; TOSHIHISA NAKANO; KAORU YOKOTA; MOTOJI OHMORI; MASAYA MIYAZAKI; MASAYA YAMAMOTO; KAORU MURASE; SENICHI ONODA; MASAO NONAKA

Relatório Descritivo da Patente de Invenção para **"DISPOSITIVO DE PROCESSAMENTO DE DADOS, MEIO DE GRAVAÇÃO E PROGRAMA DE PROCESSAMENTO DE DADOS".**

Campo Técnico

A presente invenção refere-se a uma tecnologia para verificar validade de conteúdo, especialmente com uma tecnologia para reduzir a carga de processamento envolvida em tal verificação.

Antecedentes da Técnica

Dispositivos para impedir atos fraudulentos envolvendo cópia ilegal, falsificação e substituição de conteúdo incluem aplicar informação de assinatura indicando que o conteúdo foi emitido por um mantenedor legítimo de direito bem como distribuir, junto com o conteúdo, informação de verificação para verificar se o conteúdo inclui conteúdo não autorizado no qual falsificação e assim por diante foi feita.

A Referência de Patente 1, sendo um exemplo de tal dispositivo, revela uma tecnologia para verificar a validade de conteúdo por distribuir informação de assinatura, informação de verificação e conteúdo via rede. De acordo com a tecnologia, a informação de autenticação inclui informação de assinatura de uma fonte de transmissão e informação de verificação para verificar a consistência de conteúdo individual parcial constituindo o conteúdo que é transmitido para um dispositivo de execução antes da transmissão do conteúdo. Quando recebendo a informação de autenticação, o dispositivo de execução verifica a informação de assinatura incluída na mesma. Se a verificação da informação de assinatura tiver sucesso, o dispositivo de execução recebe e executa o conteúdo. Em paralelo com a reprodução, o dispositivo de execução repete a verificação da consistência do conteúdo individual parcial por utilizar a informação de verificação e para a reprodução quando a verificação reprova.

Mesmo se o dispositivo de execução tiver recebido conteúdo incluindo conteúdo não autorizado, a tecnologia permite que o dispositivo de execução não inicie a reprodução do conteúdo ou pare a reprodução no meio. [Referência de Patente 1]

Publicação de Patente U.S. Nº 6480961;

[Referência de Patente 2]

Publicação de Patente Japonesa Exposta Nº 2002-281013;

[Referência que não é Patente 1]

http://positron.jfet.org/dvdvideo.html (Acessada em 17 de maio de 2004)

[Referência que não é de Patente 2]

http://www.pioneer.co.jp/crd1/tech/mpeg/1/html (Acessada em 17 de maior de 2004)

[Referência que não é de Patente 2]

"The Art of Computer Programming Vol.2 Seminumerical Algorithms" escrito por Donald E. Knuth, ISBN: 0-201-03822-6; e

[Referência que não é de Patente 4]

"Joho Security (Onformation Security)" escrito e editado por Atsuko Miyaji e Hiroaki Kikuchi e compilado por Information Processing Society of Japan.

Descrição da Invenção

[Problemas que a invenção é para resolver]

De acordo com a tecnologia convencional descrita acima, entretanto, o dispositivo de execução tem que continuar a verificar a informação de verificação em paralelo com a reprodução e portanto existe um problema pelo fato de que a carga de processamento do dispositivo de execução se torna alta durante a reprodução do conteúdo.

Adicionalmente, a partir de um ponto de vista de segurança, também é freqüente o caso em que o conteúdo codificado é distribuído, ao invés do conteúdo. Em tal caso, o dispositivo de execução também tem que conduzir o processamento de decriptografia em paralelo e assim a carga de processamento aumenta mais ainda.

Por conseqüência, o dispositivo de execução tem de ser equipado com um processador altamente eficiente operável para conduzir estes processos em paralelo.

A presente invenção resolve estes problemas e objetiva oferecer um dispositivo de processamento de dados, um método de processamento

de dados, um programa de processamento de dados e um meio de gravação que alcancem reprodução de conteúdo livre de obstáculos, mesmo se o processador equipado for pobremente eficiente, por reduzir a carga de processamento do dispositivo de execução durante a reprodução de conteúdo.

[Dispositivo para Resolver os Problemas]

De modo a realizar os objetivos acima, o dispositivo de processamento de dados da presente invenção utiliza um trabalho digital gravado em um meio de gravação também tendo gravado (i) uma pluralidade de valores de resumo de gravação gerados a partir de uma pluralidade de blocos de dados constituindo o trabalho digital e (ii) dados de assinatura de gravação gerados baseados em alguns ou em todos da pluralidade de valores de resumo de gravação nos mesmos. O dispositivo de processamento de dados compreende: uma unidade de utilização operável para utilizar o trabalho digital; uma unidade de seleção operável para aleatoriamente selecionar um número predeterminado de blocos de dados a partir da pluralidade de blocos de dados; uma unidade de cálculo operável para calcular um valor de resumo de cálculo com respeito a cada um dos blocos de dados selecionados; uma unidade de leitura operável para ler os valores de resumo de gravação restantes, cada um dos quais corresponde a um dos blocos de dados não selecionados, dentre a pluralidade de valores de resumo de gravação; uma unidade de verificação de assinatura operável para verificar se o trabalho digital é válido por utilizar os dados de assinatura de registro, os valores de resumo de cálculo e os valores de resumo de gravação restantes; e uma unidade de controle de utilização operável para impedir a unidade de utilização de utilizar o trabalho digital quando a unidade de verificação de assinatura julgar que o trabalho digital não é válido.

[Efeitos Vantajosos da Invenção]

De acordo com a estrutura acima, a unidade de seleção do dispositivo de processamento de dados da presente invenção seleciona um número predeterminado de blocos de dados a partir de uma pluralidade de blocos de dados. A unidade de cálculo calcula valores de resumo de cálculo a partir dos blocos de dados selecionados, enquanto a unidade de verifica-

ção de assinatura verifica a validade do trabalho digital por utilizar os valores de resumo de cálculo calculados, aos dados de assinatura de registro lidos a partir do meio de gravação e os dados de assinatura de registro restantes. Com isto, é possível reduzir uma série de cargas de processamento envolvidas na verificação dos dados de assinatura de registro por limitar os valores de resumo de cálculo para serem recentemente calculados até um número predeterminado.

Em adição, a seleção executada pela unidade de seleção é aleatória. Por conseqüência, blocos de dados diferentes serão alvos de verificação cada vez que a verificação for executada e portanto, é possível complementar, até alguma extensão, a degradação na precisão da verificação devido à limitação do número de blocos de dados utilizados para a verificação até um número predeterminado. Adicionalmente, é difícil para terceiros prognosticarem quais blocos de dados são para ser selecionados, o que torna possível impedir atos fraudulentos envolvendo falsificar ou substituir somente parte do trabalho digital não ser utilizado para verificação com a informação não autorizada.

No dispositivo de processamento de dados da presente invenção, a pluralidade de valores de resumo de registro pode incluir uma pluralidade de valores primários de resumo de registro, cada um dos quais é gerado para um da pluralidade de blocos de dados e uma pluralidade de valores secundários de resumo de registro gerados a partir de dois ou mais da pluralidade de valores primários de resumo de registro e os dados de assinatura de registro podem ser gerados por se executar uma assinatura digital na pluralidade de valores secundários de resumo de registro. A unidade de leitura pode ler os valores de resumo de registro restantes dentre a pluralidade de valores primários de resumo de registro. A unidade de verificação de assinatura pode verificar a validade do trabalho digital por calcular um ou mais valores secundários de resumo de cálculo baseada nos valores de resumo de cálculo e nos valores de resumo de registro restantes e executar uma verificação de assinatura digital com o uso dos dados de assinatura de registro, com a pluralidade de valores secundários de resumo de registro e

com os valores secundários de resumo de cálculo.

De acordo com a estrutura acima, os valores de resumo de registro incluem os primeiros valores de resumo de registro e os segundos valores de resumo de registro. A unidade de verificação de assinatura calcula um ou mais segundos valores de resumo de cálculo baseada nos valores de resumo de cálculo e nos valores de resumo de registro restantes. Por conseqüência, a unidade de leitura lê somente os primeiros valores de resumo de registro requeridos para cálculo dos segundos valores de resumo de cálculo e os segundos valores de resumo não correspondendo aos blocos de dados selecionados. Assim, é possível reduzir ao número total de valores de resumo de registro lidos a partir do meio de gravação.

No dispositivo de processamento de dados da presente invenção, o trabalho digital pode incluir uma pluralidade de arquivos, cada um dos quais corresponde a um da pluralidade de valores secundários de resumo de registro e é constituído por dois ou mais da pluralidade de blocos de dados. Cada um da pluralidade de valores secundários de resumo de registro pode ser gerado por se utilizar os valores primários de resumo de registro correspondendo um para um com os dois ou mais da pluralidade de blocos de dados constituindo um arquivo correspondendo aos valores secundários de resumo de registro. A unidade de verificação de assinatura pode incluir: uma subunidade primária de leitura operável para ler os dados de assinatura de registro a partir do meio de gravação; uma subunidade de cálculo operável para calcular um valor secundário de resumo de cálculo, com respeito a cada arquivo incluindo pelo menos um dos blocos de dados selecionados, por utilizar valores primários de resumo de registro correspondendo aos blocos de dados não selecionados incluídos no arquivo e os valores de resumo de cálculo correspondendo aos blocos de dados selecionados; uma subunidade secundária de leitura operável para ler, com respeito a cada arquivo incluindo nenhum dos blocos de dados selecionados, um valor secundário de resumo de registro correspondendo ao arquivo; uma subunidade de assinatura operável para gerar dados de assinatura de cálculo por executar a assinatura digital com o uso dos valores secundários de resumo de cálculo

calculados e os valores secundários de resumo de registro lidos e uma subunidade de comparação operável para comparar os dados de assinatura de cálculo com os dados de assinatura de registro. A unidade de verificação de assinatura pode verificar que o trabalho digital é válido quando os dados de assinatura de cálculo e os dados de assinatura de registro se conformarem um com outro e julgar que o trabalho digital não é válido quando os dados de assinatura de cálculo e os dados de assinatura de registro não se conformarem um com o outro.

De acordo com a estrutura acima, a unidade de leitura lê, com respeito a cada arquivo incluindo pelo menos um dos blocos de dados selecionados, os primeiros valores de resumo de registro correspondendo aos blocos de dados não selecionados incluídos no arquivo. Por outro lado, a segunda subunidade de leitura na unidade de verificação de assinatura lê, com respeito a cada arquivo incluindo nenhum dos blocos de dados selecionados, um segundo valor de resumo de registro correspondendo ao arquivo a partir do meio de gravação. Por conseqüência, é possível reduzir o número total de valores de resumo de registro lidos a partir do meio de gravação. Adicionalmente, é possível prontamente executar a verificação da validade do trabalho digital por gerar dados de assinatura de cálculo baseado nos segundos valores de resumo de registro e nos segundos valores de resumo de cálculo e comparar os dados de assinatura de cálculo gerados com os dados de assinatura de registro.

No dispositivo de processamento de dados da presente invenção, a pluralidade de valores de resumo de registro pode ser valores hash, cada um gerado por uma função hash. Os valores de resumo de cálculo calculados pela unidade de cálculo podem ser valores hash calculados pela aplicação da função hash junto a cada um dos blocos de dados selecionados. Os valores secundários de resumo de cálculo calculados pela subunidade de cálculo podem ser valores hash calculados pela aplicação da função hash junto aos valores primários de resumo de registro correspondendo aos blocos de dados não selecionados e aos valores de resumo de cálculo.

De acordo com a estrutura acima, os valores de resumo de re-

gistro são gerados pela função hash. A unidade de cálculo e a subunidade de cálculo calculam os valores de resumo de cálculo e os segundos valores de resumo de cálculo por utilizar a função hash.

Desde que a função hash se tornou uma função unidirecional, os blocos de dados utilizados para calcular os primeiros valores de resumo de registro correspondendo aos blocos de dados selecionados foram igualmente parcialmente diferentes dos blocos de dados selecionados e os primeiros valores de resumo de registro e os primeiros valores de resumo de cálculo não se conformam um com o outro. Por conseqüência, quando os blocos de dados selecionados tiverem sido falsificados, os valores de resumo de cálculo e os segundos valores de resumo de cálculo não concordam com os primeiros valores de resumo e com o segundo valores de resumo correspondentes gravados no meio de gravação. Desse modo, é possível precisamente detectar a falsificação dos blocos de dados selecionados.

No dispositivo de processamento de dados da presente invenção, o trabalho digital pode ser conteúdo digital e a unidade de utilização utiliza o conteúdo digital por reproduzir o conteúdo digital.

De acordo com a estrutura acima, a unidade de controle de utilização para a reprodução de conteúdo digital que foi falsificado. Com isto, é possível reduzir a circulação do conteúdo falsificado.

No dispositivo de processamento de dados da presente invenção, o trabalho digital pode ser um programa de computador e a unidade de utilização pode utilizar o programa de computador por decriptografar os códigos de instrução constituindo o programa de computador e operar de acordo com os códigos decriptografados.

De acordo com a estrutura acima, a unidade de controle de utilização para a execução do programa de computador que foi falsificado. Com isto, é possível impedir influências negativas causadas pela execução de programas não autorizados, tal como destruição de dados e de aplicação do usuário que não devem ser utilizados.

O dispositivo de processamento de dados da presente invenção pode compreender, ao invés da unidade de controle de utilização, uma uni-

dade de exibição de aviso operável para exibir, quando o trabalho digital é julgado como não sendo válido, um alerta de invalidade do trabalho digital.

De acordo com a estrutura acima, quando o trabalho digital é verificado como não sendo válido, por conseqüência, a unidade de exibição de aviso exibe e portanto, o dispositivo de processamento de dados é capaz de informar ao usuário que o trabalho digital gravado no meio de gravação não é autorizado. Desse modo, o usuário se torna ciente de que o trabalho digital gravado no meio de gravação não é autorizado e emprega medidas de proteção tal como não carregar o meio de gravação no dispositivo de processamento de dados a partir deste ponto. Assim, é possível evitar influências negativas possíveis causadas pela utilização do trabalho digital.

No dispositivo de processamento de dados da presente invenção, o meio de gravação possui adicionalmente gravado (i) conteúdo de enchimento possuindo um tamanho de dado ajustado de modo que a capacidade de espaço livre do meio de gravação se torne um valor predeterminado ou menor e (ii) dados de assinatura gerados baseados em parte ou em todo o trabalho digital e no conteúdo de enchimento. O dispositivo de processamento de dados pode adicionalmente compreender: uma unidade de verificação operável para verificar se o trabalho digital e o conteúdo de enchimento são válidos por utilizar o trabalho digital, o conteúdo de enchimento e os dados de assinatura. A unidade de controle de utilização operável para impedir a unidade de utilização de utilizar o trabalho digital quando a unidade de verificação julga que pelo menos um dentre o trabalho digital e o conteúdo de enchimento não é válido.

De acordo com a estrutura acima, o conteúdo de enchimento é gravado no meio de gravação. Se a capacidade de espaço livre for um valor predeterminado, o qual é suficientemente pequeno, ou mesmo menor do que o valor predeterminado, uma terceira pessoa não autorizada não pode adicionar informação não autorizada junto ao meio de gravação. Adicionalmente, o dispositivo de processamento de dados verifica não somente a validade do trabalho digital mas também do conteúdo de enchimento. Portanto, mesmo se parte ou todo o conteúdo de enchimento for falsificado, o dis-

positivo de processamento de dados impede o uso do trabalho digital. Por conseqüência, mesmo se informação não autorizada for distribuída de tal maneira, é possível impedir o uso da informação não autorizada.

No dispositivo de processamento de dados da presente invenção, o meio de gravação possui adicionalmente gravado (i) informação de área indicando uma área de acesso permitida, no meio de gravação, que um dispositivo externo é permitido de acessar e (ii) dados de assinatura gerados baseados em parte ou em todo o trabalho digital e na informação de área. O dispositivo de processamento de dados pode adicionalmente compreender: uma unidade de proibição de acesso operável para proibir acesso às áreas diferentes da área de acesso permitida baseado na informação de área; e uma unidade de verificação operável para verificar se o trabalho digital e a informação de área são válidos por utilizar o trabalho digital, a informação de área e os dados de assinatura. A unidade de controle de utilização operável para impedir a unidade de utilização de utilizar o trabalho digital quando a unidade de verificação julgar que pelo menos um dentre o trabalho digital e a informação de área não é válido.

Em geral, algumas vezes é o caso em que um arquivo de procedimento apresentando um procedimento para utilizar o trabalho digital está incluído, em adição ao trabalho digital, em um meio de gravação. De acordo com a estrutura acima, o dispositivo de processamento de dados não acessa áreas diferentes da área de acesso permitida indicada pela informação de área.

Por conseqüência, mesmo se uma terceira pessoa não autorizada tiver adicionado informação não autorizada para o espaço livre no meio de gravação e adicionalmente tiver falsificado o arquivo de procedimento de modo a ter a informação não autorizada utilizada, o dispositivo de processamento de dados não lê a informação não autorizada.

Em adição, desde que os dados de assinatura sejam gerados baseados no trabalho digital e na informação de área, a unidade de controle de utilização é capaz de impedir o uso do trabalho digital pela unidade de utilização mesmo se uma pessoa não autorizada tiver falsificado a informa-

ção de área. Assim, é possível impedir o uso da informação não autorizada.

Aqui, o dispositivo de processamento de dados nas reivindicações é um dispositivo de execução nas modalidades seguintes. Os blocos de dados nas reivindicações correspondem às unidades criptografadas na primeira, quinta e sexta modalidades, bem como correspondem ao conteúdo parcial na segunda até a quarta modalidades.

Breve Descrição dos Desenhos

A Figura 1 é um diagrama estrutural apresentando uma estrutura de um sistema de detecção de conteúdo não autorizado de uma primeira modalidade;

A Figura 2 é um diagrama de blocos apresentando uma estrutura de um dispositivo de distribuição 1100 da primeira modalidade;

A Figura 3 apresenta uma estrutura de conteúdo 1120 a ser informado para o dispositivo de distribuição 1100;

A Figura 4 apresenta uma estrutura de uma tabela de identificação de dispositivo 1130 armazenada por uma unidade de armazenamento de informação de dispositivo de execução 1104;

A Figura 5 apresenta os detalhes de um bloco chave 1150 gerado por uma unidade de geração de bloco chave 1103;

A Figura 6 apresenta um esboço geral de um procedimento de geração de conteúdo dividido executado por uma unidade de geração de unidade 1105;

A Figura 7 apresenta uma estrutura de informação de seleção de unidade 1200 gerada pela unidade de geração de unidade 1105;

A Figura 8 apresenta parte do processamento de criptografia executado por uma unidade de processamento de criptografia 1106;

A Figura 9 apresenta uma estrutura de conteúdo criptografado 1330 gerado pela unidade de processamento de criptografia 1106;

A Figura 10 apresenta um esboço geral de procedimento de geração de informação de cabeçalho 1260 executado por uma unidade de geração de informação de cabeçalho 1107;

A Figura 11 apresenta um procedimento de geração de uma pri-

meira tabela hash executado pela unidade de geração de informação de cabeçalho 1107;

A Figura 12 apresenta os detalhes de uma segunda tabela hash gerada pela unidade de geração de informação de cabeçalho 1107;

A Figura 13 apresenta o processamento conduzido por uma unidade de geração de informação de assinatura 1111;

A Figura 14 apresenta informação armazenada por um DVD 1500 da primeira modalidade;

A Figura 15 é um diagrama de blocos apresentando uma estrutura de um dispositivo de execução 1600 da primeira modalidade;

A Figura 16 apresenta um esboço geral do processamento de verificação da informação de assinatura executado por uma unidade de verificação de informação de assinatura 1611;

A Figura 17 apresenta parte do processamento conduzido pela unidade de verificação de informação de assinatura 1611;

A Figura 18 apresenta um procedimento de geração de uma primeira tabela hash substituída executado pela unidade de verificação de informação de assinatura 1611;

A Figura 19 apresenta um procedimento de geração de uma segunda tabela hash substituída executado pela unidade de verificação de informação de assinatura 1611;

A Figura 20 apresenta a verificação da informação de assinatura executada pela unidade de verificação de informação de assinatura 1611;

A Figura 21 é um fluxograma apresentando o comportamento operacional do dispositivo de distribuição 1100;

A Figura 22 é um fluxograma apresentando o comportamento operacional do dispositivo de distribuição 1100 (continuado a partir da Figura 21);

A Figura 23 apresenta um procedimento de verificação da informação de assinatura executada pelo dispositivo de execução 1600;

A Figura 24 é um fluxograma apresentando o comportamento operacional do dispositivo de execução 1600;

A Figura 25 é um fluxograma apresentando o comportamento operacional do dispositivo de execução 1600 (continuado a partir da Figura 24);

A Figura 26 é um diagrama de blocos apresentando uma estrutura de um dispositivo de execução 1100b de acordo com uma modificação da primeira modalidade;

A Figura 27 é um diagrama de blocos apresentando uma estrutura de um dispositivo de distribuição 2100 de acordo com uma segunda modalidade;

A Figura 28 apresenta o conteúdo 2120 e pedaços de informação de identificação a serem informados para o dispositivo de distribuição 2100;

A Figura 29 apresenta um esboço geral do processamento conduzido por uma unidade de seleção 2105;

A Figura 30 apresenta uma estrutura da informação de posição selecionada 2160 gerada por uma unidade de geração de informação de cabeçalho 2107;

A Figura 31 apresenta uma estrutura da informação de cabeçalho 2200 gerada pela unidade de geração de informação de cabeçalho 2107;

A Figura 32 apresenta uma estrutura de conteúdo criptografado gerado por uma unidade de processamento de criptografia 2109;

A Figura 33 apresenta informação gravada nem um DVD 2500 da segunda modalidade;

A Figura 34 é um diagrama de blocos apresentando uma estrutura de um aparelho de execução 2600 da segunda modalidade;

A Figura 35 é um fluxograma apresentando o comportamento operacional do dispositivo de distribuição 2100;

A Figura 36 é um fluxograma apresentando o comportamento operacional do dispositivo de execução 2600;

A Figura 37 é um diagrama de blocos apresentando uma estrutura de um dispositivo de distribuição 3100 de uma terceira modalidade;

A Figura 38 apresenta uma estrutura de informação de seleção de cabeçalho 3130 gerada por uma unidade de geração de informação de cabeçalho 3107;

A Figura 39 apresenta informação gravada em um DVD 3500 da terceira modalidade;

A Figura 40 é um diagrama de blocos apresentando uma estrutura de um dispositivo de execução 3600 da terceira modalidade;

A Figura 41 é um diagrama de blocos apresentando uma estrutura de um dispositivo de distribuição 4100 de uma quarta modalidade;

A Figura 42 apresenta conteúdo dividido e pedaços de informação de identificação gerados por uma unidade de geração de conteúdo parcial 4105;

A Figura 43 apresenta uma estrutura de informação de posição de conteúdo 4140 gerada por uma unidade de geração de informação de cabeçalho 4107;

A Figura 44 apresenta uma estrutura de informação de cabeçalho 4160 gerada pela unidade de geração de informação de cabeçalho 4107;

A Figura 45 apresenta informação gravada em um DVD 4500 da quarta modalidade;

A Figura 46 é um diagrama de blocos apresentando uma estrutura de um dispositivo de execução 4600 da quarta modalidade;

A Figura 47 apresenta um esboço geral de um procedimento de geração da informação de posição selecionada 4620 executado por uma unidade de seleção 46 11;

A Figura 48 apresenta um esboço geral de um procedimento de geração de informação de cabeçalho selecionada 4630 executado pela unidade de seleção 4611;

A Figura 49 apresenta um esboço geral do processamento de decriptografia conduzido por uma unidade de decriptografia de conteúdo parcial 4616;

A Figura 50 é um fluxograma apresentando o comportamento

operacional do dispositivo de distribuição 4100;

A Figura 51 apresenta um procedimento de geração de informação de assinatura 4170 executado pelo dispositivo de distribuição 4100;

A Figura 52 é um fluxograma apresentando o comportamento operacional do dispositivo de execução 4600;

A Figura 53 é um fluxograma apresentando o comportamento operacional do dispositivo de execução 4600 (continuado a partir da Figura 52);

A Figura 54 apresenta um procedimento de verificação para informação de assinatura e informação de cabeçalho executado pelo dispositivo de execução 4600;

A Figura 55 é um diagrama de blocos apresentando uma estrutura de um dispositivo de distribuição 5100 de uma quinta modalidade;

A Figura 56 apresenta uma estrutura de conteúdo de enchimento dividido 5120 gerado por uma unidade de geração de conteúdo de enchimento 5108;

A Figura 57 apresenta uma estrutura de informação de seleção de unidade 5140 emitida a partir da unidade de geração de conteúdo de enchimento 5108;

A Figura 58 apresenta um esboço geral de um procedimento de geração de informação de cabeçalho 5109 executado por uma unidade de geração de informação de cabeçalho 5107;

A Figura 59 apresenta uma estrutura de uma segunda tabela hash gerada por uma unidade de geração de informação de cabeçalho 5107;

A Figura 60 apresenta informação gravada em um DVD 5500 da quinta modalidade;

A Figura 61 é um diagrama de blocos apresentando uma estrutura de um dispositivo de execução 5600 da quinta modalidade;

A Figura 62 é um fluxograma apresentando o comportamento operacional do dispositivo de distribuição 5100;

A Figura 63 é um fluxograma apresentando o comportamento

operacional do dispositivo de distribuição 5100 (continuado a partir da Figura 62);

A FIG 64 é um fluxograma apresentando o comportamento operacional do dispositivo de execução 5600;

A Figura 65 apresenta um DVD não autorizado previsto 5500b;

A Figura 66 apresenta um DVD não autorizado previsto 5500c;

A Figura 67 é um diagrama de blocos apresentando uma estrutura de um dispositivo de distribuição 6100 de uma sexta modalidade;

A Figura 68 apresenta a informação de alocação escrita gerada por uma unidade de geração de alocação 6108;

A Figura 69 apresenta informação gravada em um DVD 6500 da sexta modalidade;

A Figura 70 é um digrama de blocos apresentando uma estrutura de um dispositivo de execução 6600 da sexta modalidade; e

A Figura 71 apresenta uma configuração do DVD 1500 e uma estrutura de uma unidade de aquisição 1601.

Melhor Modo para Realizar a Invenção

1. Primeira Modalidade

O dito a seguir descreve um sistema de detecção de conteúdo não autorizado 1 como um exemplo de modalidades da presente invenção, com o auxílio dos desenhos.

1.1 Sistema de Detecção de Conteúdo Não Autorizado 1

Como apresentado na Figura 1, o sistema de detecção de conteúdo não autorizado 1 compreende um dispositivo de distribuição 1100, um dispositivo de execução 1600 e um monitor 1620.

O dispositivo de distribuição 1100 é, como um exemplo, um dispositivo possuído por um mantenedor legítimo de direito de conteúdo incluindo vídeo e áudio. De acordo com as operações conduzidas por um operador, o dispositivo de distribuição 1100 adquire conteúdo e gera conteúdo criptografado por criptografar o conteúdo adquirido. Em adição, o dispositivo de distribuição de 1100 gera vários tipos de informação por utilizar o conteúdo. A informação gerada pelo dispositivo de distribuição 1100 inclui, por

exemplo, informação de cabeçalho utilizada no dispositivo de execução 1600 para verificar se conteúdo não autorizado está incluído no conteúdo. Adicionalmente, o dispositivo de distribuição 1100 gera informação de assinatura por utilizar uma chave de assinatura para ele próprio e grava o conteúdo criptografado gerado, a informação de assinatura, a informação de cabeçalho e assim por diante em um DVD (Disco Versátil Digital) 1500.

O DVD 1500 será vendido ou distribuído para usuários através das saídas de distribuição.

Quando carregado com o DVD 1500, o dispositivo de execução 1600 lê a informação de assinatura, a informação de cabeçalho e assim por diante a partir do DVD carregado 1500 e conduz verificação da informação de assinatura lida bem como verificação de se conteúdo não autorizado está incluído, baseado na informação lida a partir do DVD 1500.

Somente quando a verificação da informação de assinatura é bem sucedida, o dispositivo de execução 1600 inicia a reprodução do conteúdo.

Dispositivos individuais compondo o sistema de detecção de conteúdo não autorizado 1 e o DVD 1500 são descritos em detalhes abaixo.

1.2 Dispositivo de Distribuição 1100

Como apresentado na Figura 2, o dispositivo de distribuição 1100 compreende uma unidade de entrada 1101, uma unidade de geração de chave de conteúdo 1102, uma unidade de geração de bloco chave 1103, uma unidade de armazenamento de informação de dispositivo de execução 1104, uma unidade de geração de unidade 1105, uma unidade de processamento de criptografia 1106, uma unidade de geração de informação de cabeçalho 1107, uma unidade de geração de informação de assinatura 1111, uma unidade de armazenamento de chave de assinatura 1112 e uma unidade de regravação 1114.

1.2.1 Unidade de Entrada 1101

A unidade de entrada 1101 recebe conteúdo a partir de um dispositivo externo ou meio de gravação externo de acordo com operações do operador. Aqui é descrita uma estrutura dos conteúdos recebidos pela uni-

dade de entrada 1101 com o auxílio da Figura 3.

Como apresentado na Figura 3, o conteúdo 1120 recebido pela unidade de entrada 1101 é composto de c pedaços (c é um número inteiro de 1 ou maior) de arquivos "CNT1" 1121, "CNT2" 1122, "CNT3" 1123, ..., e "CNTc" 1124. Aqui, o conteúdo 1120 adquirido pela unidade de entrada 1101 é um formato executável para o dispositivo de execução 1600 (como será daqui para frente descrito em detalhes) e o formato DVD-Vídeo e o formato MPEG-2 (Moving Picture Experts Group 2) são exemplos de tais formatos executáveis. A presente modalidade é descrita pressupondo que o conteúdo 1120 está no formato DVD-Vídeo e cada um dos arquivos é um arquivo VOB (Objeto de Vídeo).

Quando adquirindo o conteúdo 1120, a unidade de entrada 1101 instrui a unidade de geração de chave de conteúdo 1102 para gerar uma chave de conteúdo e emite o conteúdo adquirido 1120 para a unidade de geração de unidade 1105.

1.2.2 Unidade de Geração de Chave de Conteúdo 1102

A unidade de geração de chave de conteúdo 1102 é instruída pela unidade de entrada 1101 para gerar a chave de conteúdo. Em resposta à instrução, a unidade de geração de chave de conteúdo 1102 gera um número pseudo-aleatório e então gera uma chave de conteúdo com 128 bits de comprimento "CK" com o uso do número pseudo-aleatório gerado. Ao invés de um número pseudo-aleatório, um número aleatório real pode ser gerado por se utilizar, por exemplo, ruído em um sinal. A referência que não é de Patente 3 fornece detalhes a cerca de um método para gerar números aleatórios. Em adição, um método diferente pode ser utilizado para gerar a chave de conteúdo.

Subseqüentemente, a unidade de geração de chave de conteúdo 1102 emite a chave de conteúdo gerada "CK" para a unidade de geração de bloco de chave 1103 e para a unidade de processamento de criptografia 1106.

1.2.3. *Unidade de Geração de Bloco de Chave 1103 e Unidade de Armazenamento de Informação de Dispositivo de Execução 1104*

A unidade de armazenamento de informação de dispositivo de execução 1104 é, por exemplo, composta de uma ROM ou de uma EEPROM, e armazena uma tabela de identificação de dispositivo 1130 como apresentado na Figura 4.

A tabela de identificação de dispositivo 1130 é composta de n pedaços de identificadores de dispositivo e n pedaços de chaves de dispositivo (n é um número natural). Os identificadores de dispositivo são pedaços de informação de identificação com cada pedaço sendo específico para um dispositivo que foi permitido de ler informação no DVD 1500 gravada pelo dispositivo de distribuição 1100 e executada pela informação lida. As chaves de dispositivo, as quais correspondem um para um com os identificadores de dispositivo, são pedaços de informação de chave respectivamente específicos para dispositivos individuais indicados pelos identificadores de dispositivo correspondentes. Por exemplo, um identificador de dispositivo "AID_1" 1131 corresponde a uma chave de dispositivo "CK" 1136.

A unidade de geração de bloco de chave 1103 recebe a chave de conteúdo "CK" a partir da unidade de geração de chave de conteúdo 1102 e gera um bloco de chave.

A Figura 5 apresenta um exemplo de uma estrutura de um bloco de chave 1150 gerado neste ponto. O bloco de chave 1150 é composto de n pedaços de identificadores de dispositivo e n pedaços de chaves de conteúdo criptografadas. Os identificadores de dispositivo são os mesmos que os identificadores de dispositivo incluídos na tabela de identificação de dispositivo 1130. Os identificadores de dispositivo correspondem um para um com as chaves de dispositivo criptografadas e as chaves de conteúdo criptografadas são geradas pela aplicação de um algorítmo de criptografia E1 junto à chave de conteúdo "CK" com o uso das chaves de dispositivo correspondentes. Por exemplo, um identificador de dispositivo "AID_1" 1141 é o mesmo que o identificador de dispositivo "AID_1" 1131 incluído na tabela de identificação de dispositivo 1130 e corresponde a uma chave de conteúdo cripto-

grafada "Enc (DK_1, CK" 1142. A chave de conteúdo criptografada "Enc (DK_1, CK)" 1142 é gerada pela criptografia da chave de conteúdo "CK" com o uso da chave de dispositivo "DK_1" 1136 incluída na tabela de identificação de dispositivo 1130. Na descrição que se segue, um texto criptografado gerado por se criptografar um texto não criptografado B com o uso de uma chave A é denotado como "Enc (A, B)".

Um procedimento para gerar um bloco de chave 1150 é descrito a seguir. Quando recebendo a chave de conteúdo "CK", a unidade de geração de bloco de chave 1103 lê o identificador de registro "AID_1" 1131 e a chave de dispositivo "DK_1" 1136 na primeira linha a partir da tabela de identificação de dispositivo 1130 da unidade de armazenamento de informação de dispositivo de execução 1104. A unidade de geração de bloco de chave 1103 gera a chave de conteúdo criptografada "Enc (DK_1, CK)" por aplicar o algorítmo de criptografia E1 junto à chave de conteúdo "CK" com o uso da chave de dispositivo lida "DK_1" 1136. Aqui, o AES (Padrão de Criptografia Avançado) é utilizado, como um exemplo, para o algorítmo de criptografia E1. A Referência que não é de Patente 4 fornece detalhes a cerca do AES. Observe que o sistema de criptografia utilizado aqui não está limitado ao AES, e um sistema diferente pode ser empregado.

A unidade de geração de bloco de chave 1103 armazena o identificador de dispositivo lido "AID_1" 1131 e a chave de conteúdo criptografada gerada "Enc (DK_1, CK)", associando estas duas uma com a outra.

A unidade de geração de bloco de chave 1103 repete o processamento do mesmo tipo para todos os n pares de identificadores de dispositivo e chaves de dispositivo, gera n pares de identificadores de dispositivo e chaves de conteúdo criptografadas e coloca estes pares juntos para formar o bloco de chave 1150.

Subseqüentemente, a unidade de geração de bloco de chave 1103 emite o bloco de chave gerado 1150 para a unidade de gravação 1114.

Aqui, como o exemplo mais simples, é descrito o caso no qual uma chave específica é designada para cada dispositivo operável para exe-

cutar a informação gravada no DVD 1500. Entretanto, as tecnologias descritas na Referência de Patente 2 incluem tecnologias para reduzir o número de chaves de conteúdo criptografadas e para impedir dispositivos específicos de executarem o conteúdo.

1.2.4 Unidade de Geração de Unidade 1105

A unidade de geração de unidade 1105 recebe o conteúdo 1120 a partir da unidade de entrada 1102. Quando recebendo o conteúdo 1120, a unidade de geração de unidade 1105 gera conteúdo dividido e informação de seleção de unidade em um procedimento descrito abaixo.

A seguir são descritas: geração de conteúdo dividido (a); e geração de informação de seleção de unidade (b).

(a) Geração de Conteúdo Dividido

Como apresentado na Figura 6, a unidade de geração de unidade 1105 gera conteúdo dividido 1160 a partir do conteúdo 1120. Um procedimento para gerar o conteúdo dividido 1160 é descrito a seguir com o auxílio da Figura 6.

Quando recebendo o conteúdo 1120, a unidade de geração de unidade 1105 gera um identificador de arquivo "FID1" 1161 e um pedaço de informação de identificação de arquivo "AD1" correspondendo ao arquivo "CNT1" 1121 incluído no conteúdo recebido 1120. O identificador de arquivo "FID1" 1161 é informação de identificação de forma única indicando o arquivo "CNT1" 1121 e é, por exemplo, um número natural indicando a ordem do arquivo "CNT1" 1121 dentro do conteúdo 1120 ou um nome do arquivo. O pedaço de informação de identificação de arquivo "AD1" é informação para identificar o arquivo "CNT1" 1121, e é, por exemplo, um deslocamento a partir do cabeçalho do conteúdo 1120, um número de setor, ou um endereço.

A seguir, a unidade de geração de unidade 1105 divide o arquivo "CNT1" 1121 com respeito a cada VOBU (Unidade de Objeto de Vídeo) para gerar m pedaços (m é qualquer número natural) de unidades "U1_1", "U1_2", ..., e "U1_m". Então, a unidade de geração de unidade 1105 gera um número de unidade "N1" que indica o número de unidades geradas (aqui, N1 = m).

A seguir, a unidade de geração de unidade 1105 gera informação de arquivo composta do identificador de arquivo "FID1" 1161, do pedaço de informação de identificação de arquivo "AD1" e do número de unidade "N1" e armazena a informação de arquivo gerada.

Então, a unidade de geração de unidade 1105 gera identificadores de unidade para as respectivas unidades. Os identificadores de unidade são pedaços de informação de identificação com cada pedaço de forma única identificando um dos m pedaços de unidades e pode ser, por exemplo, números ordinais começando a partir da unidade de cabeçalho, como 1, 2, 3, ..., e m, ou pode ser números acumulativos de bits a partir da unidade de cabeçalho. Na presente modalidade, pressupõe-se que os identificadores de unidade são números ordinais começando a partir da unidade de cabeçalho. Na explicação seguinte, um par de um identificador de unidade e uma unidade correspondente é referido como um pedaço de informação de unidade enquanto m pedaços de informação de unidade são coletivamente referidos como arquivo dividido. Assim, um arquivo dividido "splCNT1" 1171 gerado a partir do arquivo "CNT1" 1121 é composto de m pedaços de informação de unidade 1191, 1192, 1193, ..., e 1194 como apresentado na Figura 6. Cada pedaço de informação de unidade é composto de um identificador de unidade correspondente e de uma unidade. Como um exemplo, um pedaço de informação de unidade 1191 inclui um identificador de unidade "UID1_1" 1181 e uma unidade "U1_1" 1186.

A seguir, a unidade de geração de unidade 1105 gera a informação de arquivo dividido 1176 incluindo o identificador de arquivo "FID1" 1161 e o arquivo dividido "splCNT1" 1171.

A unidade de geração de unidade 1105 repete o processamento do mesmo tipo para todos os arquivos para gerar c pedaços de informação de arquivo e c pedaços de informação de arquivo dividido 1176, 1177, 1178, ..., e 1179. Aqui, os c pedaços gerados de informação de arquivo dividido são coletivamente referidos como o conteúdo dividido 1160. Observe que o número de unidades geradas m pode ser diferente de arquivo para arquivo.

A seguir, a unidade de geração de unidade 1105 emite o conte-

údo dividido gerado 1160 para a unidade de processamento de criptografia 1106.

Observe que a unidade de geração de unidade 1105 aqui gera identificadores de arquivo e informação de identificação de arquivo, entretanto, estes podem ser informados externamente junto com o conteúdo 1120.

Em adição, os arquivos individuais são divididos com respeito a cada VOBU, entretanto, a unidade de divisão não está limitada a isto. Por exemplo, cada um dos arquivos pode ser dividido a cada 64 kilobytes, ou cada parte correspondendo a um segundo do tempo de reprodução. Alternativamente, pode ser projetado deixar o operador informar a informação indicando a unidade de divisão.

(b) Geração de Informação de Seleção de Unidade

Após terminar a saída do conteúdo dividido 1160, a unidade de geração de unidade 1105 gera a informação seleção de unidade composta de c pedaços de informação de arquivo. A Figura 7 apresenta uma estrutura de informação de seleção de unidade 1200 gerada neste ponto.

A informação de seleção de unidade 1200 é composta de c pedaços de informação de arquivo 1201, 1202, ..., e 1204. Cada pedaço de informação de arquivo é composto de um identificador de arquivo, um pedaço de informação de identificação de arquivo e de um número de unidade.

Como um exemplo, um pedaço de informação de arquivo 1201 inclui um identificador de arquivo "FID1" 1211, um pedaço de informação de identificação de arquivo "AD1" 1216 e um número de unidade "N1" 1221.

A unidade de geração de unidade 1105 emite a informação de seleção de unidade gerada 1200 para a unidade de geração de informação de assinatura 1111 e para a unidade de gravação 1114.

1.2.5 Unidade de Processamento de Criptografia 1106

A unidade de processamento de criptografia 1106 recebe a chave de conteúdo "CK" a partir da unidade de geração de chave de conteúdo 1102 bem como recebe o conteúdo dividido 1160 a partir da unidade de geração de unidade 1105.

A Figura 8 apresenta parte do processamento conduzido pela unidade de processamento de criptografia 1106. O dito a seguir descreve o processamento conduzido pela unidade de processamento de criptografia 1106 com o auxílio da Figura 8.

Quando recebendo o conteúdo dividido 1160, a unidade de processamento de criptografia 1106 seleciona o arquivo dividido "splCNT1" 1171 incluído na informação de arquivo dividido 1176 compondo o conteúdo dividido recebido 1160. A unidade de processamento de criptografia 1106 extrai a unidade "U1_1" 1186 a partir do pedaço de cabeçalho da informação de unidade 1191 do arquivo dividido selecionado "splCNT1" 1171, e gera uma unidade criptografada "EU1_1" 1231 pela aplicação do algorítmo de criptografia E1 junto à unidade extraída "U1_1" 1186 com o uso da chave de conteúdo "CK". Aqui, EU1_1 = Enc (CK, U1_1).

A unidade de processamento de criptografia 1106 gera a informação de unidade criptografada 1241 composta da unidade criptografada gerada "EU1_1" 1231 e do identificador de unidade "UID1_1" 1181 que estão incluídos na informação de unidade 1191. Na explicação seguinte, um par de um identificador de unidade e de uma unidade criptografada correspondentes é referido como um pedaço de informação de unidade criptografada.

A unidade de processamento de criptografia 1106 repete o processamento do mesmo tipo para o resto da informação de unidade 1192, 1193, ..., 1994 para gerar pedaços correspondentes de informação de unidade criptografada 1242, 1243, ..., e 1244. Aqui, m pedaços de informação de unidade criptografada gerados a partir de um arquivo dividido são coletivamente referidos como arquivo dividido criptografado.

Como apresentando na Figura 8, um arquivo dividido criptografado "EsplCNT1" 1251 gerado a partir do arquivo dividido "splCNT1" 1171 no procedimento mencionado acima é composto de m pedaços da informação de unidade criptografada 1241, 1242, 1243, ..., e 1244. Cada pedaço da informação de unidade criptografada é gerado baseado em um pedaço da informação de unidade compondo o arquivo dividido 1171 e inclui um identi-

ficador de unidade e uma unidade criptografada. Por exemplo, a informação de unidade criptografada 1241 é gerada baseado na informação de unidade 1191 e inclui o identificador de unidade "UID1_1" 1181 e a unidade criptografada "EU1_1" 1231.

A seguir, a unidade de processamento de criptografia 1106 extrai uma unidade criptografada de cada pedaço da informação de unidade criptografada compondo o arquivo dividido criptografado gerado "EsplCNT1" 1251. Aqui, m pedaços de unidades criptografadas extraídas são corretivamente referidas como um arquivo criptografado "ECNT1".

Então, a unidade de processamento de criptografia 1106 gera a informação de arquivo dividido criptografada por substituir o arquivo dividido "splCNT1" 1171 incluído na informação de arquivo dividido 1176 pelo arquivo dividido criptografado gerado "EsplCNT1" 1251.

A unidade de processamento de criptografia 1106 faz o mesmo com os pedaços da informação de arquivo dividido 1177, 1178, ..., e 1179 para gerar a informação de arquivo dividido criptografado e os arquivos criptografados.

C pedaços de informação de arquivo dividido criptografado gerados neste ponto são coletivamente referidos como conteúdo dividido criptografado. Então, a unidade de processamento de criptografia 1106 emite o conteúdo dividido criptografado gerado para a unidade de geração de informação de cabeçalho 1107. A Figura 10 apresenta uma estrutura do conteúdo dividido criptografado 1210 emitido aqui.

A seguir, a unidade de processamento de criptografia 1106 emite c pedaços dos arquivos criptografados como conteúdo criptografado para a unidade de gravação 1114. A Figura 9 apresenta uma estrutura de conteúdo criptografado 1330 gerado aqui. O conteúdo criptografado 1330 é composto de c pedaços de arquivos criptografados "ECNT1" 1331, "ECNT2" 1332, "ECNT3" 1333, ..., e "ECNTc" 1334. Cada um dos arquivos criptografados é gerado baseado em um arquivo dividido criptografado incluído no conteúdo dividido criptografado e inclui uma pluralidade de unidades criptografadas. Como um exemplo, o arquivo criptografado "ECNT1" 1331 inclui

as unidades criptografadas "EU1_1", "EU1_2", ..., e assim por diante.

1.2.6 Unidade de Geração de Informação de Cabeçalho 1107

A unidade de geração de informação de cabeçalho 1107 recebe o conteúdo dividido criptografado 1210 a partir da unidade de processamento de criptografia 1106. Quando recebendo o conteúdo dividido criptografado 1210, a unidade de geração de informação de cabeçalho 1107 gera a informação de cabeçalho 1260 com o uso do conteúdo dividido criptografado recebido como apresentado na Figura 10.

A Figura 10 apresenta um esboço geral de um procedimento de geração da informação de cabeçalho 1260 executado pela unidade de geração de informação de cabeçalho 1107. O conteúdo dividido criptografado 1210 recebido pela unidade de geração de informação de cabeçalho 1107 é composto de c pedaços de informação de arquivo dividido criptografado 1246, 1247, 1248, ..., 1249. Cada pedaço da informação de arquivo dividido criptografado inclui um identificador de arquivo e um arquivo dividido criptografado. Por exemplo, um pedaço de informação de arquivo dividido criptografado 1246 inclui um identificador de arquivo "FID1" 1161 e um arquivo dividido criptografado "EsplCNT1" 1251.

A unidade de geração de informação de cabeçalho 1107 gera uma primeira tabela hash baseado em cada arquivo dividido incluído na informação de arquivo dividido criptografado 1246. Por exemplo, a unidade de geração de informação de cabeçalho 1107 gera uma primeira tabela hash "HA1TBL1" 1261 baseada no arquivo dividido criptografado "EsplCNT1" 1251. A unidade de geração de informação de cabeçalho 1107 gera uma segunda tabela hash "HA2TBL" 1269 a partir dos c pedaços gerados das primeiras tabelas hash.

Os procedimentos de geração da primeira e da segunda tabela hash mencionados acima são descritos em detalhes abaixo.

1.2.6.1 Geração da Primeira Tabela Hash

A Figura 11 apresenta um esboço geral de um procedimento de geração da primeira tabela hash "HA1TBL1" 1261 executado pela unidade de geração de informação de cabeçalho 1107.

O procedimento de geração da primeira tabela hash "HA1TBL1" 1261 é descrito abaixo com o auxílio da Figura 11. Um procedimento de geração para todas as primeiras tabelas hash "HA1TBL2", "HA1TBL3", ..., e "HA1TBLc" é o mesmo para a primeira tabela hash "HA1TBL1" 1261.

Primeiro, a unidade de geração de informação de cabeçalho 1107 extrai uma unidade criptografada "EU1_1" 1231 a partir da informação de unidade criptografada de cabeçalho 1241 compondo o arquivo dividido criptografado "EsplCNT1" 1251 e gera um valor hash da unidade "UHA1_1" 1271 por designar a unidade criptografada extraída "EU1_1" 1231 para uma função hash.

Aqui, SHA-1 (Algorítmo Hash Seguro 1) ou CBC-MAC (Encadeamento de Bloco Cifrado – Código de Autenticação de Mensagem) utilizando uma cifra de bloco é aplicado para a função hash.

Aqui, a unidade de geração de informação de cabeçalho 1107 gera a informação hash da unidade 1281 por substituir a unidade criptografada "EU1_1" 1231 da informação de unidade criptografada 1241 pelo valor hash da unidade gerado "UHA1_1" 1271.

A unidade de geração de informação de cabeçalho 1107 repete o processamento do mesmo tipo para o resto da informação de unidade criptografada 1242, 1243, ..., 1244 para gerar pedaços correspondentes de informação hash da unidade 1282, 1293, ..., e 1284. m pedaços de informação hash da unidade gerados neste ponto são coletivamente referidos como a primeira tabela hash "HA1TBL1" 1261. A Figura 11 apresenta uma estrutura da primeira tabela hash "HA1TBL1" 1261 gerada neste ponto.

1.2.6.2 Geração da Segunda tabela Hash

A unidade de geração de informação de cabeçalho 1107 repete o procedimento acima. Após completar a geração dos c pedaços das primeiras tabelas hash a partir do conteúdo dividido criptografado 1210, a unidade de geração de informação de cabeçalho 1107 gera a segunda tabela hash 1269 como apresentado na Figura 12 a partir dos c pedaços gerados das primeiras tabelas hash. A segunda tabela hash "HA2TBL" 1269 é composta de c pedaços da informação hash do arquivo 1301, 1302, 1303, ..., e 1304 e

cada pedaço da informação hash do arquivo inclui um identificador de arquivo e um valor hash do arquivo. Como um exemplo, um pedaço de informação hash do arquivo 1301 inclui o identificador de arquivo "FID1" 1161 e um valor hash de arquivo "FHA1" 1291.

Um procedimento de geração da segunda tabela hash 1269 é descrito abaixo.

A unidade de geração de informação de cabeçalho 1107 gera o valor hash do arquivo "FHA1" 1291 por designar, para a função hash, um resultado combinado formado pela combinação de todos os identificadores de unidade e os valores hash de unidade compondo a primeira tabela hash gerada "HA1TBL1" 1261.

Subseqüentemente, a unidade de geração de informação de cabeçalho 1107 extrai o identificador de arquivo "FID1" 1161 da informação de arquivo dividido criptografado 1246 correspondendo à primeira tabela hash "HA1TBL1" 1261, e gera a informação hash de arquivo 1301 composta do identificador de arquivo extraído "FID1" 1161 e do valor hash de arquivo gerado "FHA1" 1291.

A unidade de geração de informação de cabeçalho 1107 repete o processamento do mesmo tipo para as primeiras tabelas hash 1262, 1263, ..., e 1264 para gerar os pedaços de informação hash de arquivo 1302, 1303, ..., e 1304, respectivamente.

A seguir, a unidade de geração de informação de cabeçalho 1107 coloca estes c pedaços gerados de primeiras informações hash de arquivo juntas para formar a segunda tabela hash "HA2TBL" 1269.

Desse modo se conclui as descrições dos procedimentos de geração das primeiras tabelas hash (1.2.6.1) e da segunda tabela hash (1.2.6.2). A unidade de geração de informação de cabeçalho 1107 gera a informação de cabeçalho 1260 incluindo os c pedaços da primeira tabela hash e um único pedaço da segunda tabela hash "HA2TBL" 1269 gerada nos procedimentos mencionados acima e emite a informação de cabeçalho gerada 1260 para a unidade de gravação 1114.

Adicionalmente, a unidade de geração de informação de cabe-

çalho 1107 emite a segunda tabela hash gerada "HA2TBL" 1269 para a unidade de geração de informação de assinatura 1111.

1.2.7 Unidade de Geração de Informação de Assinatura 1111 e Unidade de Armazenamento de Chave de Assinatura 1112

A unidade de armazenamento de chave de assinatura 1112 que é composta de uma ROM armazena uma chave de assinatura 1113 específica para o dispositivo de distribuição 1100.

A Figura 13 apresenta um esboço geral do comportamento operacional da unidade de geração de informação de assinatura 1111. A geração de informação de assinatura executada pela unidade de geração de informação de assinatura 1111 é descrita abaixo com o auxílio da Figura 13.

A unidade de geração de informação de assinatura 1111 recebe a informação de seleção de unidade 1200 a partir da unidade de geração de unidade 1105 enquanto recebendo a segunda tabela hash "HA2TBL" 1269 a partir da unidade de geração de informação de cabeçalho 1107. Quando recebendo a informação de seleção de unidade 1200 e a segunda tabela hash 1269, a unidade de geração de informação de assinatura 1111 lê a chave de assinatura 1113 a partir da unidade de armazenamento de chave de assinatura 1112.

Subseqüentemente, a unidade de geração de informação de assinatura 1111 gera a informação de assinatura 1310 a partir da informação de seleção de unidade 1200 recebida e da segunda tabela hash 1269 com o uso da chave de assinatura lida 1113. Para ser mais específico, a unidade de geração de informação de assinatura 1111 aplica, com o uso da chave de assinatura lida 1113, um algorítmo de geração de assinatura S junto ao resultado combinado formado pela combinação dos c pedaços dos valores hash de arquivo incluídos na segunda tabela hash recebida 1269 com os c pedaços de informação de arquivo incluídos na informação de seleção de unidade 1200.

Como um exemplo, o DSA (Algorítmo de Assinatura Digital) é utilizado para o algorítmo de geração de assinatura S.

Então, a unidade de geração de informação de assinatura 1111

emite a informação de assinatura gerada 1310 para a unidade de gravação 1114.

1.2.8 Unidade de Gravação 1114

A unidade de gravação 1114 é carregada com o DVD 1500.

A unidade de gravação 1114 recebe: o bloco de chave 1150 a partir da unidade de geração de bloco de chave 1103; a informação de seleção de unidade 1200 a partir da unidade de geração de unidade 1105; o conteúdo criptografado 1330 a partir da unidade de processamento de criptografia 1106; a informação de cabeçalho 1260 a partir da unidade de geração de informação de cabeçalho 1107; e a informação de assinatura 1310 a partir da unidade de geração de informação de assinatura 1111.

Quando recebendo as informações acima, a unidade de gravação 1114 grava o bloco de chave recebido 1150, a informação de seleção de unidade 1200, a informação de cabeçalho 1260, a informação de assinatura 1310 e o conteúdo criptografado 1330 junto ao DVD 1500.

1.3 DVD 1500

O DVD 1500 é um meio de disco óptico transportável carregado no dispositivo de execução 1600.

Como apresentado na Figura 14, o DVD 1500 armazena um bloco de chave 1510, a informação de seleção de unidade 1530, a informação de cabeçalho 1550, a informação de assinatura 1570 e o conteúdo criptografado 1580. Estes foram gravados pelo dispositivo de distribuição 1100 e são os mesmos que o bloco de chave 1150, a informação de seleção de unidade 1200, a informação de cabeçalho 1260, a informação de assinatura 1310 e o conteúdo criptografado 1330 gerados pelo dispositivo de distribuição 1100, respectivamente. Portanto, descrições resumidas serão proporcionadas para estes itens.

1.3.1 Bloco de Chave 1510

O bloco de chave 1510 é composto de n pedaços de identificadores de dispositivo "AID_1", "AID_2", "AID_3", ..., e "AID_n" e n pedaços de chaves de conteúdo criptografadas "Enc (DK_1, CK)", "Enc (DK_2, CK)", "Enc (DK_3, CK)", ..., e "Enc (DK_n, CK)" que correspondem aos n pedaços

de identificadores de dispositivo, respectivamente.

1.3.2 Informação de Seleção de Unidade 1530

A informação de seleção de unidade 1530 é composta de c pedaços de informação de arquivo 1541, 1542, ..., e assim por diante e cada pedaço de informação de arquivo inclui um identificador de arquivo, informação de identificação de arquivo e um número de unidade. Pedaços individuais da informação de arquivo correspondem aos arquivos criptografados 1580. Em adição, cada um dos arquivos corresponde a uma primeira tabela hash incluída na informação de cabeçalho 1550.

1.3.3 Conteúdo Criptografado 1580

O conteúdo criptografado 1580 é composto de c pedaços de arquivos criptografados 1581, 1582, 1583, ..., e 1587. Cada um dos arquivos criptografados inclui uma pluralidade de unidades criptografadas.

1.3.4 Informação de Cabeçalho 1550

A informação de cabeçalho 1550 é composta de c pedaços de primeiras tabelas hash 1551, 1552, ..., e 1557 e de uma segunda tabela hash 1556.

Cada uma das primeiras tabelas hash é composta de uma pluralidade de pedaços de informação hash da unidade e cada pedaço da informação hash da unidade inclui um identificador de unidade e um valor hash da unidade.

A segunda tabela hash 1556 é composta de c pedaços de informação hash do arquivo 1561, 1562, 1563, ..., e 1567 e cada pedaço da informação hash do arquivo inclui um identificador de arquivo e um valor hash do arquivo.

1.3.5 Informação de Assinatura 1570

A informação de assinatura 1570 é gerada pela aplicação do algorítmo de geração de assinatura S junto a um resultado combinado formado pela combinação de c pedaços de valores hash do arquivo incluídos a segunda tabela hash 1556 com c pedaços de informação de arquivo incluídos na informação de seleção de unidade 1530.

1.4. Dispositivo de Execução 1600

Como apresentado na Figura 15, o dispositivo de execução 1600 é composto de uma unidade de aquisição 1601, de uma unidade de aquisição de chave de conteúdo 1602, de uma unidade de armazenamento de chave de dispositivo 1604, de uma unidade de execução 1606, de uma unidade de verificação de informação de assinatura 1611 e de uma unidade de armazenamento de chave de verificação 1612.

1.4.1 Unidade de Aquisição 1601

A unidade de aquisição 1601 é carregada com o DVD 1500. Quando detectando que o DVD 1500 está sendo carregado na mesma, a unidade de aquisição 1601 lê o bloco de chave 1510, a informação de seleção de unidade 1530, e a informação de assinatura 1570 a partir do DVD 1500 e emite o bloco de chave lido 1510 para a unidade de aquisição de chave de conteúdo 1602 enquanto emitindo a informação de seleção de unidade lida 1530 e a informação de assinatura 1570 para a unidade de verificação de informação de assinatura 1611.

Em adição, a unidade de aquisição 1601 lê toda ou parte da informação de cabeçalho 1550 e o conteúdo criptografado 1580 a partir do DVD 1500 de acordo com instruções a partir da unidade de execução 1606 e da unidade de verificação de informação de assinatura 1611.

1.4.2 Unidade de Aquisição de Chave de Conteúdo 1602 e Unidade de Armazenamento de Chave de Dispositivo 1604

A unidade de armazenamento de chave de dispositivo 1604 é composta de uma ROM que armazena um identificador de dispositivo "AID_p" 1608 e uma chave de dispositivo "DK_p" 1609 (p é um número natural de n ou menor) como apresentado na Figura 15.

O identificador de dispositivo "AID_p" 1608 é informação de identificação de forma única indicando o dispositivo de execução 1600, enquanto a chave de dispositivo "DK_p" 1609 é informação de chave específica para o dispositivo de execução 1600.

A unidade de aquisição de chave de conteúdo 1602 recebe o bloco de chave 1510 a partir da unidade de aquisição 1601. Quando rece-

bendo o bloco de chave 1510, a unidade de aquisição de chave de conteúdo 1602 lê o identificador de dispositivo "AID_p" 1608 a partir da unidade de armazenamento de chave de dispositivo 1604. Então, a unidade de aquisição de chave de conteúdo 1602 detecta um identificador de dispositivo correspondendo ao identificador de dispositivo "AID_p" 1608 lido a partir do bloco de chave recebido 1510 e extrai uma chave de conteúdo criptografada correspondendo ao identificador de dispositivo detectado.

Subseqüentemente, a unidade de aquisição de chave de conteúdo 1602 lê a chave de dispositivo "DK_p" 1609 a partir da unidade de armazenamento de chave de dispositivo 1604. A unidade de aquisição de chave de conteúdo 1602 gera a chave de conteúdo "CK" pela aplicação de um algorítmo de decriptografia D1 junto à chave de conteúdo criptografada extraída com o uso da chave de dispositivo lida "DK_p" 1609 e então emite a chave de conteúdo gerada "CK" para a unidade de execução 1606.

Aqui, o algorítmo de decriptografia D1 é um algorítmo utilizado para decriptografar textos criptografados gerados pela utilização do algorítmo de criptografia E1.

1.4.3 Unidade de Verificação de Informação de Assinatura 1611 e Unidade de Armazenamento de Chave de Verificação 1612

A unidade de armazenamento de chave de verificação 1612 que é composta de uma ROM, armazena uma chave de verificação 1613. A chave de verificação 1613 é a informação de chave correspondendo à chave de assinatura 1113 armazenada pelo dispositivo de distribuição 1100.

A unidade de verificação de informação de assinatura 1611 recebe a informação de seleção de unidade 1530 e a informação de assinatura 1570 a partir da unidade de aquisição 1601.

A Figura 16 apresenta um esboço geral das operações de verificação para a informação de assinatura, executadas pela unidade de verificação de informação de assinatura 1611. Quando recebendo a informação de seleção de unidade 1530 e a informação de assinatura 1570, a unidade de verificação de informação de assinatura 1611 seleciona i pedaços (i é um número natural de c ou menor) de identificadores de arquivo a partir da in-

formação de seleção de unidade recebida 1530, como apresentado na Figura 16. Aqui, a descrição seguinte é proporcionada com a suposição de que a unidade de verificação de informação de assinatura 1611 selecionou os identificadores de arquivo "FID1", 1531, "FID3", 1533, ..., e assim por diante.

A unidade de verificação de informação de assinatura 1611 gera uma primeira tabela hash substituída "REPHA1TBL1" 1631 baseada na primeira tabela hash "HA1TBL1" 1551 e no arquivo criptografado "ECNT1" 1581 correspondendo ao identificador de arquivo selecionado "FID1" 1531. A unidade de verificação de informação de assinatura 1611 faz o mesmo com os outros identificadores de arquivo selecionados "FID3", ..., e assim por diante para gerar as primeiras tabelas hash substituídas 1633, ..., e assim por diante. A unidade de verificação de informação de assinatura 1611 gera uma segunda tabela hash substituída "REPHA2TBL" 1639 baseada na primeira tabela hash substituída gerada 1631, 1633, ..., e assim por diante e na segunda tabela hash "HA2TBL" 1556 armazenada no DVD 1500 e verifica a informação de assinatura 1570 por utilizar a segunda tabela hash substituída gerada "REPHA2TBL" 1639.

Isto conclui o esboço geral apresentado na Figura 16. O dito a seguir proporciona descrição detalhada sobre: geração das primeiras tabelas hash substituídas (1.4.3.1); geração de uma segunda tabela hash substituída (1.4.3.2); e um procedimento de verificação da informação de assinatura (1.4.3.3), com o auxílio dos desenhos.

1.4.3.1 Geração das Primeiras Tabelas Hash Substituídas

Um procedimento para gerar as primeiras tabelas hash substituídas é explicado com o auxílio das Figuras 17 e 18.

Como apresentado na Figura 17, a unidade de verificação de informação de assinatura 1611 seleciona i pedaços (i é um número natural de c ou menor) dentre os c pedaços de informação de arquivo incluídos na informação de seleção de unidade recebida 1530. Como selecionar i pedaços é, por exemplo, gerar i pedaços de números pseudo-aleatórios (r1, r2, ..., e ri), cada um dos quais é 1 ou maior mas c ou menor e selecionar o r1-ésimo, r2-ésimo, ..., e ri-ésimo identificadores de arquivo. O método de sele-

ção não está limitado a isto e qualquer método é aplicável contanto que seja difícil prognosticar quais identificadores de arquivo são selecionados. Por exemplo, uma temperatura, umidade, ruído em um sinal eletrônico e coisas parecidas podem ser utilizados.

Na presente modalidade, a descrição seguinte é proporcionada supondo que i = 7 e sete pedaços de informação de arquivo 1541, 1543, ..., e assim por diante, são selecionados.

Subseqüentemente, a unidade de verificação de informação de assinatura 1611 seleciona qualquer uma dentre as unidades criptografadas no arquivo criptografado "ECNT1" 1581 correspondendo ao identificador de arquivo "FIF1" incluído na informação de arquivo selecionada 1541 e lê a unidade criptografada selecionada a partir do DVD 1500, como apresentado na Figura 18. Para ser mais específico, a unidade de verificação de informação de assinatura 1611 lê o número de unidade "N1" incluído na informação de arquivo selecionada 1541 e gera um número pseudo-aleatório t (aqui, t = 3), o qual é "N1" ou menor. Então, a unidade de verificação de informação de assinatura 1611 lê uma unidade criptografada "EU1_3", a qual é a terceira unidade criptografada no arquivo criptografado "ECNT1" 1581, a partir do DVD 1500 via a unidade de aquisição 1601 baseada na informação de identificação de arquivo "AD1" incluída na informação de arquivo selecionada 1541.

A seguir, a unidade de verificação de informação de assinatura 1611 gera um valor hash da unidade de substituição "H3" por designar a unidade criptografada lida "EU1_3" para uma função hash. Aqui, a unidade de verificação de informação de assinatura 1611 utiliza a mesma função hash utilizada pela unidade de geração de informação de cabeçalho 1107 do dispositivo de distribuição 1100.

A seguir, a unidade de verificação de informação de assinatura 1611 lê a primeira tabela hash "HA1TBL1" 1551 incluída na informação de cabeçalho 1550 via a unidade de aquisição 1601.

Então, ma unidade de verificação de informação de assinatura 1611 substitui, com o valor hash da unidade de substituição calculado "H3",

um valor hash da unidade "UHA1_3" correspondendo a um identificador de unidade "UID1_3" se conformando com t = 3, dentro dos m pedaços de informação de hash de unidade compondo a primeira tabela hash lida "HA1TBL1" 1551. O resultado é a primeira tabela hash substituída "REPHA1TBL1" 1631.

A unidade de verificação de informação de assinatura 1611 repete o processamento do mesmo tipo para os outros pedaços de informação de arquivo selecionados 1542, ..., e assim por diante, para gerar as primeiras tabelas hash substituídas "REPHATBL3" 1633, ..., e assim por diante, respectivamente.

1.4.3.2 Geração da Segunda Tabela Hash Substituída

O dito a seguir descreve um procedimento para gerar uma segunda tabela hash substituída com o auxílio da Figura 19.

Após completar a geração das primeiras tabelas hash substituídas baseado nos pedaços selecionados de informação de arquivo, a unidade de verificação de informação de assinatura 1611 combina todos os identificadores de unidade, todos os valores hash de unidade e os valores hash substituídos compondo a primeira tabela hash substituída "REPHA1TBL1" 1631 e gera um valor hash de arquivo de substituição "fha1" por designar o resultado combinado para a função hash. De um modo similar, a unidade de verificação de informação de assinatura 1611 gera os valores hash de arquivo de substituição "fha3", ..., e assim por diante baseado nas primeiras tabelas hash substituídas 1633 "REPHA1TBL3", ..., e assim por diante, respectivamente.

A seguir, a unidade de verificação de informação de assinatura 1611 lê a segunda tabela hash "HA2TBL" 1556 incluída na informação de cabeçalho 1550 a partir do DVD 1500. Dentre os c pedaços de informação hash de arquivo incluídos na segunda tabela hash lida "HA2TBL" 1556, a unidade de verificação de informação de assinatura 1611 substitui os valores hash de arquivo da informação hash de arquivo incluindo os identificadores de arquivo "FID1", "FID3", ..., e assim por diante, os quais estão incluídos nos sete pedaços selecionados de informação de arquivo, pelos valores

hash de arquivo de substituição gerados "fha1", "fha3", ..., e assim por diante, respectivamente. A segunda tabela hash "HA2TBL" 1556 para a qual esta substituição foi conduzida é a segunda tabela hash substituída "REPHA2TBL" 1639.

1.4.3.3 Verificação de Informação de Assinatura

O dito a seguir descreve a verificação de informação de assinatura com o auxílio da Figura 20.

Após gerar a segunda tabela hash substituída "REPHA2TBL" 1639, a unidade de verificação de informação de assinatura 1611 lê a chave de verificação 1613 a partir da unidade de armazenamento de chave de verificação 1612.

Subseqüentemente, a unidade de verificação de informação de assinatura 1611 gera um resultado combinado formado pela combinação de todos os valores hash de arquivo com os valore hash de arquivo de substituição incluídos na segunda tabela hash substituída "REPHA2TBL" 1639 com c pedaços de informação de arquivo incluídos na informação de seleção de unidade 1530 e gera a informação de verificação de assinatura por aplicar um algorítmo de verificação de assinatura V junto ao resultado combinado gerado com o uso da chave de verificação 1613. Então, a unidade de verificação de informação de assinatura 1611 compara a informação de verificação de assinatura gerada com a informação de assinatura 1570 recebida a partir da unidade de aquisição 1601. Quando estas duas não concordam, a unidade de verificação de informação de assinatura 1611 julga que a verificação de assinatura não obteve sucesso e emite a informação de proibição de reprodução indicando a proibição da reprodução de conteúdo para a unidade de execução 1606. Aqui, o algorítmo de verificação de assinatura V é um algorítmo para verificar uma assinatura gerada por se utilizar o algorítmo de geração de assinatura S.

Quando os dois concordam, a unidade de verificação de informação de assinatura 1611 termina o processamento de verificação.

1.4.4 Unidade de Execução 1606

A unidade de execução 1606 recebe a chave de conteúdo "CK"

a partir da unidade de aquisição de chave de conteúdo 1602.

Em adição, a unidade de execução 1606 pode receber a informação de proibição de execução a partir da unidade de verificação de informação de assinatura 1611.

Quando recebendo a chave de conteúdo "CK", a unidade de execução 1606 lê o arquivo criptografado "ECNT1" compondo o conteúdo criptografado 1580 a partir do DVD 1500 via a unidade de aquisição 1601. A unidade de execução 1606 seqüencialmente aplica o algorítmo de decriptografia D1 junto às unidades criptografadas "EU1_1", "EU1_2", ..., e assim por diante, compondo o arquivo criptografado lido 1581 com o uso da chave de conteúdo recebida "CK" para gerar o arquivo "CNT1" composto das unidades "U1_1", "U1_2", ..., e assim por diante.

Subseqüentemente, a unidade de execução 1606 expande o arquivo gerado "CNT1" para gerar dados de vídeo e de áudio. A unidade de execução 1606 gera os sinais de vídeo e de áudio baseada nos dados de vídeo e de áudio gerados e emite os sinais de vídeo e de áudio para o monitor 1620.

Com respeito aos arquivos criptografados "ECNT2". ..., "ECNTc", a unidade de execução 1606 repete a leitura, decriptografia e expansão bem como a emissão dos sinais de vídeo e de áudio de um modo similar.

Se recebendo a informação de proibição de reprodução a partir da unidade de verificação de informação de assinatura 1611 durante a repetição, a unidade de execução 1606 aborta a repetição e notifica ao usuário da impraticabilidade da reprodução do DVD carregado no dispositivo de execução 1600, por exemplo, por ligar uma lâmpada indicadora ou tendo o monitor 1620 exibindo uma tela notificando um erro.

1.4.5 Monitor 1620

O monitor 1620 possui um alto-falante embutido que é conectado com o dispositivo de execução 1600 por um cabo.

O monitor 1620 recebe sinais de áudio e de vídeo a partir da unidade de execução 1606 do dispositivo de execução 1600, gera telas a

partir do sinal de imagem recebido e exibe as telas. Adicionalmente, o monitor 1620 gera áudio a partir do sinal de áudio e emite o áudio gerado a partir do alto-falante.

1.5 Comportamentos Operacionais

O dito a seguir descreve comportamentos operacionais do dispositivo de distribuição 1100 e do dispositivo de execução 1600.

1.5.1 Comportamento Operacional do Dispositivo de Distribuição 1100

O comportamento operacional do dispositivo de distribuição 1100 é descrito com o auxílio dos fluxogramas apresentados nas Figuras 21 e 22.

A unidade de entrada 1101 adquire o conteúdo 1120 composto de c pedaços de arquivos de acordo com as operações conduzidas por um operador (Etapa S1011), e instrui a unidade de geração de chave de conteúdo 1102 para gerar a chave de conteúdo.

A unidade de geração de chave de conteúdo 1102 gera a chave de conteúdo "CK" utilizando um número aleatório e emite a chave de conteúdo gerada "CK" para a unidade de geração de bloco de chave 1103 (Etapa S1012).

A unidade de geração de bloco de chave 1103 recebe a chave de conteúdo "CK" e lê a tabela de identificação de dispositivo 1130 a partir da unidade de armazenamento de dispositivo de execução 1104 (Etapa S1013). A unidade de geração de bloco de chave 1103 gera o bloco de chave 1150, utilizando a chave de conteúdo recebida "CK" e a tabela de identificação de dispositivo lida 1130 (Etapa S1016).

Nas Etapas S1017 até S1023, a unidade de geração de unidade 1105 do dispositivo de distribuição 1100 repete o processamento para das Etapas S1018 até S1022 com respeito a cada arquivo compondo o conteúdo 1120.

A unidade de geração de unidade 1105 gera um identificador de arquivo e a informação de identificação de arquivo correspondendo a um arquivo (Etapa S1018). Subseqüentemente, a unidade de geração de unidade 1105 gera m pedaços de unidades por dividir o arquivo (Etapa S1019),

gera um número de unidades indicando o número de unidades geradas e gera informação de arquivo composta do identificador de arquivo gerado, da informação de identificação de arquivo e do número de unidades (Etapa S1020).

A seguir, a unidade de geração de unidade 1105 gera identificadores de unidade correspondendo um para um com as unidades geradas (Etapa S1021). Subseqüentemente, a unidade de geração de unidade 1105 gera m pedaços de informação de unidade, cada pedaço incluindo um identificador de unidade e uma unidade correspondente e coloca estes pedaços de informação de unidade juntos para formar um arquivo dividido. Então, a unidade de geração de unidade 1105 gera a informação de arquivo dividido composta do arquivo dividido e do identificador de arquivo (Etapa S1022).

Após completar a repetição das Etapas S1017 até S1023 para todos os arquivos e a geração de c pedaços de informação de arquivo dividido e a informação de arquivo, a unidade de geração de unidade 1105 gera a informação de seleção de unidade 1200 composta dos c pedaços de informação de arquivo (Etapa S1024) e emite a informação de seleção de unidade gerada 1200 para a unidade de geração de informação de assinatura 1111 e para a unidade de gravação 1114. Em adição, a unidade de geração de unidade 1105 emite o conteúdo dividido 1160 composto dos c pedaços de informação de arquivo dividido para a unidade de processamento de criptografia 1106.

A unidade de processamento de criptografia 1106 recebe o conteúdo dividido 1160 a partir da unidade de geração de unidade 1105 e gera o conteúdo dividido criptografado 1210 por criptografar cada unidade de arquivos divididos individuais compondo o conteúdo dividido 1160 com o uso da chave de conteúdo "CK" (Etapa S1026).

A seguir, a unidade de processamento de criptografia 1106 gera c pedaços de arquivos criptografados por extrair unidades criptografadas de cada arquivo dividido criptografado e coloca estes arquivos criptografados juntos para formar o conteúdo criptografado 1330 (Etapa S2027). A seguir, a unidade de processamento de criptografia 1106 emite o conteúdo dividido

criptografado 1210 para a unidade de geração de informação de cabeçalho 1107 enquanto emitindo o conteúdo criptografado 1330 para a unidade de gravação 1114.

A unidade de geração de informação de cabeçalho 1107 recebe o conteúdo dividido criptografado 1210 a partir da unidade de processamento de criptografia 1106. A unidade de geração de informação de cabeçalho 1107 calcula os valores hash de unidade por designar as unidades criptografadas incluídas em cada arquivo dividido criptografado compondo o conteúdo dividido criptografado 1210 para a função hash e gera c pedaços de primeiras tabelas hash (Etapa S1028).

A seguir, a unidade de geração de informação de cabeçalho 1107 calcula, com respeito a cada uma das primeiras tabelas hash, um valor hash de arquivo baseado na primeira tabela hash e gera a segunda tabela hash 1269 incluindo c pedaços de valores hash de arquivo calculados (Etapa S1029).

A seguir, a unidade de geração de informação de cabeçalho 1107 gera a informação de cabeçalho 1260 incluindo a segunda tabela hash gerada 1269 e os c pedaços das primeiras tabelas hash (Etapa S1031).

A unidade de geração de informação de assinatura 1111 lê a chave de assinatura 1113 a partir da unidade de armazenamento de chave de assinatura 1112 (Etapa S1032) e gera a informação de assinatura por aplicar o algorítmo de geração de assinatura junto à segunda tabela hash 1269 e à informação de seleção de unidade com o uso da chave de assinatura lida 1113 (Etapa S1033).

A unidade de gravação 1114 grava o bloco de chave 1150, a informação de unidade 1200, a informação de cabeçalho 1260, a informação de assinatura 1310 e o conteúdo criptografado 1330 junto ao DVD 1500 (Etapa S1034).

1.5.2 Comportamento Operacional do Dispositivo de Execução 1600

A Figura 23 apresenta um processo de fabricação de informação envolvido na verificação da informação de assinatura. Por conveniência da descrição, com respeito à informação de cabeçalho 1550, somente valores

hash de unidade incluídos nas primeiras tabelas hash e valores hash de arquivo incluídos na segunda tabela hash são representados na Figura. As Figuras 24 e 25 são fluxogramas apresentando o comportamento operacional do dispositivo de execução 1600. Observe que os mesmos números de etapa nas Figuras 23 até 25 indicam o mesmo processamento.

O dito a seguir explica o comportamento operacional do dispositivo de execução 1600 com o auxílio das Figuras 23 até 25.

Quando sendo carregada com o DVD 1500, a unidade de aquisição 1601 lê o bloco de chave 1510, a informação de seleção de unidade 1530 e a informação de assinatura 1570 a partir do DVD 1500 e emite o bloco de chave 1510 para a unidade de aquisição de chave de conteúdo 1602 enquanto emitindo a informação de seleção de unidade 1530 e a informação de assinatura 1570 para a unidade de verificação de informação de assinatura 1611 (Etapa S1041).

A unidade de verificação de informação de assinatura 1611 recebe a informação de seleção de unidade 1530 e a informação de assinatura 1570 e seleciona i pedaços dentro dos c pedaços de identificadores de arquivo incluídos na informação de seleção de unidade 1530 com o uso de um número aleatório (Etapa S1046).

Nas Etapas S1047 até S1057, a unidade de verificação de informação de assinatura 1611 repete o processamento das Etapas S1048 até S1056 com respeito a cada um dos i pedaços de identificadores de arquivo selecionados para gerar i pedaços de primeiras tabelas hash substituídas.

A unidade de verificação de informação de assinatura 1611 extrai um número de unidade correspondendo a um dos identificadores de arquivo selecionados a partir da informação de unidade (Etapa S1048). Subseqüentemente, a unidade de verificação de informação de assinatura 1611 gera um número aleatório t que é 1 ou maior mas também o número de unidades lido ou menor (Etapa S1049). A unidade de verificação de informação 161 extrai um pedaço de informação de identificação de arquivo correspondendo ao identificador de arquivo selecionado a partir da informação de uni-

dade e lê ao t-ésima unidade criptografada no arquivo criptografado correspondendo ao identificador de arquivo selecionado a partir do DVD 1500 baseado na informação de identificação de unidade extraída (Etapa S1051). Na Figura 23, cada vez que o processamento acima é repetido, a unidade de verificação de informação de assinatura 1161 seqüencialmente lê: uma unidade criptografada 1511 incluída no arquivo criptografado 1581; uma unidade criptografada 1512 incluída no arquivo criptografado 1583; ...; e uma unidade criptografada 1513 incluída no arquivo criptografado 1587.

A unidade de verificação de informação de assinatura 1611 calcula os valores hash de unidade de substituição por designar a unidade criptografadas lidas para as funções hash (Etapa S1052).

A seguir, a unidade de verificação de informação de assinatura 1611 lê uma primeira tabela hash correspondendo ao identificador de arquivo selecionado a partir do DVD 1500 (Etapa S1054) e gera uma primeira tabela hash substituída por substituir, com o valor hash de unidade de substituição calculado, um valor hash de unidade correspondendo ao valor hash de unidade de substituição calculado (Etapa S1056). Na Figura 23, cada vez que o processamento acima é repetido, a unidade de verificação de informação de assinatura 1611 gera: a primeira tabela hash substituída 1631 a partir da unidade criptografada 1511 e a primeira tabela hash 1551; a primeira tabela hash substituída 1633 a partir da unidade criptografada 1512 e a primeira tabela hash 1553; ...; e a primeira tabela hash substituída 1637 a partir da unidade criptografada 1513 e a primeira tabela hash 1557.

Após completar a repetição das Etapas S1047 até S1057 para todos os i pedaços de identificadores de arquivo, a unidade de verificação de informação de assinatura 1611 calcula i pedaços de valores hash de arquivo de substituição por individualmente designar as primeiras tabelas hash substituídas para a função hash (Etapa S1059).

A seguir, a unidade de verificação de informação de assinatura 1611 lê a segunda tabela hash 1556 a partir do DVD 1500 (Etapa S1061) e gera uma segunda tabela hash substituída 1639 por substituir os valores hash de arquivo correspondendo aos i pedaços selecionados de identifica-

dores de arquivo pelos i pedaços calculados de valores hash de arquivo de substituição (Etapa S1063). Na Figura 23, a segunda tabela hash substituída gerada 1639 inclui: um valor hash de arquivo de substituição 1641 calculado a partir da primeira tabela hash substituída 1631; um valor hash de arquivo 1572 lido a partir do DVD 1500; um valor hash de arquivo de substituição 1643 calculado a partir da primeira tabela hash substituída 1633; ..., e um valor hash de arquivo de substituição 1647 calculado a partir da primeira tabela hash substituída 1637.

A seguir, a unidade de verificação de informação de assinatura 1611 lê a chave de verificação 1613 a partir da unidade de armazenamento de chave de verificação 1612 (Etapa S1064) e executa a verificação da informação de assinatura 1570 por utilizar a informação de seleção de unidade 1530, a segunda tabela hash substituída gerada e a chave de verificação lida 1613 (Etapa S1066).

Quando a verificação da informação de assinatura obtém sucesso (Etapa S1067: SIM), a unidade de verificação de informação de assinatura 1611, então, termina a verificação da informação de assinatura 1570.

Se a verificação de assinatura não tiver sucesso (Etapa S1067: NÃO), a unidade de verificação de informação de assinatura 1611 emite a informação de proibição de reprodução para a unidade de execução 1606 (Etapa S1073).

A unidade de aquisição de chave de conteúdo 1602 recebe o bloco de chave 1510 e lê o identificador de dispositivo 1608 e a chave de dispositivo 1609 a partir da unidade de armazenamento de chave de dispositivo 1604 (Etapa S1071). Então, a unidade de aquisição de chave de conteúdo 1602 gera a chave de conteúdo "CK" a partir do identificador de dispositivo lido 1608, da chave de dispositivo 1609 e do bloco de chave 1510 e emite a chave de conteúdo gerada "CK" para a unidade de execução 1606 (Etapa S1072).

A unidade de execução 1606 recebe a chave de conteúdo "CK". Aqui, se tiver recebido a informação de proibição de reprodução a partir da unidade de verificação de informação de assinatura 1611 (Etapa S1074:

SIM), a unidade de execução 1606 notifica ao usuário da impraticabilidade de reprodução do conteúdo armazenado no DVD 1500 (Etapa S1076) e termina a reprodução.

Se não tiver recebido a informação de proibição de reprodução (Etapa S1074: NÃO), a unidade de execução 1606 lê os arquivos criptografados compondo o conteúdo criptografado 1580 a partir do DVD 1500 (Etapa S1077). A unidade de execução 1606 primeiro gera os arquivos por decriptografar os arquivos criptografados lidos com o uso da chave de conteúdo "CK" (Etapa S1079) e então gera dados de áudio e de vídeo por expandir os arquivos gerados (Etapa S1081). Então, a unidade de execução 1606 gera sinais de áudio e de vídeo a partir dos dados de vídeo e de áudio gerados, respectivamente, e emite estes sinais para o monitor 1400 e tem o monitor 1400 executando o vídeo e o áudio (Etapa S1082). Quando tiver terminado a leitura de todos os arquivos criptografados ou tiver instruído para terminar a reprodução pelas operações conduzidas pelo usuário (Etapa S1084: SIM), a unidade de execução 1606 termina a reprodução.

Se ainda existirem arquivos criptografados que ainda não foram lidos e a unidade de execução 1606 não tiver recebido uma instrução para terminar a reprodução a partir do usuário, a unidade de execução 1606 retornar para a etapa S1074 e repete o processamento das Etapas 1074 até S1084.

1.6 Sumário e Efeitos Vantajosos

Como foi descrito, na presente modalidade, o DVD 1500 armazena: conteúdo criptografado incluindo c pedaços de arquivos criptografados, cada um dos quais inclui uma pluralidade de unidades criptografadas; informação de cabeçalho incluindo c pedaços de primeiras tabelas hash geradas baseado na pluralidade de unidade criptografadas bem como em uma segunda tabela hash; e informação de assinatura gerada baseado na segunda tabela hash.

Ao mesmo tempo, quando iniciando a leitura, decriptografia e reprodução do conteúdo criptografado, o dispositivo de execução 1600 aleatoriamente seleciona i pedaços de unidades criptografadas com o uso de

números aleatórios e calcula os valores hash de unidade de substituição e substitui os valores hash de arquivo baseado nos i pedaços selecionados de unidades criptografadas.

A seguir, o dispositivo de execução 1600 lê a segunda tabela hash a partir do DVD e gera uma segunda tabela hash substituída por substituir, dentre os valores hash de arquivo incluídos na segunda tabela hash lida, os valores hash de arquivo correspondendo aos valores hash de arquivo de substituição calculados pelo valor hash de arquivo de substituição calculado. Então, o dispositivo de execução 1600 executa a verificação de informação de assinatura por utilizar a segunda tabela hash substituída. Se a verificação não tiver sucesso, o dispositivo de execução 1600 aborta a reprodução do conteúdo.

Assim, por limitar o número de valores hash de unidade mais recentemente calculados para verificação da informação de assinatura a i pedaços, é possível reduzir a quantidade de cálculo envolvido na verificação da informação de assinatura, o que leva a uma redução na carga de processamento na reprodução de conteúdo.

Adicionalmente, por executar a verificação da informação de assinatura com o uso de uma estrutura com duas camadas composta da primeira e da segunda tabela hash, o dispositivo de execução 1600 é capaz de reduzir a quantidade de informação lida a partir do DVD 1500. Mais especificamente, na primeira modalidade da presente invenção, não existe necessidade de ler as primeiras tabelas hash correspondendo à informação de arquivo que não foi selecionado. Por conseqüência, é possível encurtar o tempo requerido para ler informação.

Adicionalmente, as primeiras tabelas hash correspondendo à informação de arquivo selecionada são lidas na primeira modalidade. Entretanto, dentre os componentes constituindo as primeiras tabelas hash correspondendo à informação de arquivo selecionada, somente os componentes deferentes dos valores hash de unidade correspondendo aos valores hash de unidade de substituição calculados podem ser lidos. O mesmo se aplica à leitura de uma segunda tabela hash. Com isto, é possível reduzir a

quantidade de informação lida a partir do DVD 1500.

Por executar a verificação da informação de assinatura com o uso dos valores hash substituídos gerados a partir das unidades criptografadas, é possível ao mesmo tempo completar tanto a verificação de se conteúdo não autorizado está incluído como a verificação de se a informação de assinatura foi gerada por se utilizar uma chave de assinatura possuída por um mantenedor legítimo de direito.

No processamento de verificação, se parte ou todo o conteúdo criptografado do DVD 1500 for substituído por conteúdo não autorizado, a primeira modalidade possui uma alta chance de detectar o conteúdo não autorizado, desde que somente i pedaços de unidade criptografadas são aleatoriamente selecionados para uso.

Aqui, é proporcionada uma descrição específica supondo que metade do conteúdo criptografado foi regravado como conteúdo não autorizado. A probabilidade de uma única unidade criptografada selecionada ser uma unidade criptografada válida gerada pelo dispositivo de distribuição 1100 é ½. Por exemplo, no caso de se selecionar sete unidades criptografadas e executar a verificação, a probabilidade de todas as sete unidade criptografadas selecionadas serem unidades criptografadas válidas é $(1/2)^7$ = 1/128. A saber, neste caso, a probabilidade de não estar apto a detectar conteúdo não autorizado é menor do que 1%. Com isto, a primeira modalidade atua como um dissuasor para impedir atos fraudulentos envolvendo substituir parte do conteúdo distribuído por um mantenedor legítimo de direito por conteúdo não autorizado e distribuir o mesmo.

1.7 Modificação da Primeira Modalidade

Na primeira modalidade, o dispositivo de distribuição 1100 divide cada arquivo compondo o conteúdo adquirido em unidades, e então conduz a criptografia para cada unidade. Entretanto, o dispositivo de distribuição 1100 pode conduzir a criptografia com respeito a cada arquivo para gerar arquivos criptografados e gerar unidade criptografadas por dividir cada um dos arquivos criptografados gerados. Neste caso, a unidade de execução 1606 do dispositivo de execução 1600 lê o conteúdo criptografado a partir

do DVD 1500, decriptografa o conteúdo criptografado lido com respeito a cada arquivo criptografado e executa o conteúdo decriptografado.

Um dispositivo de distribuição 1100b da presente modificação é descrito com o auxílio da Figura 26.

O dispositivo de distribuição 1100b é composto de uma unidade de entrada 1101b, de uma unidade de geração de chave de conteúdo 1102, de uma unidade de geração de bloco de chave 1103, de uma unidade de armazenamento de informação de dispositivo de execução 1104, de uma unidade de geração de unidade 1105b, de uma unidade de processamento de criptografia 1106b, de uma unidade de geração de informação de cabeçalho 1107, de uma unidade de geração de informação de assinatura 1111, de uma unidade de armazenamento de chave de assinatura 1112 e de uma unidade de gravação 1114.

Desde que a unidade de geração de chave de conteúdo 1102, a unidade de geração de bloco de chave 1103 e a unidade de armazenamento de informação de dispositivo de execução 1104, a unidade de geração de informação de cabeçalho 1107, a unidade de geração de informação de assinatura 1111, a unidade de armazenamento de chave de assinatura 1112 e a unidade de gravação 1114 são as mesmas que na primeira modalidade, a descrição para estes componentes será omitida.

Adicionalmente, desde que a unidade de entrada 1101b é a mesma que a unidade de entrada 1101 da primeira modalidade, exceto por emitir o conteúdo para a unidade de processamento de criptografia ao invés do que para a unidade de geração de unidade, a descrição também é omitida.

1.7.1 Unidade de Processamento de Criptografia 1106b

A unidade de processamento de criptografia 1106b recebe a chave de conteúdo "CK" a partir da unidade de geração de chave de conteúdo 1102.

A unidade de processamento de criptografia 1106 recebe o conteúdo a partir da unidade de entrada 1101b. Aqui, o conteúdo é composto de arquivos "CNT1", "CNT2", ..., "CNTc", como é o caso com o conteúdo

1120 apresentado na Figura 3.

Quando recebendo o conteúdo, a unidade de processamento de criptografia 1106 gera o arquivo criptografado "ECNT1" por aplicar o algorítmo de criptografia E1 junto ao arquivo "CNT1" incluído no conteúdo recebido com o uso da chave de conteúdo "CK".

A unidade de processamento de criptografia 1106 faz o mesmo com os arquivos "CNT2" até "CNTc" para gerar arquivos criptografados "ECNT2" até "ECNTc".

A seguir, a unidade de processamento de criptografia 1106 emite o conteúdo criptografado composto dos arquivos criptografados gerados "ECNT1", "ECNT2", "ECNT3", ..., "ECNTc" para a unidade de geração de unidade 1105b e para a unidade de gravação 1114b.

1.7.2 Unidade de Geração de Unidade 1105b

A unidade de geração de unidade 1105b recebe o conteúdo criptografado a partir da unidade de processamento de criptografia 1106b. Quando recebendo o conteúdo criptografado, a unidade de geração de unidade 1105b gera o identificador de arquivo "FID1" e o pedaço de informação de identificação de arquivo "AD1" correspondendo ao arquivo criptografado "ECNT1" incluído no conteúdo criptografado recebido.

A seguir, a unidade de geração de unidade 1105b divide o arquivo criptografado "ECNT1" a cada 64 quilobytes para gerar m pedaços de unidades criptografadas. Neste ponto, se a última unidade criptografada for menor do que 64 quilobytes, a unidade criptografada é suplementada com dados tipo "000 ... 000".

A seguir, a unidade de geração de unidade 1105b gera um número "N1" indicando o número de unidades criptografadas geradas, e então gera a informação de arquivo composta do identificador de arquivo gerado "FID1", do pedaço de informação de identificação de arquivo "AD1" e do número de unidades "N1".

A seguir, a unidade de geração de unidade 1105 gera os identificadores de unidade "UID1_1", "UID1_2", "UID1_3", ..., "UID1_m" correspondendo aos m pedaços gerados de unidades criptografadas "EU1_1",

"EU1_2", "EU1_3", ..., e "EU1_m", respectivamente. Subseqüentemente, a unidade de geração de unidade 1105b forma m pedaços de informação de unidade criptografada por corresponder as unidades criptografadas correspondentes com os identificadores de unidade.

A seguir, a unidade de geração de unidade 1105b coloca os m pedaços de informação de unidade criptografada juntos para formar o arquivo dividido criptografado "SplECNT1".

A unidade de geração de unidade 1105b repete o processamento do mesmo tipo para o resto dos arquivos criptografados "ECNT2", "ECNT3", ..., e "ECNTc" incluídos no conteúdo criptografado para gerar arquivos divididos criptografados "SplECNT2", "SplECNT3", ..., e "SplECNTc" bem como os pedaços restantes de informação de arquivo. Então, a unidade de geração de unidade 1105b emite os c pedaços gerados de arquivos divididos criptografados "SplECNT1", "SplECNT2", "SplECNT3", ..., e "SplECNTc" para a unidade de geração de informação de cabeçalho 1107b como conteúdo dividido criptografado.

Em adição, a unidade de geração de unidade 1105b gera informação de seleção de unidade composta dos c pedaços de informação de arquivo e emite a informação de seleção de unidade gerada para a unidade de gravação 1114 e para a unidade de geração de informação de assinatura 1111b.

2. Segunda Modalidade

Uma segunda modalidade de acordo com a presente invenção é descrita com o auxílio dos desenhos.

2.1 Sistema de Detecção de Conteúdo Não Autorizado

Um sistema de detecção de conteúdo não autorizado de uma segunda modalidade é composto de um dispositivo de distribuição, de um dispositivo de execução e de um monitor, como no sistema de detecção de conteúdo não autorizado 1 da primeira modalidade.

O dispositivo de distribuição adquire conteúdo de acordo com as operações conduzidas por um operador e gera conteúdo criptografado por criptografar o conteúdo adquirido. Em adição, o dispositivo de distribuição

extrai parte do conteúdo e gera informação tal como informação de cabeçalho utilizada para detectar se conteúdo não autorizado está incluído no conteúdo, informação de assinatura para proporcionar que o conteúdo seja emitido por um mantenedor legítimo de direito e assim por diante, baseado na parte extraída do conteúdo (daqui para frente referido como "conteúdo parcial representativo"). O dispositivo de distribuição grava o conteúdo criptografado gerado, a informação de assinatura e assim por diante junto a um DVD.

O DVD será vendido ou distribuído para usuários através de saídas de distribuição.

Quando carregado com o DVD, o dispositivo de execução gera conteúdo parcial representativo a partir do conteúdo criptografado armazenado no DVD carregado e executa verificação da informação de assinatura e da informação de cabeçalho baseado no conteúdo parcial representativo gerado. Se a verificação obtiver sucesso, o dispositivo de execução inicia a reprodução do conteúdo. Quando a verificação não obtém sucesso, o dispositivo de execução proíbe a reprodução do conteúdo.

Dispositivos individuais compondo o sistema de detecção de conteúdo não autorizado da presente modalidade e o DVD são descritos em detalhes abaixo.

2.2 Dispositivo de Distribuição 2100

A Figura 27 apresenta uma estrutura de um dispositivo de distribuição constituindo o sistema de detecção de conteúdo não autorizado da presente modalidade. Como apresentado na Figura 27, o dispositivo de distribuição 2100 é composto de uma unidade de entrada 2101, de uma unidade de geração de chave de conteúdo 2102, de uma unidade de geração de bloco chave 2103, de uma unidade de armazenamento de informação de dispositivo de execução 2104, de uma unidade de seleção 2105, de uma unidade de geração de informação de cabeçalho 2107, de uma unidade de geração de informação de assinatura 2108, de uma unidade de armazenamento de chave de assinatura 1112, de uma unidade de processamento de criptografia 2109 e de uma unidade de gravação 2114.

Componentes individuais compondo o dispositivo de distribuição são descritos em detalhes abaixo. Observe que, desde que a unidade de armazenamento de informação de dispositivo de execução 1104 e a unidade de armazenamento de chave de assinatura 1112 são as mesmas que na primeira modalidade, as descrições para estes componentes são omitidas.

2.2.1 Unidade de Entrada 2101

A unidade de entrada 2101 adquire conteúdo e vários pedaços de informação de identificação a partir de um dispositivo externo ou meio de gravação externo de acordo com operações do operador.

A Figura 28 apresenta um exemplo de uma estrutura do conteúdo e da informação de identificação adquiridos pela unidade de entrada 2101. O conteúdo 2120 é composto de c pedaços de conteúdo parcial "CNT1" 2121, "CNT2" 2122, "CNT3" 2123, ..., e "CNTc" 2124. Aqui, o conteúdo 2120 adquirido pela unidade de entrada 2101 é um formato executável para um dispositivo de execução 2600 (como será daqui para frente descrito em detalhes) e o formato DVD-Vídeo e o formato MPEG-2 são exemplos de tais formatos executáveis.

Cada pedaço de informação de identificação é informação unicamente indicando um dos conteúdos parciais constituindo o conteúdo 2120 e por exemplo, é um deslocamento de um pedaço corresponde de conteúdo parcial a partir do cabeçalho do conteúdo, um número de setor, ou um ponto inicial de reprodução do pedaço de conteúdo parcial especificado pela referência ao cabeçalho do conteúdo. Por exemplo, um pedaço de informação de identificação "AD1" 2131 corresponde ao conteúdo parcial "CNT1" 2121 e o cabeçalho do conteúdo parcial "CNT1" 2121 está posicionado em "AD1" a partir do cabeçalho do conteúdo 2120.

A unidade de entrada 2101 emite o conteúdo adquirido 2120 e c pedaços de informação de identificação para a unidade de geração de chave de conteúdo 2102.

2.2.2 Unidade de Geração de Chave de Conteúdo 2102

A unidade de geração de chave de conteúdo 2102 recebe o conteúdo 2120 e os c pedaços de informação de identificação a partir da

unidade de entrada 2101. Quando recebendo o conteúdo 2120 e os c pedaços de informação de identificação, a unidade de geração de chave de conteúdo 2102 gera um número pseudo-aleatório e gera uma chave de conteúdo "CK" com o comprimento de 128 bits com o uso do número pseudo-aleatório gerado. Ao invés de um número pseudo-aleatório, um número aleatório real pode ser gerado por se utilizar, por exemplo, ruído em um sinal.

A seguir, a unidade de geração de chave de conteúdo 2102 emite a chave de conteúdo gerada "CK", o conteúdo recebido 2120 e os c pedaços de informação de identificação para a unidade de geração de bloco de chave 2103 e para a unidade de processamento de criptografia 2109.

2.2.3. Unidade de Geração de Bloco de Chave 2103

A unidade de geração de bloco de chave 2103 recebe a chave de conteúdo "CK", o conteúdo 2120 e os c pedaços de informação de identificação a partir da unidade de geração de chave de conteúdo 2102. Quando recebendo a chave de conteúdo "CK", a unidade de geração de bloco de chave 2103 gera um bloco de chave por utilizar a tabela de identificação de dispositivo 1130 armazenada na unidade de armazenamento de informação de dispositivo de execução 1104 e a chave de conteúdo recebida "CK". Desde que o procedimento para gerar o bloco de chave é o mesmo que na primeira modalidade, a descrição é omitida. Em adição, o bloco de chave gerado aqui possui a mesma estrutura que o bloco de chave 1150 apresentado na Figura 5.

A seguir, a unidade de geração de bloco de chave 2103 emite o bloco de chave gerado e a chave de conteúdo recebida "!CK", o conteúdo 2120 e os c pedaços de informação de identificação para a unidade de seleção 2105.

2.2.4 Unidade de Seleção 2105

A Figura 29 apresenta um esboço geral do processamento executado pela unidade de seleção 2105. O dito a seguir descreve a unidade de seleção 2105 com o auxílio da Figura 29.

A unidade de seleção 2105 recebe o bloco de chave, a chave de conteúdo "CK", o conteúdo 2120 e os c pedaços de informação de identifi-

cação a partir da unidade de geração de bloco de chave 2103. Quando recebendo este conjunto de informações, a unidade de seleção 2105 seleciona k pedaços dentre os c pedaços recebidos de informação de identificação. A descrição, aqui, é proporcionada supondo que k = 3.

Com respeito ao método de seleção, os k pedaços podem ser selecionados, por exemplo, por se utilizar números aleatórios, ou selecionados a partir de datas, temperaturas, e assim por diante. Alternativamente, pode ser projetado para aceitar as seleções a partir do operador. Se o conteúdo 2120 estiver no formato MPEG, os pedaços de informação de identificação indicando intra-imagens podem ser selecionados. Em adição, a unidade de seleção 2105 pode pré armazenar informação identificando k pedaços a serem selecionados, ou pode executar a seleção em resposta a uma instrução a partir do operador.

Como apresentado na Figura 29, a unidade de seleção 2105 aqui seleciona pedaços de informação de identificação "AD3" 2133, "AD7" 2134 e "ADc" 2137.

A seguir, a unidade de seleção 2105 extrai um pedaço de conteúdo parcial "CNT3" correspondendo ao pedaço de informação de identificação "AD3" 2133 selecionado a partir do conteúdo recebido 2120, e gera um pedaço de informação representativa 2141 composta do pedaço de informação de identificação selecionado "AD3" 2133 e do pedaço de conteúdo parcial extraído "CNT3". Aqui, o pedaço selecionado de conteúdo parcial é referido como "um pedaço de conteúdo parcial representativo".

A unidade de seleção 2105 repete o processamento do mesmo tipo para os pedaços de informação de identificação "AD7" 2134 e "ADc" 2137 para gerar pedaços de informação representativa 2142 e 2143.

A seguir, a unidade de seleção 2105 emite para a unidade de geração de informação de cabeçalho 2107: os três pedaços gerados de informação representativa 2141, 2142 e 2143; e o bloco de chave recebido, a chave de conteúdo "CK" e o conteúdo 2120.

2.2.5 Unidade de Geração de Informação de Cabeçalho 2107

A unidade de geração de informação de cabeçalho 2107 recebe

os três pedaços de informação representativa 2141, 2142, e 2143, o bloco de chave, a chave de conteúdo "CK" e o conteúdo 2120 a partir da unidade de seleção 2105.

Quando recebendo os mesmos, a unidade de geração de informação de cabeçalho 2107 gera um identificador de informação de identificação "ADID1" unicamente identificando o pedaço de informação representativa recebido 2141. Métodos para gerar o identificador de informação de identificação incluem, por exemplo, uma designação seqüencial de números naturais e uma designação aleatória utilizando números aleatórios.

A seguir, a unidade de geração de informação de cabeçalho 2107 extrai o pedaço de informação de identificação "AD3" a partir do pedaço de informação representativa recebido 2141 e gera um pedaço de informação de detecção representativa composta do identificador de informação de identificação gerado "ADID1" e do pedaço de informação de identificação "AD3".

Subseqüentemente, a unidade de geração de informação de cabeçalho 2107 extrai o pedaço de conteúdo parcial representativo "CNT3" a partir do pedaço de informação representativa recebido 2141 e gera um valor hash parcial "HA3" por designar o conteúdo parcial representativo extraído "CNT3" para uma função hash. A unidade de geração de informação de cabeçalho 2107 gera um pedaço de informação hash representativa composta do identificador de informação de identificação gerado "ADID1" e do valor hash parcial "HA3".

A unidade de geração de informação de cabeçalho 2107 repete o processamento do mesmo tipo para os pedaços de informação representativa 2142 e 2143 e gera pedaços de informação de detecção representativa e de informação hash representativa. A unidade de geração de informação de cabeçalho 2107 gera a informação de posição selecionada composta dos três pedaços gerados de informação de detecção representativa.

A Figura 30 apresenta uma estrutura da informação de posição selecionada gerada neste ponto. A informação de posição selecionada 2160 é composta dos pedaços de informação de detecção representativa 2161,

2162 e 2163, os quais correspondem aos pedaços de informação representativa 2141, 2142 e 2143, respectivamente. Cada pedaço de informação de detecção representativa é composto de um identificador de informação de identificação e de um pedaço de informação de identificação. Como um exemplo, o pedaço de informação de detecção representativa 2161 corresponde ao pedaço de informação representativa 2141 e inclui um identificador de informação de identificação "ADID1" 2171 e um pedaço de informação de identificação "AD3" 2176.

Em adição, a unidade de geração de informação de cabeçalho 2107 gera a informação de cabeçalho composta dos três pedaços gerados de informação hash representativa.

A Figura 31 apresenta uma estrutura da informação de cabeçalho gerada neste ponto. Como apresentado na Figura 31, a informação de cabeçalho 2200 é composta de pedaços de informação hash representativa 2201, 2202 e 2203, os quais correspondem aos pedaços de informação de detecção representativa 2161, 2162 e 2163, respectivamente.

Cada pedaço de informação hash representativa inclui um identificador de informação de identificação e um valor hash parcial. Por exemplo, o pedaço de informação hash representativa 2201 é gerado baseado no pedaço de informação representativa 2141 e inclui um identificador de informação de identificação "ADID1" 2211 e um valor hash parcial "HA3".

A seguir, a unidade de geração de informação de cabeçalho 2107 emite a informação de posição selecionada gerada 2160, a informação de cabeçalho 2200, e o bloco de chave recebido, a chave de conteúdo "CK" e o conteúdo 2120 para a unidade de geração de informação de assinatura 2108.

2.2.6 Unidade de Geração de Informação de Assinatura 2108

A unidade de geração de informação de assinatura 2108 recebe a informação de posição selecionada 2160, a informação de cabeçalho 2200, a chave de bloco, a chave de conteúdo "CK" e o conteúdo 2120 a partir da unidade de geração de informação de cabeçalho 2107. Quando recebendo estes conjuntos de informação, a unidade de geração de informação

de assinatura 2108 extrai os valores hash parciais "HA3", "HA5" e "HAc" incluídos na informação de cabeçalho recebida 2200.

A seguir, a unidade de geração de informação de assinatura 2108 lê uma chave de assinatura 1113 a partir da unidade de armazenamento de chave de assinatura 1112. A unidade de geração de informação de assinatura 2108 gera a informação de assinatura por designar o algorítmo de geração de assinatura S para um resultado combinado formado por se combinar os valores hash parciais extraídos "HA3", "HA5" e "HAc" com o uso da leitura da chave de assinatura 1113.

A seguir, a unidade de geração de informação de assinatura 2108 emite a informação de assinatura gerada e a informação de posição selecionada 2160, a informação de cabeçalho 2200, a chave de bloco, a chave de conteúdo "CK" e o conteúdo 2120, recebidos, para a unidade de processamento de criptografia 2109.

2.2.7 Unidade de Processamento de Criptografia 2109

A unidade de processamento de criptografia 2109 recebe a informação de assinatura, a informação de posição selecionada 2160, a informação de cabeçalho 2200, o bloco de chave, a chave de conteúdo "CK" e o conteúdo 2120 a partir da unidade de geração de informação de assinatura 2108.

Quando recebendo estes conjuntos de informações, a unidade de processamento de criptografia 2109 gera pedaços de conteúdo parcial criptografado "ECNT1", "ECNT2", "ECNT3", ..., e "ECNTc" por aplicar o algorítmo de criptografia E1 respectivamente para os pedaços de conteúdo parcial "CNT1", "CNT2", "CNT3", ..., e "CNTc" constituindo o conteúdo recebido 2120 com o uso da chave de conteúdo recebida "CK". Os pedaços gerados de conteúdo parcial criptografado "ECNT1", "ECNT2", "ECNT3", ..., "ECNTc" são coletivamente referidos como conteúdo criptografado. Aqui, o conteúdo de criptografia pode ser denotado como ECNTb = Enc (CK, CNTb), onde b é um número natural de c ou menor. A Figura 32 apresenta uma estrutura do conteúdo criptografado 2220 gerado neste ponto.

Subseqüentemente, a unidade de processamento de criptografia

2109 gera a informação de posição selecionada criptografada por aplicar o algorítmo de criptografia E1 junto à informação de posição selecionada recebida com o uso da chave de conteúdo recebida "CK".

A seguir, a unidade de processamento de criptografia 2109 emite o conteúdo criptografado gerado 2220 e a informação de posição selecionada criptografada e a informação de assinatura recebida, a informação de cabeçalho 2200 e o bloco de chave para a unidade de gravação 2114.

2.2.8 Unidade de gravação 2114

A unidade de gravação 2114 é capaz de ser carregada com o DVD.

A unidade de gravação 2114 recebe o conteúdo criptografado 2220, a informação de posição selecionada criptografada, a informação de assinatura, a informação de cabeçalho 2200 e o bloco de chave a partir da unidade de processamento de criptografia 2109 e grava o conteúdo criptografado recebido 2200, a informação de posição selecionada criptografada, a informação de assinatura, a informação de cabeçalho 2200 e o bloco de chave junto ao DVD.

2.3 DVD 2500

Como apresentado na Figura 33, um DVD 2500 armazena uma chave de bloco 2510, a informação de posição selecionada criptografada 2530, a informação de cabeçalho 2550, a informação de assinatura 2570 e o conteúdo criptografado 2580.

A chave de bloco 2510, a informação de posição selecionada criptografada 2530, a informação de cabeçalho 2550, a informação de assinatura 2570, e o conteúdo criptografado 2580 foram gravadas pelo dispositivo de distribuição 2100 e as estruturas destes componentes são como declarado acima.

2.4 Dispositivo de Execução 2600

Como apresentado na Figura 34, o dispositivo de execução 2600 é composto de uma unidade de aquisição 2601, uma unidade de aquisição de chave de conteúdo 2602, uma unidade de armazenamento de chave de dispositivo 1604, uma unidade de decriptografia de informação de po-

sição 2606, uma unidade de verificação de informação de assinatura 2611, uma unidade de armazenamento de chave de verificação 1612, uma unidade de decriptografia de conteúdo parcial representativo 2616, uma unidade de verificação de informação de cabeçalho 2617 e uma unidade de execução 2618

Os componentes individuais constituindo o dispositivo de execução 2600 são descritos em detalhes abaixo. Observe que, desde que a unidade de armazenamento de chave de dispositivo 1604 e a unidade de armazenamento de chave de verificação 1612 são as mesmas que estas constituindo o dispositivo de execução 1600 da primeira modalidade, as descrições destes componentes são omitidas.

2.4.1 Unidade de Aquisição 2601

A unidade de aquisição 2601 é carregada com o DVD 2500. Quando detectando o DVD 2500 sendo carregado na mesma, a unidade de aquisição 2601 lê o bloco de chave 2510, a informação de posição selecionada criptografada 2530, a informação de cabeçalho 2500, a informação de assinatura 2570 e o conteúdo criptografado 2580 a partir do DVD 2500. A unidade de aquisição 2601 emite o bloco de chave lido 2510, a informação de posição selecionada criptografada 2530, a informação de cabeçalho 2550, a informação de assinatura 2570 e o conteúdo criptografado 2580 para a unidade de aquisição de chave de conteúdo 2602.

2.4.2 Unidade de Aquisição de Chave de Conteúdo 2602

A unidade de aquisição de chave de conteúdo 2602 recebe o bloco de chave 2510, a informação de posição selecionada criptografada 2530, a informação de cabeçalho 2550, a informação de assinatura 2570 e o conteúdo criptografado 2580 a partir da unidade de aquisição 2601.

Quando recebendo estes conjuntos de informações, a unidade de aquisição de chave de conteúdo 2602 gera a chave de conteúdo "CK" por utilizar o identificador de dispositivo "AID_p" e a chave de dispositivo "DK_p" armazenada pela unidade de armazenamento de chave de dispositivo 1604 e o bloco de chave. Um procedimento para gerar a chave de conteúdo "CK" é o mesmo que o procedimento de geração da chave de conteúdo

"CK" conduzido pela unidade de aquisição de chave de conteúdo 1602 constituindo o dispositivo de execução 1600 da primeira modalidade e portanto, a descrição é omitida.

A seguir, a unidade de aquisição de chave de conteúdo 2602 emite a chave de conteúdo gerada "CK" e a informação de posição selecionada criptografada recebida 2530, a informação de cabeçalho 2550, a informação de assinatura 2570 e o conteúdo criptografado 2580 para a unidade de decriptografia de informação de posição 2606.

2.4.3 Unidade de decriptografia de Informação de Posição 2606

A unidade de decriptografia de informação de posição 2606 recebe a chave de conteúdo "CK", a informação de posição selecionada criptografada 2530, a informação de cabeçalho 2550, a informação de assinatura 2570 e o conteúdo criptografado 2580 a partir da unidade de aquisição de chave de conteúdo 2602.

Quando recebendo estes conjuntos de informações, a unidade de decriptografia de informação de posição 2606 gera a informação de posição selecionada pela aplicação do algorítmo de decriptografia D1 junto à informação de posição de posição selecionada criptografada recebida 2530 com o uso da chave de conteúdo recebida "CK". A informação de posição selecionada gerada neste ponto possui a mesma estrutura que a informação de posição selecionada 2160 apresentada na Figura 30.

A seguir, a unidade de decriptografia de informação de posição 2606 emite a informação de posição selecionada gerada e a chave de conteúdo recebida "CK", a informação de cabeçalho 2550, a informação de assinatura 2570 e o conteúdo criptografado 2580 para a unidade de verificação de informação de assinatura 2611.

2.4.4 Unidade de Verificação de Informação de Assinatura 2611

A unidade de verificação de informação de assinatura 2611 recebe a informação de posição selecionada, a chave de conteúdo "CK", a informação de cabeçalho 2550, a informação de assinatura 2570 e o conteúdo criptografado 2580 a partir da unidade de decriptografia de informação de posição 2606.

Quando recebendo estes conjuntos de informação, a unidade de verificação de informação de assinatura 2611 lê uma chave de verificação a partir da unidade de armazenamento de chave de verificação 1612. A seguir, a unidade de verificação de informação de assinatura 2611 extrai os valores hash parciais "HA3", "HA7" e "HAc" a partir dos três pedaços de informação hash representativa, respectivamente, constituindo a informação de cabeçalho recebida 2550 e gera a informação de verificação de assinatura por aplicar o algorítmo de verificação de assinatura V junto ao resultado combinado formado pela combinação dos valores hash parciais extraídos "HA3", "HA7" e "HAc" com o uso da chave de verificação lida. A unidade de verificação de informação de assinatura 2611 compara a informação de verificação de assinatura gerada com a informação de assinatura recebida. Quando estes dois não concordam, a unidade de verificação de informação de assinatura 2611 julga que a verificação de assinatura obteve sucesso e aborda o processamento subseqüente.

Quando estes dois concordam, a unidade de verificação de informação de assinatura 2611 julga que a verificação de assinatura obteve sucesso e emite a informação de posição selecionada recebida, a chave de conteúdo "CK", a informação de cabeçalho 2550 e o conteúdo criptografado 2580 para a unidade de decriptografia de conteúdo parcial representativo 2616.

2.4.5 Unidade de Decriptografia de Conteúdo Parcial Representativo 2616

A unidade de decriptografia de conteúdo parcial representativo 2616 recebe a informação de posição selecionada, a chave de conteúdo "CK", a informação de cabeçalho 2550 e o conteúdo criptografado 2580 a partir da unidade de verificação de informação de assinatura 2611.

Quando recebendo estes conjuntos de informação, a unidade de decriptografia de conteúdo parcial representativo 2616 extrai o identificador de informação de identificação "ADID1" e o pedaço correspondendo de informação de identificação "AD3" incluído na primeira informação de detecção representativa constituindo a informação de posição selecionada recebida e adicionalmente extrai um pedaço de conteúdo parcial criptografado

"ECNT3" a partir do conteúdo criptografado recebido 2580 baseado no pedaço de informação de identificação extraída "AD3". A seguir, a unidade de decriptografia de conteúdo parcial representativo 2616 gera o pedaço de conteúdo parcial representativo "CNT3" pela aplicação do algorítmo de decriptografia D1 junto ao conteúdo parcial criptografado extraído "ECNT3" com o uso da chave de conteúdo recebida "CK". Aqui, um par de pedaço gerado de conteúdo parcial representativo "CNT3" e de pedaço extraído do identificador da informação de identificação "ADID1" é referido como "um pedaço de informação representativa de verificação".

A seguir, a unidade de decriptografia de conteúdo parcial representativo 2616 repete o processamento do mesmo tipo para os pedaços restantes de informação de detecção representativa para gerar um pedaço de informação representativa de verificação composta do identificador de informação de identificação "ADID2" e do pedaço de conteúdo parcial representativo "CNT7" bem como um pedaço de informação representativa de verificação composta do identificador de informação de identificação "ADID3" e do pedaço de conteúdo parcial representativo "CNTc".

A seguir, a unidade de decriptografia de conteúdo parcial representativo 2616 emite os três pedaços gerados de informação representativa de verificação e a chave de conteúdo recebida "CK", a informação de cabeçalho 2550 e o conteúdo criptografado 2580 para a unidade de verificação de informação de cabeçalho 2617.

2.4.6 Unidade de Verificação de Informação de Cabeçalho 2617

A unidade de verificação de informação de cabeçalho 2617 recebe os três pedaços de informação representativa de verificação, a chave de conteúdo "CK", a informação de cabeçalho 2550 e o conteúdo criptografado 2580 a partir da unidade de decriptografia de conteúdo parcial representativo 2616.

Quando recebendo estes conjuntos de informação, a unidade de verificação de informação de cabeçalho 2617 gera valores hash de verificação "H3", "H7" e "Hc" por respectivamente designar os pedaços de conteúdo parcial representativo "CNT3", "CNT7" e "CNTc" incluídos nas três informa-

ções representativas de verificação recebidas para a função hash. A função hash utilizada aqui é a mesma que esta utilizada na unidade de geração de informação de cabeçalho 2107 do dispositivo de distribuição 2100.

A seguir, a unidade de verificação de informação de cabeçalho 2617 pesquisa, na informação de cabeçalho 2550, um identificador de informação de identificação se conformando com o identificador de informação de identificação "ADID1" incluído no pedaço correspondente de informação representativa de verificação e extrai o valor hash parcial "HA3" correspondendo ao identificador de informação de identificação detectado. Então, a unidade de verificação de informação de cabeçalho 2617 compara o valor hash parcial extraído "HA3" com o valor hash de verificação gerado "H3".

Em adição, a unidade de verificação de informação de cabeçalho 2617 extrai o valor hash parcial "HA7" a partir da informação de cabeçalho 2550 baseado no identificador de informação de identificação "ADID2" incluído no pedaço correspondente da informação representativa de verificação e compara o valor hash parcial extraído "HA7" com o valor hash de verificação gerado "H7".

A unidade de verificação de informação de cabeçalho 2617 extrai o valor hash parcial "HAc" a partir da informação de cabeçalho 2550 baseada no identificador de informação de identificação "ADIDc" incluído no pedaço correspondente da informação representativa de verificação e compara o valor parcial extraído "HAc" com o valor hash de verificação gerado "Hc".

Quando cada um dos três pares é comparado e existe mesmo um par discordando de outro, a unidade de verificação de informação de cabeçalho 2617 aborta o processamento subseqüente.

Quando todos os três pares concordam na comparação acima dos três pares, a unidade de verificação de informação de cabeçalho 2617 julga que a verificação da informação de cabeçalho 2550 obteve sucesso e emite a chave de conteúdo recebida "CK" e o conteúdo criptografado 2580 para a unidade de execução 2618.

2.4.7 Unidade de Execução 2618

A unidade de execução 2618 recebe a chave de conteúdo "CK" e o conteúdo criptografado 2580 a partir da unidade de verificação de informação de cabeçalho 2617.

Quando recebendo estes conjuntos de informações, a unidade de execução 2618 gera o conteúdo composto dos pedaços de conteúdo parcial "CNT1", "CNT2", "CNT3", ..., e "CNTc" por aplicar o algorítmo de decriptografia D1 junto a cada pedaço criptografado de conteúdo parcial "ECNT1", "ECNT2", "ECNT3", ..., e "ECNTc" compondo o conteúdo criptografado recebido 2580 com o uso da chave de conteúdo recebida "CK".

A seguir, a unidade de execução 2618 expande o conteúdo gerado para gerar dados de vídeo e de áudio e gera sinais de vídeo e de áudio a partir dos dados de vídeo e de áudio gerados. A unidade de execução 2618 emite os sinais de vídeo e de áudio gerados para o monitor.

2.5 Comportamentos Operacionais do Dispositivo de Distribuição 2100 e do Dispositivo de Execução 2600

Os comportamentos operacionais do dispositivo de distribuição 2100 e do dispositivo de execução 2600 são descritos a seguir.

2.5.1 Comportamento Operacional do Dispositivo de Distribuição 2100

O comportamento operacional do dispositivo de distribuição 2100 é descrito com o auxílio do fluxograma apresentado na Figura 35.

A unidade de entrada 2101 recebe o conteúdo 2120 composto de c pedaços de conteúdo parcial e de c pedaços de informação de identificação (Etapa S2011) e emite o conteúdo recebido 2120 e a informação de identificação para a unidade de geração de chave de conteúdo 2102.

A unidade de geração de chave de conteúdo 2102 recebe o conteúdo 2120 e os c pedaços de informação de identificação e gera uma chave de conteúdo (Etapa S2012).

A unidade de geração de bloco de chave 2103 recebe a chave de conteúdo, o conteúdo 2120 e os c pedaços de informação de identificação a partir da unidade de geração de chave de conteúdo 2102 e lê os identificadores de conteúdo e as chaves de dispositivo a partir da unidade de

armazenamento de informação de dispositivo de execução 1104 (Etapa S2013). A unidade de geração de bloco de chave 2103 gera um bloco de chave por utilizar os identificadores de dispositivo lidos e as chaves de dispositivo (Etapa S2014) e emite no bloco de chave gerado, a chave de conteúdo recebida, o conteúdo 2120 e os c pedaços de informação de identificação para a unidade de seleção 2105.

A unidade de seleção 2105 recebe o bloco de chave, a chave de conteúdo, o conteúdo 2120 e a informação de identificação e gera k pedaços de informação representativa por selecionar k pedaços de conteúdo parcial representativo a partir do conteúdo recebido 2120 (Etapa S2016). Então, a unidade de seleção 2105 emite os k pedaços gerados de informação representativa e a chave de conteúdo recebida e o conteúdo 2120 para a unidade de geração de informação de cabeçalho 2107.

A unidade de geração de informação de cabeçalho 2107 recebe os k pedaços de informação representativa, a chave de conteúdo e o conteúdo 2120 a partir da unidade de seleção 2105 e gera a informação de posição selecionada 2160 e a informação de cabeçalho 2200 a partir dos k pedaços recebidos de informação representativa (Etapa S2018). A seguir, a unidade de geração de informação de cabeçalho 2107 emite a informação de posição selecionada gerada 2160 e a informação de cabeçalho 2200 e o bloco de chave recebido, a chave de conteúdo e o conteúdo 2120 para a unidade de geração de informação de assinatura 2108.

Subseqüentemente, a unidade de geração de informação de assinatura 2108 recebe a informação de posição selecionada 2160, a informação de cabeçalho 2200, o bloco de chave, a chave de conteúdo e o conteúdo 2120 a partir da unidade de geração de informação de cabeçalho 2107. Quando recebendo estes conjuntos de informações, a unidade de geração de informação de assinatura 2108 lê a chave de assinatura 1113 a partir da unidade de armazenamento de chave de assinatura 1112 (Etapa S2019) e gera a informação de assinatura a partir da chave de assinatura lida 1113 e da informação de cabeçalho 2200 (Etapa S2021). A seguir, a unidade de geração de informação de assinatura 2108 emite a informação

de assinatura gerada e o bloco de chave recebido, a informação de posição selecionada 2160, a informação de cabeçalho 2200, a chave de conteúdo e o conteúdo 2120 para a unidade de processamento de criptografia 2109.

A unidade de processamento de criptografia 2109 recebe a informação de assinatura, o bloco de chave, a informação de posição selecionada 2160, a informação de cabeçalho 2200, a chave de conteúdo e o conteúdo 2120 a partir da unidade de geração de informação de assinatura 2108 e gera a informação de posição selecionada criptografada por criptografar a informação de posição selecionada 2160 com o uso da chave de conteúdo recebida (Etapa S2022). Subseqüentemente, a unidade de processamento de criptografia 2109 gera o conteúdo criptografado por criptografar o conteúdo 2120 com o uso da chave de conteúdo (Etapa S2023) e então emite a informação de posição selecionada criptografada gerada, o conteúdo criptografado, o bloco de chave recebido, a informação de assinatura e a informação de cabeçalho 2200 para a unidade de gravação 2114.

A unidade de gravação 2114 grava o bloco de chave, a informação de posição selecionada criptografada, a informação de cabeçalho 2200, a informação de assinatura e o conteúdo criptografado recebido a partir da unidade de processamento de criptografia 2109 junto ao DVD 2500 (Etapa S2024).

2.5.2 Comportamento Operacional do Dispositivo de Execução 2600

O comportamento operacional do dispositivo de execução 2600 é descrito com o auxílio de um fluxograma apresentando na Figura 36.

Quando sendo carregada com o DVD 2500, a unidade de aquisição 2601 lê o bloco de chave 2510, a informação de posição selecionada criptografada 2530, a informação de cabeçalho 2550, a informação de assinatura 2570 e o conteúdo criptografado 2580 a partir do DVD 2500 (Etapa S2041). Então, a unidade de aquisição 2601 emite o bloco de chave lido 2510, a informação de posição selecionada criptografada 2530, a informação de cabeçalho 2550, a informação de assinatura 2570 e o conteúdo criptografado 2580 para a unidade de aquisição de chave de conteúdo 2602.

Quando recebendo o bloco de chave 2510, a informação de po-

sição selecionada criptografada 2530, a informação de cabeçalho 2550, a informação de assinatura 2570 e o conteúdo criptografado 2580 a partir da unidade de aquisição 2601, a unidade de aquisição de chave de conteúdo 2602 lê os identificadores de dispositivo e as chaves de dispositivo a partir da unidade de armazenamento de chave de dispositivo 1604 (Etapa S2042). A unidade de aquisição de chave de conteúdo 2602 gera uma chave de conteúdo a partir dos identificadores de dispositivo e das chaves de dispositivos lidas e do bloco de chave recebido 2510 (Etapa S2043). A unidade de aquisição de chave de conteúdo 2602 emite a chave de conteúdo gerada e a informação de posição selecionada criptografada recebida, da informação de cabeçalho 2550, a informação de assinatura 2570 e o conteúdo criptografado 2580 para a unidade de decriptografia de informação de posição 2606.

A unidade de decriptografia de informação de posição 2606 recebe a chave de conteúdo, a informação de posição selecionada criptografada 2530, a informação de cabeçalho 2550, a informação de assinatura 2570 e o conteúdo criptografado 2580 a partir da unidade de aquisição de chave de conteúdo 2602 e gera a informação de posição selecionada por decriptografar a informação de posição selecionada criptografada 2530 com o uso da chave de conteúdo recebida (Etapa S2044). A seguir, a unidade de decriptografia de informação de posição 2606 emite a informação de posição selecionada gerada e a chave de conteúdo recebida, a informação de cabeçalho 2550, a informação de assinatura 2570 e o conteúdo criptografado 2580 para a unidade de verificação de informação de assinatura 2611.

A unidade de verificação de informação de assinatura 2611 recebe a informação de posição selecionada, a chave de conteúdo, a informação de cabeçalho 2550, a informação de assinatura 2570 e o conteúdo criptografado 2580 a partir da unidade de decriptografia de informação de posição 2606 e lê uma chave de verificação a partir da unidade de armazenamento de chave de verificação 1612 (Etapa S2046). Então, a unidade de verificação de informação de assinatura 2611 verifica a informação de assinatura 2570 por utilizar a chave de verificação lida e a informação de cabe-

çalho recebida 2550 (Etapa S2048). Quando a verificação da informação de assinatura 2570 é malsucedida (Etapa S2049: NÃO), a unidade de verificação de informação de assinatura 2611 aborta o processamento subseqüente no dispositivo de execução 2600.

Quando a verificação da informação de assinatura 2570 obtém sucesso (Etapa S2049: SIM), a unidade de verificação de informação de assinatura 2611 emite a informação de posição selecionada recebida, a chave de conteúdo, a informação de cabeçalho 2550, e o conteúdo criptografado 2580 para a unidade de decriptografia de conteúdo parcial representativo 2616.

A unidade de decriptografia de conteúdo parcial representativo 2616 recebe a informação de posição selecionada, a chave de conteúdo, a informação de cabeçalho 2550 e o conteúdo criptografado 2580 a partir da unidade de verificação de informação de assinatura 2611 e gera k pedaços de conteúdo parcial representativo baseada na informação de posição selecionada recebida, no conteúdo criptografado 2580 e na chave de conteúdo (Etapa S2051). Então, a unidade de decriptografia de conteúdo parcial representativo 2616 gera k pedaços de informação representativa de verificação composta dos pedaços correspondentes de conteúdo parcial representativo e dos identificadores de informação de identificação (Etapa S2052) e emite os k pedaços gerados de informação representativa de verificação e a chave de conteúdo recebida, a informação de cabeçalho 2550 e o conteúdo criptografado 2580 para a unidade de verificação de informação de cabeçalho 2617.

A unidade de verificação de informação de cabeçalho 2617 recebe os k pedaços de informação representativa de verificação, a chave de conteúdo, a informação de cabeçalho 2550 e o conteúdo criptografado 2580 a partir da unidade de decriptografia de conteúdo parcial representativo 2616 e executa a verificação da informação de cabeçalho 2550 por utilizar os k pedaços recebidos de informação representativa de verificação (Etapa S2054). Se a verificação for malsucedida (Etapa S2056: NÃO), a unidade de verificação de informação de cabeçalho 2617 aborta o processamento sub-

seqüente.

Quando a verificação é bem sucedida (Etapa S2056:SIM), a unidade de verificação de informação de cabeçalho 2617 emite a chave de conteúdo recebida e o conteúdo criptografado 2580 para a unidade de execução 2618.

Quando recebendo a chave de conteúdo e o conteúdo criptografado 2580 a partir da unidade de verificação de informação de cabeçalho 2617, a unidade de execução 2618 gera o conteúdo por decriptografar o conteúdo criptografado 2580 com o uso da chave de conteúdo recebida (Etapa S2057), expande o conteúdo gerado (Etapa S2058) e tem o monitor executando o conteúdo (Etapa S2059).

2.6 Sumário e Efeitos Vantajosos

Como foi descrito, na segunda modalidade, o dispositivo de distribuição 2100 gera a informação de cabeçalho por utilizar somente k pedaços de conteúdo parcial representativo dentre os c pedaços de conteúdo parcial constituindo o conteúdo e adicionalmente gera a informação de assinatura por aplicar o algorítmo de geração de assinatura junto à informação de cabeçalho.

O dispositivo de execução 2600 executa a verificação de se conteúdo não autorizado está incluído por gerar k pedaços de conteúdo parcial representativo baseado na informação de posição selecionada e por executar a verificação da informação de cabeçalho por utilizar os k pedaços gerados de conteúdo parcial representativo. Quando a verificação é bem sucedida, o dispositivo de execução 2600 começa a reprodução do conteúdo, julgando que nenhum conteúdo não autorizado está incluído.

Assim, executar a verificação da informação de cabeçalho com o uso de somente k pedaços dentro dos c pedaços de conteúdo parcial constituindo o conteúdo alcança uma redução na carga de processamento do dispositivo de execução 2600 para a verificação.

Adicionalmente, também é possível reduzir a carga de processamento envolvida na geração da informação de cabeçalho no dispositivo de distribuição 2100.

3. Terceira Modalidade

O dito a seguir descreve um sistema de detecção de conteúdo não autorizado de acordo com uma terceira modalidade da presente invenção.

3.1 Sistema de detecção de conteúdo não autorizado

O sistema de detecção de conteúdo não autorizado de uma terceira modalidade é composto de um dispositivo de distribuição, de um dispositivo de execução e de um monitor, como no sistema de detecção de conteúdo não autorizado da primeira modalidade.

O dispositivo de distribuição adquire conteúdo de acordo com as operações conduzidas por um operador e gera conteúdo criptografado por criptografar o conteúdo adquirido.

Em adição, o dispositivo de distribuição extrai parte do conteúdo e gera informação tal como informação de cabeçalho utilizada para detectar se conteúdo não autorizado está incluído no conteúdo, informação de assinatura para proporcionar que o conteúdo seja emitido por um mantenedor legítimo de direito e assim por diante, baseado na parte extraída do conteúdo (daqui para frente referido como "um pedaço de conteúdo parcial representativo"). O dispositivo de distribuição repete a extração de um pedaço de conteúdo parcial representativo, a geração de um pedaço de informação de cabeçalho e a geração de um pedaço de informação de assinatura para gerar vários pedaços de informação de cabeçalho e de assinatura e grava o conteúdo criptografado gerado e os vários pedaços de informação de cabeçalho e de assinatura junto a um DVD.

O DVD será vendido ou distribuído para usuários através de saídas de distribuição.

O dispositivo de execução seleciona um pedaço, cada um a partir dos vários pedaços de informação de assinatura e dos vários pedaços de informação de cabeçalho gravados no DVD e executa a verificação dos pedaços selecionados de informação de assinatura e de cabeçalho.

Dispositivos individuais compondo o sistema de detecção de conteúdo não autorizado da presente modalidade e o DVD são descritos em

detalhes abaixo.

3.2 Dispositivo de Distribuição 3100

A Figura 37 apresenta uma estrutura de um dispositivo de distribuição da presente modalidade. Como apresentado na Figura 37, o dispositivo de distribuição 3100 é composto de uma unidade de entrada 2101, de uma unidade de geração de chave de conteúdo 2102, de uma unidade de geração de bloco chave 2103, de uma unidade de armazenamento de informação de dispositivo de execução 1104, de uma unidade de seleção 3105, de uma unidade de geração de informação de cabeçalho 3107, de uma unidade de geração de informação de assinatura 3108, de uma unidade de armazenamento de chave de assinatura 1112, de uma unidade de processamento de criptografia 3109 e de uma unidade de gravação 3114. A unidade de entrada 2101, a unidade de geração de chave de conteúdo 2102, a unidade de geração de bloco de chave 2103, a unidade de armazenamento de informação de dispositivo de execução 1104 e a unidade de armazenamento de chave de assinatura 1112 são as mesmas que na segunda modalidade e portanto as descrições para estes componentes são omitidas.

2.2.1 Unidade de Seleção 3105

A unidade de seleção 3105 pré-armazena o número de repetição "x" (x é um número inteiro 2 ou maior).

A unidade de seleção 3105 recebe o bloco de chave, a chave de conteúdo "CK", o conteúdo e os c pedaços de informação de identificação a partir da unidade de geração de bloco de chave 2103. Quando recebendo o bloco de chave, a chave de conteúdo "CK", o conteúdo e os c pedaços de informação de identificação, a unidade de seleção 3105 gera k pedaços de informação representativa do mesmo modo que a unidade de seleção 2105 da segunda modalidade.

A unidade de seleção 3105 repete o processamento do mesmo tipo x vezes para gerar x grupos de k pedaços de informação representativa. Aqui, o primeiro grupo de informação representativa é referido como o "primeiro grupo representativo" enquanto o segundo grupo, ..., e o x-ésimo gru-

po de informação representativa são referidos respectivamente como um "segundo grupo representativo" e um "x-ésimo grupo representativo". Um exemplo específico aqui é que todos dentre o primeiro até o x-ésimo grupo representativo é respectivamente composto de k pedaços de informação representativa, entretanto, o número de pedaços de informação representativa pode ser diferente de grupo para grupo.

A seguir, a unidade de seleção 3105 emite o primeiro, segundo, ..., e x-ésimo grupo representativo gerado e o bloco de chave recebido, a chave de conteúdo "CK" e o conteúdo para a unidade de geração de informação de cabeçalho 3107.

3.2.2 Unidade de Geração de Informação de Cabeçalho 3105

A unidade de geração de informação de cabeçalho 3107 recebe o primeiro, segundo e x-ésimo grupo representativo, o bloco de chave, a chave de conteúdo "CK" e o conteúdo a partir da unidade de seleção 3105.

Quando recebendo estes grupos de informações, a unidade de geração de informação de cabeçalho 3107 gera a informação de posição selecionada "POS1" e a informação de cabeçalho "HEAD1" baseada nos k pedaços de informação representativa incluída no primeiro grupo representativo e no conteúdo. Um procedimento específico para gerar a informação de posição selecionada e a informação de cabeçalho é o mesmo que os procedimentos de geração da informação de posição selecionada 2160 e da informação de cabeçalho 2200 executados pela unidade de geração de informação de cabeçalho 2107 da segunda modalidade e portanto as descrições são omitidas aqui. A informação de posição selecionada "POS1" possui a mesma estrutura que a informação de posição selecionada 2160 apresentada na Figura 30 enquanto a informação de cabeçalho "HEAD1" possui a mesma estrutura que a informação de cabeçalho 2200 apresentada na Figura 31.

A seguir, a unidade de geração de informação de cabeçalho 3107 gera um identificador de cabeçalho "HEADID1" específico para um par de informação de posição selecionada gerada "POS1" e informação de cabeçalho "HEAD1". Aqui, uma coleção do identificador de cabeçalho gerado

"HEADID1", de um pedaço de informação de posição selecionada "POS1" e de um pedaço de informação de cabeçalho "HEAD1" é referida como um "primeiro grupo de cabeçalho".

A unidade de geração de informação de cabeçalho 3107 repete o processamento do mesmo tipo para o segundo, terceiro, ..., e x-ésimo grupo representativo para gerar o segundo, terceiro, ..., x-ésimo grupo representativo.

A seguir, a unidade de geração de informação de cabeçalho 3107 extrai identificadores de cabeçalho a partir do primeiro até o x-ésimo grupo e gera a informação de seleção de cabeçalho composta dos x pedaços extraídos de identificadores de cabeçalho.

A Figura 38 apresenta um exemplo de uma estrutura da informação de seleção de cabeçalho gerada neste ponto. A informação de seleção de cabeçalho 3130 é composta de x pedaços de identificadores de cabeçalho e dos identificadores de cabeçalho correspondem respectivamente ao primeiro até o x-ésimo grupo de cabeçalho.

A seguir, a unidade de geração de informação de cabeçalho 3107 emite a informação de seleção de cabeçalho gerada 3130 e o primeiro, segundo, ..., e x-ésimo grupo de cabeçalho e o bloco de chave recebido, a chave de conteúdo "CK" e o conteúdo para a unidade de geração de informação de assinatura 3108.

3.2.3 Unidade de Geração de Informação de Assinatura 3108

A unidade de geração de informação de assinatura 3108 recebe a informação de seleção de cabeçalho 3130, o primeiro, segundo, ..., e x-ésimo grupo de cabeçalho, o bloco de chave, a chave de conteúdo "CK" e o conteúdo a partir da unidade de geração de informação de cabeçalho 3107.

Quando recebendo estes conjuntos de informações, a unidade de geração de informação de assinatura 3108 lê a chave de assinatura 1113 a partir da unidade de armazenamento de chave de assinatura 1112.

A seguir, a unidade de geração de informação de assinatura 3108 gera um pedaço de informação de assinatura "Sign1" com o uso da informação de cabeçalho "HEAD1" incluída no primeiro grupo de cabeçalho

e da chave de assinatura lida 1113. Um procedimento específico para gerar o pedaço de informação de assinatura é o mesmo que o conduzido pela unidade de geração de informação de assinatura 2108.

Aqui, o termo "primeiro grupo de cabeçalho" é redesignado para um resultado formado pela adição do pedaço gerado de informação de assinatura "Sign1" para o identificador de cabeçalho "HEADID1", para o pedaço de informação selecionada "POS1" e para o pedaço da informação de cabeçalho "HEAD1".

A unidade de geração de informação de assinatura 3108 repete o processamento do mesmo tipo para o segundo até o x-ésimo grupo de cabeçalho para gerar pedaços de informação de assinatura e novamente forma o segundo até o x-ésimo grupo de cabeçalho por adicionar os pedaços gerados de informação de assinatura respectivamente para os identificadores de cabeçalho correspondente, para os pedaços de informação de posição selecionada e para os pedaços de informação de cabeçalho.

A seguir, a unidade de geração de informação de assinatura 3108 emite o primeiro, segundo, ..., e x-ésimo grupo de cabeçalho e a informação de seleção de cabeçalho recebida 3130, o bloco de chave, a chave de conteúdo "CK" e o conteúdo para a unidade de processamento de criptografia 3109.

3.2.4 Unidade de Processamento de Criptografia 3109

A unidade de processamento de criptografia 3109 recebe o primeiro, segundo, ..., e o x-ésimo grupo de cabeçalho, a informação de seleção de cabeçalho 3130, o bloco de chave, a chave de conteúdo "CK" e o conteúdo a partir da unidade de geração de informação de assinatura 3108.

A unidade de processamento de criptografia 3109 gera c pedaços de conteúdo parcial criptografado pela aplicação do algorítmo de criptografia E1 junto aos pedaços individuais de conteúdo parcial constituindo o conteúdo recebido com o uso da chave de conteúdo "CK" e coloca os c pedaços gerados de conteúdo parcial criptografado juntos para formar o conteúdo criptografado. O conteúdo criptografado gerado neste ponto possui a mesma estrutura que o conteúdo criptografado 2220 na Figura 32.

A seguir, a unidade de processamento de criptografia 3109 extrai o pedaço de informação de posição selecionada "POS1" a partir do primeiro grupo de cabeçalho e gera um pedaço de informação de posição selecionada criptografada "EPOS1" pela aplicação do algorítmo de criptografia E1 junto ao pedaço extraído de informação de posição selecionada "POS1" com o uso da chave de conteúdo "CK". A seguir, a unidade de processamento de criptografia 3109 substitui o pedaço de informação de posição selecionada "POS1" incluído no primeiro grupo de cabeçalho pelo pedaço gerado de informação de posição selecionada "EPOS1". Aqui, EPOS1 = Enc (CK, POS1).

A unidade de processamento de criptografia 3109 faz o mesmo com o segundo até o x-ésimo grupo de cabeçalho para gerar pedaços de informação de posição selecionada criptografada e substitui os pedaços correspondentes de informação de posição selecionada pelos pedaços de informação de posição selecionada criptografada.

A seguir, a unidade de processamento de criptografia 3109 emite o primeiro, segundo, ..., e x-ésimo grupo de cabeçalho, o conteúdo criptografado gerado e a informação de seleção de cabeçalho recebida 3130 e o bloco de chave para a unidade de gravação 3114.

3.2.5 Unidade de Gravação 3114

A unidade de gravação 3114 recebe o primeiro, segundo, ..., e x-ésimo grupos de cabeçalho, o conteúdo criptografado, a informação de seleção de cabeçalho 3130 e o bloco de chave a partir da unidade de processamento de criptografia 3109 e grava o primeiro, segundo, ..., e x-ésimo grupo de cabeçalho recebido, o conteúdo criptografado, a informação de seleção de cabeçalho 3130 e o bloco de chave para um DVD.

3.3 DVD 3500

A Figura 39 apresenta informação gravada por um DVD de acordo com a presente modalidade.

Como apresentado na Figura 39, um DVD 3500 armazena um bloco de chave 3510, a informação de seleção de cabeçalho 3520, um primeiro grupo de cabeçalho 3530, um segundo grupo de cabeçalho 3540, ...,

e um x-ésimo grupo de cabeçalho 3560, e conteúdo criptografado 3580.

Cada um dentre o primeiro grupo de cabeçalho 3530, o segundo grupo de cabeçalho 3540, ..., e o x-ésimo grupo de cabeçalho 3560 é composto de um identificador de cabeçalho, um pedaço de informação de posição selecionada criptografada, um pedaço de informação de cabeçalho e de um pedaço de informação de assinatura.

Por exemplo, o primeiro grupo de cabeçalho 3530 é composto de um identificador de cabeçalho "HEAD1" 3531, um pedaço de informação de posição selecionada criptografada "EPOS1" 3532, um pedaço de informação de cabeçalho "HEAD1" e de um pedaço de informação de assinatura "Sign1" 3534.

Os conjuntos de informações foram gravados junto ao DVD 3500 pelo dispositivo de distribuição 3100. A estrutura de cada conjunto de informações é como anteriormente mencionado e portanto, a descrição é omitida aqui.

3.4 Dispositivo de Execução 3600

Como apresentado na Figura 40, um dispositivo de execução 3600 é composto de uma unidade de aquisição 3601, de uma unidade de aquisição de chave de conteúdo 2602, de uma unidade de armazenamento de chave de dispositivo 1604, de uma unidade de decriptografia de informação de posição 2606, de uma unidade de verificação de informação de assinatura 2611, de uma unidade de armazenamento de chave de verificação 1612, de uma unidade de decriptografia de conteúdo parcial representativo 2616, de uma unidade de verificação de informação de cabeçalho 2617 e de uma unidade de execução 2618.

Componentes diferentes da unidade de aquisição 3601 possuem as mesmas estruturas e comportamentos operacionais que a unidade de aquisição de chave de conteúdo 2602, a unidade de armazenamento de chave de dispositivo 1604, a unidade de decriptografia de informação de posição 2606, a unidade de verificação de informação de assinatura 2611, a unidade de armazenamento de chave de verificação 1612, a unidade de decriptografia de conteúdo parcial representativo 2616, a unidade de verifi-

cação de informação de cabeçalho 2617 e a unidade de execução 2618 constituindo o dispositivo de execução 2600 da segunda modalidade. Portanto, agora, somente é descrita a unidade de aquisição 3601.

3.4.1 Unidade de Aquisição 3601

Quando detectando o DVD 3500 sendo carregado na mesma, a unidade de aquisição 3601 lê a informação de seleção de cabeçalho 3520 a partir do DVD 3500. Então, a unidade de aquisição 3601 seleciona um dos identificadores de cabeçalho "HEADID1", "HEADID2", "HEADID3", ..., e "HEADIDx" incluídos na informação de cabeçalho lida 3520 com o uso de um número aleatório. O método de seleção não está limitado a isto e qualquer método é aplicável contanto que seja difícil para uma terceira parte prognosticar qual identificador é selecionado.

A seguir, a unidade de aquisição 3601 recupera, dentre o primeiro, segundo, ..., e x-ésimo grupo de cabeçalho gravados no DVD 3500, um grupo de cabeçalho incluindo o identificador de cabeçalho selecionado e lê um pedaço de informação de posição selecionada criptografada, um pedaço de informação de cabeçalho e um pedaço de informação de assinatura a partir do grupo de cabeçalho.

Subseqüentemente, a unidade de aquisição 3601 lê o bloco de chave 3510 e o conteúdo criptografado 3580 a partir do DVD 3500 e emite o bloco de chave lido 3510, o conteúdo criptografado, a informação de posição selecionada criptografada, a informação de cabeçalho e a informação de assinatura para a unidade de aquisição de chave de conteúdo 2602.

3.5 Sumário e Efeitos Vantajosos

Como foi descrito, o dispositivo de distribuição 3100 da terceira modalidade gera x grupos, cada um dos quais é composto de um pedaço de informação de posição selecionada criptografada, de um pedaço de informação de cabeçalho e de um pedaço de informação de assinatura e o dispositivo de execução seleciona um dos x grupos e executa verificação de se conteúdo não autorizado está incluído por utilizar um pedaço de informação de posição selecionada criptografada, um pedaço de informação de cabeçalho e um pedaço de informação de assinatura do grupo selecionado.

Assim, por aumentar o número de pedaços do conteúdo parcial representativo utilizado para a verificação, é possível acentuar a precisão para detectar conteúdo não autorizado. Adicionalmente, é difícil prognosticar qual grupo de cabeçalho, dentre o primeiro até o x-ésimo grupo de cabeçalho, é selecionado no dispositivo de execução 3600 e portanto, é possível impedir atos fraudulentos envolvendo substituir especificamente somente pedaços de conteúdo parcial, de não serem utilizados para verificação com conteúdo não autorizado.

4. Quarta Modalidade

Um sistema de detecção de conteúdo não autorizado de acordo com uma quarta modalidade da presente invenção é descrito abaixo.

4.1. Sistema de Detecção de Conteúdo Não Autorizado

O sistema de detecção de conteúdo não autorizado de uma quarta modalidade é composto de um dispositivo de distribuição, de um dispositivo de execução e de um monitor, como na primeira modalidade.

O dispositivo de distribuição adquire conteúdo de acordo com operações de um operador e gera conteúdo criptografado por criptografar o conteúdo adquirido.

Em adição, o dispositivo de distribuição divide o conteúdo em vários pedaços de conteúdo parcial e gera informação de cabeçalho utilizada para verificar se conteúdo não autorizado está incluído no conteúdo bem como informação de assinatura para proporcionar que o conteúdo seja emitido por um mantenedor legítimo de direito baseado em todos os pedaços de conteúdo parcial. O dispositivo de distribuição grava o conteúdo criptografado gerado, a informação de assinatura e assim por diante junto a um DVD.

O DVD será vendido ou distribuído para usuários através de saídas de distribuição.

Quando carregado com o DVD, o dispositivo de execução seleciona alguns pedaços dentre os vários pedaços de conteúdo parcial constituindo o conteúdo e verifica a informação de cabeçalho por utilizar somente os pedaços selecionados de conteúdo parcial.

Dispositivos individuais compondo o sistema de detecção de

conteúdo não autorizado da presente modalidade e do DVD são descritos em detalhes abaixo.

4.2 Dispositivo de Distribuição 4100

A Figura 41 apresenta uma estrutura do dispositivo de distribuição da quarta modalidade. Como apresentado na Figura 41, um dispositivo de distribuição 4100 é composto de uma unidade de entrada, de uma unidade de geração de chave de conteúdo 4102, de uma unidade de geração de bloco de chave 4103, de uma unidade de armazenamento de informação de dispositivo de execução 1104, de uma unidade de geração de conteúdo parcial 4105, de uma unidade de geração de informação de cabeçalho 4107, de uma unidade de geração de informação de assinatura 4108, de uma unidade de armazenamento de chave de assinatura 1112, de uma unidade de processamento de criptografia 4109, e de uma unidade de gravação 4114.

O dito a seguir descreve componentes individuais constituindo o dispositivo de distribuição 4100. Observa-se que, desde que a unidade de armazenamento de informação de dispositivo de execução 1104 e a unidade de armazenamento de chave de assinatura 1112 são as mesmas que na primeira modalidade, as descrições para estes componentes são omitidas.

4.2.1 Unidade de Entrada 4101

A unidade de entrada 4101 adquire conteúdo a partir de um dispositivo externo ou meio de gravação externo de acordo com as operações do operador do dispositivo de distribuição 4100. O conteúdo adquirido aqui está em um formato executável para um dispositivo de execução 4600 (como será descrito daqui para frente em detalhes) e o formato DVD-Vídeo e o formato MPEG-2 são exemplos de tais formatos executáveis.

A unidade de entrada 4101 emite o conteúdo adquirido para a unidade de geração de chave de conteúdo 4102.

4.2.2 Unidade de Geração de Chave de Conteúdo 4102

A unidade de geração de chave de conteúdo 4102 recebe o conteúdo a partir da unidade de entrada 4101. Quando recebendo o conteúdo, a unidade de geração de chave de conteúdo 4102 gera um número pseudo-aleatório e gera uma chave de conteúdo com comprimento de 128

bits "CK" com o uso do número pseudo-aleatório gerado. Ao invés de um número pseudo-aleatório, um número aleatório real pode ser gerado por se utilizar, por exemplo, ruído em um sinal.

A seguir, a unidade de geração de chave de conteúdo 4102 emite a chave de conteúdo gerada "CK" e o conteúdo recebido para a unidade de geração de bloco de chave 4103.

4.2.3 Unidade de Geração de Bloco de Chave 4103

A unidade de geração de bloco de chave 4103 recebe a chave de conteúdo "CK" e o conteúdo a partir da unidade de geração de chave de conteúdo 4102. Quando recebendo a chave de conteúdo "CK" e o conteúdo, a unidade de geração de bloco de chave 4103 gera um bloco de chave por utilizar a chave de conteúdo recebida "CK" e uma tabela de identificação de dispositivo armazenada na unidade de armazenamento de informação de dispositivo de execução 1104. Um procedimento específico para gerar o bloco de chave é o mesmo que um executado pela unidade de geração de bloco de chave 1103 da primeira modalidade e portanto a descrição é omitida.

A seguir, a unidade de geração de bloco de chave 4103 emite o bloco de chave gerado e a chave de conteúdo recebida "CK" e o conteúdo para a unidade de geração de conteúdo parcial 4105.

4.2.4 Unidade de Geração de Conteúdo Parcial 4105

A unidade de geração de conteúdo parcial 4105 recebe o bloco de chave, a chave de conteúdo "CK" e o conteúdo a partir da unidade de geração de bloco de chave 4103.

Quando recebendo estes conjuntos de informações, a unidade de geração de conteúdo parcial 4105 divide o conteúdo recebido em c pedaços de conteúdo parcial "CNT1", "CNT2", "CNT3", ..., e "CNTc". Por exemplo, quando o conteúdo está no formato DVD-Vídeo, VOBs ou VOBUs podem ser utilizados como a unidade de divisão. Por outro lado, quando o conteúdo está no formato MPEG-2, GOPs (Grupo de Imagens), campos, quadros, ou intra-imagens podem ser utilizados como a unidade de divisão. Alternativamente, independente do formato do conteúdo, o conteúdo pode

ser dividido a cada 64 kilobytes, ou em cada parte correspondendo a um segundo de tempo de reprodução. Os c pedaços de conteúdo parcial gerados neste ponto são coletivamente referidos como um conteúdo dividido.

A seguir, a unidade de geração de conteúdo parcial 4105 gera pedaços de informação de identificação "AD1", "AD2", "AD3", ..., e "ADc" que respectivamente correspondem aos n pedaços gerados de conteúdo parcial. Cada pedaço de informação de identificação é informação unicamente identificando um pedaço correspondente de conteúdo parcial e é, por exemplo, um ponto inicial de reprodução do pedaço do conteúdo parcial que é especificado por referência do cabeçalho do conteúdo, ou um deslocamento a partir do cabeçalho do conteúdo.

A Figura 42 apresenta o conteúdo dividido e a informação de identificação gerados neste ponto. O conteúdo dividido 4120 é composto de c pedaços de conteúdo parcial "CNT1", 4121, "CNT2" 4122, "CNT3" 4123, ..., e "CNTc" 4127. Cada pedaço de conteúdo parcial corresponde a um pedaço de informação de identificação. Por exemplo, um pedaço de informação de identificação "AD1" 4131 é informação para identificar o pedaço de conteúdo parcial "CNT1" 4121.

A seguir, a unidade de geração de conteúdo parcial 4105 emite os c pedaços gerados de informação de identificação e o conteúdo dividido 4120 e o bloco de chave recebido e a chave de conteúdo "CK" para a unidade de geração de informação de cabeçalho 4107.

4.2.5 Unidade de Geração de Informação de cabeçalho 4107

A unidade de geração de informação de cabeçalho 4107 recebe os c pedaços de informação de identificação "AD1", "AD2", "AD3", ..., e "ADc" e o conteúdo dividido 4120, o bloco de chave e a chave de conteúdo "CK" a partir da unidade de geração de conteúdo parcial 4105.

Quando recebendo estes conjuntos de informações, a unidade de geração de informação de cabeçalho 4107 gera um identificador de informação de identificação "ADID1" unicamente identificando o pedaço de informação de identificação "AD1" com o uso de um número aleatório.

Aqui, um par de identificador de informação de identificação ge-

rado "ADID1" e pedaço recebido de informação de identificação "AD1" é referido como "um pedaço de informação de detecção de conteúdo".

A seguir, a unidade de geração de informação de cabeçalho 4107 extrai o conteúdo parcial "CNT1" 4121 a partir do conteúdo dividido 4120 baseado nos pedaços recebidos de informação de identificação "AD1" e calcula um valor hash parcial "HA1" por designar o pedaço extraído de conteúdo parcial "CNT1" 4121 para a função hash. Aqui, um par de identificador de informação de identificação "ADID1" e valor hash calculado "HA1" é referido como "um pedaço de informação hash parcial".

A unidade de geração de informação de cabeçalho 4107 repete o processamento do mesmo tipo para os pedaços restantes de informação de identificação "AD2", "AD3", ..., e "ADc" para gerar pedaços de informação de detecção de conteúdo e pedaços de informação hash parcial.

A seguir, a unidade de geração de informação de cabeçalho 4107 gera a informação de posição de conteúdo composta dos c pedaços gerados de informação de detecção de conteúdo. A Figura 43 apresenta uma estrutura da informação de posição de conteúdo gerada neste ponto. A informação de posição de conteúdo 4140 é composta de c pedaços de informação de detecção de conteúdo 4141, 4142, 4143, ..., e 4146. Cada pedaço de informação de detecção de conteúdo inclui um identificador de informação de identificação e um pedaço de informação de identificação. Como um exemplo, o pedaço de informação de detecção de conteúdo 4141 inclui um identificador de informação de identificação "ADID1" 4151 e o pedaço de informação de identificação "AD1" 4131.

Subseqüentemente, a unidade de geração de informação de cabeçalho 4107 gera a informação de cabeçalho composta dos c pedaços gerados de informação hash parcial. A Figura 44 apresenta uma estrutura da informação de cabeçalho gerada neste ponto. A informação de cabeçalho 4160 é composta de c pedaços de informação hash parcial 4161, 4162, 4163, ..., e 4166. Cada pedaço de informação hash parcial inclui um identificador de informação de identificação e um valor hash parcial e corresponde a um pedaço de informação de detecção de conteúdo constituindo a infor-

mação de posição de conteúdo 4140. Por exemplo, o pedaço de informação hash parcial 4161 inclui um identificador de informação de identificação "A-DID1" 4171 e um valor hash parcial "HA1" 4172.

A seguir, a unidade de geração de informação de cabeçalho 4107 emite a informação de posição de conteúdo gerada 4140 e a informação de cabeçalho 4160 e o conteúdo dividido recebido 4120, o bloco de chave e a chave de conteúdo "CK" para a unidade de geração de informação de assinatura 4108.

4.2.6 Unidade de Geração de Informação de Assinatura 4108

A unidade de geração de informação de assinatura 4108 recebe a informação de posição de conteúdo 4140, a informação de cabeçalho 4160, o conteúdo dividido 4120, o bloco de chave e a chave de conteúdo "CK" a partir da unidade de geração de informação de cabeçalho 4107.

Quando recebendo estes conjuntos de informação, a unidade de geração de informação de assinatura 4108 extrai os valores hash incluídos nos pedaços individuais de informação hash parcial constituindo a informação de cabeçalho recebida 4160. A unidade de geração de informação de assinatura 4108 gera um valor hash combinado por designar um resultado combinado formado por se combinar os c pedaços extraídos de valores hash parcial "HA1", "HA2", "HA3", ..., e "HAc" para a função hash.

A seguir, a unidade de geração de informação de assinatura 4108 lê a chave de assinatura 1113 a partir da unidade de armazenamento de chave de assinatura 1112 e gera a informação de assinatura pela aplicação do algorítmo de geração de assinatura S para o valor hash combinado com o uso da chave de assinatura lida 1113.

Quando tendo gerado a informação de assinatura, a unidade de geração de informação de assinatura 4108 emite a informação de assinatura gerada e a informação de posição de conteúdo recebida 4140, a informação de cabeçalho 4169, o conteúdo dividido 4120, a chave de bloco, e a chave de conteúdo "CK" para a unidade de processamento de criptografia 4109.

4.2.7 Unidade de Processamento de Criptografia 4109

A unidade de processamento de criptografia 4109 recebe a in-

formação de assinatura, a informação de posição de conteúdo 4140, a informação de cabeçalho 4160, o conteúdo dividido 4120, o bloco de chave e a chave de conteúdo "CK" a partir da unidade de geração de informação de assinatura 4108.

Quando recebendo estes conjuntos de informações, a unidade de processamento de criptografia 4109 gera um pedaço de conteúdo parcial criptografado "ECNT1" por aplicar um algorítmo de criptografia para o pedaço de conteúdo parcial "CNT1" 4121 constituindo o conteúdo dividido recebido 4120. A unidade de processamento de criptografia 4109 repete o processamento do mesmo tipo para os pedaços de conteúdo parcial "CNT2" 4122, "CNT3" 4123, ..., e "CNTc" 4127 para gerar pedaços de conteúdo parcial criptografados "ECNT2", "ECNT3", ..., e "ECNTc".

A seguir, a unidade de processamento de criptografia 4109 gera conteúdo criptografado composto dos c pedaços gerados de conteúdo parcial criptografado "ECNT1", "ECNT2", "ECNT3", ..., e "ECNTc". O conteúdo criptografado gerado neste ponto possui a mesma estrutura que o conteúdo criptografado 2220 (Figura 32) da segunda modalidade.

A seguir, a unidade de processamento de criptografia 4109 emite o conteúdo criptografado gerado e a informação de assinatura recebida, a informação de posição de conteúdo 4140, a informação de cabeçalho 4160 e o bloco de chave para a unidade de gravação 4114.

4.2.8 Unidade de Gravação 4114

A unidade de gravação 4114 é carregada com um DVD.

A unidade de gravação 4114 recebe o conteúdo criptografado, a informação de assinatura, a informação de posição de conteúdo 4140, a informação de cabeçalho 4160 e o bloco de chave a partir da unidade de processamento de criptografia 4109.

Quando recebendo estes conjuntos de informações, a unidade de gravação 4114 grava o conteúdo criptografado recebido, a informação de assinatura, a informação de posição de conteúdo 4140, a informação de cabeçalho 4160 e o bloco de chave junto ao DVD.

4.3 DVD 4500

A Figura 45 apresenta a informação armazenada em um DVD da quarta modalidade. Como apresentado na Figura 45, um DVD 4500 armazena um bloco de chave 4510, a informação de posição de conteúdo 4530, a informação de cabeçalho 4550, a informação de assinatura 4570 e o conteúdo criptografado 4580.

Estes conjuntos de informações foram gravados pelo dispositivo de distribuição 4100. As estruturas destes conjuntos de informações individuais são como declaradas acima e portanto, as descrições são omitidas aqui.

4.4 Dispositivo de Execução 4600

A Figura 46 apresenta uma estrutura do dispositivo de execução da quarta modalidade. Como apresentado na Figura 46, um dispositivo de execução 4600 é composto de uma unidade de aquisição 4601, de uma unidade de aquisição de chave de conteúdo 4602, de uma unidade de armazenamento de chave de dispositivo 1604, de uma unidade de verificação de informação de assinatura 4606, de uma unidade de armazenamento de chave de verificação 1612, de uma unidade de seleção 4611, de uma unidade de decriptografia de conteúdo parcial 4616, uma unidade de verificação de informação de cabeçalho 4617 e de uma unidade de execução 2618

Os componentes individuais constituindo o dispositivo de execução 4600 são descritos em detalhes abaixo. Observe que, desde que a unidade de armazenamento de chave de dispositivo 1604 e a unidade de armazenamento de chave de verificação 1612 são as mesmas que na primeira modalidade enquanto a unidade de execução 2618 sendo a mesma que na segunda modalidade, as descrições destes componentes são omitidas.

4.4.1 Unidade de Aquisição 4601

A unidade de aquisição 4601 é carregada com o DVD 4500. Quando detectando o DVD 4500 na mesma, a unidade de aquisição 4601 lê o bloco de chave 4510, a informação de posição de conteúdo 4530, a informação de cabeçalho 4550, a informação de assinatura 4570 e o conteúdo criptografado 4580 e emite o bloco de chave lido 4510, a informação de po-

sição de conteúdo 4530, a informação de cabeçalho 4550, a informação de assinatura 4570 e o conteúdo criptografado 4580 para a unidade de aquisição de chave de conteúdo 4602.

4.4.2 Unidade de Aquisição de Chave de Conteúdo 4602

A unidade de aquisição de chave de conteúdo 4602 recebe o bloco de chave 4510, a informação de posição de conteúdo 4530, a informação de cabeçalho 4550, a informação de assinatura 4570 e o conteúdo criptografado 4580 a partir da unidade de aquisição 4601.

Quando recebendo estes conjuntos de informações, a unidade de aquisição de chave de conteúdo 4602 gera a chave de conteúdo "CK" por utilizar o bloco de chave recebido, o identificador de dispositivo "AID_p" e a chave de dispositivo "DK_p" armazenada pelo dispositivo de armazenamento de chave de dispositivo 1604. Um procedimento para gerar a chave de conteúdo "CK" é o mesmo que o conduzido pela unidade de aquisição de chave de conteúdo 1602 constituindo o dispositivo de execução 1600 da primeira modalidade e portanto, a descrição é omitida.

A seguir, a unidade de aquisição de chave de conteúdo 4602 emite a chave de conteúdo gerada "CK" e a informação de posição de conteúdo recebida 4530, a informação de cabeçalho 4550, a informação de assinatura 4570 e o conteúdo criptografado 4580 para a unidade de verificação de informação de assinatura 4606.

4.4.3 Unidade de Verificação de Informação de Assinatura 4606

A unidade de verificação de informação de assinatura 4606 recebe a chave de conteúdo "CK", a informação de posição de conteúdo 4530, a informação de cabeçalho 4550, a informação de assinatura 4570 e o conteúdo criptografado 4580 a partir da unidade de aquisição de chave de conteúdo 4602.

Quando recebendo estes conjuntos de informações, a unidade de verificação de informação de assinatura 4606 executa a verificação da informação de assinatura 4570 no procedimento seguinte.

Primeiro, a unidade de verificação de informação de assinatura 4606 extrai valores hash parcial a partir de pedaços individuais de informa-

ção hash parcial constituindo a informação de cabeçalho recebida e calcula um valor hash combinado de verificação de assinatura por designar um resultado combinado formado pela combinação dos valores hash parciais "HA1", "HA2", "HA3", ..., e "HAc" para a função hash.

A seguir, a unidade de verificação de informação de assinatura 4606 lê uma chave de verificação 1613 a partir da unidade de armazenamento de chave de verificação 1612 e gera a informação de verificação de assinatura por aplicar o algorítmo de verificação de assinatura V junto ao valor hash combinado de verificação de assinatura calculado. Então, a unidade de verificação de informação de assinatura 4606 compara a informação de verificação de assinatura gerada com a informação de assinatura recebida. Quando estes dois não concordam, a unidade de verificação de informação de assinatura 4606 julga que a verificação da informação de assinatura 4570 é malsucedida e aborda o processamento subseqüente no dispositivo de execução 4600.

Quando estes dois concordam, a unidade de verificação de informação de assinatura 4606 julga que a verificação da informação de assinatura 4570 é bem sucedida e emite a chave de conteúdo recebida "CK", a informação de posição de conteúdo 4530, a informação de cabeçalho 4550 e o conteúdo criptografado 4580 para a unidade de seleção 4611.

4.4.4 Unidade de Seleção 4611

A unidade de seleção 4611 recebe a chave de conteúdo "CK", a informação de posição de conteúdo 4530, a informação de cabeçalho 4550 e o conteúdo criptografado 4580 a partir da unidade de verificação de informação de assinatura 4606.

Quando recebendo estes conjuntos de informações, a unidade de seleção 4611 gera a informação de posição selecionada a partir da informação de posição de conteúdo recebida 4530 em um procedimento descrito a seguir. A Figura 47 apresenta um esboço geral de um procedimento de geração da informação de posição selecionada executado pela unidade de seleção 4611 e uma estrutura da informação de posição selecionada gerada neste ponto. O dito a seguir descreve o procedimento de geração da

informação de posição selecionada com o auxílio da Figura 47.

A unidade de seleção 4611 seleciona k pedaços dentro dos c pedaços de informação de detecção de conteúdo 4531, 4532, 4533, ..., e 4536 constituindo a informação de posição de conteúdo recebida 4530 com o uso de números aleatórios. O método de seleção não está limitado a este e qualquer método é aplicável contanto que seja difícil para uma terceira parte prognosticar quais pedaços são selecionados.

A Figura 47 apresenta um caso no qual k pedaços incluindo pedaços de informação de detecção de conteúdo 4531, 4533 e 4536 foram selecionados.

A seguir, a unidade de seleção 4611 gera informação de posição selecionada 4620 composta dos k pedaços selecionados de informação de detecção de conteúdo 4531, 4533, ..., e 4536.

A seguir, a unidade de seleção 4611 gera a informação de cabeçalho de seleção no procedimento seguinte baseada na informação de cabeçalho recebida 4550. A Figura 48 apresenta um esboço geral de um procedimento para gerar a informação de cabeçalho de seleção e uma estrutura da informação de cabeçalho de seleção. O dito a seguir fornece uma descrição do procedimento de geração da informação de cabeçalho de seleção com o auxílio da Figura 48.

Primeiro, a unidade de seleção 4611 extrai um identificador de informação de identificação a partir de cada um dos pedaços de informação de detecção de conteúdo 4531, 4532, ..., e 4536 constituindo a informação de posição selecionada gerada 4620 e adicionalmente extrai pedaços de informação hash parcial 4551, 4553, ..., e 4556 incluindo os mesmos identificadores de informação de identificação que os identificadores de informação de identificação extraídos "ADID1", "ADID3", ..., e "ADIDc".

A seguir, a unidade de seleção 4611 gera a informação de cabeçalho de seleção 4630 composta dos pedaços extraídos de informação hash parcial 4551, 4553, ..., e 4556.

A seguir, a unidade de seleção 4611 emite a informação de posição selecionada gerada 4620 e a informação de cabeçalho de seleção

4630 e a chave de conteúdo recebida "CK" e o conteúdo criptografado 4580 para a unidade de decriptografia de conteúdo parcial 4616.

4.4.5 Unidade de Decriptografia de Conteúdo Parcial 4616

A unidade de decriptografia de conteúdo parcial 4616 recebe a informação de posição selecionada 4620, a informação de cabeçalho de seleção 4630, a chave de conteúdo "CK" e o conteúdo criptografado 4580 a partir da unidade de seleção 4611.

Quando recebendo estes conjuntos de informações, a unidade de decriptografia de conteúdo parcial 4616 gera o conteúdo de verificação em um procedimento explicado a seguir. A Figura 49 apresenta um esboço geral de um procedimento para gerar conteúdo de verificação e uma estrutura do conteúdo de verificação 4650 gerado neste ponto. O procedimento para gerar o conteúdo de verificação é descrito abaixo com o auxílio da Figura 49.

Primeiro, a unidade de decriptografia de conteúdo parcial 4616 extrai o pedaço de informação de identificação "AD1" a partir da informação de detecção de conteúdo 4531 constituindo a informação de posição selecionada recebida 4620 e adicionalmente extrai o pedaço de conteúdo parcial criptografado "ECNT1" a partir do conteúdo criptografado recebido 4580 baseada no pedaço extraído de informação de identificação "AD1".

A unidade de decriptografia de conteúdo parcial 4616 gera o pedaço de conteúdo parcial "CNT1" pela aplicação do algorítmo de decriptografia D1 junto ao pedaço de conteúdo parcial extraído "ECNT1". Subseqüentemente, a unidade de decriptografia de conteúdo parcial 4616 gera um pedaço de informação de conteúdo parcial de verificação 4651 composto do identificador de informação de identificação "ADID1" incluído no pedaço de informação de detecção de conteúdo 4531 e do pedaço gerado de conteúdo parcial "CNT1".

A unidade de decriptografia de conteúdo parcial 4616 repete o processamento do mesmo tipo para os pedaços restantes de informação de detecção de conteúdo 4532, ..., e 4536 para gerar pedaços de informação de conteúdo parcial de verificação 4652, ..., e 4656. A seguir, a unidade de

decriptografia de conteúdo parcial 4616 gera o conteúdo de verificação 4650 composto dos k pedaços gerados de informação de conteúdo parcial de verificação.

Quando tendo gerado o conteúdo de verificação 4650, a unidade de decriptografia de conteúdo parcial 4616 emite o conteúdo de verificação gerado 4650 e a informação de cabeçalho de seleção recebida 4630, a chave de conteúdo "CK" e o conteúdo criptografado 4580 para a unidade de verificação de informação de cabeçalho 4617.

4.4.6 Unidade de Verificação de Informação de Cabeçalho 4617

A unidade de verificação de informação de cabeçalho 4617 recebe o conteúdo de verificação 4650, a informação de cabeçalho de seleção 4630, a chave de conteúdo "CK" e o conteúdo criptografado 4580 a partir da unidade de decriptografia de conteúdo parcial 4616.

Quando recebendo estes conjuntos de informação, a unidade de verificação de informação de cabeçalho 4617 gera um valor hash de verificação "H1" por designar um pedaço de conteúdo parcial "CNT1" 4624 incluído no primeiro pedaço de informação de conteúdo parcial de verificação 4651 constituindo o conteúdo de verificação recebido 4650 para a função hash.

A seguir, a unidade de verificação de informação de cabeçalho 4617 extrai um identificador de informação de identificação "ADID1" 4621 incluído no pedaço de informação de conteúdo parcial de verificação 4651. Então, a unidade de verificação de informação de cabeçalho 4617 detecta um pedaço de informação hash parcial 4551 incluindo o mesmo identificador de informação de identificação que o identificador de informação de identificação extraído "ADID1" 4621 a partir da informação de cabeçalho de seleção recebida 4630 e extrai um valor hash parcial "HA1" 4632 incluído na informação hash parcial detectada 4551. A seguir, a unidade de verificação de informação de cabeçalho 4617 compra o valor hash parcial extraído "HA1" 4632 com o valor hash de verificação calculado "H1".

A unidade de verificação de informação de cabeçalho 4617 repete o processamento do mesmo tipo para os pedaços restantes de infor-

mação de conteúdo parcial de verificação 4652, ..., e 4656 e executa a comparação de um valor hash parcial com um valor hash de verificação k vezes.

Quando mesmo uma vez nas k comparações um valor hash parcial e um valor hash de verificação não se conformam um com o outro, a unidade de verificação de informação de cabeçalho 4617 aborda o processamento subseqüente no dispositivo de execução 4600.

Quando todos os pares de um valor hash parcial e de um valor hash de verificação concordam nas k comparações, a unidade de verificação de informação de cabeçalho 4617 emite a chave de conteúdo recebida "CK" e o conteúdo criptografado 4580 para a unidade de execução 4618.

4.5 Comportamentos Operacionais

O dito a seguir descreve os comportamentos operacionais do dispositivo de distribuição 4100 e do dispositivo de execução 4600.

4.5.1 Comportamento Operacional do Dispositivo de Distribuição 4100

A Figura 50 é um fluxograma apresentando um comportamento operacional do dispositivo de distribuição 4100, enquanto a Figura 51 apresenta um fluxo de processamento de conteúdo no comportamento operacional do dispositivo de distribuição 4100.

O comportamento operacional do dispositivo de distribuição 4100 é descrito com o auxílio das Figuras 50 e 51.

A unidade de entrada 4101 adquire o conteúdo (Etapa S4012) e emite o conteúdo adquirido para a unidade de geração de chave de conteúdo 4102.

A unidade de geração de chave de conteúdo 4102 recebe o conteúdo, gera uma chave de conteúdo com o uso de um número aleatório (Etapa S4013) e emite a chave de conteúdo gerada e o conteúdo recebido para a unidade de geração de bloco de chave 4103.

Quando recebendo a chave de conteúdo e o conteúdo, a unidade de geração de bloco de chave 4103 gera um bloco de chave e emite o bloco de chave gerado e a chave de conteúdo recebida e o conteúdo para a unidade de geração de conteúdo parcial 4105 (Etapa S4014).

A unidade de geração de conteúdo parcial 4105 recebe o bloco de chave, a chave de conteúdo, o conteúdo a partir da unidade de geração de bloco de chave 4103. A seguir, a unidade de geração de conteúdo parcial 4105 divide o conteúdo recebido 4119, como apresentado na Figura 51, para gerar c pedaços de conteúdo parcial (Etapa S4016) e coloca os c pedaços gerados de conteúdo parcial juntos para formar o conteúdo dividido 4120. A seguir, a unidade de geração de conteúdo parcial 4105 gera pedaços de informação de identificação respectivamente correspondendo aos c pedaços gerados de conteúdo parcial (Etapa S4018) e emite o conteúdo dividido gerado 4120 e os c pedaços de informação de identificação e o bloco de chave recebido, a chave de conteúdo e o conteúdo para a unidade de geração de informação de cabeçalho 4107.

A unidade de geração de informação de cabeçalho 4107 recebe o conteúdo dividido, c pedaços de informação de identificação, o bloco de chave e a chave de conteúdo a partir da unidade de geração de conteúdo parcial 4105, gera identificadores de informação de identificação respectivamente correspondendo aos pedaços recebidos de informação de identificação e adicionalmente gera a informação de posição de conteúdo 4140 incluindo os identificadores de informação de identificação gerados e os pedaços de informação de identificação. Adicionalmente, como apresentado na Figura 51, a unidade de geração de informação de cabeçalho 4107 calcula c pedaços de valores hash parciais por designar individualmente os c pedaços de conteúdo parcial constituindo o conteúdo dividido recebido 4120 para a função hash e gera a informação de cabeçalho 4160 incluindo os c pedaços calculados de valores hash parciais (Etapa S4019). A seguir, a unidade de geração de informação de cabeçalho 4107 emite a informação de posição de conteúdo gerada 4140 e a informação de cabeçalho 4160 e o bloco de chave recebido e a chave de conteúdo para a unidade de geração de informação de assinatura 4108.

A unidade de geração de informação de assinatura 4108 recebe a informação de posição de conteúdo 4140, a informação de cabeçalho 4160, o bloco de chave, e a chave de conteúdo a partir da unidade de gera-

ção de informação de cabeçalho 4107. Como apresentado na Figura 51, a unidade de geração de informação de assinatura 4108 extrai c pedaços de valores hash parciais incluídos na informação de cabeçalho recebida, combina os c pedaços extraídos de valores hash parciais e calcula um valor hash combinado por designar o resultado combinado para a função hash (Etapa S4021).

A seguir, a unidade de geração de informação de assinatura 4108 lê a chave de assinatura 1113 a partir da unidade de armazenamento de chave de assinatura 1112 (Etapa S4022). Como apresentado na Figura 51, a unidade de geração de informação de assinatura 4108 gera a informação de assinatura 4170 pela aplicação de um algorítmo de geração de assinatura junto ao valor hash combinado gerado com o uso da chave de assinatura lida 1113 (Etapa S4023).

A seguir, a unidade de geração de informação de assinatura 4108 emite a informação de assinatura gerada e a informação de posição de conteúdo recebida 4140, a informação de cabeçalho 4160, o conteúdo dividido 4120 e a chave de conteúdo para a unidade de processamento de criptografia 4109.

A unidade de processamento de criptografia 4109 recebe a informação de assinatura, a informação de posição de conteúdo 4140, a informação de cabeçalho 4160, o conteúdo dividido 4120 e a chave de conteúdo e gera conteúdo criptografado por criptografar pedaços individuais de conteúdo parcial constituindo o conteúdo dividido 4120 com o uso da chave de conteúdo recebida (Etapa S4024). A unidade de processamento de criptografia 4109 emite o conteúdo criptografado gerado e a informação de assinatura recebida, a informação de posição de conteúdo 4140, a informação de cabeçalho 4160 e o bloco de chave para a unidade de gravação 4114.

A unidade de gravação 4114 recebe o conteúdo criptografado, a informação de assinatura, a informação de posição de conteúdo 4140, a informação de cabeçalho 4160 e o bloco de chave e grava o bloco de chave recebido, a informação de posição de conteúdo 4140, a informação de cabeçalho 4160, a informação de assinatura, o conteúdo criptografado para o

DVD 4500 (Etapa S4026).

4.5.2 Comportamento Operacional do Dispositivo de Execução 4600

As FIGs 52 e 53 são fluxogramas apresentando um comportamento operacional do dispositivo de execução 4600. A Figura 54 esquematicamente apresenta informação distribuída pelos componentes individuais constituindo o dispositivo de execução 4600. Observe que os mesmos números de etapa de referência nas Figuras 52 até 54 indicam os mesmo processamento.

O dito a seguir explica o comportamento operacional do dispositivo de execução 4600 com o auxílio das Figuras 52 até 54.

Quando sendo carregado com o DVD 4500, a unidade de aquisição 4601 lê o bloco de chave 4510, a informação de posição de conteúdo 4530, a informação de cabeçalho 4550, a informação de assinatura 4570 e o conteúdo criptografado 4580 a partir do DVD 4500 (Etapa S4041) e emite estes conjuntos de informações lidos para a unidade de aquisição de chave de conteúdo 4602.

A unidade de aquisição de chave de conteúdo 4602 recebe o bloco de chave 4510, a informação de posição de conteúdo 4530, a informação de cabeçalho 4550, a informação de assinatura 4570 e o conteúdo criptografado 4580 e gera a chave de conteúdo por utilizar o bloco de chave recebido 4510, um identificador de dispositivo e uma chave de dispositivo armazenada pela unidade de armazenamento de chave de dispositivo 1604 (Etapa S4042). A seguir, a unidade de aquisição de chave de conteúdo 4602 emite a chave de conteúdo gerada e a informação de posição de conteúdo recebida 4530, a informação de cabeçalho 4550, a informação de assinatura 4570 e o conteúdo criptografado 4580 para a unidade de verificação de informação de assinatura 4606.

A unidade de verificação de informação de assinatura 4606 recebe a chave de conteúdo, a informação de posição de conteúdo 4530, a informação de cabeçalho 4550, a informação de assinatura 4570 e o conteúdo criptografado 4580, combina c pedaços de valores hash parciais incluídos na informação de cabeçalho recebida 4550 e gera um valor hash com-

binado de verificação de assinatura por designar o resultado combinado para a função hash (Etapa S4043). A seguir, a unidade de verificação de informação de assinatura 4606 lê a chave de verificação 1613 a partir da unidade de armazenamento de chave de verificação 1612 (Etapa S4044) e verifica a informação de assinatura recebida 4570 por utilizar a chave de verificação lida 1613 e o valor hash combinado de verificação de assinatura gerado (Etapa S4046).

Se a verificação da informação de assinatura 4570 for malsucedida (Etapa S4048: NÃO), a unidade de verificação de informação de assinatura 4606 aborda o processamento subseqüente no dispositivo de execução 4600.

Se a verificação da informação de assinatura 4570 for bem-sucedida (Etapa S4048: SIM), a unidade de verificação de informação de assinatura 4606 emite a chave de conteúdo recebida, a informação de posição de conteúdo 4530, a informação de cabeçalho 4550 e o conteúdo criptografado 4580 para a unidade de seleção 4611.

Quando recebendo a chave de conteúdo, a informação de posição de conteúdo 4530, a informação de cabeçalho 4550 e o conteúdo criptografado 4580, a unidade de seleção 4611 seleciona k pedaços dentro dos c pedaços de informação de detecção de conteúdo incluídos na informação de posição de conteúdo 4530 (Etapa S4049). A seguir, a unidade de seleção 4611 gera a informação de posição selecionada 4620 composta dos pedaços selecionados de informação de detecção de conteúdo (Etapa S4051). Então, a unidade de seleção 4611 seleciona k pedaços de informação hash parcial a partir da informação de cabeçalho recebida 4550 baseada nos identificadores de informação de identificação incluídos nos k pedaços de informação de detecção de conteúdo constituindo a informação de posição selecionada gerada 4620 (Etapa S4053) e gera a informação de cabeçalho de seleção 4630 composta dos k pedaços selecionados de informação hash parcial (Etapa S4056). A seguir, a unidade de seleção 4611 emite a informação de posição selecionada gerada 4620 e a informação de cabeçalho de seleção 4630, e a chave de conteúdo recebida e o conteúdo

criptografado 4580 para a unidade de decriptografia de conteúdo parcial 4616.

A unidade de decriptografia de conteúdo parcial 4616 recebe a informação de posição selecionada 4620, a informação de cabeçalho de seleção 4630, a chave de conteúdo e o conteúdo criptografado 4580 e extrai k pedaços de conteúdo parcial criptografado 4581, 4582, 4583, ..., e 4586 a partir do conteúdo criptografado 4580 baseada nos pedaços de informação de identificação incluídos na informação de posição selecionada recebida 4620 como apresentado na Figura 54 (Etapa S4057). A seguir, a unidade de decriptografia de conteúdo parcial 4616 gera pedaços de conteúdo parcial por decriptografar os k pedaços extraídos de conteúdo parcial criptografado 4581, 4582, 4583, ..., e 4586 (Etapa S4059). A seguir, a unidade de decriptografia de conteúdo parcial 4616 gera o conteúdo de verificação 4650 incluindo k pedaços de identificadores de informação de identificação incluídos na informação de posição selecionada recebida 4620 e os k pedaços gerados de conteúdo parcial (Etapa S4061). A unidade de decriptografia de conteúdo parcial 4616 emite o conteúdo de verificação gerado 4650 e a informação de cabeçalho de seleção recebida 4630, a chave de conteúdo e o conteúdo criptografado 4650 para a unidade de verificação de informação de cabeçalho 4617.

A unidade de verificação de informação de cabeçalho 4617 recebe o conteúdo de verificação 4650, a informação de cabeçalho de seleção 4530, a chave de conteúdo e o conteúdo criptografado 4580. Quando recebendo estes conjuntos de informações, a unidade de verificação de informação de cabeçalho 4617 gera k pedaços de valores hash de verificação por individualmente designar k pedaços de conteúdo parcial 4591, 4592, 4593, ..., e 4596 incluídos no conteúdo de verificação recebido 4650 para a função hash (etapa SA4062) e compara individualmente k pedaços de valores hash parciais incluídos na informação de cabeçalho recebida com os valores hash de verificação gerados correspondentes (Etapa S4064: SIM).

Na comparação de k pares, cada um dos quais é composto de um valor hash de verificação e de um valor hash parcial correspondente,

quando qualquer par não se conforma com outro (Etapa S4066: NÃO), a unidade de verificação de informação de cabeçalho 4617 aborta o processamento subseqüente no dispositivo de execução 4600.

Na comparação de k pares, quando todos os k pares apresentam concordância (Etapa S4066: SIM), a unidade de verificação de informação de cabeçalho 4617 emite a chave de conteúdo recebida e o conteúdo criptografado 4580 para a unidade de execução 2618.

A unidade de execução 2618 recebe a chave de conteúdo e o conteúdo criptografado 4580 a partir da unidade de verificação de informação de cabeçalho 4617, gera conteúdo composto de c pedaços de conteúdo parcial por decriptografar conteúdo parcial criptografado individual constituindo o conteúdo criptografado recebido 4580 com o uso da chave de conteúdo recebida (Etapa S4067), expande o conteúdo gerado (Etapa S4068) e tem o monitor executando o conteúdo expandido (etapa S4071).

4.6 Sumário e Efeitos Vantajosos

Como foi descrito, o sistema de detecção de conteúdo não autorizado da quarta modalidade é composto do dispositivo de distribuição 4100 e do dispositivo de execução 4600 e o dispositivo de distribuição 4100 gera c pedaços de conteúdo parcial por dividir o conteúdo e adicionalmente gera informação de cabeçalho e informação de verificação com o uso de todos os c pedaços gerados de conteúdo parcial.

O dispositivo de execução 4600 seleciona k pedaços dentre os c pedaços de conteúdo parcial criptografado constituindo o conteúdo criptografado e extrai k pedaços de valores hash parciais correspondendo ao k pedaços selecionados de conteúdo parcial dentre os c pedaços de valores hash parciais incluídos na informação de cabeçalho. O dispositivo de execução 4600 verifica somente os k pedaços selecionados de conteúdo parcial criptografado por utilizar os k pedaços extraídos de valores hash parciais. Somente quando a verificação é bem sucedida, o dispositivo de execução 4600 gera o conteúdo por decriptografar o conteúdo criptografado e executar o conteúdo decriptografado.

Assim, por limitar, a k pedaços, o número de pedaços de conte-

údo parcial criptografado utilizado par a verificação de se conteúdo não autorizado está incluído, é possível reduzir a carga de processamento envolvida na verificação.

Por selecionar um pedaço diferente de conteúdo parcial criptografado com o uso de um número aleatório cada vez quando o dispositivo de execução 4600 executa a verificação, é possível complementar a degradação da precisão para detectar conteúdo não autorizado devido à limitar a somente k pedaços, o número de pedaços de conteúdo parcial criptografado utilizado para a verificação.

Em adição, é difícil prognosticar quais pedaços de conteúdo parcial criptografado são para ser utilizados para a verificação e portanto, é possível impedir atos fraudulentos envolvendo substituir, dentre os pedaços de conteúdo parcial criptografado constituindo o conteúdo criptografado, especificamente somente pedaços de conteúdo parcial criptografado a não serem utilizados para a verificação com conteúdo não autorizado.

5. Quinta Modalidade

Um sistema de detecção de conteúdo não autorizado de acordo com uma quinta modalidade da presente invenção é descrito abaixo.

5.1. Sistema de Detecção de Conteúdo Não Autorizado

O sistema de detecção de conteúdo não autorizado da quinta modalidade é composto de um dispositivo de distribuição, de um dispositivo de execução e de um monitor, como na primeira modalidade.

O dispositivo de distribuição adquire conteúdo de acordo com operações de um operador e gera conteúdo criptografado por criptografar o conteúdo adquirido. Adicionalmente, o dispositivo de distribuição gera informação de seleção de unidade, informação de cabeçalho e informação de assinatura, utilizadas no dispositivo de execução para verificar a validade do conteúdo.

O dispositivo de distribuição adquire uma capacidade de armazenamento de uma área que pode ser gravada em um DVD e tamanhos de dados das várias informações geradas.

O dispositivo de distribuição calcula uma capacidade de enchi-

mento que é encontrada por se subtrair a soma dos tamanhos de dados adquiridos das várias informações a partir da capacidade de armazenamento adquirida, gera conteúdo de enchimento possuindo um tamanho de dado correspondendo à capacidade de enchimento calculada e grava o conteúdo de enchimento gerado junto ao DVD junto com as várias informações.

5.2 Dispositivo de Distribuição 5100

A Figura 55 apresenta uma estrutura de um dispositivo de distribuição de uma quinta modalidade. Como apresentado na Figura 55, um dispositivo de distribuição 5100 é composto de uma unidade de entrada 1101, de uma unidade de geração de chave de conteúdo 1102, de uma unidade de geração de bloco de chave 1103, de uma unidade de armazenamento de informação de dispositivo de execução 1104, de uma unidade de geração de unidade 5105, de uma unidade de processamento de criptografia 5106, de uma unidade de geração de informação de cabeçalho 5107, de uma unidade de geração de conteúdo de enchimento 5108, de uma unidade de geração de informação de assinatura 5111, de uma unidade de armazenamento de chave de assinatura 1112 e de uma unidade de gravação 5114.

Os componentes individuais constituindo o dispositivo de distribuição 5100 são descritos abaixo. Observe que, desde que a unidade de entrada 1101, a unidade de geração de chave de conteúdo 1102, a unidade de geração de bloco de chave 1103, a unidade de armazenamento de informação de dispositivo de execução 1104 e a unidade de armazenamento de chave de assinatura 1112 são os mesmos que no dispositivo de distribuição 1100 da primeira modalidade, as descrições destes componentes são omitidas.

5.2.1 Unidade de Geração de Unidade 5105

Como a unidade de geração de unidade 1105 descrita na primeira modalidade, a unidade de geração de unidade 5105 recebe o conteúdo, o qual é composto de c pedaços de arquivos "CNT1", "CNT2", "CNT3", ..., e assim por diante, a partir da unidade de entrada 1101 e gera informação de seleção de unidade e conteúdo dividido com o uso do conteúdo recebido. Os procedimentos para gerar a informação de seleção de unidade e

o conteúdo dividido são os mesmos que os conduzidos pela unidade de geração de unidade 1105 da primeira modalidade e as estruturas da informação de seleção de unidade e do conteúdo dividido aqui são como apresentadas nas Figuras 6 e 7, respectivamente e portanto as descrições são omitidas.

A seguir, a unidade de geração de unidade 5105 emite o conteúdo dividido gerado para a unidade de processamento de criptografia 5106, enquanto emitindo a informação de seleção de unidade gerada para a unidade de geração de conteúdo de enchimento 5108.

5.2.2 Unidade de Processamento de Criptografia 5106

A unidade de processamento de criptografia 5106 recebe o conteúdo dividido a partir da unidade de geração de unidade 5105 e gera conteúdo dividido criptografado e conteúdo criptografado baseada no conteúdo dividido recebido. Os procedimentos para gerar este conteúdo dividido criptografado são os mesmos que os executados pela unidade de processamento de criptografia 1106 da primeira modalidade e as estruturas do conteúdo criptografado gerado e do conteúdo dividido criptografado aqui são como apresentadas nas Figuras 9 e 10, respectivamente, e portanto, as descrições são omitidas.

A seguir, a unidade de processamento de criptografia 5106 emite o conteúdo dividido criptografado gerado para a unidade de geração de informação de cabeçalho 5107, enquanto emitindo o conteúdo criptografado gerado para a unidade de gravação 5114 e para a unidade de geração de conteúdo de enchimento 5108.

5.2.3 Unidade de Geração de Conteúdo de Enchimento 5108

A unidade de geração de conteúdo de enchimento 5108 pré-armazena um tamanho de bloco de chave "KBSIZE", um tamanho de informação de arquivo "FISIZE", um tamanho hash de unidade "USIZE", um tamanho hash de arquivo "FSIZE", uma proporção "RT" e um número de divisão "j".

O tamanho hash de unidade "USIZE" apresenta um tamanho de dado de pedaços de informação hash de unidade constituindo uma primeira

tabela hash gerada pela unidade de geração de informação de cabeçalho 5107. Especificamente falando, a informação hash de unidade aqui é a mesma que a informação hash de unidade gerada pela unidade de geração de informação de cabeçalho 1107 da primeira modalidade.

O tamanho hash de arquivo "FSIZE" apresenta um comprimento em bits de pedaços da informação hash de arquivo constituindo uma segunda tabela hash gerada pela unidade de geração de informação de cabeçalho 5107. Especificamente falando, a informação hash de arquivo aqui é a mesma que a informação hash de arquivo gerada pela unidade de geração de informação de cabeçalho 1107 da primeira modalidade.

A proporção "RT" apresenta uma proporção de comprimento em bits entre a informação A e uma assinatura SignA no caso onde a unidade de geração de informação de assinatura 5111 gera a assinatura SignA pela aplicação do algorítmo de geração de assinatura S junto à informação A.

O número de divisão "j" é o número de unidades geradas pela unidade de geração de conteúdo de enchimento 5108 dividindo o conteúdo de enchimento (como será descrito em detalhes adiante).

Em adição, a unidade de geração de conteúdo de enchimento 5108 pré-armazena informação de impraticabilidade de reprodução com comprimento de 56 bits "DAMY" indicando que o conteúdo de enchimento não está apto a ser executado.

A unidade de geração de conteúdo de enchimento 5108 recebe a informação de seleção de unidade a partir da unidade de geração de unidade 5105, enquanto recebendo o conteúdo criptografado a partir da unidade de processamento de criptografia 5106.

Quando recebendo a informação de seleção de unidade e o conteúdo criptografado, a unidade de geração de conteúdo de enchimento 5108 calcula uma capacidade de enchimento com o uso da informação de seleção de unidade recebida e do conteúdo criptografado no procedimento seguinte, gera conteúdo de enchimento baseado na capacidade de enchimento calculada e atualiza a informação de seleção de unidade.

O dito a seguir proporciona descrições detalhadas sobre o cál-

culo da capacidade de enchimento (a), sobre a geração para o conteúdo de enchimento (b) e sobre a atualização da informação de seleção de unidade (c) mencionada acima.

(a) Cálculo da Capacidade de Enchimento

A capacidade de enchimento indica o espaço livre em um DVD após um bloco de chave, a informação de seleção de unidade, a informação de cabeçalho, a informação de assinatura e o conteúdo criptografado terem sido gravados junto ao mesmo. O dito a seguir descreve um procedimento para gerar a capacidade de enchimento.

Primeiro, a unidade de geração de conteúdo de enchimento 5108 mede, via a unidade de gravação 5114, uma capacidade de armazenamento de uma área que pode ser gravada no DVD carregado na unidade de gravação 5114, e gera uma capacidade máxima de armazenamento "MSIZE" indicando uma capacidade disponível para gravar informação na mesma. Aqui, ao invés de medir a capacidade de armazenamento de uma área que pode ser gravada via a unidade de gravação 5114, a capacidade máxima de armazenamento "MSIZE" pode ser adquirida por uma entrada a partir do operador.

A seguir, a unidade de geração de conteúdo de enchimento 5108 mede (?) um tamanho de dado do conteúdo criptografado recebido e gera um tamanho de conteúdo "CNTSIZE".

A seguir, a unidade de geração de conteúdo de enchimento 5108 conta pedaços "c" da informação de arquivo incluída na informação de seleção de conteúdo recebida e calcula um tamanho de dado "UCSIZE" de informação de seleção de unidade após a atualização (os detalhes serão descritos na descrição seguinte em relação à atualização da informação de seleção de unidade em (c)) por utilizar a equação seguinte:

$$UCSIZE = FISIZE \times (c + 1)$$

A seguir, a unidade de geração de conteúdo de enchimento 5108 extrai c pedaços de números de unidade "N1", "N2", ..., "Nc" incluídos na informação de seleção de unidade recebida e calcula a soma "HA1SIZE" de tamanhos de dados de (c + 1) pedaços das primeiras tabelas hash (como

será descrito em detalhes adiante) gerados pela unidade de geração de informação de cabeçalho 5107 com o uso dos números de unidade extraídos "N1", "N2", "N3", ..., e "Nc" e do número de divisão armazenado "j" por utilizar a seguinte equação:

$$HA1SIZE = [N1 + N2 + N3 + ... + Nc + j] \times USIZE$$

Subseqüentemente, a unidade de geração de conteúdo de enchimento 5108 gera um tamanho de dado "HA2SIZE" de uma segunda tabela hash (como será descrito em detalhes adiante) gerada pela unidade de informação de cabeçalho 5107 por utilizar a seguinte equação:

$$HA2SIZE = FSIZE \times (c + 1),$$

e calcula um tamanho de dado "HEADSIZE" da informação de cabeçalho gerada pela unidade de geração de informação de cabeçalho 5107 a partir da soma gerada de tamanhos de dados das primeiras tabelas hash "HA1SIZE" e o tamanho de dado da segunda tabela hash "HA2SIZE" por utilizar a seguinte equação:

$$HEADSIZE = HA1SIZE + HA2SIZE.$$

A seguir, a unidade de geração de conteúdo de enchimento 5108 calcula "SigSIZE" indicando um tamanho de dado da informação de assinatura gerada pela unidade de geração de informação de assinatura 5111 com o uso da proporção "RT" por utilizar a seguinte equação:

$$SigSIZE = (UCSIZE + HA2SIZE) \times RT.$$

A seguir, a unidade de geração de conteúdo de enchimento 5108 calcula a capacidade de enchimento "FilSIZE" por utilizar a seguinte equação:

$$FilSIZE = MSIZE - [KBSIZE + UCSIZE + HEADSIZE + SigSIZE].$$

(b) Geração do Conteúdo de Enchimento

Quando tendo calculado a capacidade de enchimento "FilSIZE", a unidade de geração de conteúdo de enchimento 5108 gera um número aleatório e combina o número aleatório gerado com a informação de impraticabilidade de reprodução "DAMY" para gerar o conteúdo de enchimento cujo tamanho de dados é "FilSIZE".

A seguir, a unidade de geração de conteúdo de enchimento

5108 gera um identificador de arquivo "FIDf" para especificamente indicar o conteúdo de enchimento gerado e a informação de identificação de arquivo "ADf" para identificar o conteúdo de enchimento gerado. A seguir, a unidade de geração de conteúdo de enchimento 5108 divide o conteúdo dividido gerado, baseada no número de divisão armazenado "j", em j pedaços de unidades "Uf_1", "Uf_2", "Uf_3", ..., e "Uf_j", e gera identificadores de unidade "UIDf_1", "UIDf_2", "UIDf_3", ..., e "UIDf_j", cada um dos quais corresponde a uma das unidades. Aqui, um par de uma unidade e de um identificador de unidade correspondente é referido daqui por diante como (um pedaço de) informação de unidade. Em adição, a unidade de geração de conteúdo de enchimento 5108 gera o conteúdo de enchimento dividido composto de j pedaços de informação de unidade. A Figura 56 apresenta uma estrutura do conteúdo de enchimento dividido gerado neste ponto. Como apresentado na Figura 56, o conteúdo de enchimento dividido 5120 é composto de vários pedaços de informação de unidade 5121, 5122, 5123, ..., e 5126, e cada pedaço de informação de unidade inclui um identificador de unidade e uma unidade. Por exemplo, o pedaço de informação de unidade 5121 inclui o identificador de unidade "UIDf_1" 5131 e uma unidade "Uf_1" 5132. Um procedimento para gerar o conteúdo de enchimento dividido a partir do conteúdo de enchimento é o mesmo que um procedimento para gerar arquivos divididos a partir de um arquivo e portanto, somente uma breve descrição é proporcionada aqui.

Aqui, um par gerado de identificador de arquivo "FIDf" e de conteúdo de enchimento dividido 5120 é referido como "informação enchimento de arquivo".

(c) Atualização da Informação de Seleção de Unidade

Quando tendo gerado o conteúdo de enchimento e o conteúdo de enchimento dividido 5120, a unidade de geração de conteúdo de enchimento 5108 gera um pedaço de informação de arquivo composto do identificador de arquivo gerado "FIDf", do pedaço gerado de informação de identificação de arquivo "ADf" e de um número de unidades "Nf" indicando o número de unidades geradas e adiciona o pedaço gerado de informação de ar-

quivo para a informação de seleção de unidade recebida. A Figura 57 apresenta a informação de seleção de unidade 5140 após o pedaço gerado de informação de arquivo ter sido adicionado para a mesma. A informação de seleção de unidade 5140 é composta de (c + 1) pedaços de informação de arquivo 5141, 5142, 5143, ..., 5146 e 5147 e cada pedaço de informação de arquivo inclui um identificador de arquivo, um pedaço de informação de identificação de arquivo e um número de unidades. Os pedaços de informação de arquivo 5141, 5142, 5143, ..., e 5146 são gerados pela unidade de geração de unidade 5105 baseada no conteúdo e são os mesmos que os pedaços da informação de arquivo 1201, 1202, 1203, ..., e 1204 constituindo a informação de seleção de unidade 1200 apresentados na Figura 7. O pedaço de informação de arquivo 5147 é gerado pela unidade de geração de conteúdo de enchimento 5108 baseada no conteúdo de enchimento e inclui um identificador de arquivo "FIDf" 5151 correspondendo ao conteúdo de enchimento, um pedaço de informação de identificação de arquivo "AD1" 5152 e um número de unidades "Nf" 5153.

A seguir, a unidade de geração de conteúdo de enchimento 5108 emite: o conteúdo de enchimento gerado e a informação de seleção de unidade 5140 para a unidade de gravação 5114; a informação de enchimento de arquivo gerada para a unidade de geração de informação de cabeçalho 5107; e a informação de seleção de unidade 5140 para a unidade de geração de informação de assinatura 5111.

5.2.4 Unidade de Geração de Informação de Cabeçalho 5107

A unidade de geração de informação de cabeçalho 5107 recebe o conteúdo dividido criptografado a partir da unidade de processamento de criptografia 5106, enquanto recebendo a informação de enchimento de arquivo 5156 incluindo o identificador de arquivo "FIDf" e o pedaço de conteúdo de enchimento dividido 5120 a partir da unidade de geração de conteúdo de enchimento 5108.

Quando recebendo a informação de enchimento de arquivo 5156 e o conteúdo dividido criptografado 5160, a unidade de geração de informação de cabeçalho 5107 gera a informação de cabeçalho 5190 a par-

tir dos conjuntos de informações recebidos como apresentado na Figura 58. A Figura 58 apresenta um esboço geral de um procedimento de geração da informação de cabeçalho 5190 executado pela unidade de geração de informação de cabeçalho 5107. O dito a seguir descreve o procedimento de geração da informação de cabeçalho 5190 com o auxílio da Figura 58.

A unidade de geração de informação de cabeçalho 5107 gera as primeiras tabelas hash "HA1TBL1", 5171, "HA1TBL2" 5172, "HA1TBL3" 5173, ..., e "HA1TBLc" 5176 a partir do conteúdo dividido criptografado recebido 5160. As primeiras tabelas hash "HA1TBL1", 5171, "HA1TBL2" 5172, "HA1TBL3" 5173, ..., e "HA1TBLc" 5176 geradas aqui são as mesmas que as primeiras tabelas hash "HA1TBL1", 1261, "HA1TBL2" 1262, "HA1TBL3" 1263, ..., e "HA1TBLc" 1264 e os procedimentos de geração também são os mesmos. Portanto, as descrições destas primeiras tabelas hash são omitidas.

A seguir, a unidade de geração de informação de cabeçalho 5107 gera uma primeira tabela hash "HA1TBLf" 5177 baseada no conteúdo de enchimento incluído na informação de enchimento de arquivo recebida 5156. O procedimento de geração é o mesmo que o procedimento para gerar uma primeira tabela hash a partir do arquivo dividido criptografado e portanto, a descrição é omitida.

A seguir, a unidade de geração de informação de cabeçalho 5107 calcula valores hash de arquivo baseada respectivamente nos (c + 1) pedaços de primeiras tabelas hash, gera pedaços de informação hash de arquivo, cada um dos quais inclui um dos (c + 1) pedaços calculados de valores hash de arquivo e um identificador de arquivo correspondendo ao valor hash de arquivo e adicionalmente gera uma segunda tabela hash "HA2TBL" 5180 composta dos (c + 1) pedaços gerados de informação de arquivo. Um procedimento específico para gerar a segunda tabela hash é o mesmo que o procedimento de geração para a segunda tabela hash 1269 na primeira modalidade, exceto por utilizar o identificador de arquivo "FIDf" 5157 e o conteúdo de enchimento dividido 5120 recebido a partir da unidade de geração de conteúdo de enchimento 5108 e portanto, a explicação detalhada é

omitida.

A Figura 59 apresenta uma estrutura da segunda tabela hash "HA2TBL" 5180 gerada neste ponto. A segunda tabela hash "HA2TBL" 5180 é composta de (c + 1) pedaços de informação hash de arquivo 5181, 5182, 5183, ..., 5186 e 5187. Cada pedaço de informação hash de arquivo inclui um identificador de arquivo e um valor hash de arquivo. Os pedaços de informação hash de arquivo 5181 até 5186 são gerados a partir do conteúdo dividido criptografado 5160 e são os mesmos que os pedaços da informação hash de arquivo 1301 até 1304 constituindo a segunda tabela hash "HA2TBL" 1269 descrita na primeira modalidade. O pedaço de informação hash de arquivo 5187 é gerado baseado na informação de enchimento de arquivo 5156.

A unidade de geração de informação de arquivo 5107 emite a segunda tabela hash gerada 5180 para a unidade de geração de informação de assinatura 5111, enquanto emitindo a informação de cabeçalho 5190 incluindo os (c + 1) pedaços gerados das primeiras tabelas hash e a segunda tabela hash "HA2TBL" 5180 para a unidade de gravação 5114.

5.2.5 Unidade de Geração de Informação de Assinatura 5111

A unidade de geração de informação de assinatura 5111 recebe a informação de seleção de unidade 5140 a partir da unidade de geração de conteúdo de enchimento 5108, enquanto recebendo a segunda tabela hash "HA2TBL" 5180 a partir da unidade de geração de informação de cabeçalho 5107.

Quando recebendo a informação de seleção de unidade 5140 e a segunda tabela hash "HA2TBL" 5180, a unidade de geração de informação de assinatura 5111 lê a chave de assinatura 1113 gravada pela unidade de armazenamento de chave de assinatura 1112.

A seguir, a unidade de geração de informação de assinatura 5111 gera informação de assinatura por aplicar o algorítmo de geração de assinatura S junto a um resultado combinado formado por se combinar os (c + 1) pedaços de valores hash de arquivo constituindo a segunda tabela hash recebida "HA2TBL" 5180 com os (c + 1) pedaços de informação de arqui-

vo constituindo a informação de seleção de unidade recebida 5140 por utilizar a chave de assinatura lida 1113.

A seguir, a unidade de geração de informação de assinatura 5111 emite a informação de assinatura gerada para a unidade de gravação 5114.

5.2.6 Unidade de Gravação 5114

A unidade de gravação 5114 é carregada com um DVD.

A unidade de gravação 5114 mede uma capacidade de armazenamento de uma área que pode ser gravada no DVD carregado em resposta a uma instrução da unidade de geração de conteúdo de enchimento 5108.

A unidade de gravação 5114 recebe: o bloco de chave a partir da unidade de geração de bloco de chave 1103; o conteúdo criptografado a partir da unidade de processamento de criptografia 5106; e o conteúdo de enchimento e a informação de seleção de unidade 5140 a partir da unidade de geração de conteúdo de enchimento 5108. Em adição, a unidade de gravação 5114 recebe a informação de cabeçalho 5190 a partir da unidade de geração de informação de cabeçalho 5107, enquanto recebendo a informação de assinatura a partir da unidade de geração de informação de assinatura 5111.

Quando recebendo estes conjuntos de informação, a unidade de gravação 5114 grava o bloco de chave recebido, o conteúdo criptografado, o conteúdo de enchimento, a informação de seleção de unidade 5140, a informação de cabeçalho 5190 e a informação de assinatura junto ao DVD.

5.3 DVD 5500

A Figura 60 apresenta a informação armazenada em um DVD da quinta modalidade. Como apresentado na Figura 60, um DVD 5500 armazena um bloco de chave 5510, a informação de seleção de unidade 5530, a informação de cabeçalho 5550, o conteúdo criptografado 5580 e o conteúdo de enchimento 5590.

Estes conjuntos de informações foram gravados pelo dispositivo de distribuição 5100. As estruturas dos conjuntos de informações individuais

são como declaradas acima e portanto, as descrições são omitidas aqui.

5.4 Dispositivo de Execução 5600

Como apresentado na Figura 61, um dispositivo de execução 5600 é composto de uma unidade de aquisição 1601, de uma unidade de aquisição de chave de conteúdo 1602, de uma unidade de armazenamento de chave de dispositivo 1604, de uma unidade de execução 5606, de uma unidade de verificação de informação de assinatura 5611 e de uma unidade de armazenamento de chave de verificação 1612.

O dito a seguir descreve os componentes individuais constituindo o dispositivo de execução 5600. Observe que, desde que a unidade de aquisição 1601, a unidade de aquisição de chave de conteúdo 1602 e a unidade de armazenamento de chave de verificação 1612 são as mesmas que na primeira modalidade, as descrições para estes componentes são omitidas.

5.4.1 Unidade de Verificação de Informação de Assinatura 5611

A unidade de verificação de informação de assinatura 5611 recebe a informação de seleção de unidade 5530 e a informação de assinatura 5570 a partir da unidade de aquisição 1601.

Quando recebendo estes conjuntos de informações, a unidade de verificação de informação de assinatura 5611 verifica a informação de assinatura recebida 5570 com o uso da informação de seleção de unidade recebida 5530 bem como com a informação de cabeçalho 5550, com o conteúdo criptografado 5580 e com o conteúdo de enchimento 5590 armazenados no DVD 5500. Um procedimento específico para verificação é omitido desde que ele é o mesmo que a verificação da informação de assinatura executado pela unidade de verificação de informação de assinatura 1611 constituindo o dispositivo de execução 1600 da primeira modalidade, exceto por utilizar o conteúdo de enchimento 5590 em adição ao conteúdo criptografado 5580.

5.4.2 Unidade de Execução 5606

A unidade de execução 5606 pré-armazena a informação de impraticabilidade de reprodução com comprimento de 56 bits "DAMY".

A unidade de execução 5606 recebe a chave de conteúdo "CK" a partir da unidade de aquisição de chave de conteúdo 1602. Em adição, a unidade de execução 5606 pode receber a informação de proibição de reprodução a partir da unidade de verificação de informação de assinatura 5611.

Quando recebendo a chave de conteúdo "CK", a unidade de execução 5606 lê, um por um, os arquivos criptografados "ECNT1", "ECNT2", "ECNT3", ..., e "ECNTc" constituindo o conteúdo criptografado 5580 ou o conteúdo de enchimento 5590 via a unidade de aquisição 1601.

A unidade de execução 5606 compara os primeiros 56 bits do arquivo criptografado lido ou os primeiros 56 bits do conteúdo de enchimento lido com a informação de impraticabilidade de reprodução armazenada "DAMY". Quando estes dois não se conformam, a informação lida é um arquivo criptografado e executável e portanto, a unidade de execução 5606 gera um arquivo por decriptografar o arquivo criptografado lido com respeito a cada unidade por utilizar a chave de conteúdo recebida "CK". A seguir, a unidade de execução 5606 expande o arquivo gerado para gerar dados de vídeo e áudio, gera sinais de vídeo e áudio a partir dos dados de vídeo e áudio gerados e executa o conteúdo por emitir os sinais de vídeo e de áudio gerados para um monitor.

Quando os primeiros 56 bytes e a informação de impraticabilidade de reprodução "DAMY" se conformam, a informação lida é o conteúdo de enchimento e não está apta a ser executada e portanto, a unidade de execução 5606 aborta a decriptografia acima, a expansão e a reprodução e se move para o processamento do próximo arquivo criptografado.

Até ter completado a leitura de todos os arquivos criptografados e conteúdo de enchimento, a unidade de execução 5606 repete a leitura, comparação com a informação de reprodução impraticável "DAMY", decriptografia, expansão e reprodução em um procedimento similar.

Se recebendo informação de proibição de execução a partir da unidade de verificação de informação de assinatura 5611 durante a repetição acima, a unidade de execução 5606 aborta a repetição.

5.5 Comportamentos Operacionais

O dito a seguir descreve os comportamentos operacionais do dispositivo de distribuição 5100 e do dispositivo de execução 5600 da quinta modalidade.

5.5.1 Comportamento Operacional do Dispositivo de Distribuição 5100

O comportamento operacional do dispositivo de distribuição 5100 é descrito com o auxílio de fluxogramas apresentados nas Figuras 62 e 63.

A unidade de entrada 5101 do dispositivo de distribuição 5100 aceita uma entrada de conteúdo (Etapa S5011), emite o conteúdo aceito para a unidade de geração de unidade 5105 e instrui a unidade de geração de chave de conteúdo 1102 para gerar uma chave de conteúdo.

A unidade de geração de chave de conteúdo 1102 gera a chave de conteúdo de acordo com a instrução da unidade de entrada 1101 (Etapa S5012) e emite a chave de conteúdo gerada para a unidade de geração de bloco de chave 1103 e para a unidade de processamento de criptografia 5106.

A unidade de geração de bloco de chave 1103 recebe a chave de conteúdo. Quando recebendo a chave de conteúdo, a unidade de geração de bloco de chave 1103 lê uma tabela de identificação de dispositivo a partir da unidade de armazenamento de informação de dispositivo de execução 1104 (Etapa S5013) e gera um bloco de chave baseada na chave de conteúdo recebida e na tabela de identificação de dispositivo lida (Etapa S5016). A seguir, a unidade de geração de bloco de chave 1103 emite o bloco de chave gerado para a unidade de gravação 5114.

Quando recebendo o conteúdo, a unidade de geração de unidade 5105 divide cada arquivo constituindo o conteúdo recebido em unidades para gerar conteúdo dividido (Etapa S5017). Quando tendo gerado o conteúdo dividido, a unidade de geração de unidade 5105 gera a informação de seleção de unidade composta de pedaços de informação de arquivo que respectivamente correspondem aos arquivos divididos (Etapa S5018), e emite a informação de seleção de unidade gerada para a unidade de gera-

ção de conteúdo de enchimento 5108 enquanto emitindo o conteúdo dividido para a unidade de processamento de criptografia 5106.

Quando recebendo a chave de conteúdo e o conteúdo dividido, a unidade de processamento de criptografia 5106 gera o conteúdo dividido criptografado por criptografar cada unidade de conteúdo incluída no conteúdo dividido recebido com o uso da chave de conteúdo (Etapa S5019). A unidade de processamento de criptografia 5106 extrai as unidades criptografadas incluídas no conteúdo dividido criptografado gerado, gera conteúdo criptografado (Etapa S5021) e emite o conteúdo criptografado gerado para a unidade de gravação 5114 e para a unidade de geração de conteúdo de enchimento 5108 enquanto emitindo o conteúdo dividido criptografado gerado para a unidade de geração de informação de cabeçalho 5107.

Quando recebendo a informação de seleção de unidade e o conteúdo criptografado, a unidade de geração de conteúdo de enchimento 5108 adquire uma capacidade máxima de armazenamento do DVD 5500 via a unidade de gravação 5114 (Etapa S5022) e mede um tamanho de dado do conteúdo criptografado recebido (Etapa S5023).

A seguir, a unidade de geração de conteúdo de enchimento 5108 calcula um tamanho de dado da informação de cabeçalho e um tamanho de dado da informação de assinatura, baseada na informação de seleção de unidade recebida (Etapa S5026) e adicionalmente calcula uma capacidade de enchimento baseada na capacidade máxima de armazenamento adquirida, nos tamanhos de dados da informação de cabeçalho e da informação de assinatura e assim por diante (Etapa S5028).

A seguir, a unidade de geração de conteúdo de enchimento 5108 gera conteúdo de enchimento possuindo um tamanho de dado da capacidade de enchimento calculada por combinar a informação de reprodução impraticável com um número aleatório (Etapa S5029) e gera um identificador de arquivo e informação de identificação de arquivo correspondendo ao conteúdo de enchimento (Etapa S5031).

A unidade de geração de conteúdo de enchimento 5108 gera conteúdo de enchimento dividido por dividir o conteúdo de enchimento ge-

rado em j pedaços de unidades baseada no número de divisão armazenado "j" (Etapa S5032).

A seguir, a unidade de geração de conteúdo de enchimento 5108 gera a informação de arquivo incluindo o identificador de arquivo gerado e a informação de identificação e um número de unidades indicando o número de unidades geradas e adiciona a informação de arquivo gerada para a informação de seleção de unidade recebida (Etapa S5033). A unidade de geração de conteúdo de enchimento 5108 emite: o conteúdo de enchimento gerado e a informação de seleção de unidade 5140 para a unidade de gravação 5114; a informação de enchimento de arquivo 5156 composta do identificador de arquivo gerado e do conteúdo de enchimento dividido 5120 para a unidade de geração de informação de cabeçalho 5107; e a informação de seleção de unidade 5140 para a unidade de geração de informação de assinatura 5111.

Quando recebendo o conteúdo dividido criptografado e a informação de enchimento de arquivo 5156, a unidade de geração de informação de cabeçalho 5107 gera c pedaços de primeiras tabelas hash a partir dos c pedaços de arquivos divididos criptografados incluídos no conteúdo dividido criptografado recebido (Etapa S5034). Subseqüentemente, a unidade de geração de informação de cabeçalho 5107 gera uma primeira tabela hash a partir do conteúdo de enchimento dividido incluído na informação de arquivo de enchimento recebida 5156 (Etapa S5036).

A unidade de geração de informação de cabeçalho 5107 gera uma segunda tabela hash baseada nos c + 1) pedaços gerados de primeiras tabelas hash (Etapa S5037), gera a informação de cabeçalho incluindo os (c + 1) pedaços de primeiras tabelas hash e a segunda tabela hash (Etapa S5039) e emite a informação de cabeçalho gerada para a unidade de gravação 5114 enquanto emitindo a segunda tabela hash gerada para a unidade de geração de informação de assinatura 5111.

Quando recebendo a informação de seleção de unidade 5140 e a segunda tabela hash, a unidade de geração de informação de assinatura 5111 gera a informação de assinatura por aplicar um algorítmo de geração

de assinatura junto à informação de seleção de unidade e à segunda tabela hash recebidas (Etapa S5041) e emite a informação de assinatura gerada para a unidade de gravação 5114.

Quando recebendo o bloco de chave, o conteúdo criptografado, o conteúdo de enchimento, a informação de seleção de unidade, a informação de cabeçalho e a informação de assinatura, a unidade de gravação 5114 grava o bloco de chave recebido, o conteúdo criptografado, o conteúdo de enchimento, a informação de seleção de unidade, a informação de cabeçalho e a informação de assinatura junto ao DVD 5500 (Etapa S5042).

5.5.2 Comportamento Operacional do Dispositivo de Execução 5600

O comportamento operacional do dispositivo de execução 5600 é descrito com o auxílio dos fluxogramas apresentados nas Figuras 64 e 65.

Quando carregada com o DVD 5500, a unidade de aquisição 1601 lê o bloco de chave 5510, a informação de seleção de unidade 5530, e a informação de assinatura 5570 a partir do DVD 5500 e emite o bloco de chave 5510 para a unidade de aquisição de chave de conteúdo 1602 enquanto emitindo a informação de seleção de unidade 5530 e a informação de assinatura 5570 para a unidade de verificação de informação de assinatura 1611 (Etapa S5061).

A unidade de verificação de informação de assinatura 5611 recebe a informação de seleção de unidade 5530 e a informação de assinatura 5570, seleciona i pedaços de várias unidades criptografadas incluídas no conteúdo criptografado 5580 e j pedaços de unidades incluídas no conteúdo de enchimento 5590 com o uso de números aleatórios e da informação de seleção de unidade 5530 e gera i pedaços de primeiras tabelas hash substituídas por utilizar os i pedaços selecionados e a informação de cabeçalho (Etapa S5063).

A unidade de verificação de informação de assinatura 5611 calcula um valor hash de arquivo de substituição a partir de cada um dos i pedaços gerados de tabelas hash substituídas (Etapa S5064).

A seguir, a unidade de verificação de informação de assinatura 5611 lê a segunda tabela hash a partir do DVD 5500 (Etapa S5066) e gera

uma segunda tabela hash substituída por substituir, com os valores hash de substituição, os valores hash de arquivo correspondendo aos i pedaços gerados de valores hash de arquivo de substituição (Etapa S5068). A unidade de verificação de informação de assinatura 5611 verifica a informação de assinatura 5570 por utilizar a segunda tabela hash substituída gerada, a informação de seleção de unidade recebida 5530 e a chave de verificação 1613 armazenada na unidade de armazenamento de chave de verificação 1612 (Etapa S5069). Se a verificação da informação de assinatura 5570 for malsucedida (Etapa S5071: NÃO), a unidade de verificação de informação de assinatura 5611 emite a informação de proibição de reprodução para a unidade de execução 5606 (Etapa S5073).

Quando a verificação da informação de assinatura 5570 é bem sucedida (Etapa S5071: SIM), a unidade de verificação de informação de assinatura 5611, então, termina a verificação.

A unidade de aquisição de chave de conteúdo 1602 recebe o bloco de chave 5510, e lê um identificador de dispositivo e uma chave de dispositivo a partir da unidade de armazenamento de chave de dispositivo 1604 (Etapa S5074). A unidade de aquisição de chave de conteúdo 1602 gera a chave de conteúdo "CK" a partir do identificador de dispositivo lido, da chave de dispositivo e do bloco de chave 5510 e emite a chave de conteúdo gerada "CK" para a unidade de execução 5606 (Etapa S5076).

A unidade de execução 5606 recebe a chave de conteúdo a partir da unidade de aquisição de chave de conteúdo 1602. Aqui, se recebendo a informação de proibição de reprodução a partir da unidade de verificação de informação de assinatura 5611 (Etapa S5077: SIM), a unidade de execução 5606 notifica ao usuário da impraticabilidade de reprodução do conteúdo armazenado no DVD 5500 (Etapa S5079) e aborda a reprodução subseqüente.

Se não recebendo a informação de proibição de reprodução (Etapa S5077: NÃO), a unidade de execução 5606 lê um dos c pedaços de arquivos criptografados constituindo o conteúdo criptografado e o conteúdo de enchimento (Etapa S5081). A unidade de execução 5606 compara o ar-

quivo criptografado lido ou os primeiros 56 bits do conteúdo de enchimento com a informação de reprodução impraticável (Etapa S5082). Quando estes se conformam (Etapa S5084: SIM), a unidade de execução 5606 retorna para a etapa S5077.

Quando estes dois não concordam (Etapa S5084: NÃO), o arquivo lido é um arquivo criptografado e executável. Portanto, a unidade de execução 5606 gera um arquivo pode decriptografar o arquivo criptografado com o uso da chave de conteúdo recebida (Etapa S5086), expande o arquivo gerado (Etapa S5087) e tem o monitor executando o arquivo expandido (Etapa S5089). Quando tendo terminado a leitura de todos os arquivos criptografados constituindo o conteúdo criptografado e o conteúdo de enchimento ou sendo instruída para terminar a reprodução pelo usuário (Etapa S5091: SIM), a unidade de execução 5606 termina a reprodução. Se não tendo terminado a leitura de todos os arquivos criptografados constituindo o conteúdo criptografado e o conteúdo de enchimento e a unidade de execução 5606 não tendo recebido uma instrução para terminar a reprodução a partir do usuário (Etapa S5091: NÃO), a unidade de execução 5606 retorna para a Etapa S5077 e repete o processamento das etapas 5077 até S5091.

5.6 Sumário e Efeitos Vantajosos

Como foi descrito, na presente modalidade, o DVD 5500 armazena, em adição às várias informações incluindo conteúdo criptografado, conteúdo de enchimento possuindo um tamanho de dado apropriado de modo a não deixar uma área de armazenamento que pode ser gravada no DVD 5500. Adicionalmente, a informação de cabeçalho e a informação de assinatura são geradas baseado não somente no conteúdo criptografado mas também no conteúdo de enchimento.

A unidade de execução 5606 constituindo o dispositivo de execução 5600 seqüencialmente lê arquivos gravados no DVD 5500 e compara os primeiros 56 bits dos arquivos individuais lidos com a informação de reprodução impraticável pré-armazenada. Quando estes dois se conformam, a unidade de execução 5606 julga que o arquivo lido é o conteúdo de enchimento e evita a reprodução do arquivo.

Quando o DVD 5500 não tem armazenado tal conteúdo de enchimento, dois casos envolvendo atos fraudulentos descritos abaixo podem ser assumidos.

A Figura 65 apresenta uma estrutura de um DVD 5500b que é criado por se adicionar um arquivo contendo conteúdo não autorizado para um DVD 5500a o qual foi gerado por um mantenedor legítimo de direito.

O DVD 5500a armazena a informação de cabeçalho, a informação de seleção de unidade, a informação de assinatura em uma área 5703 enquanto armazenado arquivo criptografados individuais constituindo o conteúdo criptografado nas áreas 5704, 5705, ..., 5707. Em adição a estes conjuntos de informações, o DVD 5500a também armazena uma tabela de arquivos e um arquivo de ordem de reprodução na área 5701 e na área 5702, respectivamente.

A tabela de arquivos armazenada na área 5701 inclui identificadores de arquivo para todos os arquivos armazenados no DVD 5500, endereços iniciais dos arquivos e números de setores que os arquivos individuais ocupam no DVD, associando os identificadores de arquivo, os endereços iniciais e os números de setores dos arquivos individuais. Por exemplo, um arquivo possuindo um identificador de arquivo "FID1" é armazenado nos 70 setores iniciando em um endereço "0XAA1".

O arquivo de ordem de execução armazenado na área 5702 apresenta uma ordem de reprodução de arquivos armazenados no DVD. Em um exemplo aqui, os arquivos são ser serem reproduzidos na ordem a partir de um arquivo possuindo um identificador de arquivo "FIF1" até um arquivo possuindo um identificador de arquivo "FIDc".

Em adição, nada foi armazenado em uma área 5711 no DVD 5500a.

Nesta situação, pressupõe-se que uma terceira pessoa não autorizada gravou um arquivo incluindo conteúdo não autorizado na área 5711 do DVD 5500a e gerou o DVD 5500b por falsificar a tabela de arquivos e o arquivo de ordem de reprodução.

Na área 5701 no DVD 5500b, um identificador de arquivo "FIDx"

correspondendo ao arquivo não autorizado, um endereço inicial "0XAAx" do arquivo não autorizado e um número de setores "200", foram adicionados. Em adição, um arquivo de ordem de reprodução armazenado na área 5702 foi falsificado de modo que a reprodução irá iniciar com o arquivo possuindo um identificador de arquivo "FIDx".

Adicionalmente, também é considerado um caso no qual um DVD 5500c apresentado na Figura 66 é gerado pela adição de conteúdo não autorizado para o arquivo válido armazenado no DVD 5500a.

O DVD 5500c armazena conteúdo não autorizado na área 5711, a qual é imediatamente após um arquivo validamente gravado em uma área 5707. O número de setores correspondendo ao arquivo armazenado na área 5707 na tabela de arquivos foi falsificado para "320", o qual foi obtido pela adição de um número de setores no qual o arquivo é originalmente armazenado para um número de setores no qual o conteúdo não autorizado adicionado é armazenado. O arquivo de ordem de reprodução foi alterado de modo que a reprodução irá iniciar com o 51º setor no arquivo possuindo o identificador de arquivo "FIDc", isto é, o conteúdo não autorizado adicionado.

Assim, quando a falsificação não autorizada foi conduzida, desde que a informação de cabeçalho, a informação de seleção de unidade, a informação de assinatura e o conteúdo criptografado não foram falsificados de modo algum, o dispositivo de execução lê o arquivo não autorizado e inicia a reprodução de acordo com a ordem indicada pelo arquivo de ordem uma vez que a verificação da informação de assinatura é completada normalmente.

Na presente modalidade, uma área de armazenamento que pode ser gravada não é deixada no DVD 5500 por causa da presença do conteúdo de enchimento. Em adição, o conteúdo de enchimento também é utilizado para a geração de informação de assinatura. Portanto, se o conteúdo de enchimento for substituído por um arquivo não autorizado, a verificação da informação de assinatura será malsucedida no dispositivo de execução 5600 e portanto, a reprodução será abortada.

6. Sexta Modalidade

Uma sexta modalidade da presente invenção é descrita abaixo.

6.1 Sistema de Detecção de Conteúdo Não Autorizado

O sistema de detecção de conteúdo não autorizado da sexta modalidade é composto de um dispositivo de distribuição, de um dispositivo de execução e de um monitor, como no sistema de detecção de conteúdo não autorizado da primeira modalidade.

O dispositivo de distribuição gera, em adição ao bloco de chave, informação de seleção de unidade, conteúdo criptografado, informação de cabeçalho e informação de assinatura descritas na primeira modalidade, informação de área para indicar uma área de armazenamento em um DVD onde a informação validamente gravada pelo dispositivo de distribuição é armazenada, e grava a informação de área gerada no DVD.

O dispositivo de execução lê a informação de área a partir do DVD e lê somente informação armazenada na área de armazenamento indicada pela informação de área lida.

6.2 Dispositivo de Distribuição 6100

A Figura 67 apresenta uma estrutura de um dispositivo de distribuição constituindo o sistema de detecção de conteúdo não autorizado da sexta modalidade. Como apresentado na Figura 67, um dispositivo de distribuição 6100 é composto de uma unidade de entrada 1101, de uma unidade de geração de chave de conteúdo 1102, de uma unidade de geração de bloco de chave 6103, de uma unidade de armazenamento de informação de dispositivo de execução 1104, de uma unidade de geração de unidade 6105, de uma unidade de processamento de criptografia 6106, de uma unidade de geração de informação de cabeçalho 6107, de uma unidade de geração de alocação 6108, de uma unidade de geração de informação de área 6109, de uma unidade de geração de informação de assinatura 6111, de uma unidade de armazenamento de chave de assinatura 1112, e de uma unidade de gravação 6114.

Os componentes individuais compondo o dispositivo de distribuição 6100 são descritos abaixo. Observe que, desde que a unidade de en-

trada 1101, a unidade de geração de chave de conteúdo 1102, a unidade de armazenamento de informação de dispositivo de execução 1104 e a unidade de armazenamento de chave de assinatura 1112 são os mesmos que no dispositivo de distribuição 1100 da primeira modalidade, as descrições para estes componentes são omitidas.

Aqui, ao invés da unidade de gravação emitindo o bloco de chave, a informação de seleção de unidade, o conteúdo criptografado e a informação de cabeçalho, a unidade de geração de bloco de chave 6103, a unidade de geração de unidade 6105, a unidade de processamento de criptografia 6106 e a unidade de geração de informação de cabeçalho 6107, individualmente emitem suas próprias informações geradas para a unidade de geração de alocação 6108. Diferente disto, a unidade de geração de bloco de chave 6103, a unidade de geração de unidade 6105, a unidade de processamento de criptografia 6106 e a unidade de geração de informação de cabeçalho 6107 são as mesmas que a unidade de geração de bloco de chave 1103, a unidade de geração de unidade 1105, a unidade de processamento de criptografia 1106 e a unidade de geração de informação de cabeçalho 1107 da primeira modalidade, respectivamente, e portanto, as descrições para estes componentes são omitidas.

6.2.1 Unidade de Geração de Alocação 6108

A unidade de geração de alocação 6108 pré-armazena um tamanho máximo de dado da informação de assinatura gerada pela unidade de geração de informação de assinatura 6111. Em adição, a unidade de geração de alocação 6108 armazena um tamanho de dado da informação de área gerada pela unidade de geração de informação de área 6109.

A unidade de geração de alocação 6108 recebe: um bloco de chave a partir da unidade de geração de bloco de chave 6103; a informação de seleção de unidade a partir da unidade de geração de unidade 6105; conteúdo criptografado a partir da unidade de processamento de criptografia 6106; e informação de cabeçalho a partir da unidade de geração de informação de cabeçalho 6107.

Quando recebendo estes conjuntos de informações, a unidade

de geração de alocação 6108 gera informação de alocação de escrita 6120 como apresentado na Figura68. A informação de alocação de escrita 6120 é criada por dispor os conjuntos de informações recebidos na mesma configuração que no DVD e gravar os conjuntos de informações dispostos na memória. Um procedimento para gerar a informação de alocação de escrita 6120 é descrito abaixo com o auxílio da Figura 68.

A unidade de geração de alocação 6108 grava: o bloco de chave em uma área 6121 na memória; a informação de unidade em uma área 6122; e a informação de cabeçalho em uma área 6123.

A seguir, a unidade de geração de alocação 6108 adquire as áreas 6124 e 6125 correspondendo respectivamente aos tamanhos máximos de dado da informação de área e da informação de assinatura armazenadas. Então, a unidade de geração de alocação 6108 grava o conteúdo criptografado em uma área 6126 seguindo a área 6125.

A unidade de geração de alocação 6108 emite a informação de alocação de escrita gerada 6120 para a unidade de geração de informação de área 6109 e para a unidade de gravação 6114.

Observe que a ordem de alocação dos conjuntos de informações apresentada na Figura 68 é meramente um exemplo e a presente invenção não está limitada a isto.

Aqui, a unidade de geração de alocação 6108 armazena o tamanho máximo de dado da informação de assinatura. Entretanto, a unidade de geração de alocação 6108 pode, por exemplo, calcular o tamanho de dado da informação de assinatura da mesma maneira que a unidade de geração de conteúdo de enchimento 5108 da quinta modalidade.

6.2.2 Unidade de Geração de Informação de Unidade 6109

A unidade de geração de informação de área 6109 recebe a informação de alocação de escrita 6120 a partir da unidade de geração de alocação 6108. Quando recebendo a informação de alocação de escrita 6120, a unidade de geração de informação de área 6109 gera a informação de área a partir da informação de alocação de escrita 6120. A informação de área é informação para indicar uma área em um DVD na qual informação

válida gravada pelo dispositivo de distribuição 6100 é armazenada. A informação de área é, por exemplo, um par de endereços de posição inicial (daqui para frente, endereço inicial) e de posição final (endereço final) para gravação da informação de alocação de escrita 6120 em um DVD.

A informação de área não está limitada a este exemplo e qualquer informação é aplicável, tal como um par de endereço inicial e número de setores no qual a informação válida é armazenada, contanto que a informação identifique uma área onde a informação válida está armazenada.

A unidade de geração de informação de área 6109 emite a informação de área gerada para a unidade de geração de informação de assinatura 6111 e para a unidade de gravação 6114.

6.2.3 Unidade de Geração de Informação de Assinatura 6111

A unidade de geração de informação de assinatura 6111 recebe: a informação de seleção de unidade a partir da unidade de geração de unidade 6105; a segunda tabela hash a partir da unidade de geração de informação de cabeçalho 6107; e a informação de área a partir da unidade de geração de área 6109.

Quando recebendo estes conjuntos de informações, a unidade de geração de informação de assinatura 6111 lê a chave de assinatura 1113 a partir da unidade de armazenamento de chave de assinatura 1112.

A seguir, a unidade de geração de informação de assinatura 6111 gera a informação de assinatura por aplicar o algorítmo de geração de assinatura S junto a um resultado combinado formado por se combinar c pedaços de valores hash de arquivo incluídos na segunda tabela hash recebida , c pedaços de informação de arquivo constituindo a informação de seleção de unidade e a informação de área recebida com o uso da chave de assinatura lida 1113.

A seguir, a unidade de geração de informação de assinatura 6111 emite a informação de assinatura gerada para a unidade de gravação 6114.

6.2.4 Unidade de Gravação 6114

A unidade de gravação 6114 é carregada com um DVD.

A unidade de gravação 6114 recebe: a informação de alocação de escrita 6120 a partir da unidade de geração de alocação 6108; a informação de área a partir da unidade de geração de informação de área 6109; e a informação de assinatura a partir da unidade de geração de informação de assinatura 6111.

Quando recebendo estes conjuntos de informações, a unidade de gravação 6114 insere a informação de área recebida na área 6124 na informação de alocação de escrita 6120 enquanto inserindo a informação de assinatura na área 6125.

Quando tendo inserido a informação de área e a informação de assinatura na informação de alocação de escrita 6120, a unidade de gravação 6114 grava a informação de alocação de escrita 6120 junto a um DVD.

6.3 DVD 6500

A Figura 69 apresenta a informação armazenada em um DVD da sexta modalidade. Como apresentado na Figura 69, um DVD 6500 armazena um bloco de chave 6510, a informação de seleção de unidade 6530, a informação de cabeçalho 6550, a informação de área 6560, a informação de assinatura 6570 e o conteúdo criptografado 6580. Estes foram gravados pelo dispositivo de distribuição 6100 e portanto, as descrições são omitidas aqui.

6.4 Dispositivo de Execução 6600

A Figura 70 apresenta uma estrutura de um dispositivo de execução da sexta modalidade. Como apresentado na Figura 70, um dispositivo de execução 6600 é composto de uma unidade de acionamento 6620 e uma unidade de execução de conteúdo 6625.

A unidade de acionamento 6620 é composta de uma unidade de aquisição 6601, de uma unidade de armazenamento de informação de área 6603, de uma unidade de comunicação de criptografia 6604 e de uma unidade de armazenamento de chave de criptografia 6605.

A unidade de execução de conteúdo 6625 é composta de uma unidade de aquisição de chave de conteúdo 1602, de uma unidade de armazenamento de chave de dispositivo 1604, de uma unidade de comunica-

ção de decriptografia 6607, da unidade de armazenamento de chave de decriptografia 6608, de uma unidade de verificação de informação de assinatura 6611, de uma unidade de armazenamento de chave de verificação 1612 e de uma unidade de execução 6606.

Os componentes individuais constituindo o dispositivo de execução 6600 são descritos abaixo. Observe que, desde que a unidade de aquisição de chave de conteúdo 1602, a unidade de armazenamento de chave de dispositivo 1604 e a unidade de armazenamento de chave de verificação 1612 são as mesmas que no dispositivo de execução 1600 da primeira modalidade, as descrições destes componentes são omitidas.

6.4.1 Unidade de Aquisição 6601

A unidade de aquisição 6601 é carregada com o DVD 6500. Quando carregada com o DVD 6500, a unidade de aquisição 6601 primeiro lê a informação de área 6560, então grava a informação de área lida 6560 na unidade de armazenamento de informação de área 6603 e emite a informação de área lida 6560 para a unidade de comunicação de criptografia 6604.

A seguir, a unidade de aquisição 6601 lê o bloco de chave 6510, a informação de seleção de unidade 6530 e a informação de assinatura 6570 a partir do DVD 6500 e emite o bloco de chave lido 6510 para a unidade de aquisição de chave de conteúdo 1602 enquanto emitindo a informação de seleção de unidade lida 6530 e a informação de assinatura 6570 para a unidade de verificação de informação de assinatura 6611.

Em adição, a unidade de aquisição 6601 recebe requisições para ler vários conjuntos de informações a partir da unidade de verificação de informação de assinatura 6611 e da unidade de execução 1606. Quando recebendo a requisição de leitura, a unidade de verificação de informação de assinatura 6611 lê a informação de área a partir da unidade de armazenamento de informação de área 6603. Quando um conjunto de informações requisitado é armazenado em uma área indicada pela informação de área, a unidade de aquisição 6601 lê a informação requisitada a partir do DVD 6500 e emite a informação lida para uma fonte de requisição, isto é, a unidade de

verificação de informação de assinatura 6611 ou a unidade de execução 1606.

Quando um conjunto de informações requisitado não está armazenado na área indicada pela informação de área lida, a unidade de aquisição 6601 emite um sinal de notificação de erro indicando que o conjunto de informações requisitado não pode ser lido.

6.4.2 Unidade de Armazenamento de Informação de Área 6603

A unidade de armazenamento de informação de área 6603 é, por exemplo, composta de uma RAM e armazena informação de área gravada pela unidade de aquisição 6601.

6.4.3 Unidade de Comunicação de Criptografia 6604 e Unidade de Armazenamento de Chave de Criptografia 6605

A unidade de armazenamento de chave de criptografia 6605 é, por exemplo, composta de uma ROM e armazena uma chave de criptografia com o comprimento de 56 bits.

A unidade de comunicação de criptografia 6604 recebe a informação de área 6560 a partir da unidade de aquisição 6601. Quando recebendo a informação de área 6560, a unidade de comunicação de criptografia 6604 lê uma chave de criptografia a partir da unidade de armazenamento de chave de criptografia 6605 e gera a informação de área criptografada por aplicar um algorítmo de criptografia E2 para a chave de criptografia lida. Aqui, DES (Padrão de Criptografia de Dados) é utilizado, como um exemplo, para o algorítmo de criptografia E2.

A seguir, a unidade de comunicação de criptografia 6604 emite a informação de área criptografada gerada para a unidade de comunicação de decriptografia 6607.

6.4.4 Unidade de Comunicação de Decriptografia 6607 e Unidade de Armazenamento de Chave de Decriptografia 6608

A unidade de armazenamento de chave de decriptografia 6608 é, por exemplo, composta de uma ROM e armazena uma chave de decriptografia com o comprimento de 56 bits. Aqui, a chave de decriptografia é a mesma que a chave de criptografia armazenada pela unidade de armaze-

namento de chave de criptografia 6605.

A unidade de comunicação de decriptografia 6607 recebe a informação de área criptografada a partir da unidade de comunicação de criptografia 6604. Quando recebendo a informação de área criptografada, a unidade de comunicação de decriptografia 6607 lê uma chave de decriptografia a partir da unidade de armazenamento de chave de decriptografia 6608 e gera a informação de área por aplicar um algorítmo de decriptografia D2 junto à informação de área criptografada recebida com o uso da chave de decriptografia lida. Aqui, o algorítmo de decriptografia D2 é um algorítmo utilizado para decriptografar textos criptografados gerados pelo algorítmo de criptografia E2.

A seguir, a unidade de comunicação de decriptografia 6607 emite a informação de área gerada para a unidade de verificação de informação de assinatura 6611.

A descrição acima é dada pressupondo que a chave de criptografia e a chave de decriptografia são as mesmas e a unidade de comunicação de decriptografia 6607 utiliza um criptossistema de chave simétrica. Entretanto, a presente invenção não está limitada a isto e um criptossistema de chave pública pode ao invés disso ser utilizado. Alternativamente, um criptossistema de chave pública e um criptossistema de chave simétrica podem ser combinados para gerar uma chave diferente cada vez que a comunicação é conduzida e a comunicação cifrada por ser executada com o uso da chave gerada.

Em adição, aqui, somente a informação de área é criptografada e então emitida para a unidade de execução de conteúdo 6625, entretanto, todas as informações enviadas e recebidas entre a unidade de execução de conteúdo 6625 e a unidade de acionamento 6620 podem ser criptografadas.

6.4.5 Unidade de Verificação de Informação de Assinatura 6611.

A unidade de verificação de informação de assinatura 6611 recebe: a informação de seleção de unidade 6530 e a informação de assinatura 6570 a partir da unidade de aquisição 6601; e a informação de área a partir da unidade de comunicação de decriptografia 6607.

Quando recebendo a informação de seleção de unidade 6530 e a informação de assinatura 6570, a unidade de verificação de informação de assinatura 6611 gera uma segunda tabela hash substituída baseada na informação de seleção de unidade recebida 6530 e no conteúdo criptografado 6580 e na informação de cabeçalho 6550 armazenados no DVD 6500. Um procedimento para gerar a segunda tabela hash substituída é o mesmo que um procedimento de geração de uma segunda tabela hash substituída executado pela unidade de verificação de assinatura 1611 da primeira modalidade e portanto, a descrição é omitida.

A seguir, a unidade de verificação de informação de assinatura 6611 lê a chave de verificação 1613 a partir da unidade de armazenamento de chave de verificação 1612. Então, a unidade de verificação de informação de assinatura 6611 gera a informação de verificação de assinatura por aplicar, com o uso da chave de verificação lida 1613, o algorítmo de verificação de assinatura V junto a um resultado combinado formado por se combinar todos os valores hash de arquivo e os valores hash de arquivo de substituição incluídos na segunda tabela hash substituída geada, todos os pedaços de informação de arquivo incluídos na informação de seleção de unidade recebida 6530 e a informação de área. A unidade de verificação de informação de assinatura 6611 compara a informação de verificação de assinatura gerada com a informação de assinatura gerada 6570.

Quando estas duas não se conformam, a unidade de verificação de informação de assinatura 6611 julga que a verificação da informação de assinatura não é bem sucedida e emite informação de proibição para a unidade de execução 1606.

Quando estas duas concordam, a unidade de verificação de informação de assinatura 6611 julga que a verificação da informação de assinatura recebida 6570 é bem sucedida e termina o processamento de verificação.

Durante o processamento acima, a unidade de verificação de informação de assinatura 6611 instrui a unidade de aquisição 6601 para ler parte do conteúdo criptografado e a informação de cabeçalho. Entretanto,

neste ponto, a unidade de verificação de informação de assinatura 6611 pode receber um sinal de notificação de erro indicando que a leitura não é possível.

Quando recebendo o sinal de notificação de erro, a unidade de verificação de informação de assinatura 6611 aborta o processamento de verificação da informação de assinatura e emite a informação de proibição de reprodução para a unidade de execução 1606.

6.4.6 Unidade de Execução 6606

A unidade de execução 6606 recebe a chave de conteúdo a partir da unidade de aquisição de chave de conteúdo 1602 e começa a repetir a leitura, decriptografia e reprodução dos arquivos criptografados, como é o caso com a unidade de execução 1606 constituindo o dispositivo de execução 1600 da primeira modalidade.

Durante a repetição, a unidade de execução 6606 pode receber a informação de proibição de reprodução a partir da unidade de verificação de informação de assinatura 6611.

Adicionalmente, na repetição, a unidade de execução 6606 requisita que a unidade de aquisição 6601 leia arquivos criptografados constituindo o conteúdo criptografado 6580. Neste ponto, entretanto, a unidade de execução 6606 pode receber a partir da unidade de aquisição 6601 um sinal de notificação de erro indicando que a leitura não é possível.

Quando recebendo a informação de proibição de reprodução ou um sinal de notificação de erro, a unidade de execução 6606 aborta o processamento de reprodução e notifica ao usuário da impraticabilidade de reprodução do DVD carregado.

6.5 Sumário e Efeitos Vantajosos

Como foi descrito, o dispositivo de distribuição 6100 constituindo o sistema de detecção de conteúdo não autorizado da presente modalidade gera informação de área indicando uma área onde informação validamente gravada pelo dispositivo de distribuição 6100 está armazenada e grava a informação de área gerada junto a um DVD. Adicionalmente, o dispositivo de distribuição 6100 gera informação de assinatura a partir da segunda ta-

bela hash, da informação de seleção de unidade e da informação de área e grava esta junto ao DVD.

Quando carregado com o DVD 6500, a unidade de aquisição 6601 do dispositivo de execução 6600 primeiro lê a informação de área a partir do DVD 6500 e então lê somente informação em uma área indicada pela informação de área lida enquanto não lendo informação gravada em outras áreas.

Com isto, mesmo quando atos fraudulentos envolvendo gravar conteúdo não autorizado em espaço livre no DVD 6500, como descrito na primeira modalidade, são comprometidos, o conteúdo não autorizado não pode ser executado no dispositivo de execução 6600.

Em adição, a informação de assinatura armazenada no DVD 6500 é gerada com o uso da informação de área e a unidade de verificação de informação de assinatura 6611 do dispositivo de execução 6600 utiliza a informação de área lida a partir do DVD 6500 de modo a verificar a informação de assinatura. Portanto, mesmo se uma terceira pessoa não autorizada falsificar a informação de área junto com a inserção de conteúdo não autorizado, a verificação da informação de assinatura executada pela unidade de verificação de informação de assinatura 6611 será mal sucedida e portanto, o conteúdo não autorizado não será executado.

Quando não existe espaço livre deixado no DVD, um ato fraudulento pode ser comprometido, tal como copiar todos os dados armazenados no DVD válido sobre outro meio possuindo uma capacidade de armazenamento maior do que o DVD válido tem e adicionando conteúdo não autorizado para o espaço livre do meio. Mesmo nesta situação. O dispositivo de execução 6600 no sistema de detecção de conteúdo não autorizado da presente modalidade não lê a informação em áreas de armazenamento diferentes de uma área indicada pela informação de área. Por conseqüência, a presente modalidade é capaz de impedir tal ato fraudulento.

6.6 Modificação da Sexta Modalidade

Na sexta modalidade, a informação de área gerada pelo dispositivo de distribuição 6100 é informação indicando uma área onde informação

validamente gravada pelo dispositivo de distribuição está armazenada. Alternativamente, a informação de área pode ser o tamanho total de dados de informação validamente gravada pelo dispositivo de distribuição 6100.

Neste caso, a unidade de aquisição 6601 do dispositivo de execução 6600 primeiro lê o tamanho total de dados a partir do DVD 6500, e então mede o tamanho total de dados da informação armazenada no DVD 6500. Quando o tamanho de dados medido é maior do que o tamanho de dados lido, a unidade de aquisição 6601 aborta a leitura de dados a partir do DVD 6500 e emite um sinal de notificação de erro para a unidade de execução 6606.

7. Outras Modificações

Apesar da presente invenção ter sido descrita baseada nas modalidades acima, é normal que a presente invenção não seja confinada a estas modalidades. A presente invenção também inclui os seguintes casos.

[1] Na primeira, quinta e sexta modalidades acima, o dispositivo de distribuição calcula valores hash de unidade por designar unidades criptografadas para uma função hash e gera a informação de cabeçalho e a informação de assinatura baseado nos valores hash de unidade calculados, enquanto o dispositivo de execução verifica a informação de assinatura por utilizar i pedaços selecionados de unidades criptografadas. Entretanto, o dispositivo de distribuição pode calcular valores hash de unidade por utilizar unidades antes da criptografia e o dispositivo de execução pode gerar i pedaços de unidades por decriptografar os i pedaços selecionados de unidades criptografadas e verificar a informação de assinatura por utilizar os i pedaços gerados de unidades.

[2] Por outro lado, na segunda até a quarta modalidades, o dispositivo de distribuição calcula valores hash parciais por designar pedaços de conteúdo parcial para uma função hash e gera a informação de cabeçalho e a informação de assinatura baseado nos valores hash parciais calculados. Entretanto, o dispositivo de distribuição pode calcular valores hash parciais por designar, para a função hash, conteúdo parcial criptografado que é gerado por se criptografar pedaços individuais de conteúdo parcial e

gerar a informação de cabeçalho e a informação de assinatura baseado nos valores hash parciais calculados.

Neste caso, o dispositivo de execução utiliza o conteúdo parcial criptografado para a verificação da informação de cabeçalho. Isto elimina a necessidade de equipar com a unidade de decriptografia de conteúdo parcial representativo e a unidade de decriptografia de conteúdo parcial, o que leva a uma redução no tamanho do circuito do sistema de detecção.

[3] Na segunda até a quarta modalidades, após as verificações de informação de assinatura e da informação de cabeçalho terem sido bem-sucedidas, a unidade de execução inicia a decriptografia, expansão e reprodução do conteúdo criptografado. Entretanto, a unidade de execução pode iniciar o processamento relacionando-se com a reprodução em paralelo com as verificações. Neste caso, quando verificações individuais executadas pela unidade de verificação de informação de assinatura e pela unidade de verificação de informação de cabeçalho, respectivamente, são mal sucedidas, a unidade de verificação de informação de assinatura e a unidade de verificação de informação de cabeçalho direcionam a unidade de execução para abortar a reprodução.

[4] Na primeira, quinta e sexta modalidades, a unidade de verificação de informação de assinatura pode ter um temporizador para medir a passagem de tempo e julgar que uma verificação é malsucedida se a verificação da informação de assinatura não estiver completada dentro de um tempo predeterminado.

No caso quando a verificação da informação de assinatura é executada em paralelo com a reprodução, se o conteúdo, a informação de assinatura, ou a informação de cabeçalho tiver sido falsificado, o conteúdo não autorizado será executado até que a verificação seja completada.

Por conseqüência, configurar um limite de tempo para a verificação da informação de assinatura permite neutralizar atos fraudulentos envolvendo estender o tempo de execução de conteúdo não autorizado por fazer a falsificação de modo que a conclusão da verificação da informação de assinatura seja retardada.

Em adição, a unidade de verificação de informação de assinatura e a unidade de verificação de informação de cabeçalho na Modificação [3] podem ter um temporizador de uma maneira similar.

[5] Na primeira até a sexta modalidades acima, o dispositivo de distribuição possui uma chave de assinatura enquanto o dispositivo de execução possui uma chave de verificação correspondente e estes dispositivos geram e verificam a informação de assinatura com o uso de um algorítmo de geração de assinatura tal como o DSA.

Em geral, qualquer algorítmo de geração de assinatura é baseado em criptossistemas de chave pública, como tipificado pelo DAS e pelo RSA (Rivest-Shamir-Adleman). Entretanto, na presente invenção, qualquer algorítmo de geração de assinatura, tal como um baseado em um criptossistema de chave simétrica, por exemplo, é aplicável contanto que ele seja capaz de proporcionar que a informação de assinatura gravada no DVD seja informação gerada por um mantenedor legítimo de direito.

Como outro exemplo, uma função unidirecional pode ser utilizada com o processamento ocultado. Neste caso, o dispositivo de distribuição e o dispositivo de execução respectivamente armazenam a mesma função unidirecional em uma área de armazenamento que não pode ser lida por dispositivos externos. O dispositivo de distribuição gera a informação de assinatura com o uso da função unidirecional, enquanto o dispositivo de execução gera a informação de verificação de assinatura por utilizar a mesma função unidirecional.

[6] A informação para a qual um algorítmo de geração de assinatura é aplicado na geração da informação de assinatura não está limitada a esta descrita nas modalidades acima. Por exemplo, na primeira modalidade, o algorítmo é aplicado junto tanto à segunda tabela hash como à informação de seleção de unidade, entretanto, o algorítmo de geração de assinatura pode ser aplicado somente junto à segunda tabela hash, ou pode ser aplicado junto à chave de conteúdo "CK" e ao tamanho de dado do conteúdo criptografado em adição à segunda tabela hash. No caso da segunda modalidade, o algorítmo de geração de assinatura pode ser aplicado junto

aos próprios pedaços de conteúdo parcial representativo, ao invés de se aplicar um algorítmo de geração de assinatura junto aos valores hash parciais gerados a partir dos pedaços de conteúdo parcial representativo.

Especialmente, na segunda modalidade, quando a informação de assinatura é gerada a partir dos pedaços de conteúdo parcial representativo, k pedaços de informação de assinatura podem ser gerados por respectivamente aplicar o algorítmo de geração de assinatura junto aos k pedaços de conteúdo parcial representativo.

Neste caso, o dispositivo de execução gera k pedaços de conteúdo parcial representativo baseado na informação de posição selecionada e verifica os k pedaços de informação de assinatura por utilizar os k pedaços gerados de conteúdo parcial representativo.

Alternativamente, o dispositivo de distribuição pode gerar informação de assinatura por aplicar o algorítmo de geração de assinatura junto a um resultado combinado formado por se combinar os k pedaços de conteúdo parcial representativo, enquanto o dispositivo de execução verifica a informação de assinatura por utilizar o resultado combinado.

Nesta situação, se a verificação da informação de assinatura for bem sucedida, a duas coisas seguintes são confirmadas de uma vez: a informação de assinatura foi gerada por um mantenedor legítimo de direito; e o conteúdo parcial representativo está livre de falsificação. Isto elimina a necessidade de gerar a informação de cabeçalho e gravar a informação de cabeçalho junto ao DVD, o que leva a uma redução no tamanho dos dados gravados junto ao DVD.

[7] Na segunda e na terceira modalidades, o dispositivo de execução pode pré-armazenar a informação de posição selecionada e a informação de posição selecionada criptografada pode não ser gravada no DVD. Com isto, o dispositivo de execução válido é capaz de executar verificação de informação de cabeçalho com o uso da informação de posição selecionada pré-armazenada.

[8] Na terceira modalidade, a informação de seleção de cabeçalho e x pedaços de grupos de cabeçalho são gravados junto ao DVD. Entre-

tanto, no caso da Modificação [7], o dispositivo de distribuição pode selecionar um dentre o primeiro grupo até o x-ésimo grupo de cabeçalho, extrair um identificador de cabeçalho, a informação de cabeçalho e a informação de assinatura incluída no grupo de cabeçalho selecionado e gravar estes junto ao DVD.

O dispositivo de execução pode pré-armazenar x pares de um pedaço de informação de posição selecionada e um identificador de cabeçalho, selecionar um pedaço de informação de posição selecionada baseado em um identificador de cabeçalho gravado junto a DVD e utilizar o pedaço selecionado de informação de posição selecionada no processamento subseqüente.

[9] A primeira até a sétima modalidades acima são descritas pressupondo que o dispositivo de execução é um único dispositivo. Entretanto, vários dispositivos podem ser empregados para realizar a função do dispositivo de execução.

[10] Na terceira modalidade, a unidade de aquisição do dispositivo de execução seleciona um dos x pedaços de identificadores de cabeçalho. Entretanto, a presente invenção não está limitada a isto e dois ou mais identificadores podem ser ao invés disso selecionados e as verificações da informação de assinatura e da informação de cabeçalho podem ser repetidas duas vezes ou mais. Com isto, é possível detectar conteúdo não autorizado mais confiavelmente.

[11] Nas modalidades e modificações acima, a unidade de armazenamento de chave de assinatura do dispositivo de distribuição e a unidade de armazenamento de chave de verificação do dispositivo de execução respectivamente armazenam um pedaço de informação de chave, entretanto, a presente invenção não está confinada a isto.

[11-1] Por exemplo, a unidade de armazenamento de chave de assinatura pode armazenar uma chave de assinatura e um identificador de chave correspondendo à chave de assinatura e a unidade de gravação grava o identificador de chave junto ao DVD junto com a informação de assinatura.

A unidade de armazenamento de chave de verificação do dispositivo de execução armazena várias chaves de verificação e identificadores de chave correspondendo um para um com as chaves de verificação. A unidade de verificação de informação de assinatura recebe os identificadores de chave junto com a informação de assinatura, recupera um identificador de chave se conformando com o identificador de chave recebido a partir dos vários identificadores de chave armazenados pela unidade de armazenamento de chave de verificação, lê uma chave de verificação correspondendo a um identificador de chave de verificação recuperado e utiliza a chave de verificação lida para verificar a informação de assinatura.

Com isto, a presente invenção é aplicável mesmo se existir uma pluralidade de diferentes dispositivos de distribuição.

[11-2] O dispositivo de execução pode não ter a unidade de armazenamento de chave de verificação e uma chave de assinatura e uma chave de verificação correspondendo à chave de assinatura pode ser armazenada na unidade de armazenamento de chave de assinatura do dispositivo de distribuição. Nesta situação, a unidade de gravação grava a chave de verificação junto ao DVD junto com a informação de assinatura.

[11-3] O dispositivo de distribuição pode armazenar, em adição à chave de assinatura e à chave de verificação, informação de autenticação da chave de verificação gerada por uma terceira pessoa imparcial. Aqui, pressupõe-se que a informação de autenticação é uma assinatura de chave gerada por se aplicar um algorítmo de geração de assinatura junto à chave de verificação com o uso de uma chave secreta da terceira parte.

A unidade de gravação grava a chave de verificação e a assinatura da chave no DVD junto com a informação de assinatura.

A unidade de armazenamento de chave de verificação do dispositivo de execução armazena a informação de verificação de chave, ao invés da chave de verificação. A informação de verificação de chave é informação para verificar a assinatura da chave e é, neste caso, uma chave pública emparelhada com a chave secreta da terceira pessoa imparcial que gerou a assinatura da chave.

A unidade de verificação de informação de assinatura recebe a assinatura da chave e a chave de verificação e executa a verificação da assinatura de chave por utilizar a chave recebida e a informação de verificação de chave. Somente quando a verificação é bem sucedida, a unidade de verificação de informação de assinatura começa a verificação da informação de assinatura como descrita nas modalidades acima.

Com isto, mesmo quando existem vários dispositivos de distribuição, o dispositivo de execução somente tem que manter a informação de verificação de chave da terceira parte e não tem que ter várias chaves de verificação.

[12] Na Modificação [1], o dispositivo de execução pode armazenar uma lista de anulação que indica chaves de verificação invalidadas. A unidade de verificação de informação de assinatura julga se os identificadores de chave recebidos ou a chave de verificação foram registrados na lista de anulação e aborta a verificação da informação de assinatura quando ela foi registrada.

[13] O dispositivo de execução pode adquirir a lista de anulação, descrita na Modificação [12], a partir de uma fonte externa. Por exemplo, a lista de anulação pode ser adquirida via um meio de gravação tal como DVD, ou pode ser recuperada via a Internet, difusão e assim por diante. Alternativamente, o dispositivo de execução pode periodicamente adquirir uma lista de anulação atualizada.

Com isto, a presente invenção é capaz de lidar com uma situação onde uma chave de verificação que precisou se invalidada é novamente encontrada.

[14] O dispositivo de distribuição distribui várias informações, tal como conteúdo criptografado e informação de assinatura, para o dispositivo de execução via o DVD. Entretanto, a presente invenção não está limitada ao DVD e a informação pode ser distribuída via: um disco óptico tal como CD-ROM e DVD-ROM; um disco óptico que pode ser gravado tal como CD-R, DVD-R e DVD-RAM; um disco óptico magnético; e um cartão de memória. Alternativamente, uma memória semicondutora, tal como uma memória

instantânea e um disco rígido, pode ser incorporada dentro do dispositivo de execução.

Adicionalmente, a presente invenção não está limitada a tal meio de gravação e a informação pode ser distribuída via sistemas de comunicação tal como uma Internet, ou pode ser distribuída via difusão.

[15] Apesar das modalidades e modificações acima descreverem pressupondo que o conteúdo é conteúdo de vídeo composto de imagens e áudio, o conteúdo pode ser um programa de computador. Por exemplo, pressupõe-se que o dispositivo de execução é um console de jogo; o conteúdo é um programa de computador armazenado em uma memória instantânea incorporada no console de jogo. Aqui, o programa de computador é um programa de julgamento para julgar se o software de jogo (tal como um disco óptico ou cartão de memória) carregado no console de jogo é software válido. Nesta situação, mesmo se um usuário não autorizado falsificar o programa de julgamento de modo a permitir a execução de software de jogo não autorizado, a presente invenção é capaz de detectar a falsificação por executar a verificação de se conteúdo não autorizado está incluído com o uso da informação de assinatura e da informação de cabeçalho e assim, a execução do próprio programa de julgamento é impedida ou abortada. Assim, por parar a própria execução, é possível impedir operações não autorizadas materializadas pelo programa de julgamento no qual falsificação não autorizada foi conduzida, a saber, impedir a execução de software de jogo não autorizado.

[16] Como descrito na modificação acima, no caso em que o conteúdo é um programa de computador armazenado em uma memória instantânea carregada em um microcomputador incorporado no dispositivo de execução, atos fraudulentos descritos na quinta modalidade podem acontecer. Especificamente falando, primeiro, um programa não autorizado é adicionado para o espaço livre da memória instantânea sem falsificação do programa de computador válido armazenado na memória instantânea envolvida. Então, um enchimento de memória temporária é causado por utilizar um erro de programação no programa de computador válido de modo que

um ponto inicial do programa salte para o cabeçalho do programa não autorizado adicionado e a execução do programa não autorizado é iniciada.

Aqui, atos fraudulentos mencionados acima podem ser impedidos pela gravação do conteúdo de enchimento na memória instantânea de modo a não deixar espaço livre na memória instantânea, como na quinta modalidade, desde que conteúdo não autorizado não pode ser adicionado.

Alternativamente, como na sexta modalidade, a informação de área indicando uma área onde informação válida gravada pelo dispositivo de distribuição está armazenada pode ser gravada na memória instantânea antecipadamente e o dispositivo de execução é projetado para não ler informação em áreas diferentes de uma área indicada pela informação de área. Desse modo, mesmo quando um programa não autorizado é adicionado, o dispositivo de execução não executa o programa não autorizado.

[17] A primeira até a sexta modalidades acima e as modificações descritas pressupõem-se que a unidade de execução é um componente que executa o conteúdo composto de vídeo e áudio, entretanto, a unidade de execução pode ser um componente que emite o conteúdo para um meio de gravação externo, ou um componente que possui uma função de impressão e imprime dados de imagem em papel e assim por diante.

[18] Nas modalidades acima, a unidade de geração de chave de conteúdo gera uma chave de conteúdo cada vez que um conjunto de conteúdos é informado para o dispositivo de distribuição. Entretanto, a unidade de geração de chave de conteúdo pode pré-armazenar várias chaves de conteúdo e selecionar e emitir uma das chaves de conteúdo armazenadas.

[19] Nas modalidades acima, o dispositivo de execução é projetado para começar as verificações de informação de cabeçalho, de informação de assinatura e assim por diante quando um DVD é carregado no mesmo, entretanto, a presente invenção não está confinada a isto.

Por exemplo, o dispositivo de execução pode iniciar tais verificações quando sendo direcionado para executar a reprodução de acordo com as operações do botão do usuário, ou pode executar as verificações em intervalos regulares a partir de quando o DVD é carregado no mesmo.

[20] Na segunda e na terceira modalidades, não é indispensável que a informação de cabeçalho seja gravada no DVD.

Quando a informação de cabeçalho não é gravada no DVD, o dispositivo de execução extrai k pedaços de conteúdo parcial representativo baseado na informação de posição selecionada e calcula os valores hash de verificação por respectivamente designar os pedaços extraídos de conteúdo parcial representativo para uma função hash.

Então, o dispositivo de execução gera informação de verificação de assinatura por aplicar o algorítmo de verificação de assinatura V para um resultado combinado formado por se combinar os valores hash de verificação calculados, com o uso da chave de verificação. O dispositivo de execução verifica a informação de assinatura por comparar com a informação de verificação de assinatura gerada.

Neste caso, o dispositivo de execução não mais exige a unidade de verificação de informação de cabeçalho, o que leva a uma redução no tamanho do circuito do sistema de detecção. Em adição, a verificação de se conteúdo não autorizado está incluído pode ser completada ao mesmo tempo por se verificar a informação de assinatura.

[21] Na quarta modalidade, o dispositivo de execução 4600 verifica somente k pedaços dentre os c pedaços de valores hash parciais incluídos na informação de cabeçalho após a verificação da informação de assinatura executada pela unidade de verificação de informação de assinatura 4606 ter sido bem sucedida. Entretanto, tanto a informação de assinatura como a informação de cabeçalho podem ser verificadas com uma única verificação por se utilizar k pedaços de conteúdo parcial criptografado e a informação de cabeçalho.

Mais especificamente, o dispositivo de execução extrai k pedaços de conteúdo parcial criptografado a partir do conteúdo criptografado baseado na informação de posição de conteúdo e gera k pedaços de conteúdo parcial por decriptografar os k pedaços extraídos de conteúdo parcial criptografado. Então, o dispositivo de execução calcula valores hash parciais de substituição por respectivamente designar os k pedaços gerados de conteú-

do parcial para uma função hash.

A seguir, o dispositivo de execução substitui, dentre os c pedaços de valores hash parciais incluídos na informação de cabeçalho, os valores hash parciais correspondendo aos k pedaços selecionados de conteúdo parcial criptografado pelos valores hash parciais de substituição calculados.

O dispositivo de execução verifica a informação de assinatura por utilizar a chave de verificação e um resultado combinado formado por se combinar os valores hash parciais de substituição com os valores hash parciais incluídos na informação de cabeçalho substituída.

Neste caso, o dispositivo de execução não mais exige a unidade de verificação de informação de cabeçalho, o que resulta em uma redução no tamanho do circuito do sistema de detecção. Em adição, a verificação de se conteúdo não autorizado está incluído pode ser completada ao mesmo tempo por verificar a informação de assinatura.

[22] Na primeira até a sexta modalidades acima, gravados no DVD estão somente um conjunto de conteúdo criptografado e um pedaço de cada dentre a informação de assinatura e a informação de cabeçalho correspondendo a este conjunto de conteúdo criptografado. Entretanto, uma série de conjuntos diferentes de conteúdo criptografado junto com os pedaços de informação de cabeçalho e de assinatura respectivamente correspondendo a estes conjuntos podem ser ao invés disso armazenados.

Em adição, o DVD pode incluir somente um pedaço de informação de assinatura gerado baseado em todos os pedaços de informação de cabeçalho. Adicionalmente, o DVD pode incluir, além destes conjuntos de conteúdo criptografado, conteúdo que não exijam proteção de direito autoral, por exemplo, anúncios, uma tela de abertura, uma tela de menu e assim por diante. Esses conteúdo livres de proteção de direito autoral podem ser executados enquanto as verificações de informação de assinatura e de informação de cabeçalho são executadas.

[23] Na primeira até a sexta modalidades e nas modificações, quando pelo menos uma dentre a verificação de informação de assinatura e a verificação de informação de cabeçalho não é bem sucedida, o dispositivo

de execução pode armazenar um identificador de disco para identificar um DVD carregado na unidade de aquisição e um identificador de conteúdo para identificar um conjunto de conteúdo a ponto de ser executado.

Quando um DVD possuindo o mesmo identificador de disco que o identificador gravado é carregado, o dispositivo de execução aborta a reprodução do conteúdo. Alternativamente, quando sendo direcionado para executar um conjunto de conteúdos possuindo o mesmo identificador que o identificador gravado, o dispositivo de execução aborta a reprodução do conjunto de conteúdos.

[24] Na modalidades acima e nas modificações, quando pelo menos uma dentre a verificação de informação de assinatura e a verificação de informação de cabeçalho é mal sucedida, o dispositivo de execução aborta a reprodução do conteúdo e notifica ao usuário que o conteúdo não é autorizado, por exemplo, por exibir uma tela de notificação de erro no monitor. O comportamento operacional assumido pelo dispositivo de execução na hora da falha na verificação não está limitado a isto e os casos seguintes também podem ser considerados. Adicionalmente, as três modificações seguintes podem ser combinadas.

[24-1] Tanto o dispositivo de distribuição como o dispositivo de execução estão conectados com uma Internet. Quando pelo menos uma dentre a verificação de informação de assinatura e a verificação de informação de cabeçalho é mal sucedida, o dispositivo de execução notifica o dispositivo de distribuição da falha de verificação via uma Internet. Neste ponto, o dispositivo de execução também envia um identificador de conteúdo indicando o conteúdo cuja verificação foi mal sucedida.

O dispositivo de distribuição pré-armazena o identificador de conteúdo e uma data de criação do conteúdo indicado pelo identificador de conteúdo, associando estes dois um com o outro.

O dispositivo de distribuição recebe a notificação da falha de verificação e o identificador de conteúdo a partir do dispositivo de execução via uma Internet. O dispositivo de distribuição gera uma informação de permissão de reprodução indicando a permissão da reprodução de conteúdo ou

a informação de proibição de reprodução indicando a proibição da reprodução de acordo com uma data de criação correspondendo ao identificador de conteúdo recebido. Por exemplo, quando o identificador de conteúdo indica novo conteúdo menor do que a metade de um ano a partir da data de criação, o dispositivo de distribuição gera a informação de proibição de reprodução. Por outro lado, quando o identificador de conteúdo indica conteúdo antigo tendo sido ao redor da metade de um ano ou mais do que a data de criação, o dispositivo de distribuição gera a informação de permissão de reprodução.

A seguir, o dispositivo de distribuição envia a informação de permissão de reprodução gerada ou a informação de proibição de reprodução para o dispositivo de execução via uma Internet e o dispositivo de execução decriptografa e executa o conteúdo criptografado armazenado no DVD somente quando recebendo a informação de permissão de reprodução.

Pressupõe-se o caso onde o conteúdo já estava ao redor de um período de tempo estabelecido desde a liberação e uma demanda por conteúdo foi encontrada até alguma extensão e portanto, as vendas futuras do conteúdo são prognosticadas como não sendo muito significativas. Neste caso, a modificação acima permite estabelecer prioridade em relação aos interesses de um usuário que comprou o DVD por permitir ao usuário ver o conteúdo. Por outro lado, quando o conteúdo foi recentemente liberado, e as vendas futuras do conteúdo são esperadas de serem significativas, esta modificação permite estabelecer prioridade em relação aos direitos de um mantenedor de direito autoral por proibir a reprodução. A saber, a modificação é capaz de ajustar os interesses do usuário e os interesses do mantenedor do direito autoral.

Observe que um meio para decidir qual dentre a informação de permissão e a informação de proibição de reprodução é para ser enviada não está limitado a isto, e o dispositivo de distribuição pode armazenar, com respeito a cada conjunto de conteúdos, termos de permissão refletindo as intenções, por exemplo, do mantenedor do direito autoral do conjunto de

conteúdos e da agência de venda.

[24-2] Como já foi descrito, um meio gravando o conteúdo não está limitado ao DVD mas pode ser um meio de gravação que pode ser escrito várias vezes. Aqui, um cartão de memória equipado com uma memória instantânea é utilizado como um exemplo.

Quando a verificação da informação de assinara ou da informação de cabeçalho não é bem sucedida, o dispositivo de execução apaga parte ou toda a informação do conteúdo criptografado gravado no cartão de memória.

Com isto, é possível de forma confiável impedir o uso futuro do conteúdo não autorizado.

[24-3] No caso quando o conteúdo é dado de vídeo HD (Alta Definição), o dispositivo de execução executa os dados de vídeo após converter os mesmos para SD (definição padrão) se as verificação não for bem sucedida.

Quando o conteúdo é dados de áudio de som de alta qualidade (canal 5.1), o dispositivo de execução executa os dados de áudio após converter os mesmos para dados de áudio de som de qualidade padrão (canal 2) se a verificação for malsucedida.

Assim, por permitir a reprodução na condição de degradar a qualidade da reprodução, é possível ajustar a conveniência do usuário e os interesses do mantenedor de direito autoral até alguma extensão.

[25] Na segunda e terceira modalidades, o dispositivo de execução lê o bloco de chave, a informação de posição selecionada criptografada, a informação de cabeçalho, a informação de assinatura e o conteúdo criptografado quando o DVD é carregado no mesmo. Entretanto, o dispositivo de execução pode ler somente a informação requerida de acordo com o progresso do processamento de cada componente via a unidade de aquisição.

Por exemplo, o dispositivo de execução conseqüentemente lê: somente o bloco de chave quando o DVD é carregado; a informação de posição selecionada criptografada quando a geração da chave de conteúdo é completada; e a informação de assinatura e a informação de cabeçalho

quando a decriptografia da informação de posição selecionada criptografada é completada e então executa a verificação da informação de assinatura. Uma vez que a verificação da informação de assinatura seja completada, o dispositivo de execução lê k pedaços de blocos criptografados indicados pela informação de posição selecionada.

Além disso, na quarta modalidade, somente a informação requerida pode ser lida a medida que necessário de um modo similar.

[26] Na primeira modalidade, quando os i pedaços selecionados de unidades criptografadas são lidos, a velocidade da leitura pode ser aumentada por dispor a ordem da leitura como descrito abaixo.

Para facilidade de descrição, pressupõe-se aqui que i = 4 e o caso no qual quatro pedaços de unidades criptografadas são para ser lidos é considerado.

Em um disco óptico, tal como DVD, uma região para gravar dados se divide em parte e áreas em um padrão árvore-anel são respectivamente referidas como trilhas. Vários setores estão incluídos em cada trilha e os dados são lidos e gravados setor por setor. Um tamanho de um setor é, por exemplo, 512 bytes. Neste caso, pedaços dos dados almejados para leitura no DVD podem ser identificados utilizando os números de identificação de trilha, os números de identificação de setor, ou tamanhos de setor.

A Figura 71 apresenta uma configuração do DVD 1500 e uma estrutura da unidade de aquisição 1601. Áreas concêntricas na figura são trilhas.

Como apresentado na Figura 71, a unidade de aquisição 1601 possui uma parte de cabeçote (também referida como "captador") 1628 e um eixo de rotação 1629. O DVD 1500 é girado em uma direção no sentido horário pela rotação do eixo de rotação 1629. As setas com uma linha pontilhada na figura indicam a direção de rotação. Por especificar um número de identificação de trilha, número de identificação de setor ou um tamanho de setor, a unidade de aquisição 1601 move a parte de cabeçote 1628 e adquire um pedaço de dado almejado para leitura.

Em geral, é conhecido que mover a parte de cabeçote 1628 pa-

ra uma trilha onde um pedaço de leitura alvo de dados está armazenado exige tempo. Em outras palavras, conforme a distância de movimento no DVD a partir da circunferência interna para a externa ou da circunferência externa para a interna, leva-se um tempo mais longo para ler os dados.

Aqui, quatro unidades criptografadas "EU1_3", "EU3_1", "EU8_7" e "EU9_2" são alvos lidos e são armazenadas nas partes 1591, 1592, 1593 e 1594, respectivamente, no DVD 1500.

No DVD 1500, pressupõe-se que a parte de cabeçote 1628 está na localização apresentada na Figura 71.

Neste caso, de acordo com o procedimento descrito na primeira modalidade, a unidade de aquisição 1601 primeiro move a parte de cabeçote 1628 para uma trilha 1501 na qual a parte 1591 existe e lê a unidade criptografada "EU1_3" gravada na parte 1591. Então, a unidade de aquisição 1601 move a parte de cabeçote 1628 para uma trilha 1504 e lê a unidade criptografada "EU3_1" a partir da parte 1592. Então, de um modo similar, a unidade de aquisição 1601 move a parte de cabeçote 1628 para uma trilha 1502 para ler a unidade criptografada "EU8_7" na parte 1593 e subseqüentemente para uma trilha 1503 para ler a unidade criptografada "EU9_2" na parte 1594.

Assim, quando o procedimento descrito na primeira modalidade é seguido, a distância de movimento da parte de cabeçote 1628 torna-se longa e como resultado, ela leva um longo tempo para ler todas as unidades criptografadas.

Aqui, a ordem de leitura das quatro unidade criptografadas é altera de modo que a parte de cabeçote 1628 sempre se mova para a trilha mais próxima da qual ela está localizada no momento. A saber, a unidade de aquisição 1601 compra um número de trilha indicando uma localização da parte de cabeçote 1628 com números de setor e com números de trilha indicando localizações das partes 1591, 1592, 1593 e 1594 onde as quatro unidades criptografadas estão armazenadas. Então, a unidade de aquisição 1601 reorganiza a ordem dos números de setor e dos números de trilha adquiridos das quatro partes de modo que a parte de cabeçote 1628 pegue a

distância de movimento mais curta para a leitura e acesse cada parte na ordem reorganizada.

Com isto, o tempo requerido para a leitura de dados pode ser reduzido. Adicionalmente, no caso onde as unidades criptografadas a serem lidas estão localizadas na mesma trilha ou em trilhas próximas, a ordem de leitura pode ser alterada baseado na localização corrente da parte de cabeçote 1628 e nos números de setor indicando as partes nas quais unidades criptografadas individuais estão armazenadas.

Observe que um dispositivo para otimizar a ordem de leitura depende dos atributos operacionais do eixo de rotação e da parte de cabeçote da unidade de aquisição 1601 e portanto, o procedimento de otimização descrito aqui é meramente um exemplo. Por exemplo, o método de controle de rotação do disco óptico inclui um método de velocidade angular constante e um método de velocidade linear constante e as características de tal método podem ser levadas em consideração. Em adição, quando um disco rígido é utilizado ao invés de um disco óptico tal como o DVD, a disposição da ordem de leitura pode ser alcançada de um modo similar.

Além disso, na quinta e na sexta modalidade, a velocidade de leitura pode ser aperfeiçoada de um modo similar. Isto também é o caso com a Modificação [20] de acordo com a segunda até a quarta modalidades.

[27] Na primeira, quinta e sexta modalidades, o dispositivo de execução seleciona i pedaços de arquivos criptografados aleatoriamente e adicionalmente seleciona um pedaço de unidade criptografada a partir de cada um dos arquivos criptografados selecionados. Entretanto, o procedimento de seleção não está limitado a este e várias unidades criptografadas podem ser selecionadas a partir de um arquivo criptografado contanto que os pedaços selecionados totalizem i.

[28] Na primeira, quinta e sexta modalidades, pedaços "i" das unidades criptografadas selecionadas pelo dispositivo de execução podem ser preestabelecidos no dispositivo de execução, ou podem ser gravados no DVD.

A medida que o número de unidades criptografadas seleciona-

das "i" torna-se maior, a precisão da validação de se conteúdo não autorizado está incluído aumenta, enquanto a carga de processamento envolvida na verificação da informação de assinatura também aumenta.

Assim, o número "i" de unidades criptografadas a serem selecionadas é gravado no DVD e então o dispositivo de execução executa a verificação da informação de assinatura de acordo com o "i" adquirido a partir do DVD. Com isto, é possível refletir as intenções do produtor do DVD na verificação.

Adicionalmente, esta técnica também é aplicável para selecionar k pedaços de conteúdo parcial criptografado na quarta modalidade.

[29] Na primeira, quinta e sexta modalidades, a informação de assinatura é gerada por se aplicar um algorítmo de geração de assinatura para um resultado combinado formado por se combinar c pedaços de valores hash de arquivo. Entretanto, a informação de assinatura pode ser gerada por se calcular um valor hash combinado por adicionalmente designar o resultado combinado para uma função hash e aplicar o algorítmo de geração de assinatura para o valor hash combinado calculado.

[30] Na primeira, quinta e sexta modalidades, a informação de cabeçalho é composta de valores hash possuindo uma estrutura de duas camadas. Ou seja, a estrutura de duas camadas é constituída de: valores hash de unidade gerados a partir das respectivas unidade criptografadas; e valores hash de arquivo gerados a partir de m pedaços de valores hash de unidade gerados baseado no mesmo arquivo. Por outro lado, a informação de assinatura é composta de c pedaços de valores de arquivo hash de arquivo.

Ao invés disso, a informação de cabeçalho pode incluir valores hash possuindo uma estrutura de três camadas. Especificamente falando, a informação de cabeçalho inclui y pedaços de valores hash de arquivo combinados. Os y pedaços de valores hash de arquivo combinados são gerados por primeiro dividir c pedaços de valores hash de arquivo em y pedaços de grupos e individualmente designar resultados combinados, os quais são formados por se combinar valores hash de arquivo com respeito a cada gru-

po, com uma função hash. Neste caso, a informação de assinatura é gerada por se utilizar os y pedaços de valores hash de arquivo combinados.

Assim, por aumentar o número de camadas na estrutura, é possível reduzir a informação a ser lida a partir do DVD.

[31] Como foi descrito na quinta modalidade, algumas vezes é o caso em que um arquivo de ordem de reprodução apresentando a ordem de reprodução de conteúdos é armazenado em um DVD. Neste caso, o DVD pode incluir informação de assinatura para o arquivo de ordem de reprodução.

Com isto, como é descrito na quinta modalidade, mesmo se uma terceira pessoa não autorizada executar adição ou substituição de conteúdo não autorizado e falsificar o arquivo de ordem de reprodução, a falsificação será detectada por se verificar a informação de assinatura do arquivo de ordem de reprodução e desse modo o conteúdo não autorizado não será executado.

[32] Na terceira modalidade o total de pedaços de conteúdo parcial representativo que a unidade de seleção 3105 do dispositivo de distribuição 3100 seleciona a partir de um conjunto de conteúdos é (k x x) pedaços.

Neste caso, pode ser projetado que todos os c pedaços de conteúdo parcial sejam selecionados pelo menos uma vez como um pedaço de conteúdo parcial representativo. Com isto, no caso em que parte do conteúdo criptografado armazenado no DVD é substituído, é possível aumentar a precisão de detecção de conteúdo não autorizado.

[33] Na primeira, quinta e sexta modalidades, o dispositivo de distribuição grava a informação de seleção de unidade no DVD. Ao invés disso, o dispositivo de distribuição pode gravar, no DVD, informação de seleção de unidade criptografada gerada por se criptografar a informação de seleção de unidade com o uso da chave de conteúdo.

Adicionalmente, na quarta modalidade, o dispositivo de distribuição grava a informação de posição de conteúdo no DVD. Ao invés disso, o dispositivo de distribuição pode gravar, no DVD, a informação de posição de conteúdo criptografada gerada por se criptografar a informação de posição

de conteúdo com o uso da chave de conteúdo.

[34] Na primeira até a sexta modalidades e nas modificações, os valores hash de unidade são calculados por respectivamente designar unidades criptografadas para uma função hash, enquanto os valores hash parciais são calculados por respectivamente designar pedaços de conteúdo parcial para a função hash. Entretanto, cada um dos valores hash de unidade pode ser calculado a partir de um resultado combinado formado por se combinar um identificador correspondendo a uma unidade criptografada, um pedaço de informação de identificação e a unidade criptografada. De um modo similar, cada um dos valores hash parciais pode ser calculado a partir de um resultado combinado formado por se combinar um identificador correspondendo a um pedaço de conteúdo parcial, um pedaço de informação de identificação, e o pedaço de conteúdo parcial.

[35] Na quinta modalidade, o tamanho de dado do conteúdo de enchimento a ser gerado é o mesmo que a capacidade de enchimento. Entretanto, o tamanho de dado não está limitado a isto, contanto que o tamanho de dado possa deixar o espaço livre deixado no DVD suficientemente pequeno.

[36] Na primeira até a sexta modalidade, o dispositivo de execução executa o conteúdo por emitir os sinais de vídeo e de áudio para o monitor externo. Entretanto, o dispositivo de execução pode ter al monitor embutido.

[37] Parte ou todos os componentes constituindo os dispositivos individuais acima podem ser montados como um único sistema LSI (Integração em Grande Escala). O sistema LSI é um LSI ultramultifuncional produzido por se integrar vários componentes em um chip e mais especificamente, é um sistema de computador composto de um microprocessador, ROM, RAM e assim por diante. Um programa de computador é armazenado na RAM. O micro processador opera de acordo com o programa de computador e desse modo, o sistema LSI realiza sua função. Alternativamente, cada componente pode ser estruturado em um circuito integrado individual.

Apesar de ser referido aqui como um sistema LSI, também pode

ser referido como IC, LSI super LSI e ultra LSI, dependendo do grau de integração. Em adição, o método para montar circuitos integrados não está limitado ao LSI e um circuito de comunicação dedicado ou um processador de propósito geral pode ser utilizado para alcançar isto. Uma FPGA (Série de Portas de Campo Programáveis), a qual é programável após o LSI ser produzido, ou um processador reconfigurável, o qual permite a reconfiguração da conexão e dos parâmetros das células do circuito dentro do LSI, pode ser utilizado.

[38] A presente invenção pode ser um método para realizar o sistema de detecção de conteúdo não autorizado descrito acima. A presente invenção pode ser um programa de computador que executa o método por um computador, ou pode ser um sinal digital representando o programa de computador.

A presente invenção também pode ser alcançada por um meio de gravação legível por computador, tal como um disco flexível, um disco rígido, um CD-ROM (Disco Compacto – Memória Somente Para Leitura), disco MO (Magnético – Óptico), um DVD, um DVD-ROM (Disco Versátil Digital – Memória Somente Para Leitura), um DVD-RAM (Disco Versátil Digital – Memória de Acesso Aleatório), um BD (Disco blu-ray), ou uma memória semicondutora, na qual o programa de computador ou o sinal digital mencionado acima é gravado. A presente invenção também pode ser o programa de computador ou sinal digital gravado em tal meio de armazenamento.

A presente invenção também pode ser o programa de computador ou sinal digital a ser transmitido via redes, como representado por telecomunicações, comunicações com fios / sem fios e a Internet, ou via difusão de dados.

A presente invenção também pode ser um sistema de computador possuindo um microprocessador e memória, onde a memória armazena o programa de computador e o microprocessador opera de acordo com o programa de computador.

O programa de computador ou sinal digital pode ser gravado no meio de armazenamento acima e transferido para um sistema de computa-

dor independente, ou alternativamente, pode ser transferido para um sistema de computador independente via a rede acima. Então, o sistema de computador independente pode executar o programa de computador ou sinal digital.

[39] A presente invenção inclui uma estrutura na qual duas ou mais das modalidades e modificações acima são combinadas.

Aplicabilidade Industrial

A presente invenção é aplicável operacionalmente, continuamente e repetidamente, em industrias que produzem, vendem, transferem e utilizam conteúdo e também em industrias que fabricam, vendem e utilizam vários aparelhos elétricos para executar, editar e processar os conteúdos.

REIVINDICAÇÕES

1. Dispositivo de processamento de dados para utilizar um trabalho digital gravado em um meio de gravação que tem também gravados (i) uma pluralidade de valores de resumo de registro gerados a partir de uma pluralidade de blocos de dados que constituem o trabalho digital e (ii) dados de assinatura de registro gerados com base em parte ou em todos da pluralidade de valores de resumo de registro no mesmo, **caracterizado** por compreender:

uma unidade de utilização operável para utilizar o trabalho digital;

uma unidade de seleção operável para aleatoriamente selecionar um número predeterminado de blocos de dados a partir da pluralidade de blocos de dados;

uma unidade de cálculo operável para calcular um valor de resumo de cálculo com respeito a cada um dos blocos de dados selecionados;

uma unidade de leitura operável para ler pelo menos os valores de resumo de registro restantes, cada um dos quais corresponde a um dos blocos de dados não selecionados, dentre a pluralidade de valores de resumo de registro;

uma unidade de verificação de assinatura operável para verificar se o trabalho digital é válido ao utilizar os dados de assinatura de registro, os valores de resumo de cálculo e os valores de resumo de registro restantes; e

uma unidade de controle de uso operável para fazer com que a unidade de utilização pare de utilizar o trabalho digital quando a unidade de verificação de assinatura julgar que o trabalho digital não é válido.

2. Dispositivo de processamento de dados, de acordo com a reivindicação 1, **caracterizado** pelo fato de que a pluralidade de valores de resumo de registro inclui uma pluralidade de valores primários de resumo de registro, cada um dos quais é gerado para um da pluralidade de blocos de dados, e uma pluralidade de valores secundários de resumo de registro gerados a partir de dois ou mais da pluralidade de valores primários de resumo de registro, e os dados de assinatura de registro são gerados ao se executar uma assinatura digital na pluralidade de valores secundários de resumo de registro,

a unidade de leitura lê os valores de resumo de registro restantes dentre a pluralidade de valores primários de resumo de registro, e

a unidade de verificação de assinatura verifica a validade do trabalho digital ao calcular um ou mais valores secundários de resumo de cálculo com base nos valores de resumo de cálculo e nos valores de resumo de registro restantes, e executa uma verificação de assinatura digital com o uso dos dados de assinatura de registro, da pluralidade de valores secundários de resumo de registro, e dos valores secundários de resumo de cálculo.

3. Dispositivo de processamento de dados, de acordo com a reivindicação 2, **caracterizado** pelo fato de que o trabalho digital inclui uma pluralidade de arquivos, cada um dos quais corresponde a um da pluralidade de valores secundários de resumo de registro e é constituído por dois ou mais da pluralidade de blocos de dados,

cada um da pluralidade de valores secundários de resumo de registro é gerado ao se utilizar os valores primários de resumo de registro correspondendo um para um com os dois ou mais da pluralidade de blocos de dados constituindo um arquivo correspondendo ao valor secundário de resumo de registro,

a unidade de verificação de assinatura incluindo

uma subunidade primária de leitura operável para ler os dados de assinatura de registro a partir do meio de gravação;

uma subunidade de cálculo operável para calcular um valor secundário de resumo de cálculo, com respeito a cada arquivo incluindo pelo menos um dos blocos de dados selecionados, ao utilizar valores primários de resumo de registro correspondendo aos blocos de dados não selecionados incluídos no arquivo e os valores de resumo de cálculo correspondendo aos blocos de dados selecionados;

uma subunidade secundária de leitura operável para ler, com respeito a cada arquivo não incluindo blocos de dados selecionados, um valor secundário de resumo de registro correspondendo ao arquivo;

uma subunidade de assinatura operável para gerar dados de assinatura de cálculo por executar a assinatura digital com o uso dos valores

secundários de resumo de cálculo calculados e os valores secundários de resumo de registro lidos; e

uma subunidade de comparação operável para comparar os dados de assinatura de cálculo com os dados de assinatura de registro, e

a unidade de verificação de assinatura verifica que o trabalho digital é válido quando os dados de assinatura de cálculo e os dados de assinatura de registro estão de acordo um com o outro, e julga que o trabalho digital não é válido quando os dados de assinatura de cálculo e os dados de assinatura de registro não estão de acordo um com o outro.

4. Dispositivo de processamento de dados, de acordo com a reivindicação 3, **caracterizado** pelo fato de que a pluralidade de valores de resumo de registro são valores hash, cada um gerado por uma função hash,

os valores de resumo de cálculo calculados pela unidade de cálculo são valores hash calculados pela aplicação da função hash junto a cada um dos blocos de dados selecionados, e

os valores secundários de resumo de cálculo calculados pela subunidade de cálculo são valores hash calculados pela aplicação da função hash junto aos valores primários de resumo de registro correspondendo aos blocos de dados não selecionados e aos valores de resumo de cálculo.

5. Dispositivo de processamento de dados, de acordo com a reivindicação 3, **caracterizado** pelo fato de que o trabalho digital é conteúdo digital e a unidade de utilização utiliza o conteúdo digital ao reproduzir o conteúdo digital.

6. Dispositivo de processamento de dados, de acordo com a reivindicação 3, **caracterizado** pelo fato de que o trabalho digital é um programa de computador e a unidade de utilização utiliza o programa de computador ao decodificar os códigos de instrução constituindo o programa de computador e ao operar de acordo com os códigos decodificados.

7. Dispositivo de processamento de dados, de acordo com a reivindicação 3, **caracterizado por** compreender, ao invés da unidade de controle de uso:

uma unidade de exibição de advertência operável para exibir,

quando o trabalho digital é julgado como não sendo válido, uma notificação de invalidade do trabalho digital.

8. Dispositivo de processamento de dados, de acordo com a reivindicação 1, **caracterizado** pelo fato de que o meio de gravação possui adicionalmente gravado:

(i) informação de área indicando uma área de acesso permitido, no meio de gravação, a qual um dispositivo externo é permitido de acessar e

(ii) dados de assinatura gerados com base em parte ou em todo o trabalho digital e na informação de área, e o dispositivo de processamento de dados adicionalmente compreende:

uma unidade de proibição de acesso operável para proibir o acesso às áreas que não sejam a área com acesso permitido baseado na informação de área; e

uma unidade de verificação operável para verificar se o trabalho digital e a informação de área são válidos ao utilizar o trabalho digital, a informação de área e os dados de assinatura, e

a unidade de controle de uso operável para fazer com que a unidade pare de utilizar o trabalho digital quando a unidade de verificação julgar que pelo menos um dentre o trabalho digital e a informação de área não é válido.

9. Dispositivo de processamento de dados, de acordo com a reivindicação 1, **caracterizado** pelo fato de que a unidade de seleção, a unidade de cálculo, a unidade de leitura e a unidade de verificação de assinatura são montadas juntas em uma integração única de larga escala.

10. Dispositivo de processamento de dados, de acordo com a reivindicação 1, **caracterizado** pelo fato de que

a unidade de leitura adicionalmente lê os valores de resumo de gravação correspondentes aos blocos de dados selecionados do meio de gravação, e

dispositivo de processamento de dados compreende adicionalmente:

uma unidade de verificação de valor de resumo operável para

verificar se os valores de resumo de gravação gravados no meio de gravação e os valores de resumo de cálculo combinam um com o outro; e

uma unidade de controle de 2º uso operável para parar a unidade de utilização da utilização do trabalho digital quando o trabalho digital for julgado como inválido de acordo com um resultado da verificação pela unidade de verificação de valor de resumo.

11. Meio de gravação **caracterizado** por possuir gravado no mesmo:

um trabalho digital;

uma pluralidade de valores de resumo gravados gerados a partir de uma pluralidade de blocos de dados constituindo o trabalho digital; e

dados de assinatura gravados gerados baseados na pluralidade de valores de resumo.

12. Meio de gravação de acordo com a reivindicação 11, **caracterizado** por ser utilizado com o dispositivo de processamento de dados como definido na reivindicação 1 e prover o dispositivo de processamento de dados com o trabalho digital, os valores de resumo de gravação e dados de assinatura de gravação.

13. Método de processamento de dados para utilizar um trabalho digital gravado em um meio de gravação possuindo também gravado (i) uma pluralidade de valores de resumo de registro gerados a partir de uma pluralidade de blocos de dados constituindo o trabalho digital e (ii) dados de assinatura de registro gerados com base em parte ou em todos da pluralidade de valores de resumo de registro no mesmo, **caracterizado** por compreender as etapas de:

(a) utilizar o trabalho digital;

(b) aleatoriamente selecionar um número predeterminado de blocos de dados a partir da pluralidade de blocos de dados;

(c) calcular um valor de resumo de cálculo com respeito a cada um dos blocos de dados selecionados;

(d) ler pelo menos os valores de resumo de registro restantes, cada um dos quais corresponde a um dos blocos de dados não selecionados

dentre a pluralidade de valores de resumo de registro;

(e) verificar se o trabalho digital é válido ao utilizar os dados de assinatura de registro, os valores de resumo de cálculo e os valores de resumo de registro restantes; e

(f) para a etapa (a) quando o trabalho digital for julgado como não sendo válido na etapa (e).

14. Programa de processamento de dados para utilizar um trabalho digital gravado em um meio de gravação possuindo também gravado (i) uma pluralidade de valores de resumo de registro gerados a partir de uma pluralidade de blocos de dados constituindo o trabalho digital e (ii) dados de assinatura de registro gerados com base em parte ou em todos da pluralidade de valores de resumo de registro no mesmo, **caracterizado** por compreender as etapas de:

(a) utilizar o trabalho digital;

(b) aleatoriamente selecionar um número predeterminado de blocos de dados a partir da pluralidade de blocos de dados;

(c) calcular um valor de resumo de cálculo com respeito a cada um dos blocos de dados selecionados;

(d) ler pelo menos os valores de resumo de registro restantes, cada um dos quais corresponde a um dos blocos de dados não selecionados dentre a pluralidade de valores de resumo de registro;

(e) verificar se o trabalho digital é válido ao utilizar os dados de assinatura de registro, os valores de resumo de cálculo e os valores de resumo de registro restantes; e

(f) para a etapa (a) quando o trabalho digital for julgado como não sendo válido na etapa (e).

15. Programa de processamento de dados, de acordo com a reivindicação 14, **caracterizado** por ser gravado em um meio de gravação legível por computador.

16. Programa de processamento de dados, de acordo com a reivindicação 14, **caracterizado** por ser transmitido e recebido via telecomunicações.

FIG. 1

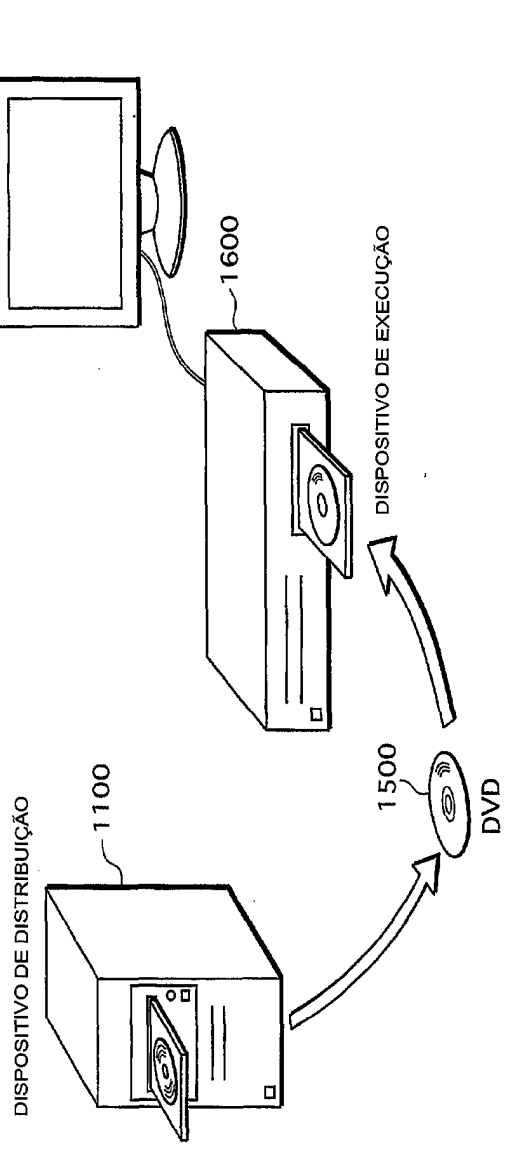

1
MONITOR
1620
1600
DISPOSITIVO DE EXECUÇÃO
1500
DVD
1100
DISPOSITIVO DE DISTRIBUIÇÃO

FIG.2

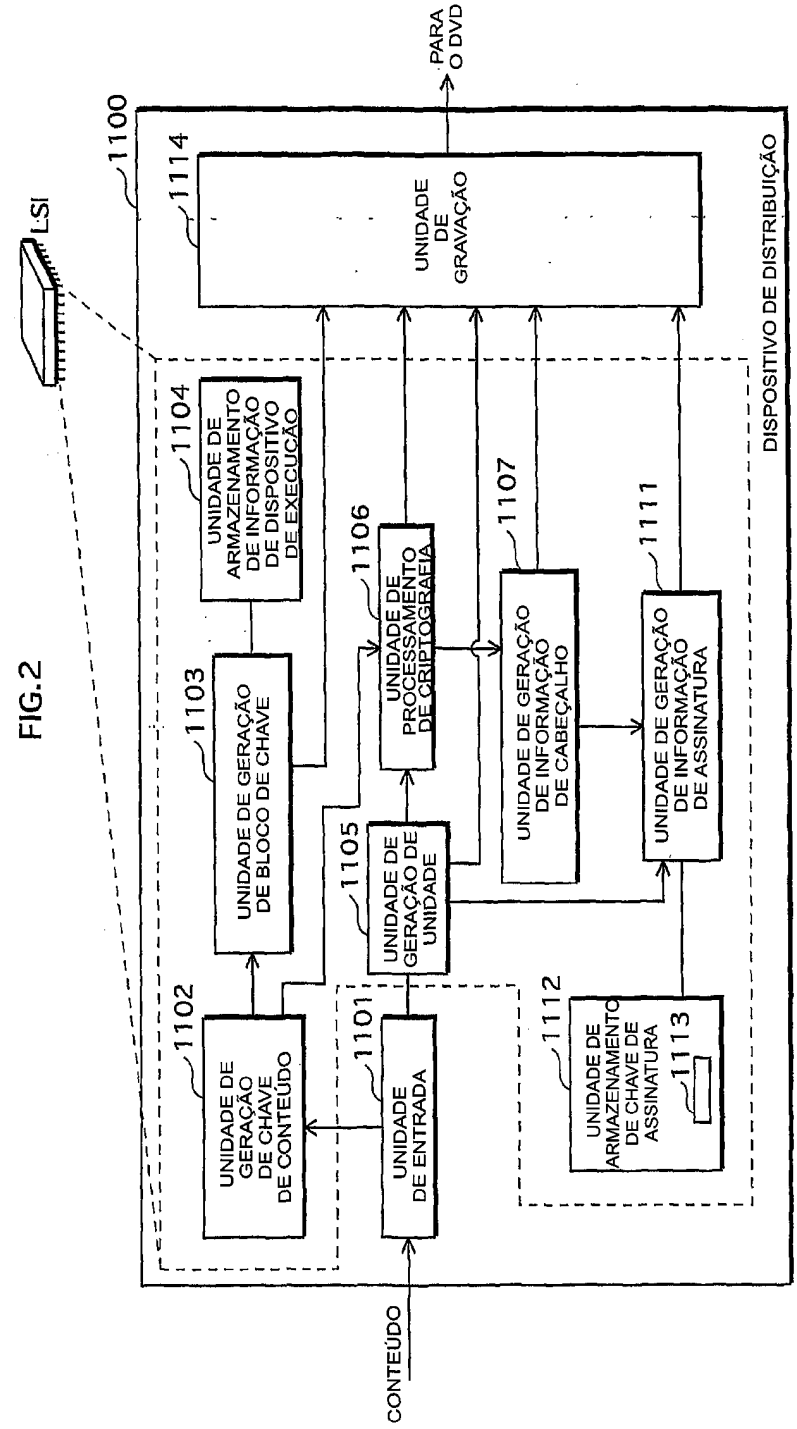

1100
LSI
1114
UNIDADE DE GRAVAÇÃO
PARA O DVD
DISPOSITIVO DE DISTRIBUIÇÃO
1104
UNIDADE DE ARMAZENAMENTO DE INFORMAÇÃO DE DISPOSITIVO DE EXECUÇÃO
1103
UNIDADE DE GERAÇÃO DE BLOCO DE CHAVE
1106
UNIDADE DE PROCESSAMENTO DE CRIPTOGRAFIA
1107
UNIDADE DE GERAÇÃO DE INFORMAÇÃO DE CABEÇALHO
1111
UNIDADE DE GERAÇÃO DE INFORMAÇÃO DE ASSINATURA
1102
UNIDADE DE GERAÇÃO DE CHAVE DE CONTEÚDO
1105
UNIDADE DE GERAÇÃO DE UNIDADE
1101
UNIDADE DE ENTRADA
1112
UNIDADE DE ARMAZENAMENTO DE CHAVE DE ASSINATURA
1113
CONTEÚDO

FIG.3

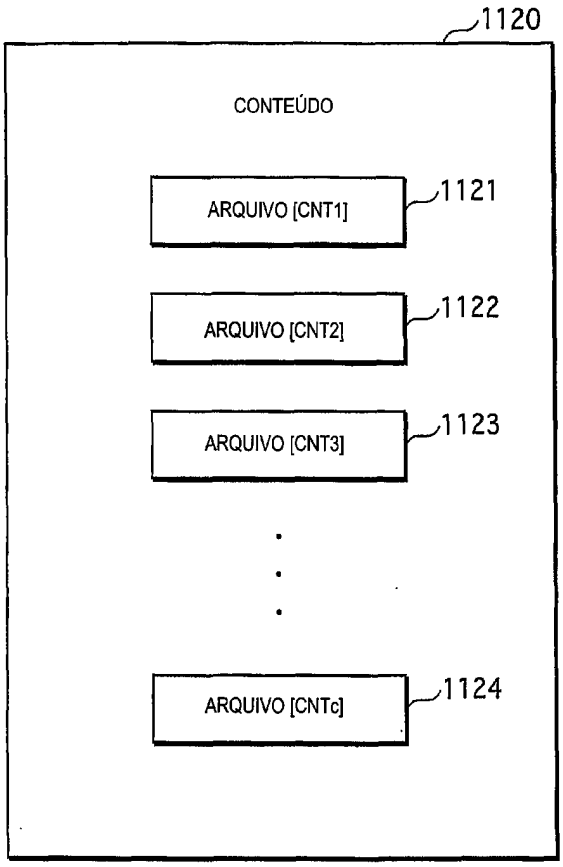

1120
CONTEÚDO
ARQUIVO [CNT1]
1121
ARQUIVO [CNT2]
1122
ARQUIVO [CNT3]
1123
ARQUIVO [CNTc]
1124

FIG.4

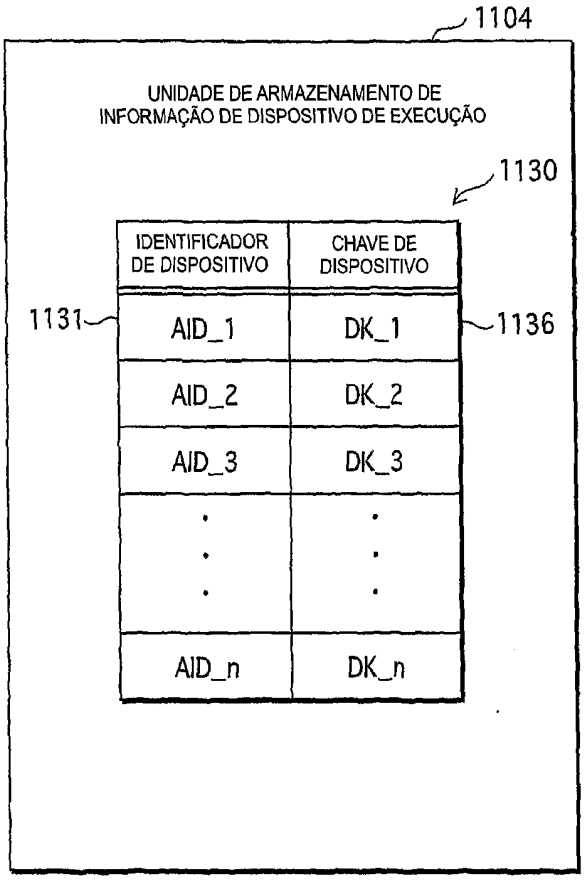

1104
UNIDADE DE ARMAZENAMENTO DE INFORMAÇÃO DE DISPOSITIVO DE EXECUÇÃO
1130
IDENTIFICADOR DE DISPOSITIVO
CHAVE DE DISPOSITIVO
1131
1136
AID_1
DK_1
AID_2
DK_2
AID_3
DK_3
AID_n
DK_n

FIG.5

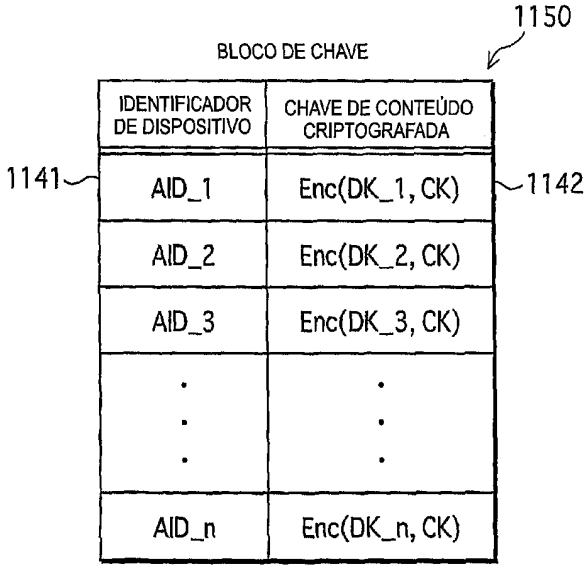

1150
BLOCO DE CHAVE
IDENTIFICADOR DE DISPOSITIVO
CHAVE DE CONTEÚDO CRIPTOGRAFADA
1141
1142
AID_1
Enc(DK_1, CK)
AID_2
Enc(DK_2, CK)
AID_3
Enc(DK_3, CK)
AID_n
Enc(DK_n, CK)

FIG.6

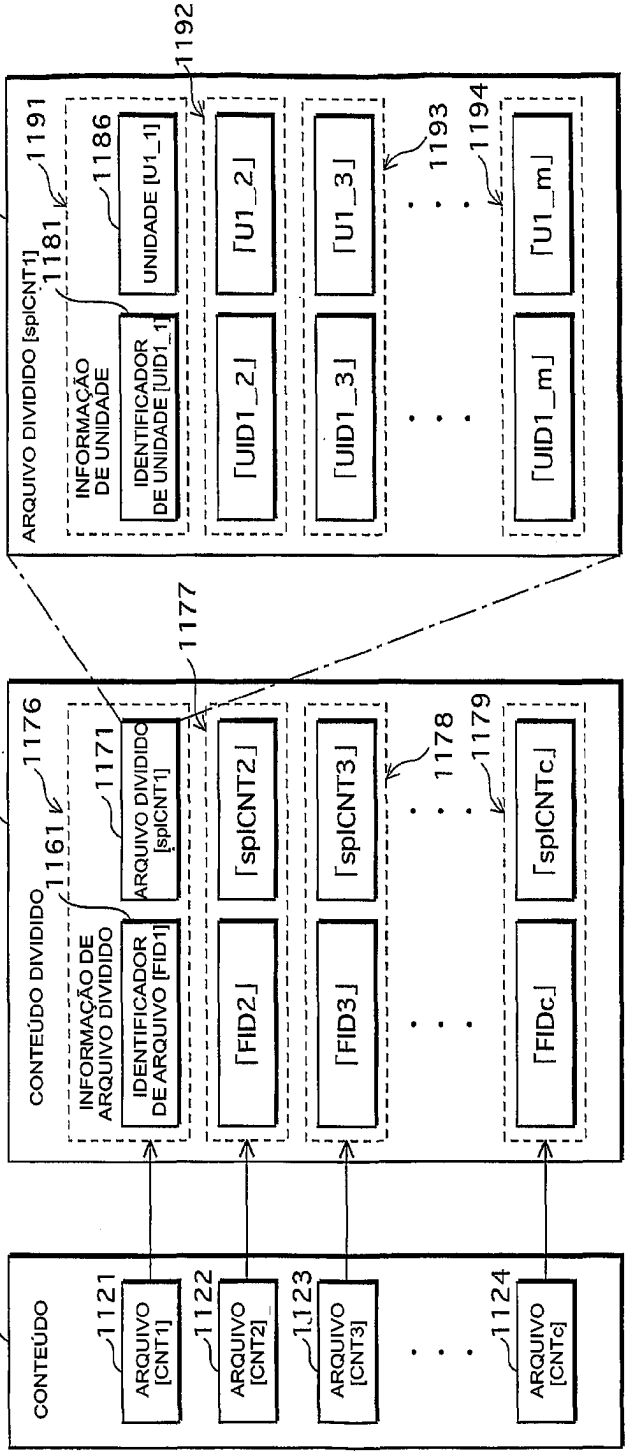

1120
CONTEÚDO
1121
ARQUIVO [CNT1]
1122
ARQUIVO [CNT2]
1123
ARQUIVO [CNT3]
1124
ARQUIVO [CNTc]
1160
1176
CONTEÚDO DIVIDIDO
1161
INFORMAÇÃO DE ARQUIVO DIVIDIDO
IDENTIFICADOR DE ARQUIVO [FID1]
1171
ARQUIVO DIVIDIDO [splCNT1]
1177
「FID2」
「splCNT2」
「FID3」
「splCNT3」
1178
1179
「FIDc」
「splCNTc」
1171
ARQUIVO DIVIDIDO [splCNT1]
1191
INFORMAÇÃO DE UNIDADE
1181
IDENTIFICADOR DE UNIDADE [UID1_1]
1186
UNIDADE [U1_1]
1192
「UID1_2」
「U1_2」
「UID1_3」
「U1_3」
1193
1194
「UID1_m」
「U1_m」

FIG.7

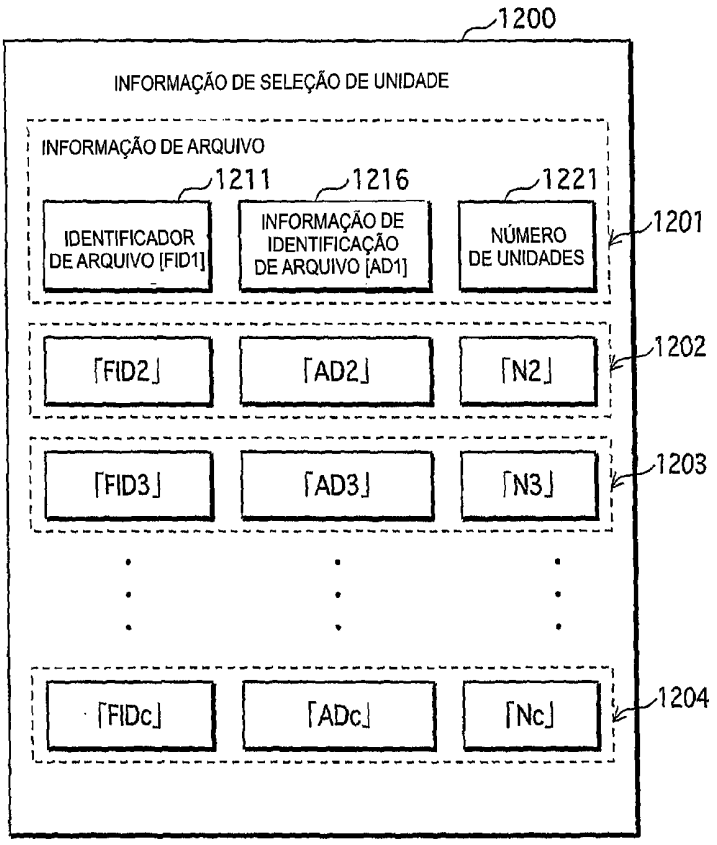

1200
INFORMAÇÃO DE SELEÇÃO DE UNIDADE
INFORMAÇÃO DE ARQUIVO
1211
1216
1221
IDENTIFICADOR DE ARQUIVO [FID1]
INFORMAÇÃO DE IDENTIFICAÇÃO DE ARQUIVO [AD1]
NÚMERO DE UNIDADES
1201
「FID2」
「AD2」
「N2」
1202
「FID3」
「AD3」
「N3」
1203
「FIDc」
「ADc」
「Nc」
1204

FIG.8

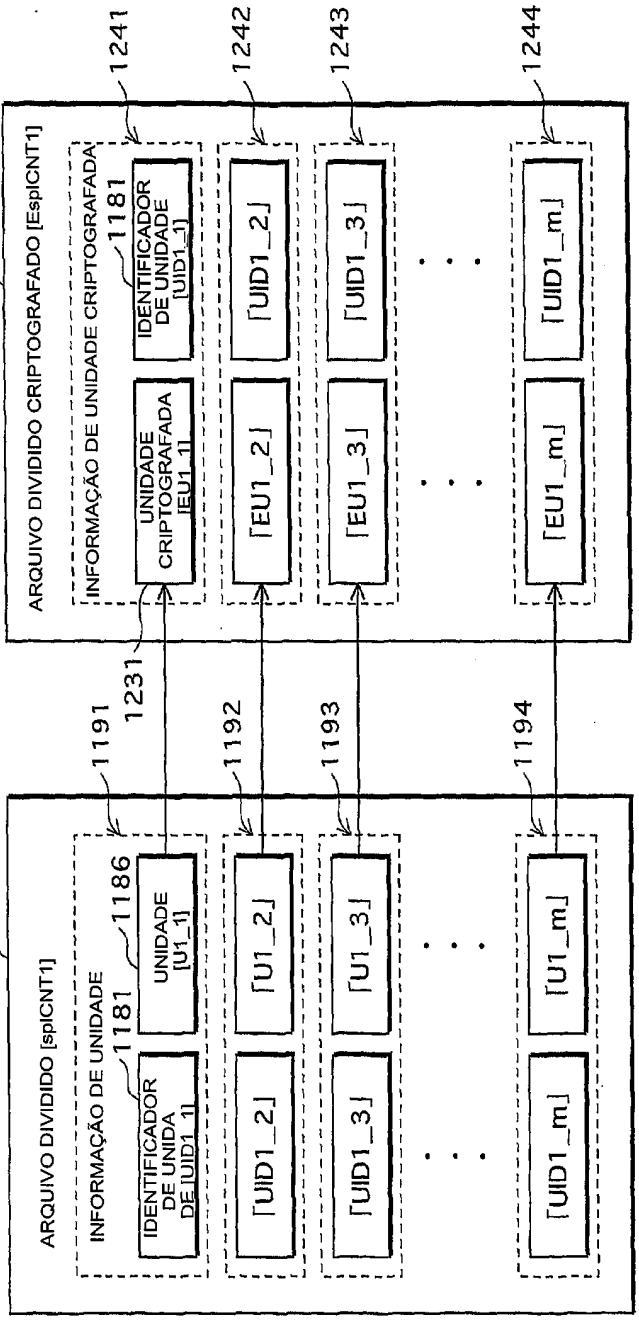

1171
ARQUIVO DIVIDIDO [splCNT1]
INFORMAÇÃO DE UNIDADE
1181
IDENTIFICADOR DE UNIDA DE [UID1_1]
1186
UNIDADE [U1_1]
1191
1231
1192
1193
1194
「U1_2」
「U1_3」
「U1_m」
「UID1_2」
「UID1_3」
「UID1_m」
1251
ARQUIVO DIVIDIDO CRIPTOGRAFADO [EsplCNT1]
INFORMAÇÃO DE UNIDADE CRIPTOGRAFADA
1181
IDENTIFICADOR DE UNIDADE [UID1_1]
UNIDADE CRIPTOGRAFADA [EU1_1]
1241
1242
1243
1244
「EU1_2」
「EU1_3」
「EU1_m」
「UID1_2」
「UID1_3」
「UID1_m」

FIG.9

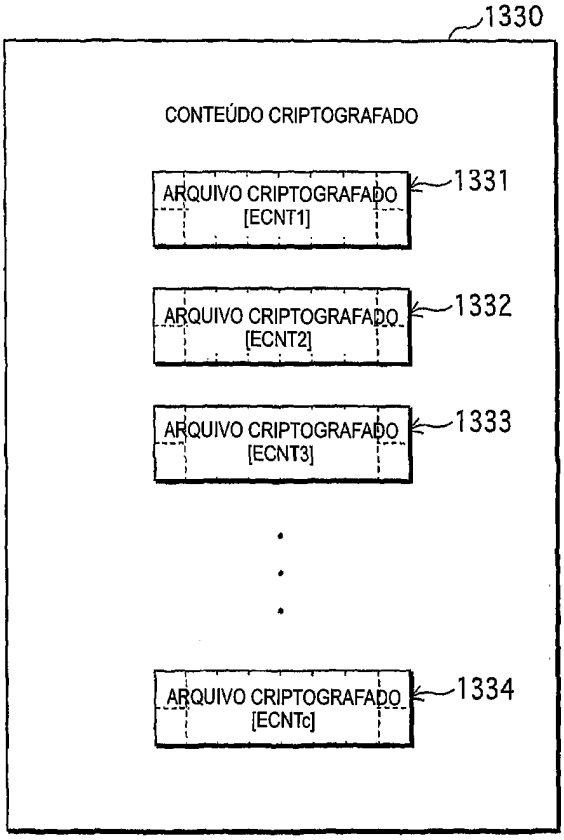

1330
CONTEÚDO CRIPTOGRAFADO
ARQUIVO CRIPTOGRAFADO [ECNT1]
1331
ARQUIVO CRIPTOGRAFADO [ECNT2]
1332
ARQUIVO CRIPTOGRAFADO [ECNT3]
1333
ARQUIVO CRIPTOGRAFADO [ECNTc]
1334

FIG.10

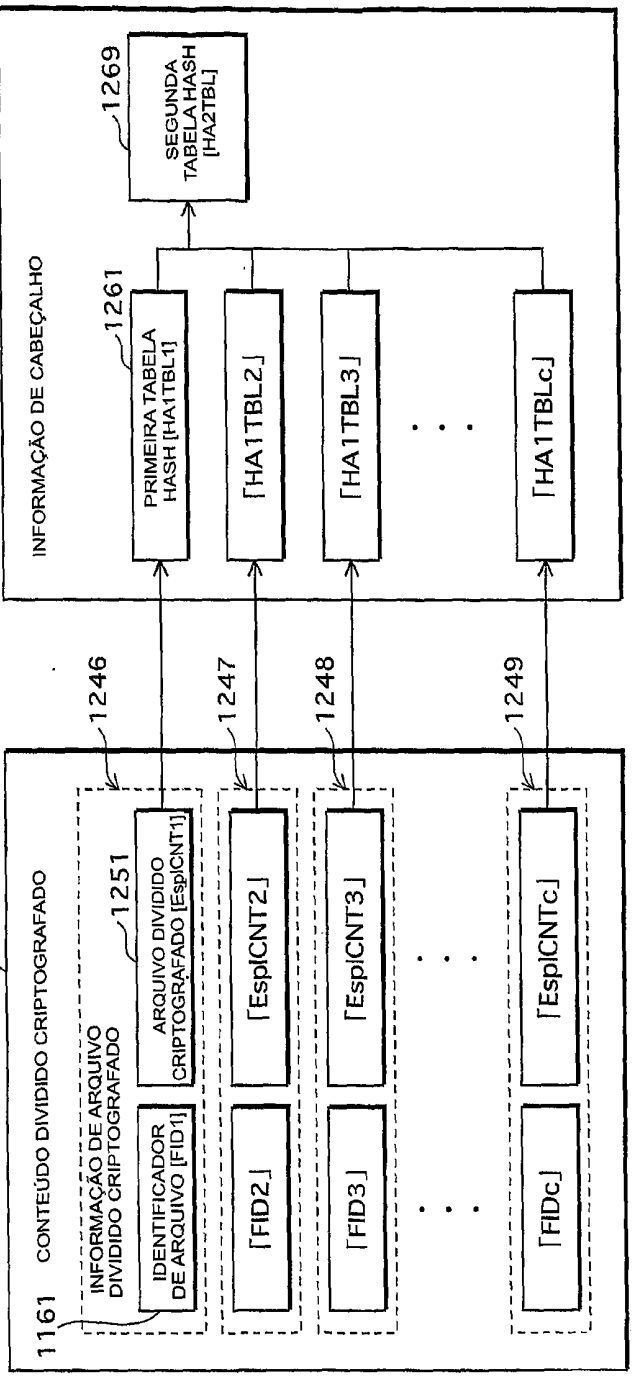

1210
CONTEÚDO DIVIDIDO CRIPTOGRAFADO
1161
INFORMAÇÃO DE ARQUIVO DIVIDIDO CRIPTOGRAFADO
IDENTIFICADOR DE ARQUIVO [FID1]
1251
ARQUIVO DIVIDIDO CRIPTOGRAFADO [EspICNT1]
1246
1247
1248
1249
「FID2」
「FID3」
「FIDc」
「EspICNT2」
「EspICNT3」
「EspICNTc」
1260
INFORMAÇÃO DE CABEÇALHO
1261
PRIMEIRA TABELA HASH [HA1TBL1]
1269
SEGUNDA TABELA HASH [HA2TBL]
「HA1TBL2」
「HA1TBL3」
「HA1TBLc」

FIG.11

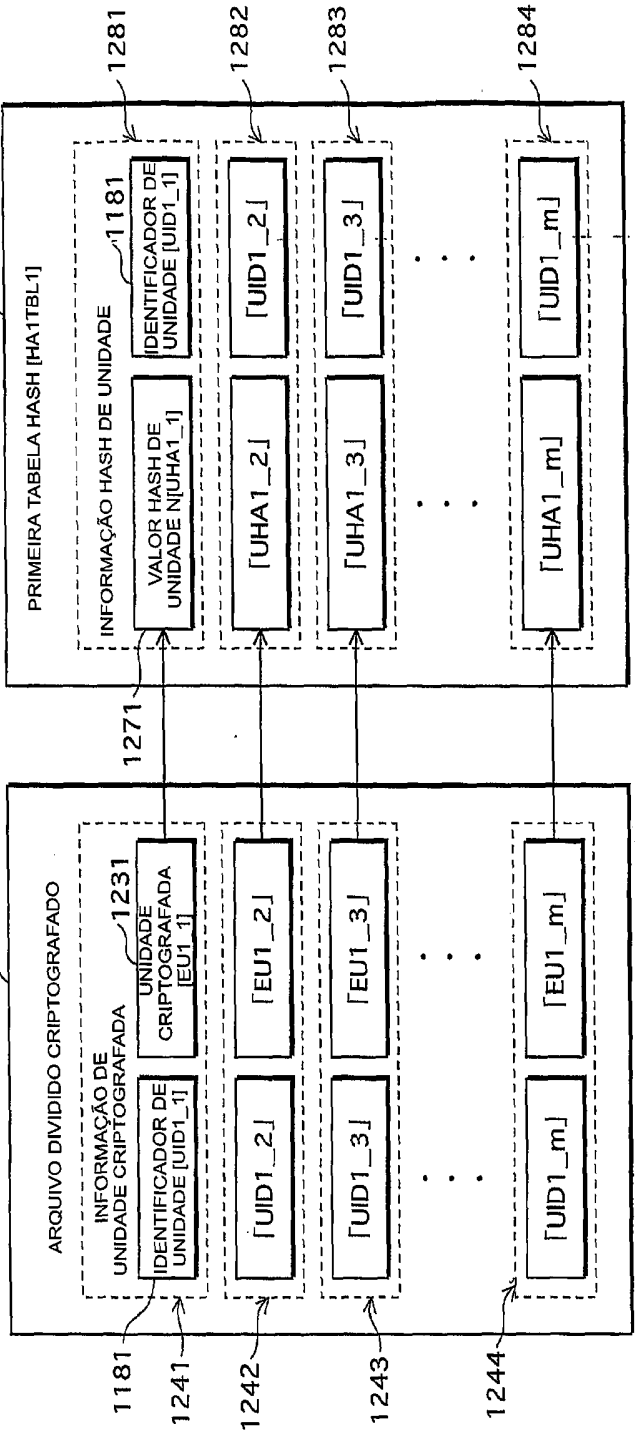

1251
ARQUIVO DIVIDIDO CRIPTOGRAFADO
INFORMAÇÃO DE UNIDADE CRIPTOGRAFADA
IDENTIFICADOR DE UNIDADE [UID1_1]
1231
UNIDADE CRIPTOGRAFADA [EU1_1]
「UID1_2」
「EU1_2」
「UID1_3」
「EU1_3」
「UID1_m」
「EU1_m」
1181
1241
1242
1243
1244
1271
1261
PRIMEIRA TABELA HASH [HA1TBL1]
INFORMAÇÃO HASH DE UNIDADE
1181
IDENTIFICADOR DE UNIDADE [UID1_1]
VALOR HASH DE UNIDADE N[UHA1_1]
「UHA1_2」
「UHA1_3」
「UHA1_m」
1281
1282
1283
1284

FIG.12

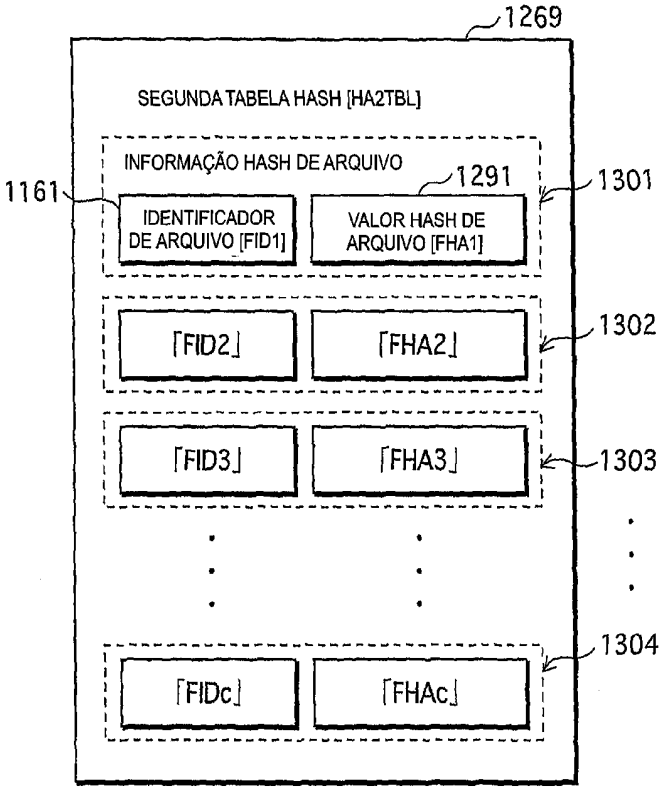

1269
SEGUNDA TABELA HASH [HA2TBL]
INFORMAÇÃO HASH DE ARQUIVO
1161
1291
1301
IDENTIFICADOR DE ARQUIVO [FID1]
VALOR HASH DE ARQUIVO [FHA1]
1302
「FID2」
「FHA2」
1303
「FID3」
「FHA3」
1304
「FIDc」
「FHAc」

FIG.13

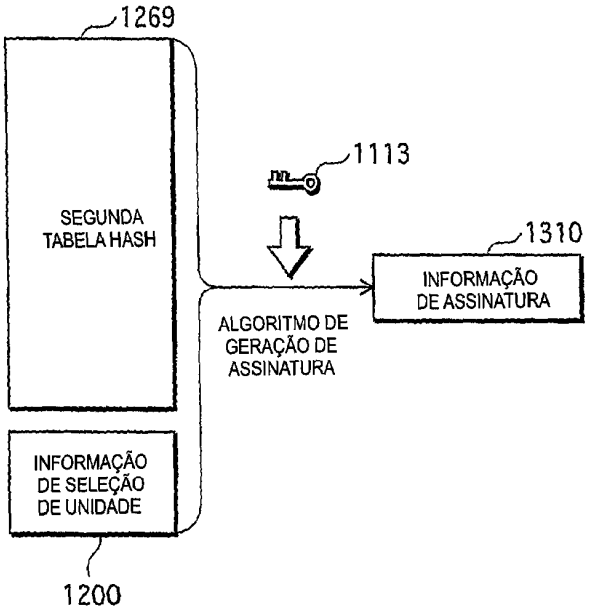

1269
SEGUNDA TABELA HASH
1113
1310
INFORMAÇÃO DE ASSINATURA
ALGORITMO DE GERAÇÃO DE ASSINATURA
INFORMAÇÃO DE SELEÇÃO DE UNIDADE
1200

FIG.14

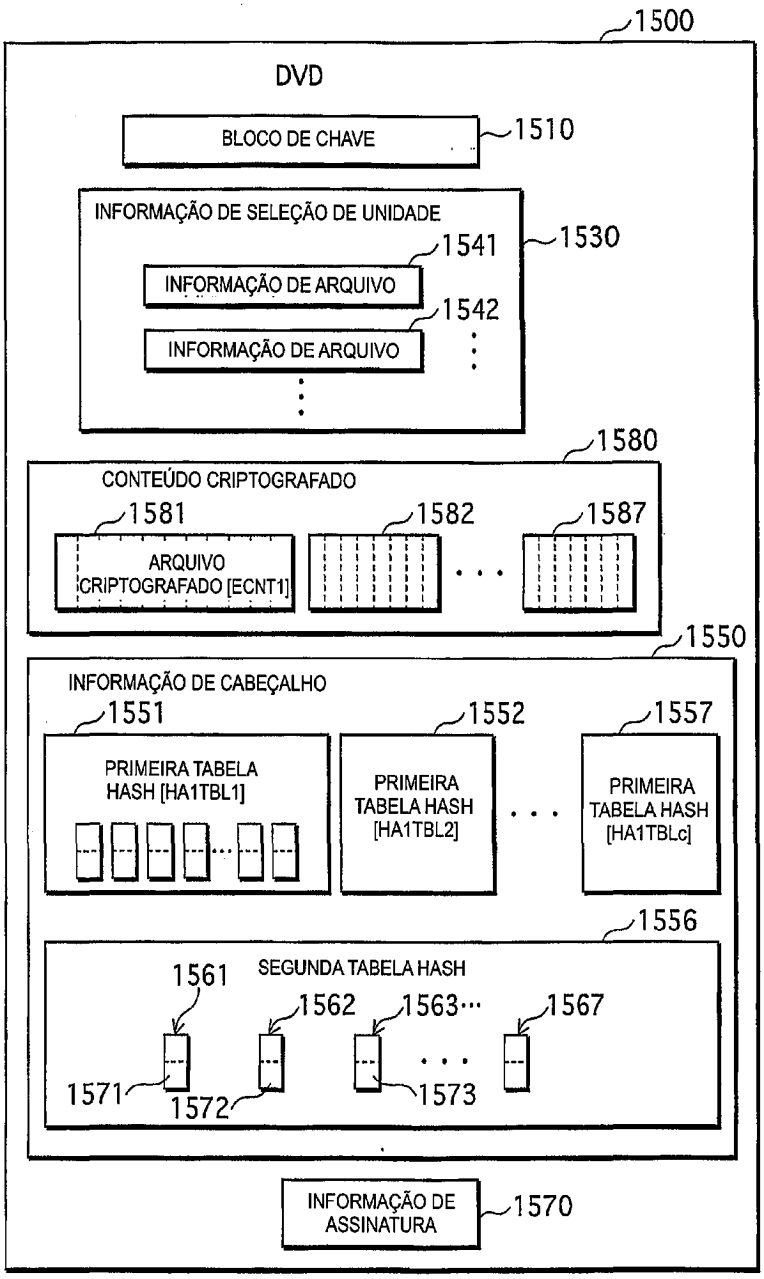

1500
DVD
BLOCO DE CHAVE
1510
INFORMAÇÃO DE SELEÇÃO DE UNIDADE
1530
1541
INFORMAÇÃO DE ARQUIVO
1542
INFORMAÇÃO DE ARQUIVO
1580
CONTEÚDO CRIPTOGRAFADO
1581
1582
1587
ARQUIVO CRIPTOGRAFADO [ECNT1]
1550
INFORMAÇÃO DE CABEÇALHO
1551
1552
1557
PRIMEIRA TABELA HASH [HA1TBL1]
PRIMEIRA TABELA HASH [HA1TBL2]
PRIMEIRA TABELA HASH [HA1TBLc]
1556
1561
SEGUNDA TABELA HASH
1562
1563
1567
1571
1572
1573
INFORMAÇÃO DE ASSINATURA
1570

FIG.15

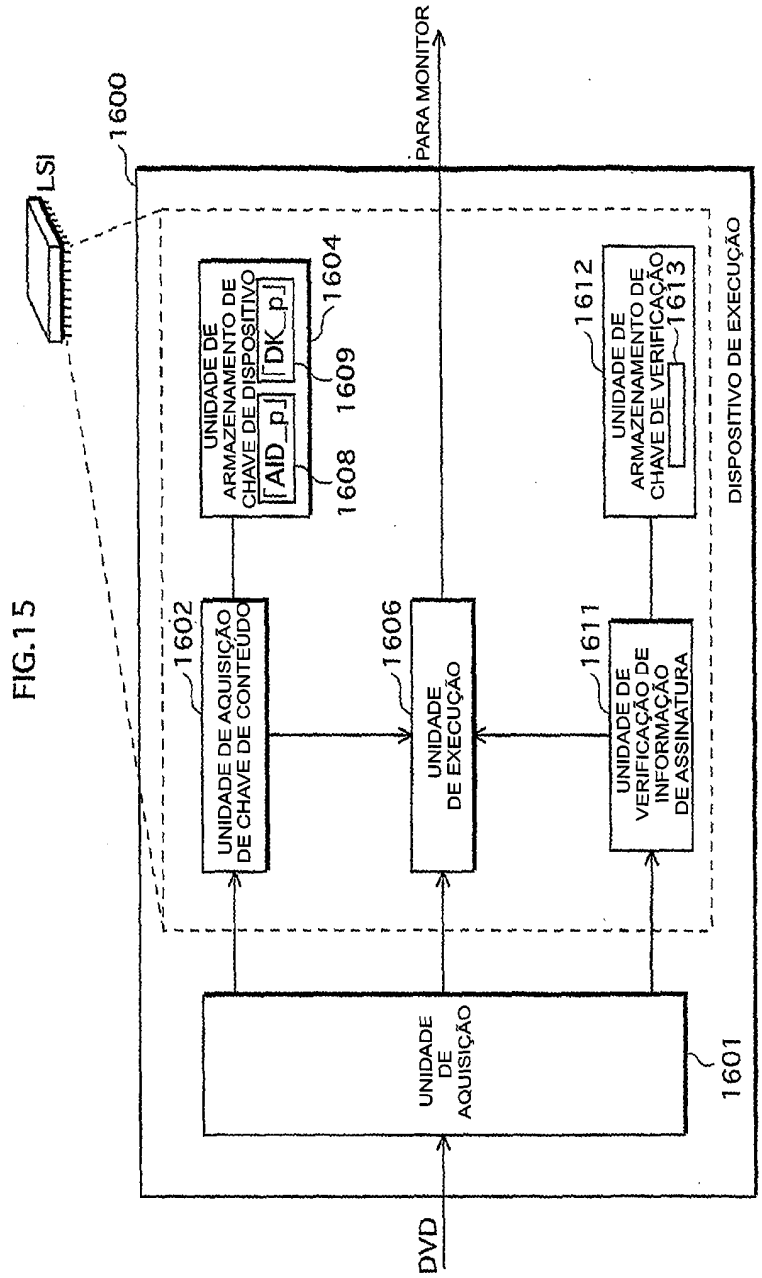

1600
LSI
PARA MONITOR
DISPOSITIVO DE EXECUÇÃO
UNIDADE DE ARMAZENAMENTO DE CHAVE DE DISPOSITIVO
AID_pJ
DK_pJ
1604
1609
1608
1612
UNIDADE DE ARMAZENAMENTO DE CHAVE DE VERIFICAÇÃO
1613
1602
UNIDADE DE AQUISIÇÃO DE CHAVE DE CONTEÚDO
1606
UNIDADE DE EXECUÇÃO
1611
UNIDADE DE VERIFICAÇÃO DE INFORMAÇÃO DE ASSINATURA
UNIDADE DE AQUISIÇÃO
1601
DVD

FIG.16

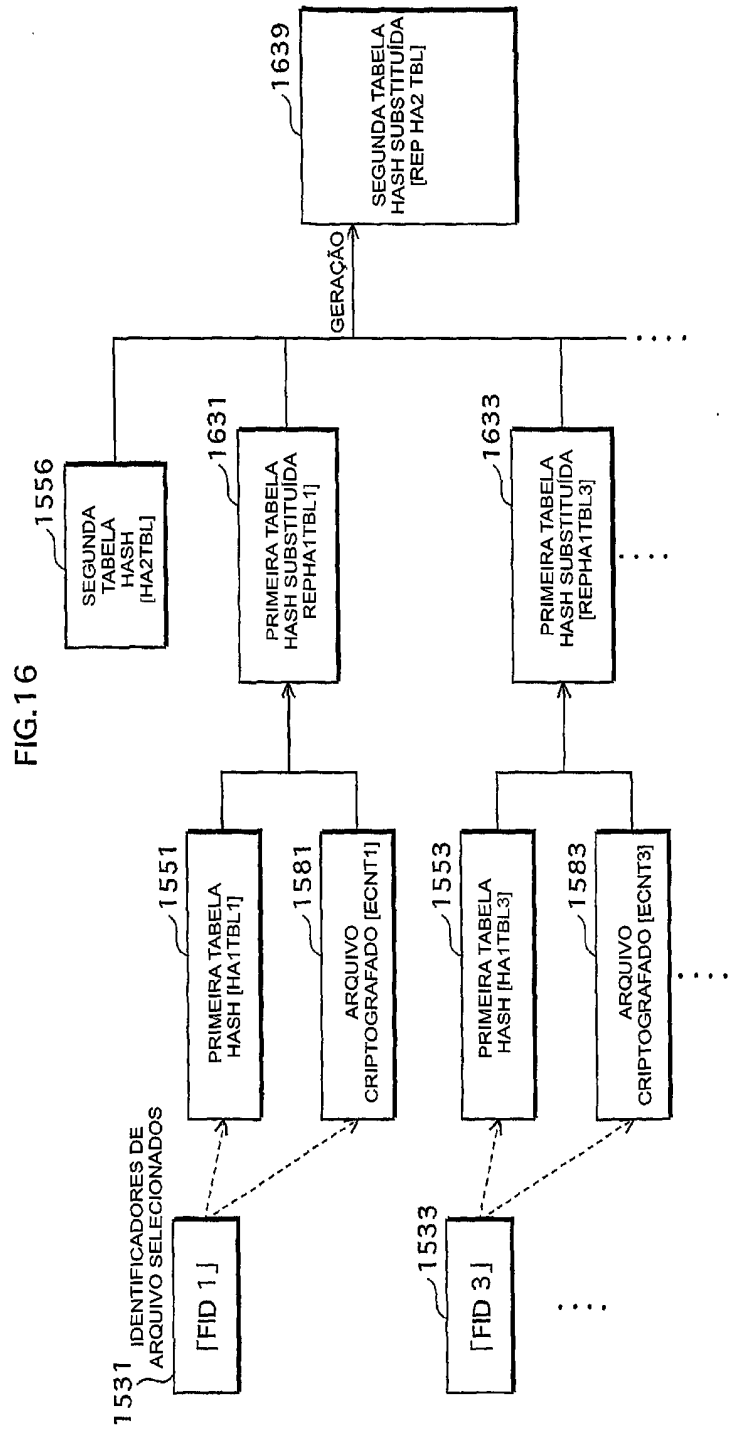

1639
SEGUNDA TABELA HASH SUBSTITUÍDA [REP HA2 TBL]
GERAÇÃO
1556
SEGUNDA TABELA HASH [HA2TBL]
1631
PRIMEIRA TABELA HASH SUBSTITUÍDA REPHA1TBL1]
1633
PRIMEIRA TABELA HASH SUBSTITUÍDA [REPHA1TBL3]
1551
PRIMEIRA TABELA HASH [HA1TBL1]
1581
ARQUIVO CRIPTOGRAFADO [ECNT1]
1553
PRIMEIRA TABELA HASH [HA1TBL3]
1583
ARQUIVO CRIPTOGRAFADO [ECNT3]
1531
IDENTIFICADORES DE ARQUIVO SELECIONADOS
「FID 1」
1533
「FID 3」

FIG. 17

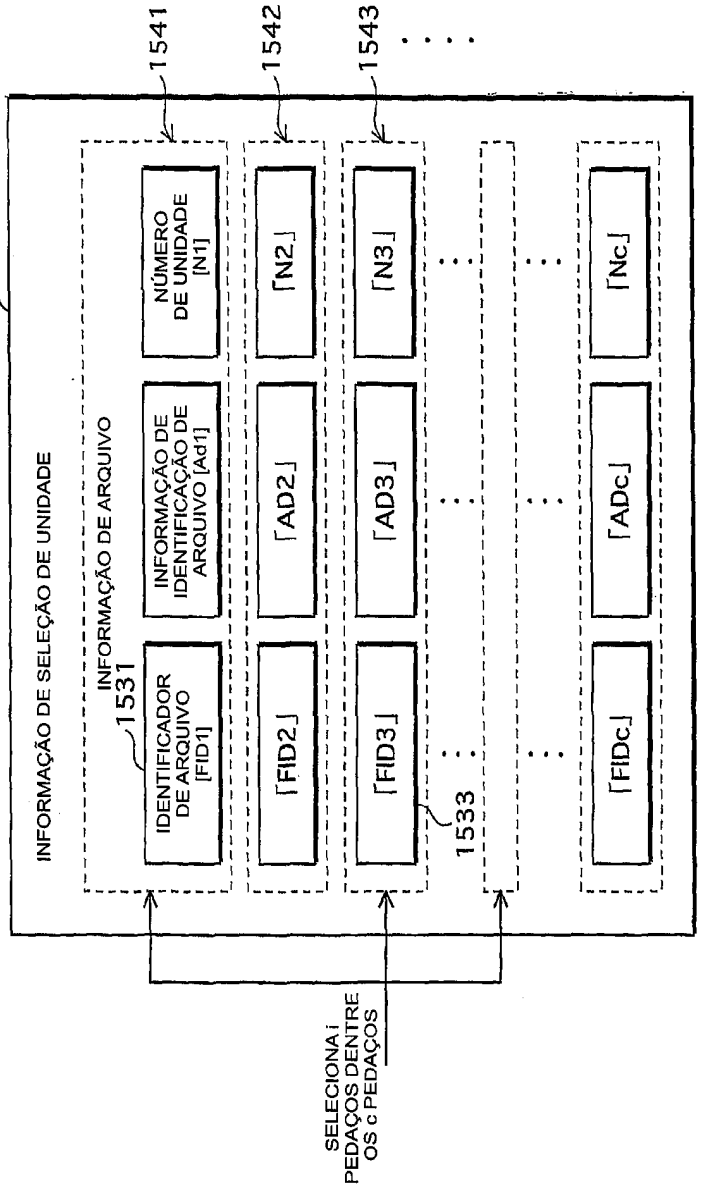

1530
INFORMAÇÃO DE SELEÇÃO DE UNIDADE
INFORMAÇÃO DE ARQUIVO
1531
IDENTIFICADOR DE ARQUIVO [FID1]
INFORMAÇÃO DE IDENTIFICAÇÃO DE ARQUIVO [Ad1]
NÚMERO DE UNIDADE [N1]
1541
1542
1543
「FID2」
「AD2」
「N2」
「FID3」
「AD3」
「N3」
1533
「FIDc」
「ADc」
「Nc」
SELECIONAi PEDAÇOS DENTRE OS c PEDAÇOS

FIG.18

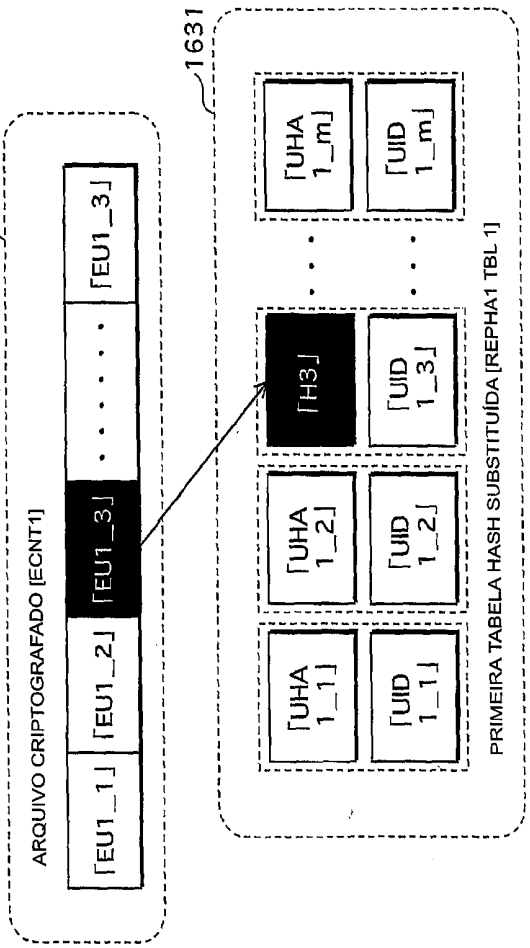

1581
ARQUIVO CRIPTOGRAFADO [ECNT1]
⌈EU1_1⌋
⌈EU1_2⌋
⌈EU1_3⌋
⌈EU1_3⌋
1631
⌈UHA 1_1⌋
⌈UID 1_1⌋
⌈UHA 1_2⌋
⌈UID 1_2⌋
⌈H3⌋
⌈UID 1_3⌋
⌈UHA 1_m⌋
⌈UID 1_m⌋
PRIMEIRA TABELA HASH SUBSTITUÍDA [REPHA1 TBL 1]

FIG.19

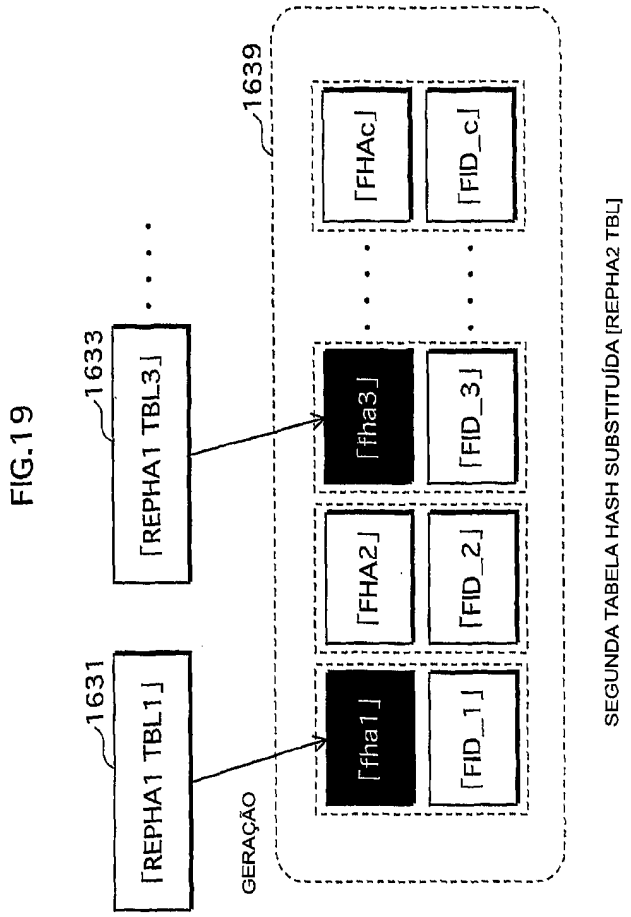

1631
「REPHA1 TBL1」
1633
「REPHA1 TBL3」
1639
GERAÇÃO
「fha1」
「FID_1」
「FHA2」
「FID_2」
「fha3」
「FID_3」
「FHAc」
「FID_c」
SEGUNDA TABELA HASH SUBSTITUÍDA [REPHA2 TBL]

FIG.20

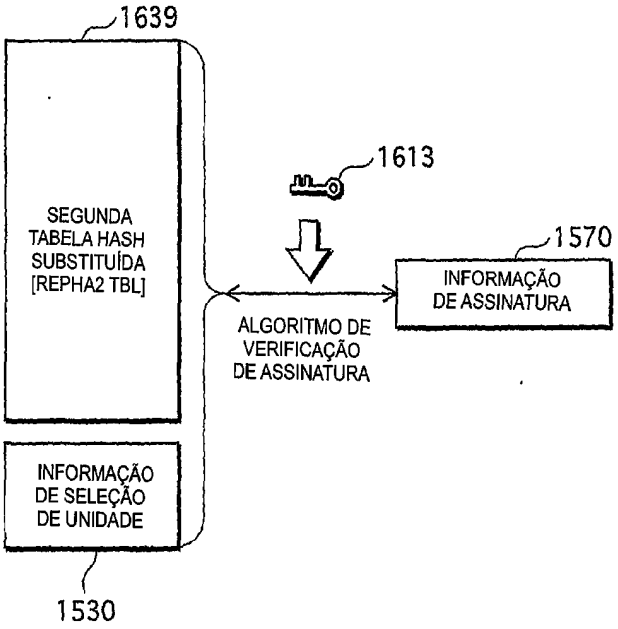

1639
SEGUNDA TABELA HASH SUBSTITUÍDA [REPHA2 TBL]
1613
1570
INFORMAÇÃO DE ASSINATURA
ALGORITMO DE VERIFICAÇÃO DE ASSINATURA
INFORMAÇÃO DE SELEÇÃO DE UNIDADE
1530

FIG.21

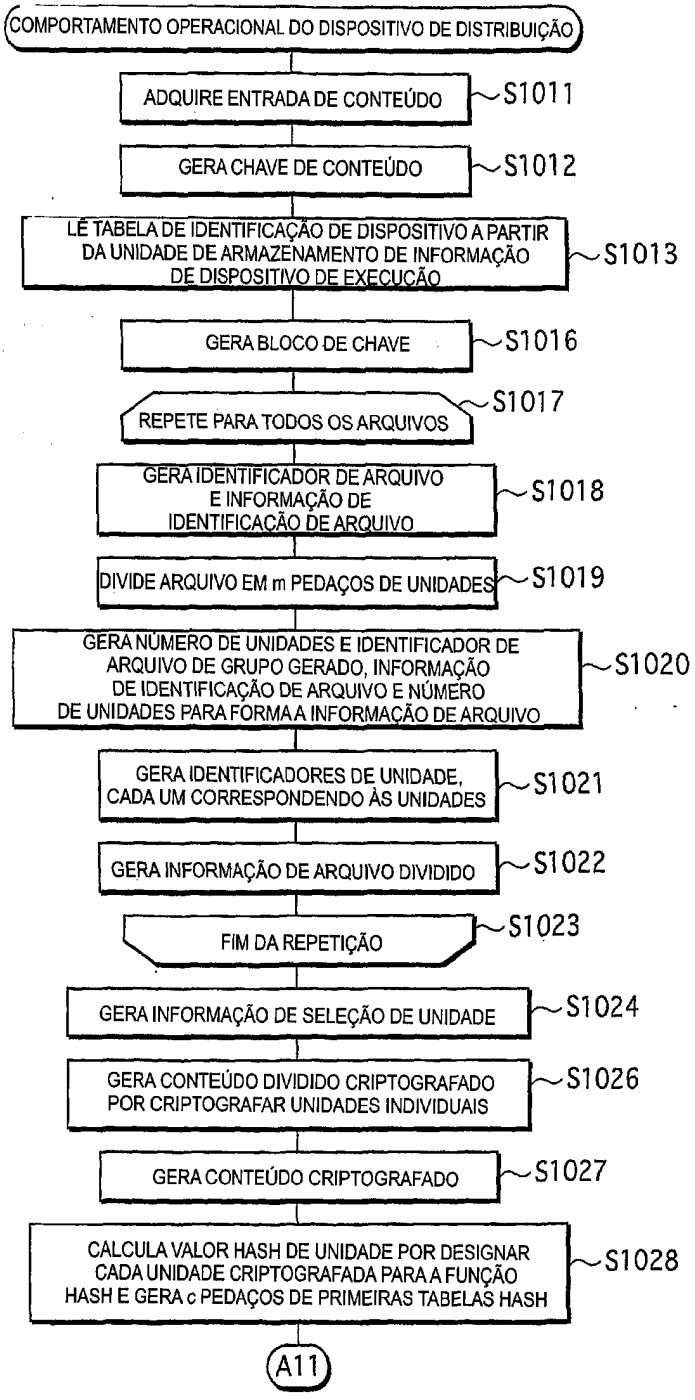

COMPORTAMENTO OPERACIONAL DO DISPOSITIVO DE DISTRIBUIÇÃO
ADQUIRE ENTRADA DE CONTEÚDO
S1011
GERA CHAVE DE CONTEÚDO
S1012
LÊ TABELA DE IDENTIFICAÇÃO DE DISPOSITIVO A PARTIR DA UNIDADE DE ARMAZENAMENTO DE INFORMAÇÃO DE DISPOSITIVO DE EXECUÇÃO
S1013
GERA BLOCO DE CHAVE
S1016
REPETE PARA TODOS OS ARQUIVOS
S1017
GERA IDENTIFICADOR DE ARQUIVO E INFORMAÇÃO DE IDENTIFICAÇÃO DE ARQUIVO
S1018
DIVIDE ARQUIVO EM m PEDAÇOS DE UNIDADES
S1019
GERA NÚMERO DE UNIDADES E IDENTIFICADOR DE ARQUIVO DE GRUPO GERADO, INFORMAÇÃO DE IDENTIFICAÇÃO DE ARQUIVO E NÚMERO DE UNIDADES PARA FORMAR A INFORMAÇÃO DE ARQUIVO
S1020
GERA IDENTIFICADORES DE UNIDADE, CADA UM CORRESPONDENDO ÀS UNIDADES
S1021
GERA INFORMAÇÃO DE ARQUIVO DIVIDIDO
S1022
FIM DA REPETIÇÃO
S1023
GERA INFORMAÇÃO DE SELEÇÃO DE UNIDADE
S1024
GERA CONTEÚDO DIVIDIDO CRIPTOGRAFADO POR CRIPTOGRAFAR UNIDADES INDIVIDUAIS
S1026
GERA CONTEÚDO CRIPTOGRAFADO
S1027
CALCULA VALOR HASH DE UNIDADE POR DESIGNAR CADA UNIDADE CRIPTOGRAFADA PARA A FUNÇÃO HASH E GERA c PEDAÇOS DE PRIMEIRAS TABELAS HASH
S1028
A11

FIG.22

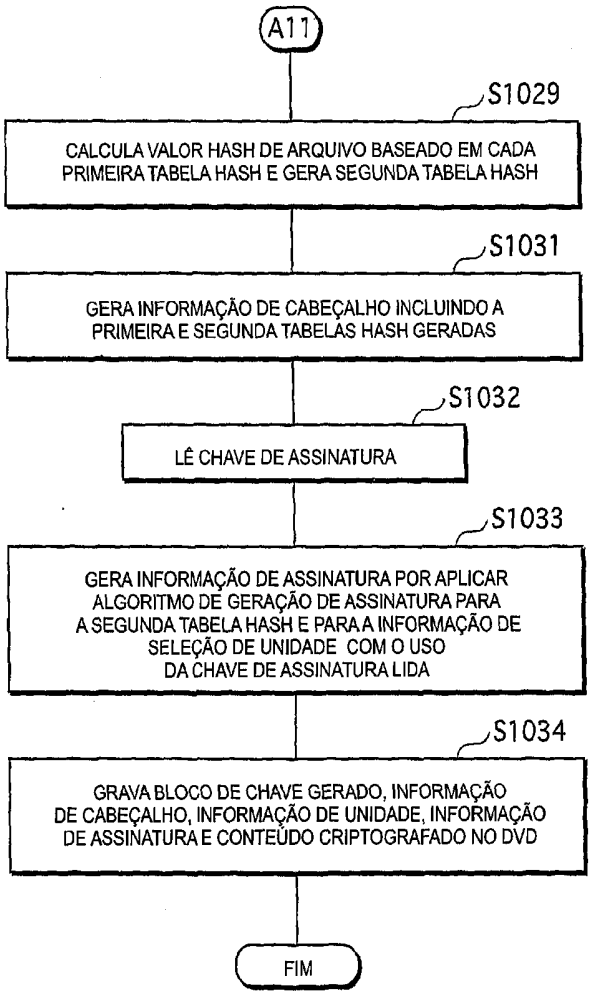

A11
S1029
CALCULA VALOR HASH DE ARQUIVO BASEADO EM CADA PRIMEIRA TABELA HASH E GERA SEGUNDA TABELA HASH
S1031
GERA INFORMAÇÃO DE CABEÇALHO INCLUINDO A PRIMEIRA E SEGUNDA TABELAS HASH GERADAS
S1032
LÊ CHAVE DE ASSINATURA
S1033
GERA INFORMAÇÃO DE ASSINATURA POR APLICAR ALGORITMO DE GERAÇÃO DE ASSINATURA PARA A SEGUNDA TABELA HASH E PARA A INFORMAÇÃO DE SELEÇÃO DE UNIDADE COM O USO DA CHAVE DE ASSINATURA LIDA
S1034
GRAVA BLOCO DE CHAVE GERADO, INFORMAÇÃO DE CABEÇALHO, INFORMAÇÃO DE UNIDADE, INFORMAÇÃO DE ASSINATURA E CONTEÚDO CRIPTOGRAFADO NO DVD
FIM

FIG.23

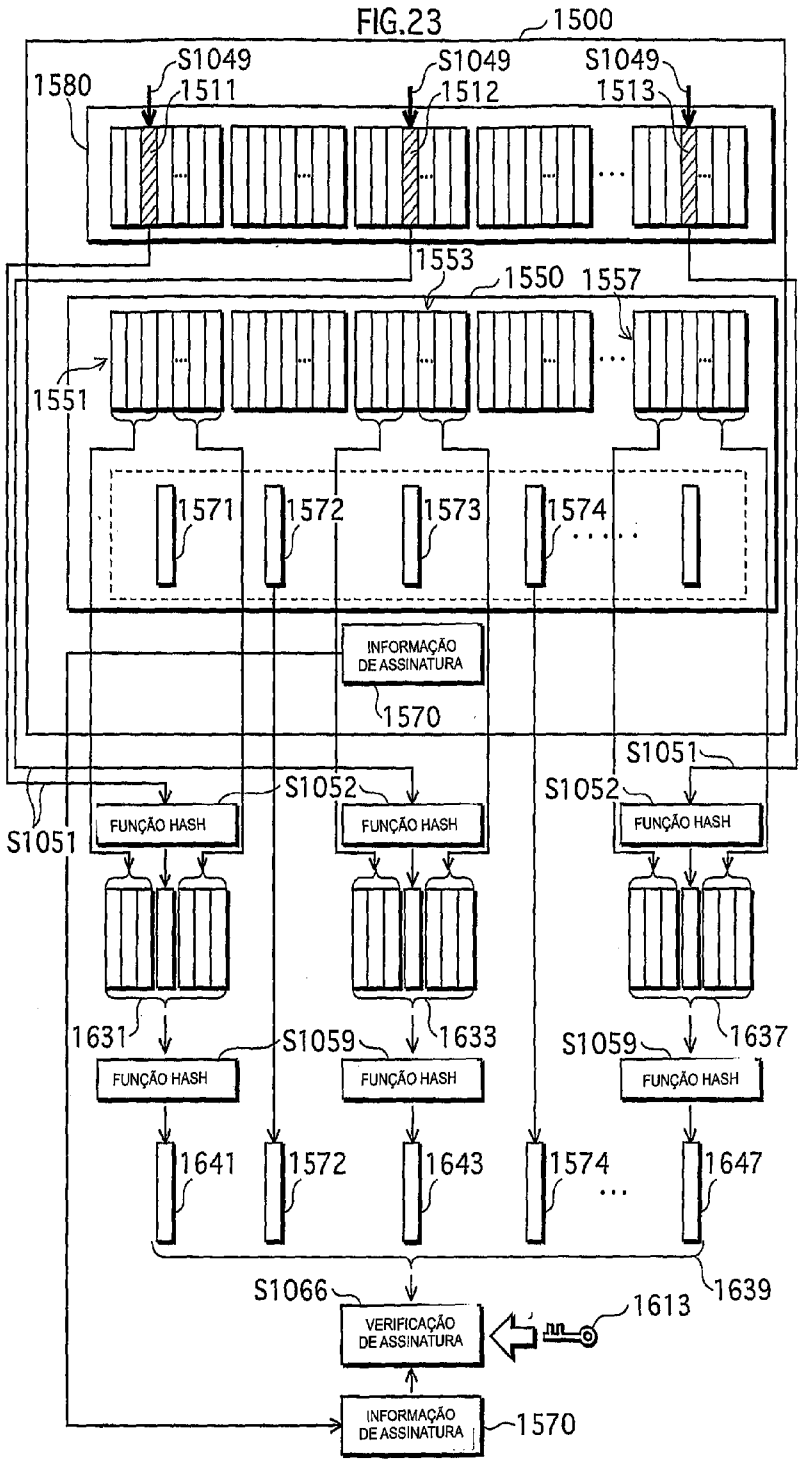

1500
S1049
S1049
S1049
1580
1511
1512
1513
1553
1550
1557
1551
1571
1572
1573
1574
INFORMAÇÃO DE ASSINATURA
1570
S1051
S1052
S1052
S1051
FUNÇÃO HASH
FUNÇÃO HASH
FUNÇÃO HASH
1631
S1059
1633
S1059
1637
FUNÇÃO HASH
FUNÇÃO HASH
FUNÇÃO HASH
1641
1572
1643
1574
1647
1639
S1066
1613
VERIFICAÇÃO DE ASSINATURA
INFORMAÇÃO DE ASSINATURA
1570

FIG.24

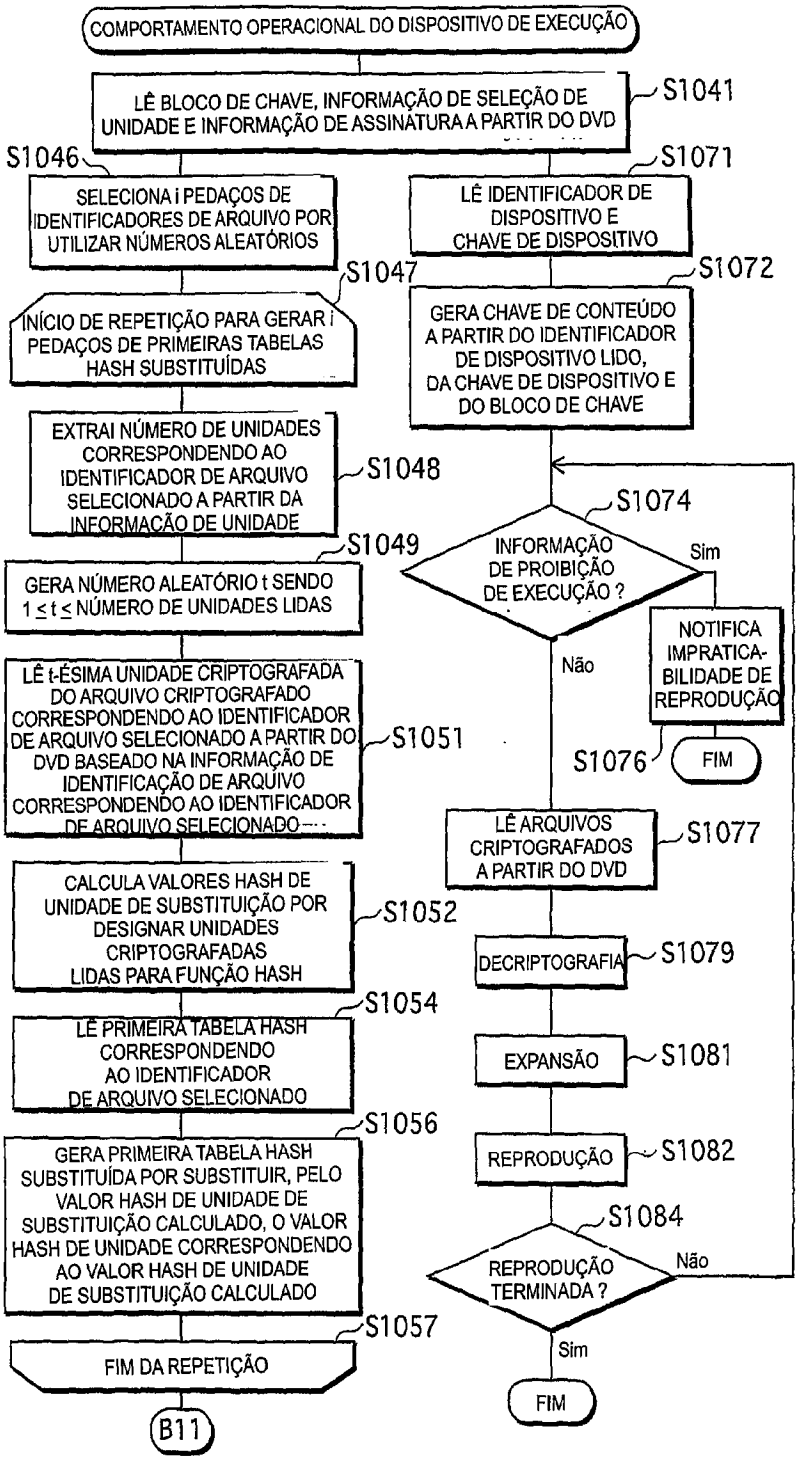

COMPORTAMENTO OPERACIONAL DO DISPOSITIVO DE EXECUÇÃO
LÊ BLOCO DE CHAVE, INFORMAÇÃO DE SELEÇÃO DE UNIDADE E INFORMAÇÃO DE ASSINATURA A PARTIR DO DVD
S1041
S1046
SELECIONA i PEDAÇOS DE IDENTIFICADORES DE ARQUIVO POR UTILIZAR NÚMEROS ALEATÓRIOS
S1047
INÍCIO DE REPETIÇÃO PARA GERAR i PEDAÇOS DE PRIMEIRAS TABELAS HASH SUBSTITUÍDAS
EXTRAI NÚMERO DE UNIDADES CORRESPONDENDO AO IDENTIFICADOR DE ARQUIVO SELECIONADO A PARTIR DA INFORMAÇÃO DE UNIDADE
S1048
S1049
GERA NÚMERO ALEATÓRIO t SENDO 1 ≤ t ≤ NÚMERO DE UNIDADES LIDAS
LÊ t-ÉSIMA UNIDADE CRIPTOGRAFADA DO ARQUIVO CRIPTOGRAFADO CORRESPONDENDO AO IDENTIFICADOR DE ARQUIVO SELECIONADO A PARTIR DO DVD BASEADO NA INFORMAÇÃO DE IDENTIFICAÇÃO DE ARQUIVO CORRESPONDENDO AO IDENTIFICADOR DE ARQUIVO SELECIONADO
S1051
CALCULA VALORES HASH DE UNIDADE DE SUBSTITUIÇÃO POR DESIGNAR UNIDADES CRIPTOGRAFADAS LIDAS PARA FUNÇÃO HASH
S1052
LÊ PRIMEIRA TABELA HASH CORRESPONDENDO AO IDENTIFICADOR DE ARQUIVO SELECIONADO
S1054
GERA PRIMEIRA TABELA HASH SUBSTITUÍDA POR SUBSTITUIR, PELO VALOR HASH DE UNIDADE DE SUBSTITUIÇÃO CALCULADO, O VALOR HASH DE UNIDADE CORRESPONDENDO AO VALOR HASH DE UNIDADE DE SUBSTITUIÇÃO CALCULADO
S1056
FIM DA REPETIÇÃO
S1057
B11
S1071
LÊ IDENTIFICADOR DE DISPOSITIVO E CHAVE DE DISPOSITIVO
S1072
GERA CHAVE DE CONTEÚDO A PARTIR DO IDENTIFICADOR DE DISPOSITIVO LIDO, DA CHAVE DE DISPOSITIVO E DO BLOCO DE CHAVE
S1074
INFORMAÇÃO DE PROIBIÇÃO DE EXECUÇÃO ?
Sim
Não
NOTIFICA IMPRATICA-BILIDADE DE REPRODUÇÃO
S1076
FIM
LÊ ARQUIVOS CRIPTOGRAFADOS A PARTIR DO DVD
S1077
DECRIPTOGRAFIA
S1079
EXPANSÃO
S1081
REPRODUÇÃO
S1082
S1084
REPRODUÇÃO TERMINADA ?
Não
Sim
FIM

FIG.25

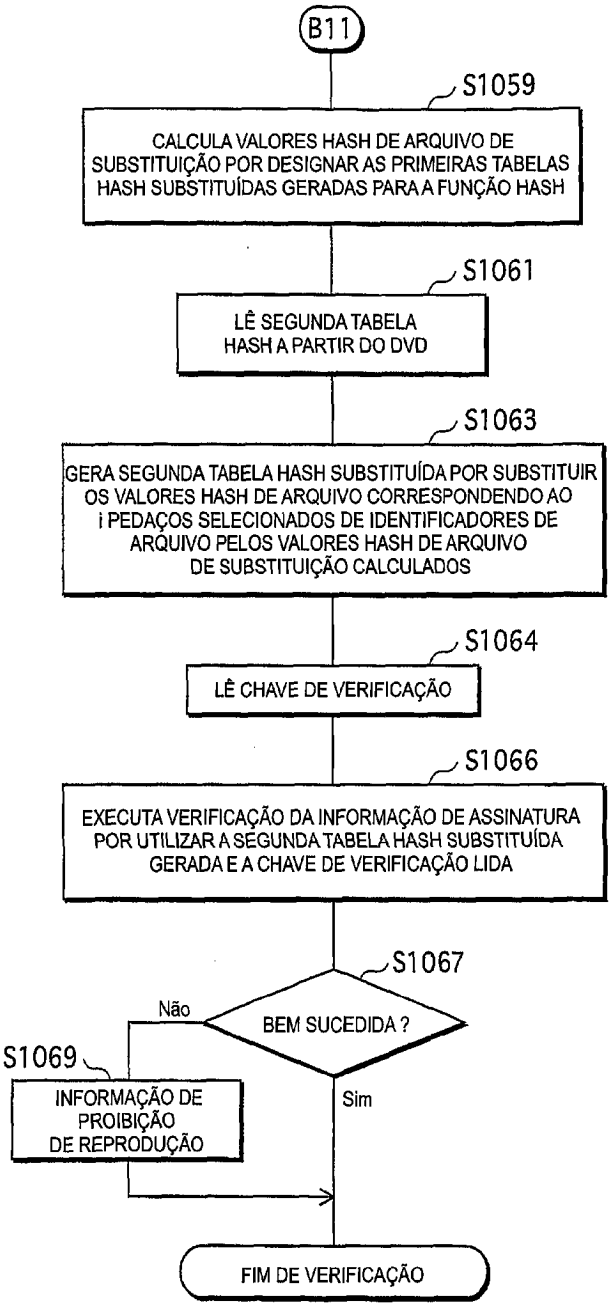

B11
S1059
CALCULA VALORES HASH DE ARQUIVO DE SUBSTITUIÇÃO POR DESIGNAR AS PRIMEIRAS TABELAS HASH SUBSTITUÍDAS GERADAS PARA A FUNÇÃO HASH
S1061
LÊ SEGUNDA TABELA HASH A PARTIR DO DVD
S1063
GERA SEGUNDA TABELA HASH SUBSTITUÍDA POR SUBSTITUIR OS VALORES HASH DE ARQUIVO CORRESPONDENDO AO i PEDAÇOS SELECIONADOS DE IDENTIFICADORES DE ARQUIVO PELOS VALORES HASH DE ARQUIVO DE SUBSTITUIÇÃO CALCULADOS
S1064
LÊ CHAVE DE VERIFICAÇÃO
S1066
EXECUTA VERIFICAÇÃO DA INFORMAÇÃO DE ASSINATURA POR UTILIZAR A SEGUNDA TABELA HASH SUBSTITUÍDA GERADA E A CHAVE DE VERIFICAÇÃO LIDA
S1067
BEM SUCEDIDA ?
Não
Sim
S1069
INFORMAÇÃO DE PROIBIÇÃO DE REPRODUÇÃO
FIM DE VERIFICAÇÃO

FIG.26

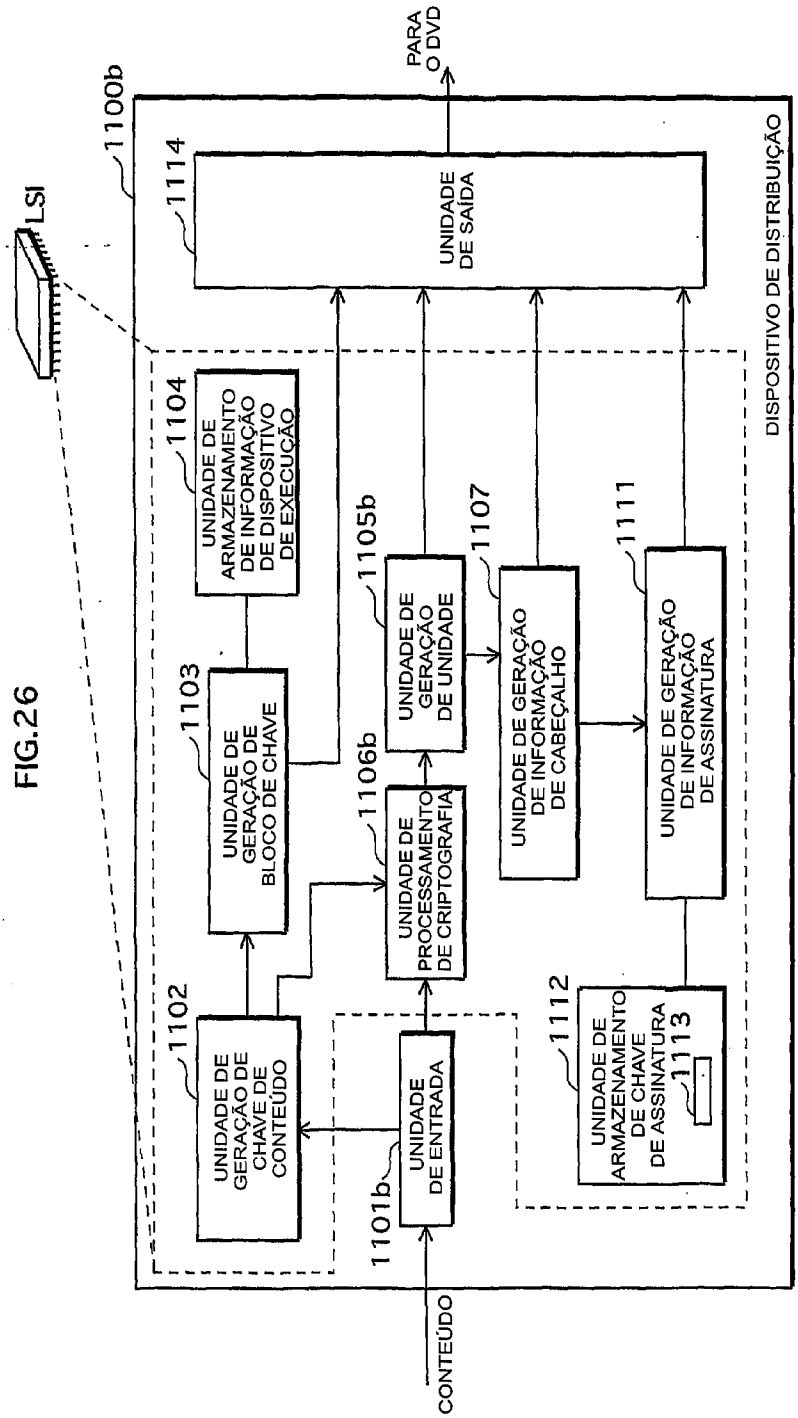

LSI
1100b
PARA O DVD
1114
UNIDADE DE SAÍDA
DISPOSITIVO DE DISTRIBUIÇÃO
1104
UNIDADE DE ARMAZENAMENTO DE INFORMAÇÃO DE DISPOSITIVO DE EXECUÇÃO
1105b
UNIDADE DE GERAÇÃO DE UNIDADE
1107
1111
1103
UNIDADE DE GERAÇÃO DE BLOCO DE CHAVE
1106b
UNIDADE DE PROCESSAMENTO DE CRIPTOGRAFIA
UNIDADE DE GERAÇÃO DE INFORMAÇÃO DE CABEÇALHO
UNIDADE DE GERAÇÃO DE INFORMAÇÃO DE ASSINATURA
1102
UNIDADE DE GERAÇÃO DE CHAVE DE CONTEÚDO
1112
UNIDADE DE ARMAZENAMENTO DE CHAVE DE ASSINATURA
1113
1101b
UNIDADE DE ENTRADA
CONTEÚDO

FIG.27

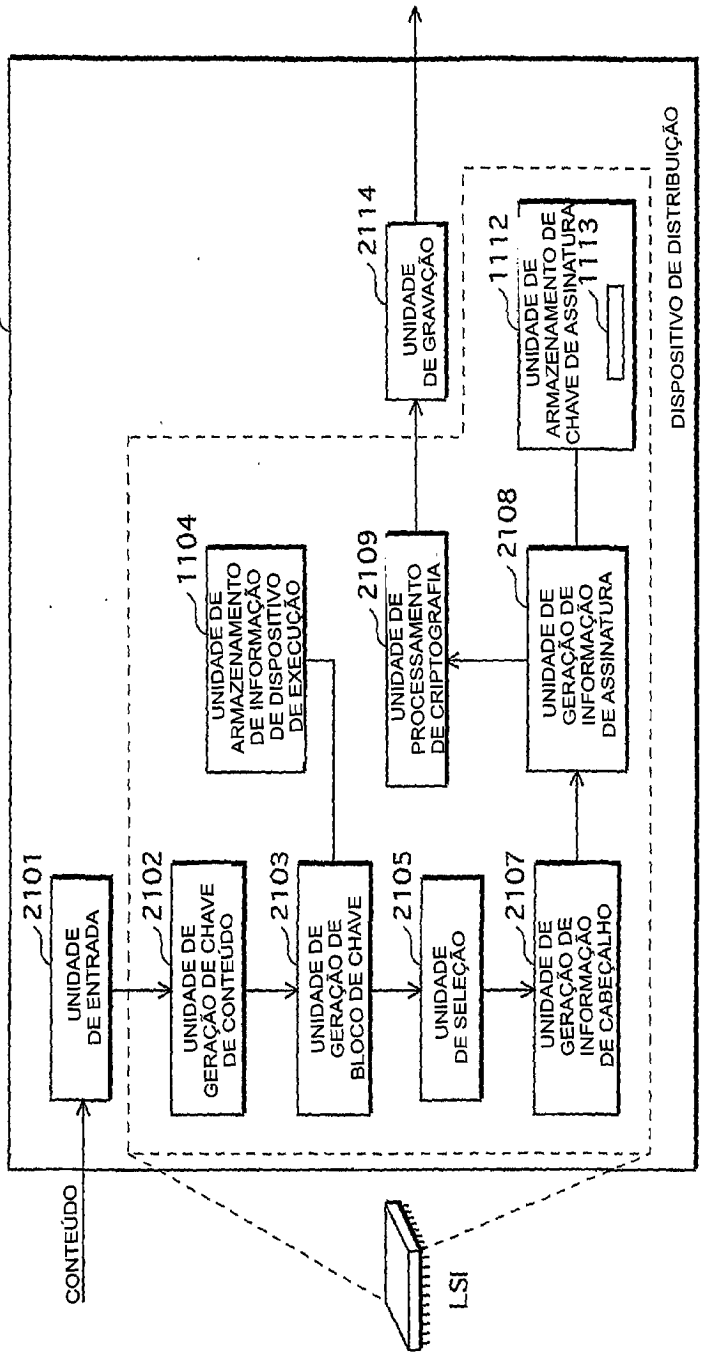

2100
DISPOSITIVO DE DISTRIBUIÇÃO
UNIDADE DE ENTRADA
2101
UNIDADE DE GERAÇÃO DE CHAVE DE CONTEÚDO
2102
UNIDADE DE GERAÇÃO DE BLOCO DE CHAVE
2103
UNIDADE DE SELEÇÃO
2105
UNIDADE DE GERAÇÃO DE INFORMAÇÃO DE CABEÇALHO
2107
UNIDADE DE GERAÇÃO DE INFORMAÇÃO DE ASSINATURA
2108
UNIDADE DE PROCESSAMENTO DE CRIPTOGRAFIA
2109
UNIDADE DE ARMAZENAMENTO DE INFORMAÇÃO DE DISPOSITIVO DE EXECUÇÃO
1104
UNIDADE DE GRAVAÇÃO
2114
UNIDADE DE ARMAZENAMENTO DE CHAVE DE ASSINATURA
1112
1113
CONTEÚDO
LSI

FIG.28

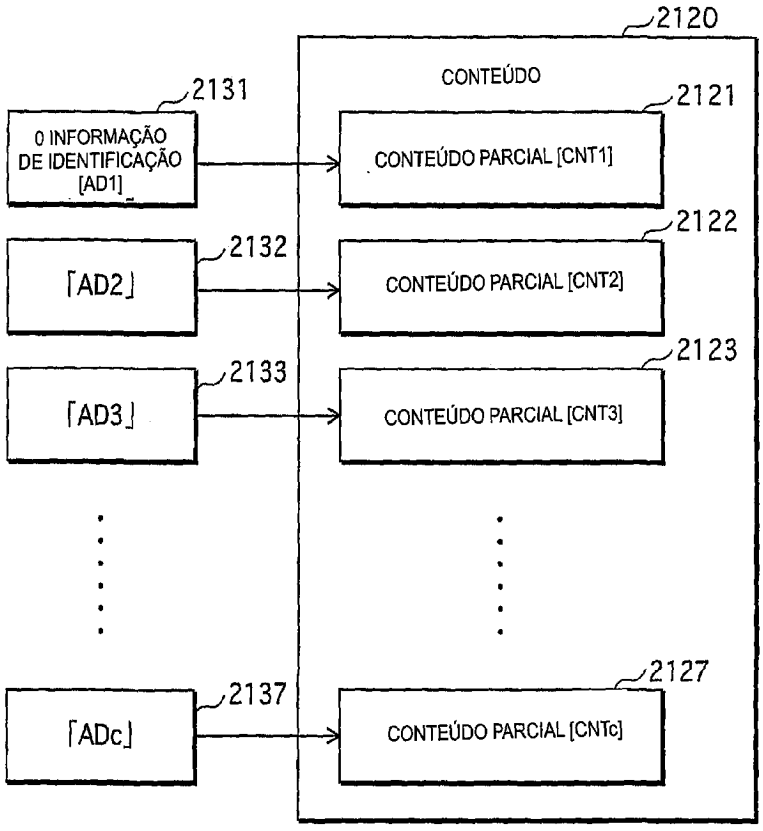

2120
CONTEÚDO
2131
0 INFORMAÇÃO DE IDENTIFICAÇÃO [AD1]
2121
CONTEÚDO PARCIAL [CNT1]
2122
2132
「AD2」
CONTEÚDO PARCIAL [CNT2]
2123
2133
「AD3」
CONTEÚDO PARCIAL [CNT3]
2127
2137
「ADc」
CONTEÚDO PARCIAL [CNTc]

FIG.29

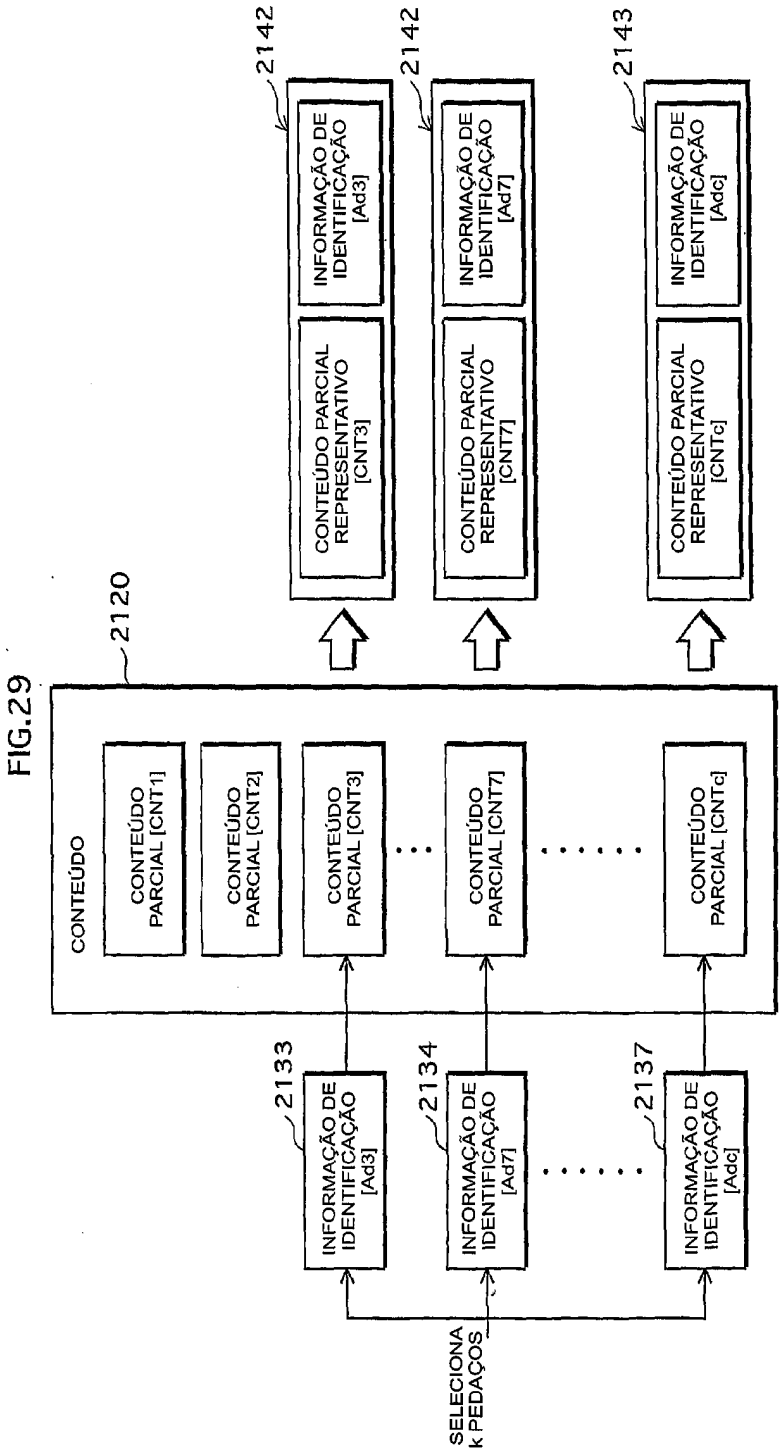

2142
2142
2143
INFORMAÇÃO DE IDENTIFICAÇÃO [Ad3]
INFORMAÇÃO DE IDENTIFICAÇÃO [Ad7]
INFORMAÇÃO DE IDENTIFICAÇÃO [Adc]
CONTEÚDO PARCIAL REPRESENTATIVO [CNT3]
CONTEÚDO PARCIAL REPRESENTATIVO [CNT7]
CONTEÚDO PARCIAL REPRESENTATIVO [CNTc]
2120
CONTEÚDO
CONTEÚDO PARCIAL [CNT1]
CONTEÚDO PARCIAL [CNT2]
CONTEÚDO PARCIAL [CNT3]
CONTEÚDO PARCIAL [CNT7]
CONTEÚDO PARCIAL [CNTc]
2133
2134
2137
INFORMAÇÃO DE IDENTIFICAÇÃO [Ad3]
INFORMAÇÃO DE IDENTIFICAÇÃO [Ad7]
INFORMAÇÃO DE IDENTIFICAÇÃO [Adc]
SELECIONA k PEDAÇOS

FIG.30

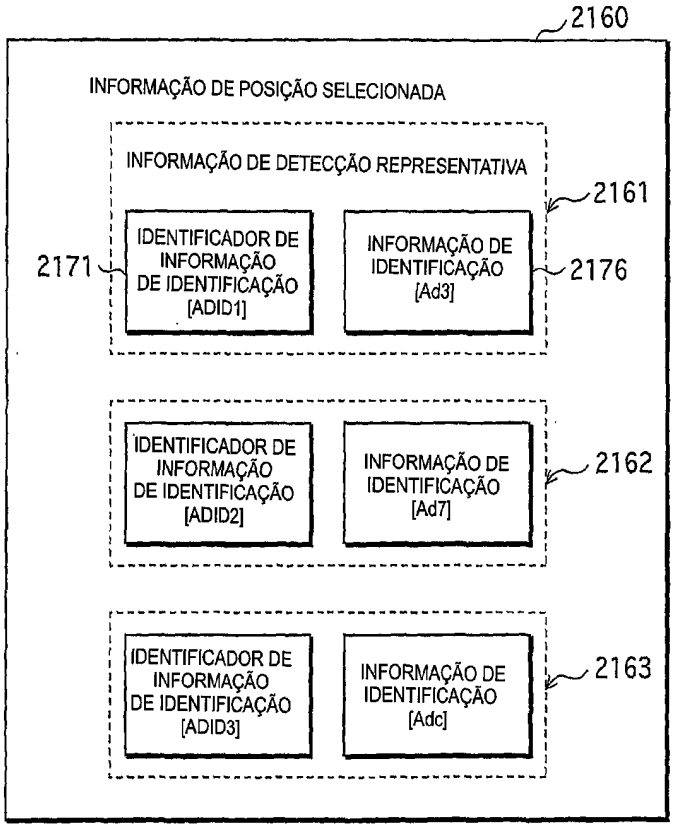

2160
INFORMAÇÃO DE POSIÇÃO SELECIONADA
INFORMAÇÃO DE DETECÇÃO REPRESENTATIVA
2161
2171
IDENTIFICADOR DE INFORMAÇÃO DE IDENTIFICAÇÃO [ADID1]
INFORMAÇÃO DE IDENTIFICAÇÃO [Ad3]
2176
IDENTIFICADOR DE INFORMAÇÃO DE IDENTIFICAÇÃO [ADID2]
INFORMAÇÃO DE IDENTIFICAÇÃO [Ad7]
2162
IDENTIFICADOR DE INFORMAÇÃO DE IDENTIFICAÇÃO [ADID3]
INFORMAÇÃO DE IDENTIFICAÇÃO [Adc]
2163

FIG.31

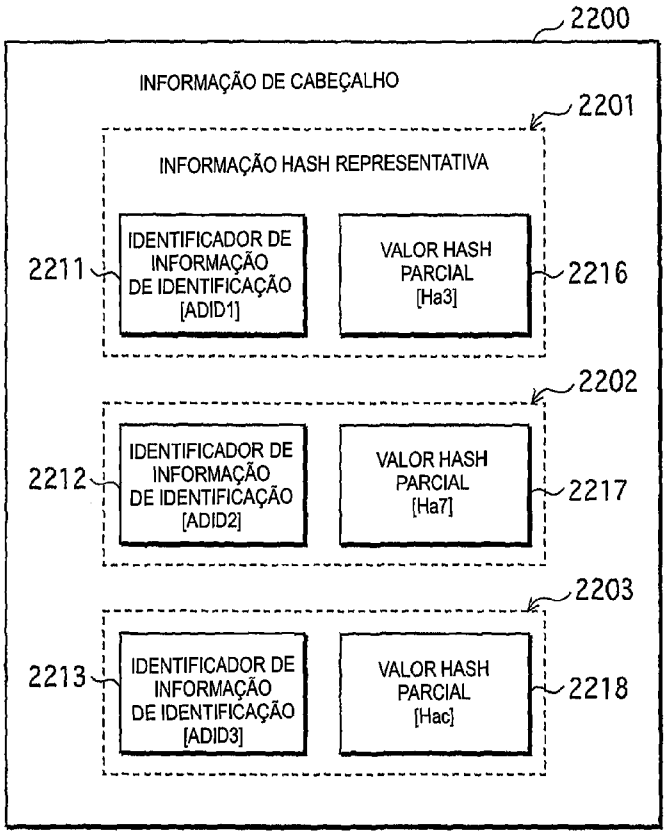

2200
INFORMAÇÃO DE CABEÇALHO
2201
INFORMAÇÃO HASH REPRESENTATIVA
2211
IDENTIFICADOR DE INFORMAÇÃO DE IDENTIFICAÇÃO [ADID1]
VALOR HASH PARCIAL [Ha3]
2216
2202
2212
IDENTIFICADOR DE INFORMAÇÃO DE IDENTIFICAÇÃO [ADID2]
VALOR HASH PARCIAL [Ha7]
2217
2203
2213
IDENTIFICADOR DE INFORMAÇÃO DE IDENTIFICAÇÃO [ADID3]
VALOR HASH PARCIAL [Hac]
2218

FIG.32

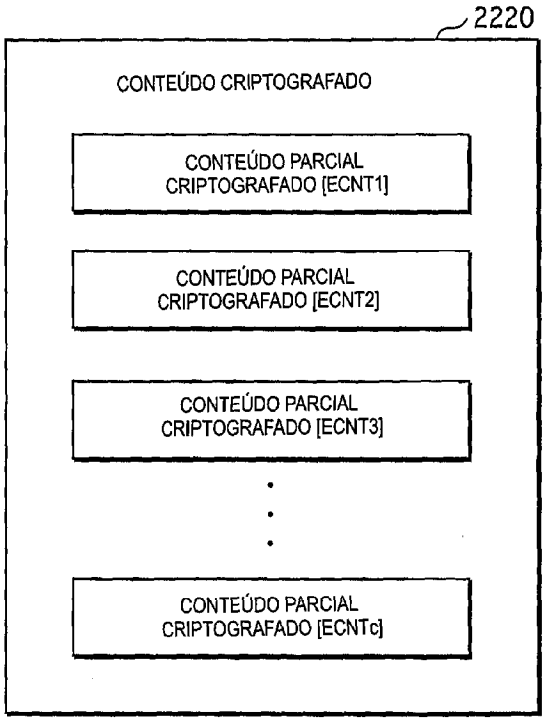

2220
CONTEÚDO CRIPTOGRAFADO
CONTEÚDO PARCIAL CRIPTOGRAFADO [ECNT1]
CONTEÚDO PARCIAL CRIPTOGRAFADO [ECNT2]
CONTEÚDO PARCIAL CRIPTOGRAFADO [ECNT3]
CONTEÚDO PARCIAL CRIPTOGRAFADO [ECNTc]

FIG.33

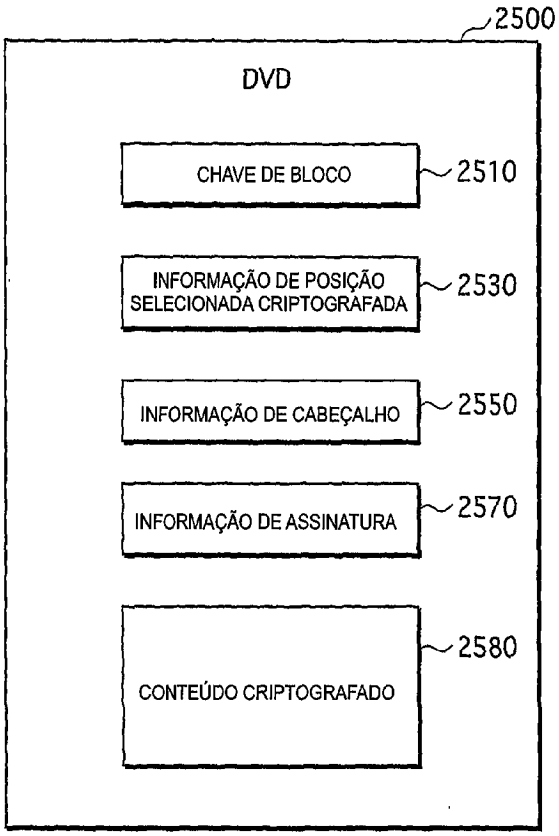

2500
DVD
CHAVE DE BLOCO
2510
INFORMAÇÃO DE POSIÇÃO SELECIONADA CRIPTOGRAFADA
2530
INFORMAÇÃO DE CABEÇALHO
2550
INFORMAÇÃO DE ASSINATURA
2570
CONTEÚDO CRIPTOGRAFADO
2580

FIG.34

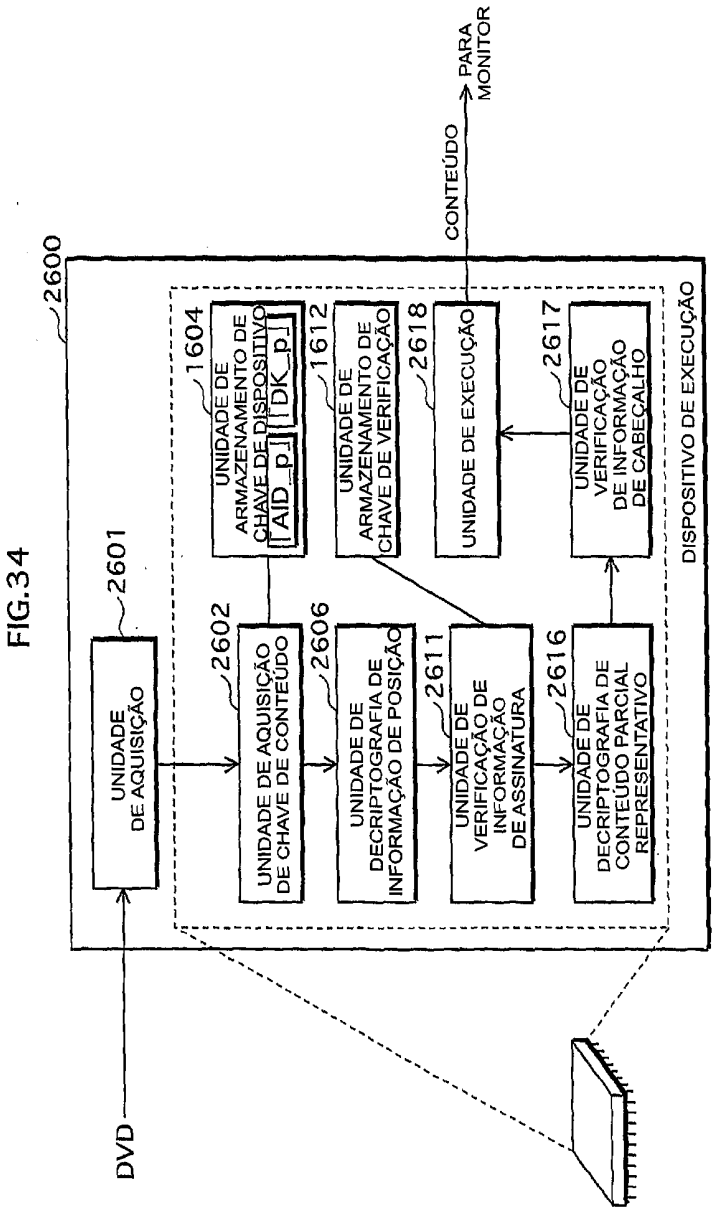

DVD
2600
2601
UNIDADE DE AQUISIÇÃO
2602
UNIDADE DE AQUISIÇÃO DE CHAVE DE CONTEÚDO
2606
UNIDADE DE DECRIPTOGRAFIA DE INFORMAÇÃO DE POSIÇÃO
2611
UNIDADE DE VERIFICAÇÃO DE INFORMAÇÃO DE ASSINATURA
2616
UNIDADE DE DECRIPTOGRAFIA DE CONTEÚDO PARCIAL REPRESENTATIVO
1604
UNIDADE DE ARMAZENAMENTO DE CHAVE DE DISPOSITIVO
[AID_p]
[DK_p]
1612
UNIDADE DE ARMAZENAMENTO DE CHAVE DE VERIFICAÇÃO
2618
UNIDADE DE EXECUÇÃO
2617
UNIDADE DE VERIFICAÇÃO DE INFORMAÇÃO DE CABEÇALHO
DISPOSITIVO DE EXECUÇÃO
CONTEÚDO
PARA MONITOR

FIG.35

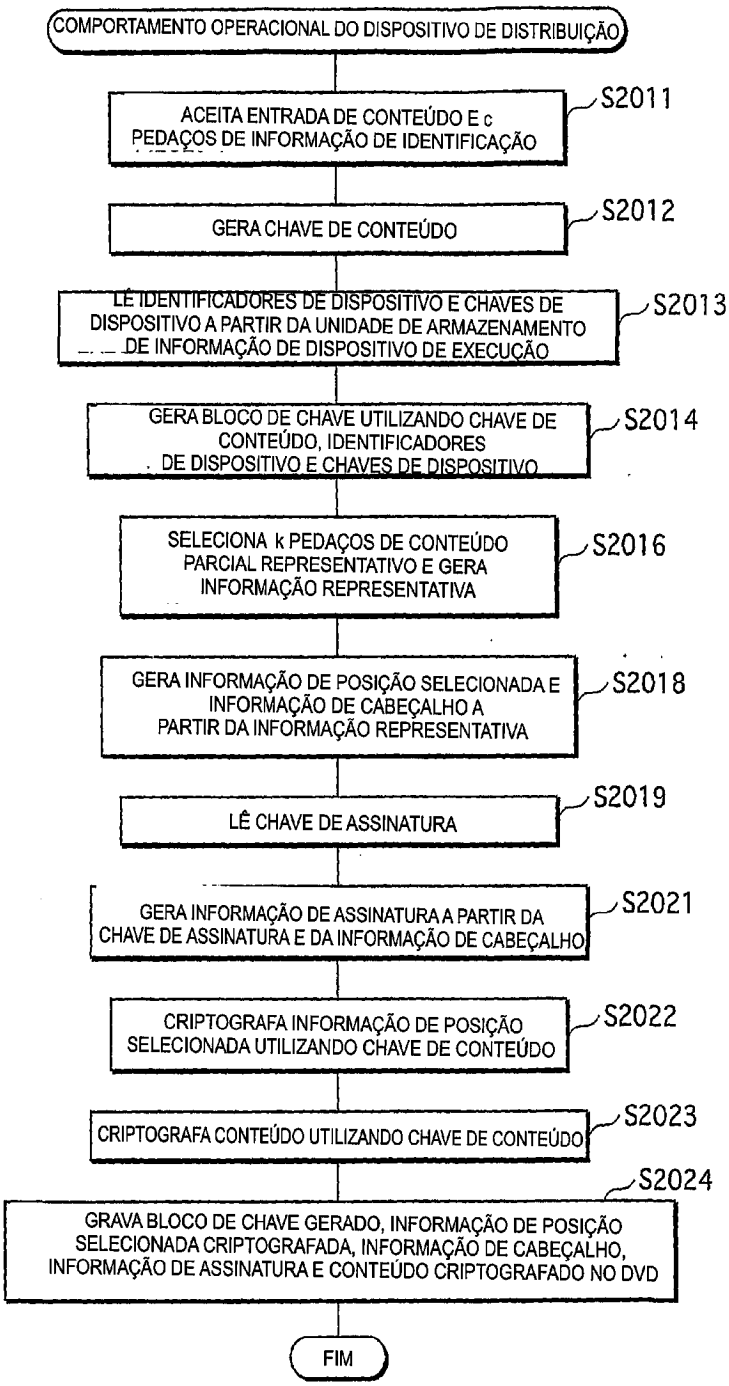

COMPORTAMENTO OPERACIONAL DO DISPOSITIVO DE DISTRIBUIÇÃO
ACEITA ENTRADA DE CONTEÚDO E c PEDAÇOS DE INFORMAÇÃO DE IDENTIFICAÇÃO
S2011
GERA CHAVE DE CONTEÚDO
S2012
LÊ IDENTIFICADORES DE DISPOSITIVO E CHAVES DE DISPOSITIVO A PARTIR DA UNIDADE DE ARMAZENAMENTO DE INFORMAÇÃO DE DISPOSITIVO DE EXECUÇÃO
S2013
GERA BLOCO DE CHAVE UTILIZANDO CHAVE DE CONTEÚDO, IDENTIFICADORES DE DISPOSITIVO E CHAVES DE DISPOSITIVO
S2014
SELECIONA k PEDAÇOS DE CONTEÚDO PARCIAL REPRESENTATIVO E GERA INFORMAÇÃO REPRESENTATIVA
S2016
GERA INFORMAÇÃO DE POSIÇÃO SELECIONADA E INFORMAÇÃO DE CABEÇALHO A PARTIR DA INFORMAÇÃO REPRESENTATIVA
S2018
LÊ CHAVE DE ASSINATURA
S2019
GERA INFORMAÇÃO DE ASSINATURA A PARTIR DA CHAVE DE ASSINATURA E DA INFORMAÇÃO DE CABEÇALHO
S2021
CRIPTOGRAFA INFORMAÇÃO DE POSIÇÃO SELECIONADA UTILIZANDO CHAVE DE CONTEÚDO
S2022
CRIPTOGRAFA CONTEÚDO UTILIZANDO CHAVE DE CONTEÚDO
S2023
GRAVA BLOCO DE CHAVE GERADO, INFORMAÇÃO DE POSIÇÃO SELECIONADA CRIPTOGRAFADA, INFORMAÇÃO DE CABEÇALHO, INFORMAÇÃO DE ASSINATURA E CONTEÚDO CRIPTOGRAFADO NO DVD
S2024
FIM

FIG.36

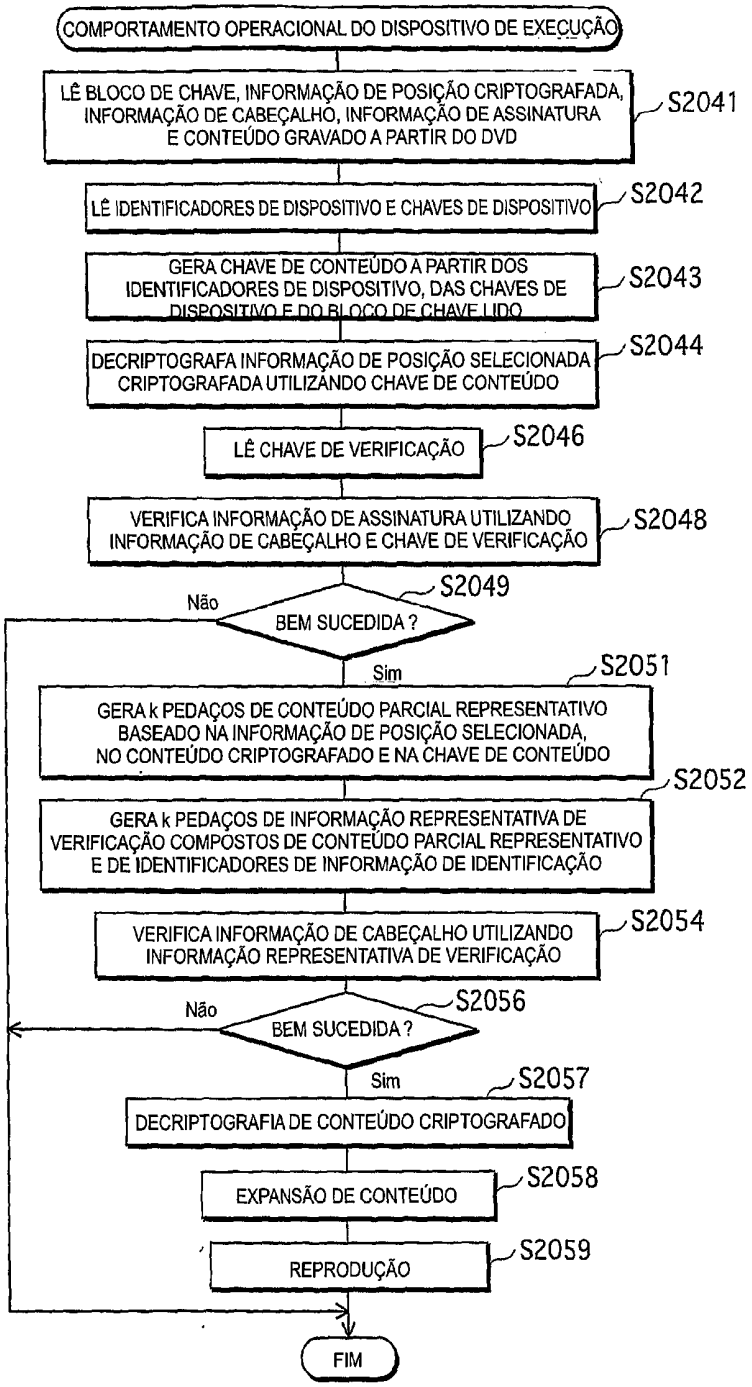

COMPORTAMENTO OPERACIONAL DO DISPOSITIVO DE EXECUÇÃO
LÊ BLOCO DE CHAVE, INFORMAÇÃO DE POSIÇÃO CRIPTOGRAFADA, INFORMAÇÃO DE CABEÇALHO, INFORMAÇÃO DE ASSINATURA E CONTEÚDO GRAVADO A PARTIR DO DVD
S2041
LÊ IDENTIFICADORES DE DISPOSITIVO E CHAVES DE DISPOSITIVO
S2042
GERA CHAVE DE CONTEÚDO A PARTIR DOS IDENTIFICADORES DE DISPOSITIVO, DAS CHAVES DE DISPOSITIVO E DO BLOCO DE CHAVE LIDO
S2043
DECRIPTOGRAFA INFORMAÇÃO DE POSIÇÃO SELECIONADA CRIPTOGRAFADA UTILIZANDO CHAVE DE CONTEÚDO
S2044
LÊ CHAVE DE VERIFICAÇÃO
S2046
VERIFICA INFORMAÇÃO DE ASSINATURA UTILIZANDO INFORMAÇÃO DE CABEÇALHO E CHAVE DE VERIFICAÇÃO
S2048
BEM SUCEDIDA ?
S2049
Não
Sim
GERA k PEDAÇOS DE CONTEÚDO PARCIAL REPRESENTATIVO BASEADO NA INFORMAÇÃO DE POSIÇÃO SELECIONADA, NO CONTEÚDO CRIPTOGRAFADO E NA CHAVE DE CONTEÚDO
S2051
GERA k PEDAÇOS DE INFORMAÇÃO REPRESENTATIVA DE VERIFICAÇÃO COMPOSTOS DE CONTEÚDO PARCIAL REPRESENTATIVO E DE IDENTIFICADORES DE INFORMAÇÃO DE IDENTIFICAÇÃO
S2052
VERIFICA INFORMAÇÃO DE CABEÇALHO UTILIZANDO INFORMAÇÃO REPRESENTATIVA DE VERIFICAÇÃO
S2054
BEM SUCEDIDA ?
S2056
Não
Sim
DECRIPTOGRAFIA DE CONTEÚDO CRIPTOGRAFADO
S2057
EXPANSÃO DE CONTEÚDO
S2058
REPRODUÇÃO
S2059
FIM

FIG.37

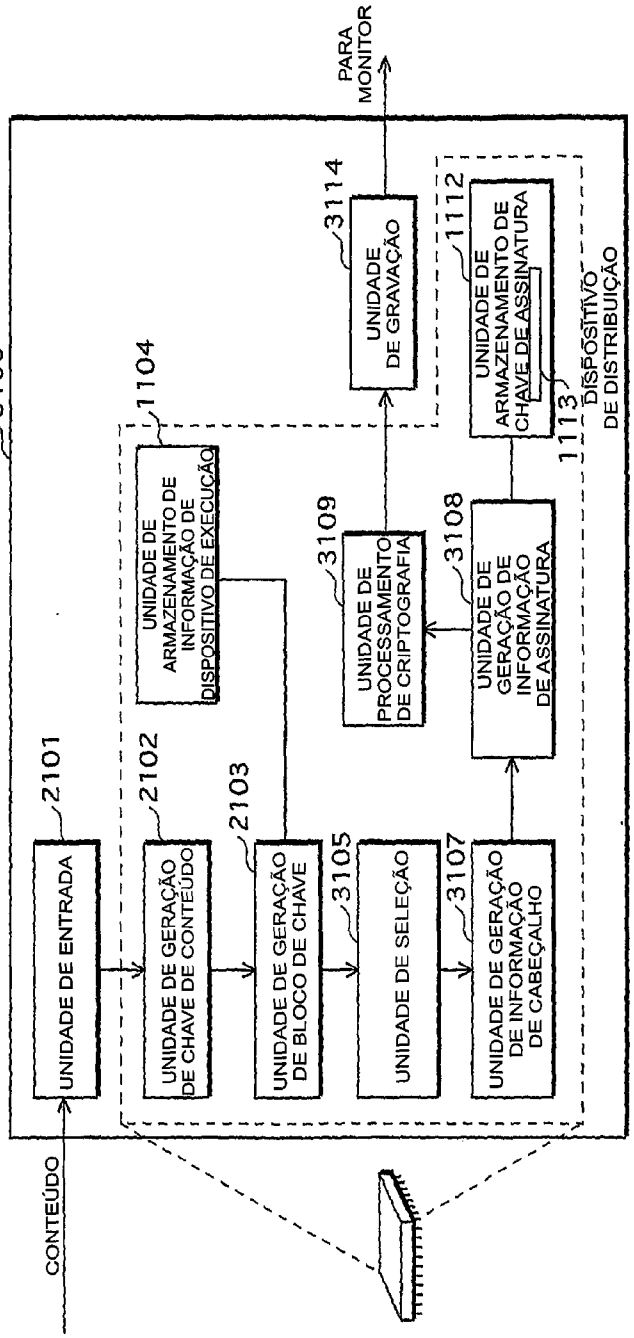

3100
CONTEÚDO
PARA MONITOR
UNIDADE DE ENTRADA
2101
UNIDADE DE GERAÇÃO DE CHAVE DE CONTEÚDO
2102
UNIDADE DE GERAÇÃO DE BLOCO DE CHAVE
2103
UNIDADE DE SELEÇÃO
3105
UNIDADE DE GERAÇÃO DE INFORMAÇÃO DE CABEÇALHO
3107
UNIDADE DE ARMAZENAMENTO DE INFORMAÇÃO DE DISPOSITIVO DE EXECUÇÃO
1104
UNIDADE DE PROCESSAMENTO DE CRIPTOGRAFIA
3109
UNIDADE DE GERAÇÃO DE INFORMAÇÃO DE ASSINATURA
3108
UNIDADE DE GRAVAÇÃO
3114
UNIDADE DE ARMAZENAMENTO DE CHAVE DE ASSINATURA
1112
1113
DISPOSITIVO DE DISTRIBUIÇÃO

FIG.38

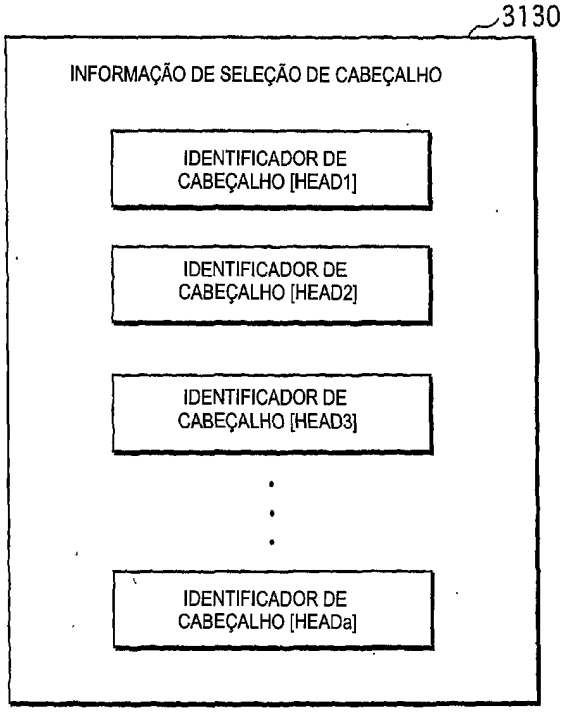

3130
INFORMAÇÃO DE SELEÇÃO DE CABEÇALHO
IDENTIFICADOR DE CABEÇALHO [HEAD1]
IDENTIFICADOR DE CABEÇALHO [HEAD2]
IDENTIFICADOR DE CABEÇALHO [HEAD3]
IDENTIFICADOR DE CABEÇALHO [HEADa]

FIG.39

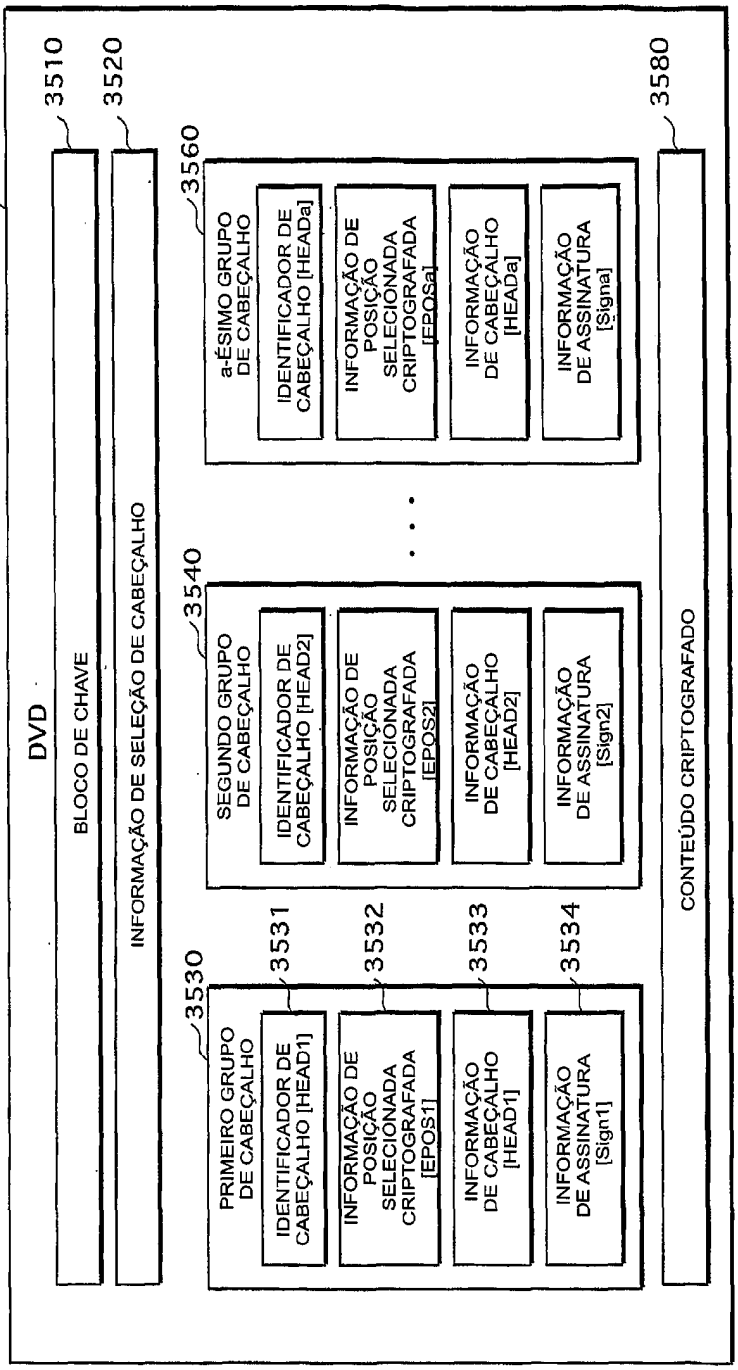

3500
DVD
3510
BLOCO DE CHAVE
3520
INFORMAÇÃO DE SELEÇÃO DE CABEÇALHO
3530
PRIMEIRO GRUPO DE CABEÇALHO
IDENTIFICADOR DE CABEÇALHO [HEAD1]
3531
INFORMAÇÃO DE POSIÇÃO SELECIONADA CRIPTOGRAFADA [EPOS1]
3532
INFORMAÇÃO DE CABEÇALHO [HEAD1]
3533
INFORMAÇÃO DE ASSINATURA [Sign1]
3534
3540
SEGUNDO GRUPO DE CABEÇALHO
IDENTIFICADOR DE CABEÇALHO [HEAD2]
INFORMAÇÃO DE POSIÇÃO SELECIONADA CRIPTOGRAFADA [EPOS2]
INFORMAÇÃO DE CABEÇALHO [HEAD2]
INFORMAÇÃO DE ASSINATURA [Sign2]
. . .
3560
a-ÉSIMO GRUPO DE CABEÇALHO
IDENTIFICADOR DE CABEÇALHO [HEADa]
INFORMAÇÃO DE POSIÇÃO SELECIONADA CRIPTOGRAFADA [EPOSa]
INFORMAÇÃO DE CABEÇALHO [HEADa]
INFORMAÇÃO DE ASSINATURA [Signa]
3580
CONTEÚDO CRIPTOGRAFADO

FIG.40

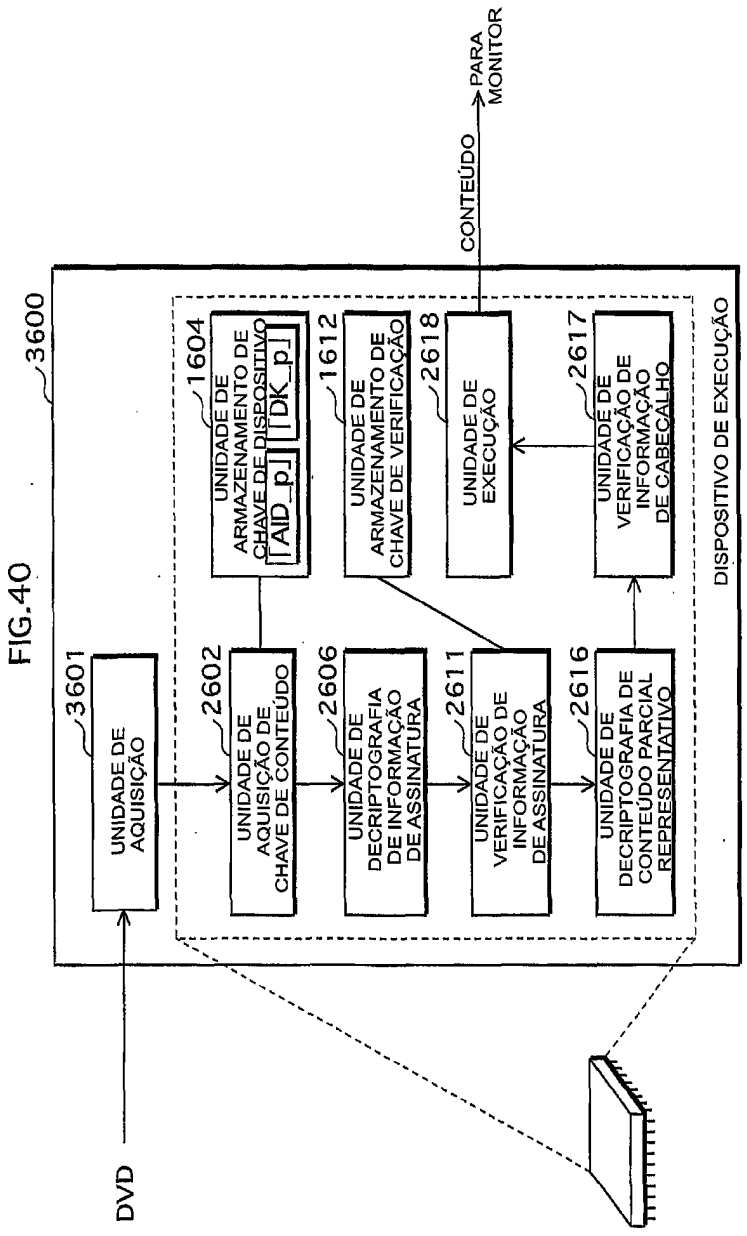

DVD
3600
DISPOSITIVO DE EXECUÇÃO
3601
UNIDADE DE AQUISIÇÃO
2602
UNIDADE DE AQUISIÇÃO DE CHAVE DE CONTEÚDO
2606
UNIDADE DE DECRIPTOGRAFIA DE INFORMAÇÃO DE ASSINATURA
2611
UNIDADE DE VERIFICAÇÃO DE INFORMAÇÃO DE ASSINATURA
2616
UNIDADE DE DECRIPTOGRAFIA DE CONTEÚDO PARCIAL REPRESENTATIVO
1604
UNIDADE DE ARMAZENAMENTO DE CHAVE DE DISPOSITIVO
[AID_p]
[DK_p]
1612
UNIDADE DE ARMAZENAMENTO DE CHAVE DE VERIFICAÇÃO
2618
UNIDADE DE EXECUÇÃO
2617
UNIDADE DE VERIFICAÇÃO DE INFORMAÇÃO DE CABEÇALHO
CONTEÚDO
PARA MONITOR

FIG.41

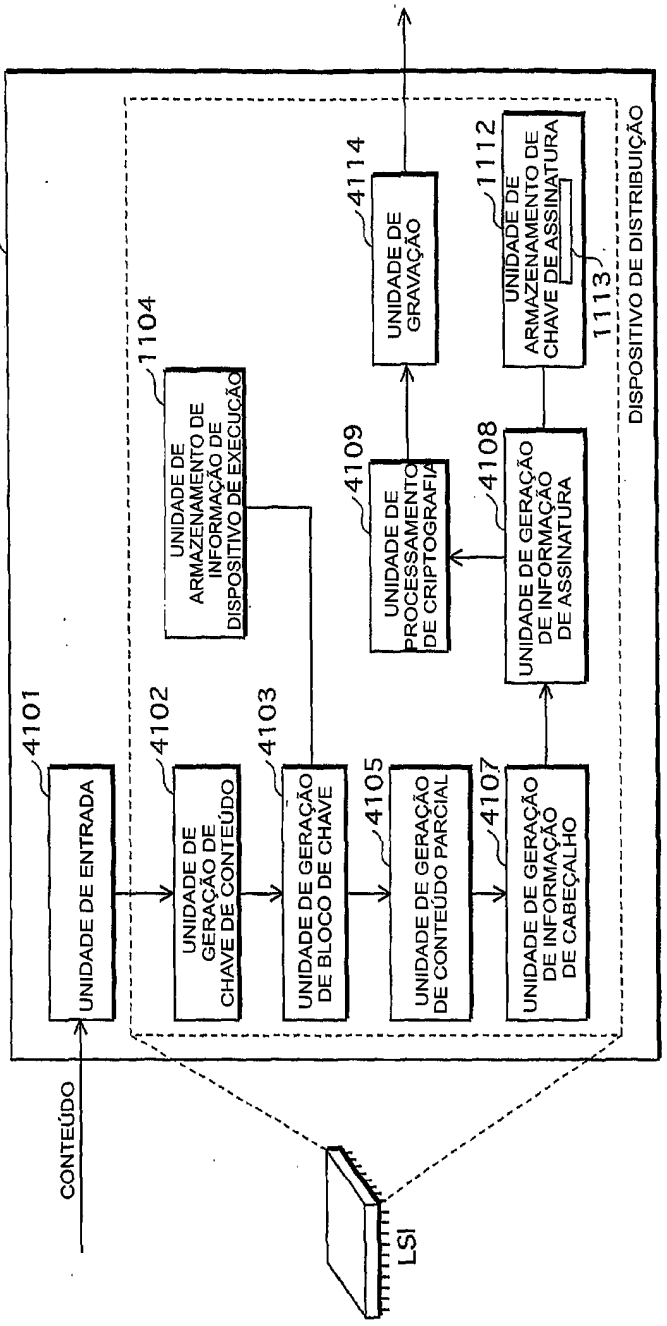

4100
DISPOSITIVO DE DISTRIBUIÇÃO
4101
UNIDADE DE ENTRADA
4102
UNIDADE DE GERAÇÃO DE CHAVE DE CONTEÚDO
4103
UNIDADE DE GERAÇÃO DE BLOCO DE CHAVE
4105
UNIDADE DE GERAÇÃO DE CONTEÚDO PARCIAL
4107
UNIDADE DE GERAÇÃO DE INFORMAÇÃO DE CABEÇALHO
1104
UNIDADE DE ARMAZENAMENTO DE INFORMAÇÃO DE DISPOSITIVO DE EXECUÇÃO
4109
UNIDADE DE PROCESSAMENTO DE CRIPTOGRAFIA
4108
UNIDADE DE GERAÇÃO DE INFORMAÇÃO DE ASSINATURA
4114
UNIDADE DE GRAVAÇÃO
1112
UNIDADE DE ARMAZENAMENTO DE CHAVE DE ASSINATURA
1113
CONTEÚDO
LSI

FIG.42

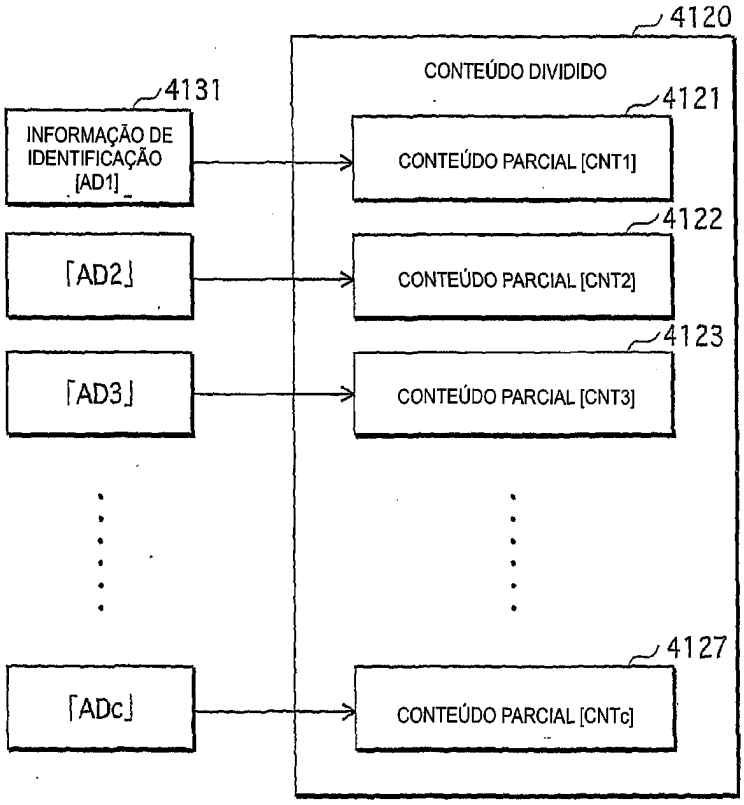

4120
CONTEÚDO DIVIDIDO
4131
INFORMAÇÃO DE IDENTIFICAÇÃO [AD1]
4121
CONTEÚDO PARCIAL [CNT1]
「AD2」
4122
CONTEÚDO PARCIAL [CNT2]
「AD3」
4123
CONTEÚDO PARCIAL [CNT3]
「ADc」
4127
CONTEÚDO PARCIAL [CNTc]

FIG.43

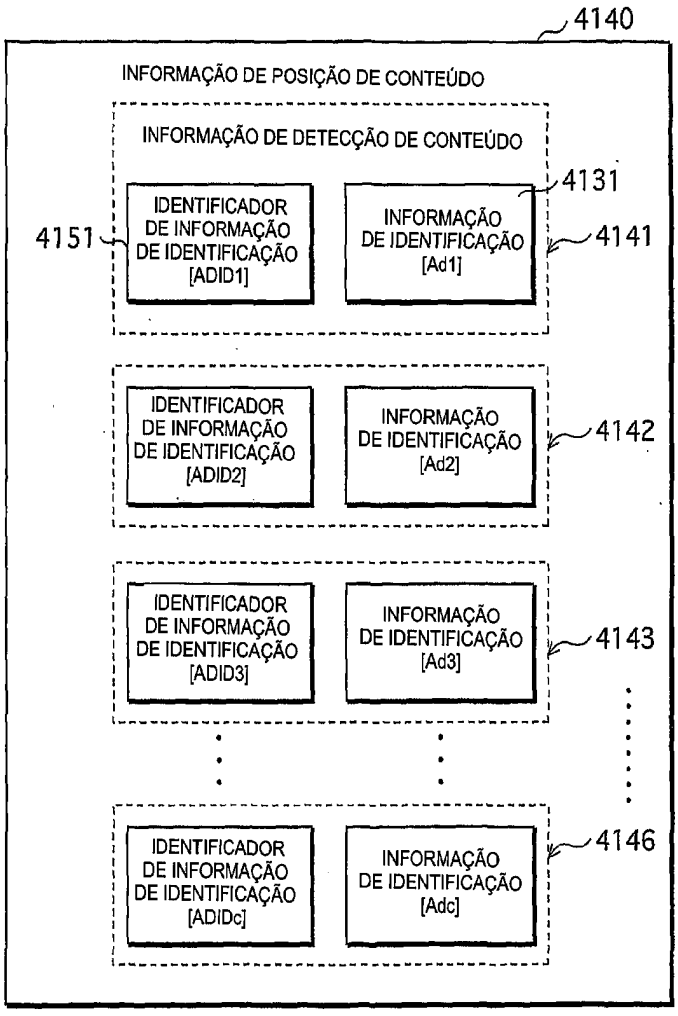

4140
INFORMAÇÃO DE POSIÇÃO DE CONTEÚDO
INFORMAÇÃO DE DETECÇÃO DE CONTEÚDO
4131
4151
IDENTIFICADOR DE INFORMAÇÃO DE IDENTIFICAÇÃO [ADID1]
INFORMAÇÃO DE IDENTIFICAÇÃO [Ad1]
4141
IDENTIFICADOR DE INFORMAÇÃO DE IDENTIFICAÇÃO [ADID2]
INFORMAÇÃO DE IDENTIFICAÇÃO [Ad2]
4142
IDENTIFICADOR DE INFORMAÇÃO DE IDENTIFICAÇÃO [ADID3]
INFORMAÇÃO DE IDENTIFICAÇÃO [Ad3]
4143
IDENTIFICADOR DE INFORMAÇÃO DE IDENTIFICAÇÃO [ADIDc]
INFORMAÇÃO DE IDENTIFICAÇÃO [Adc]
4146

FIG.44

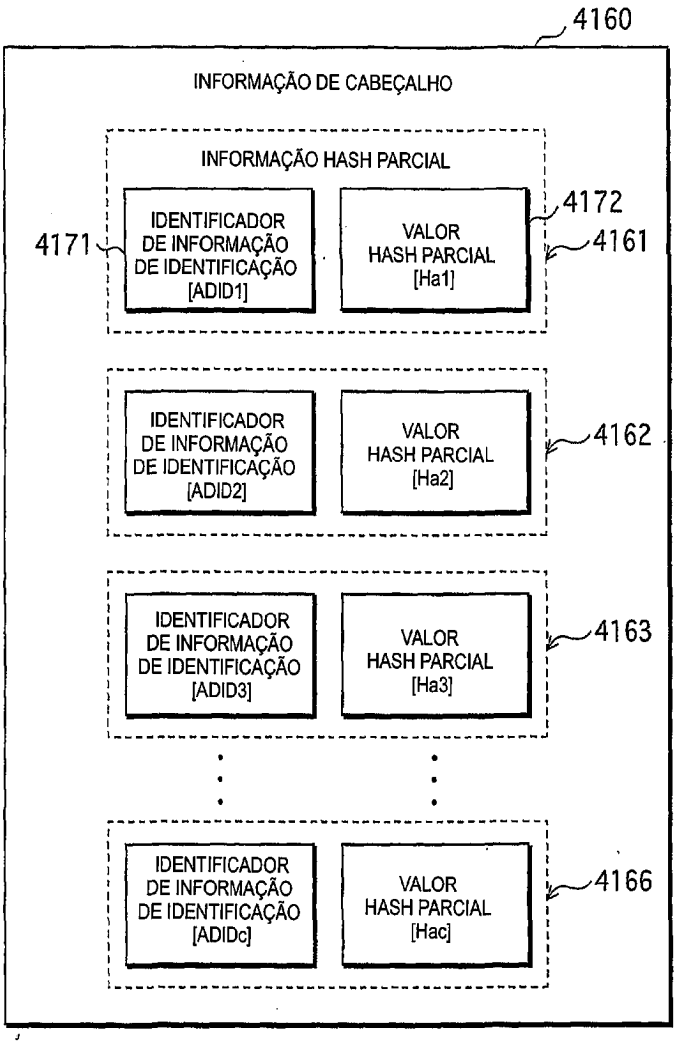

4160
INFORMAÇÃO DE CABEÇALHO
INFORMAÇÃO HASH PARCIAL
4171
IDENTIFICADOR DE INFORMAÇÃO DE IDENTIFICAÇÃO [ADID1]
VALOR HASH PARCIAL [Ha1]
4172
4161
IDENTIFICADOR DE INFORMAÇÃO DE IDENTIFICAÇÃO [ADID2]
VALOR HASH PARCIAL [Ha2]
4162
IDENTIFICADOR DE INFORMAÇÃO DE IDENTIFICAÇÃO [ADID3]
VALOR HASH PARCIAL [Ha3]
4163
IDENTIFICADOR DE INFORMAÇÃO DE IDENTIFICAÇÃO [ADIDc]
VALOR HASH PARCIAL [Hac]
4166

FIG.45

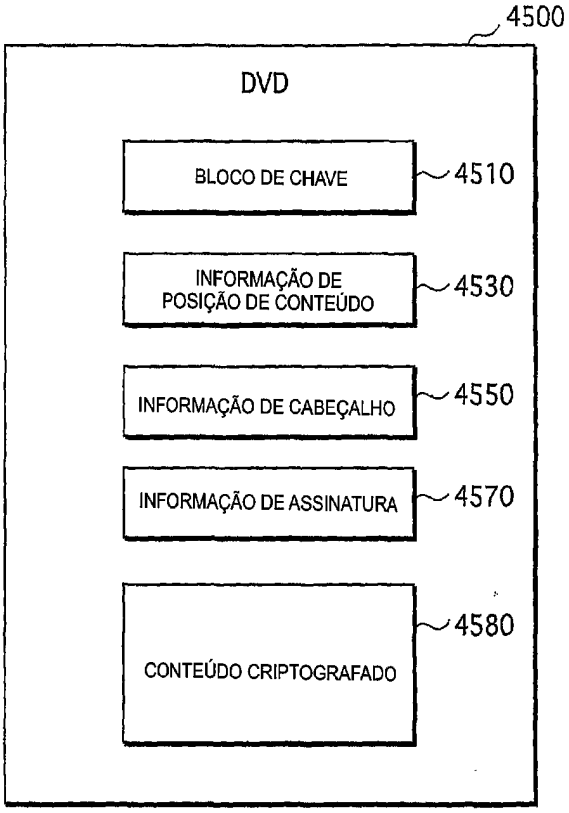

4500
DVD
BLOCO DE CHAVE
4510
INFORMAÇÃO DE POSIÇÃO DE CONTEÚDO
4530
INFORMAÇÃO DE CABEÇALHO
4550
INFORMAÇÃO DE ASSINATURA
4570
CONTEÚDO CRIPTOGRAFADO
4580

FIG.46

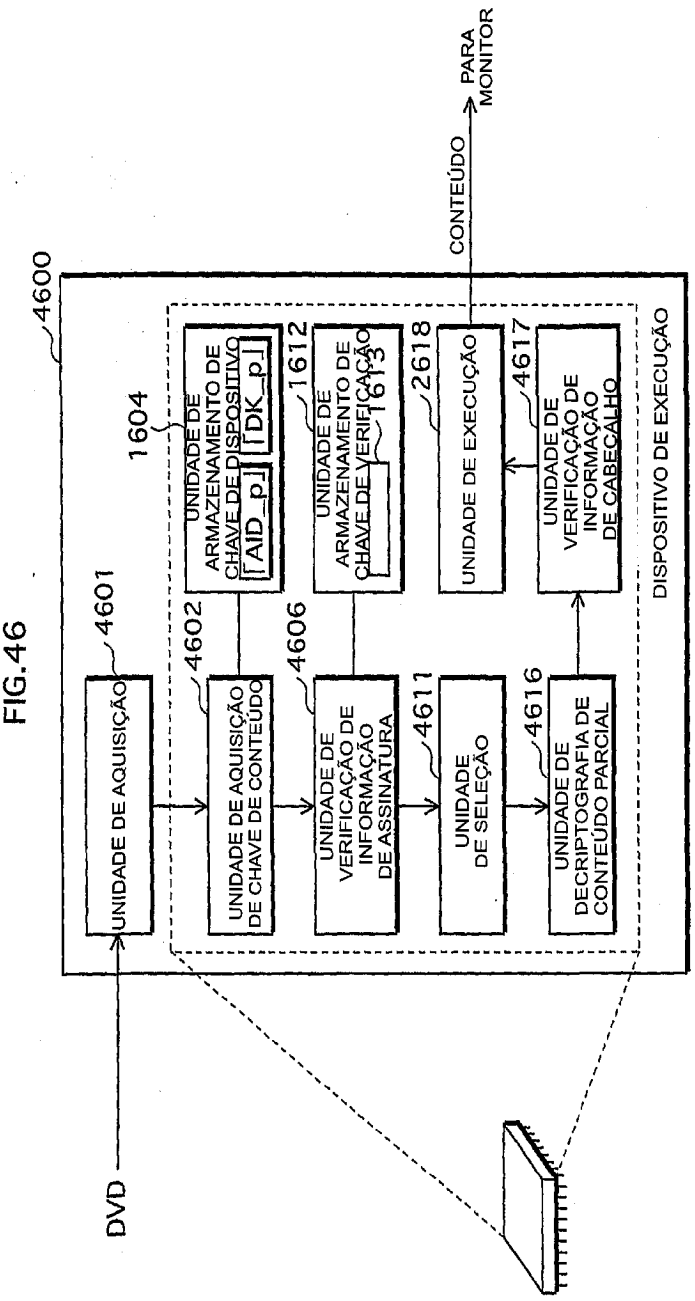

4600
DISPOSITIVO DE EXECUÇÃO
1604
UNIDADE DE AQUISIÇÃO
4601
UNIDADE DE AQUISIÇÃO DE CHAVE DE CONTEÚDO
4602
UNIDADE DE VERIFICAÇÃO DE INFORMAÇÃO DE ASSINATURA
4606
UNIDADE DE SELEÇÃO
4611
UNIDADE DE DECRIPTOGRAFIA DE CONTEÚDO PARCIAL
4616
UNIDADE DE ARMAZENAMENTO DE CHAVE DE DISPOSITIVO
[AID_p] [DK_p]
1612
UNIDADE DE ARMAZENAMENTO DE CHAVE DE VERIFICAÇÃO
1613
UNIDADE DE EXECUÇÃO
2618
UNIDADE DE VERIFICAÇÃO DE INFORMAÇÃO DE CABEÇALHO
4617
CONTEÚDO
PARA MONITOR
DVD

FIG.47

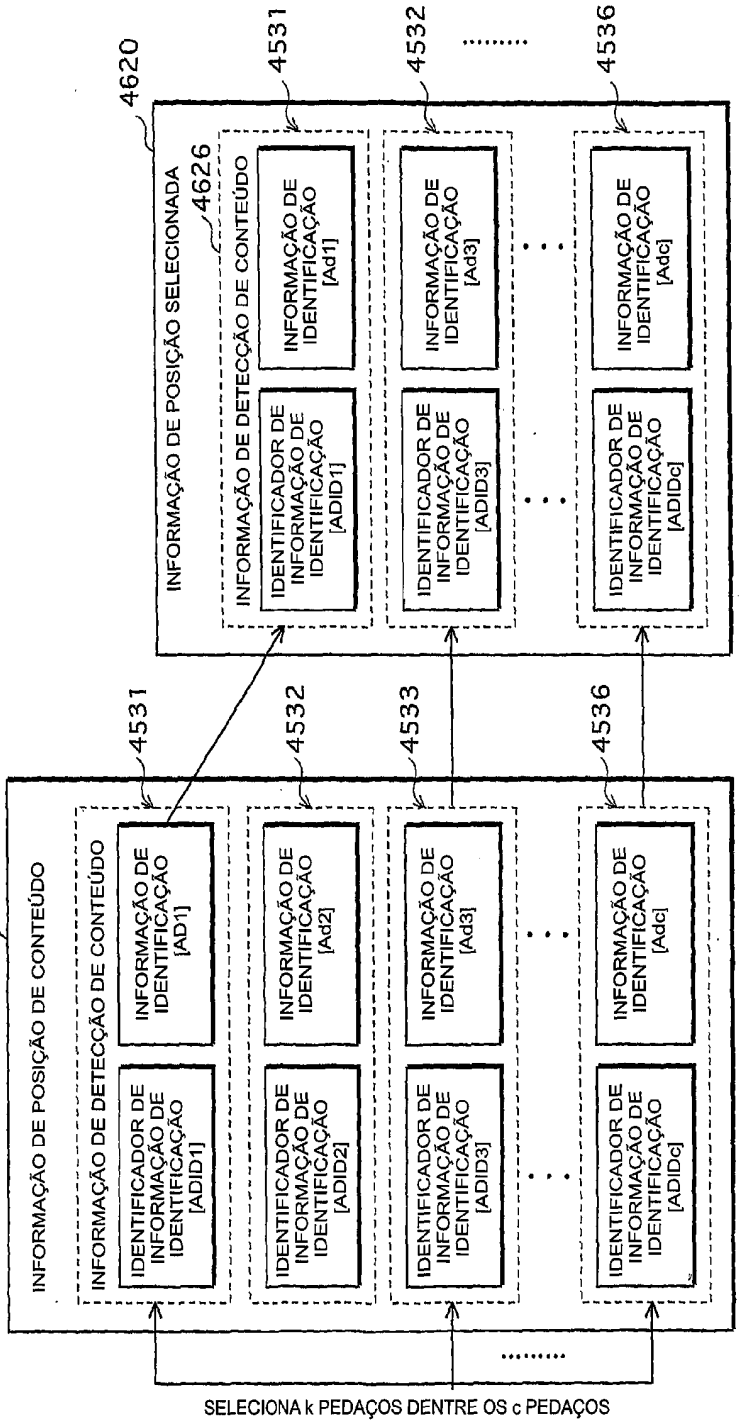

4620
4531
4532
4536
INFORMAÇÃO DE POSIÇÃO SELECIONADA
4626
INFORMAÇÃO DE DETECÇÃO DE CONTEÚDO
INFORMAÇÃO DE IDENTIFICAÇÃO [Ad1]
INFORMAÇÃO DE IDENTIFICAÇÃO [Ad3]
INFORMAÇÃO DE IDENTIFICAÇÃO [Adc]
IDENTIFICADOR DE INFORMAÇÃO DE IDENTIFICAÇÃO [ADID1]
IDENTIFICADOR DE INFORMAÇÃO DE IDENTIFICAÇÃO [ADID3]
IDENTIFICADOR DE INFORMAÇÃO DE IDENTIFICAÇÃO [ADIDc]
4530
4531
4532
4533
4536
INFORMAÇÃO DE POSIÇÃO DE CONTEÚDO
INFORMAÇÃO DE DETECÇÃO DE CONTEÚDO
INFORMAÇÃO DE IDENTIFICAÇÃO [AD1]
INFORMAÇÃO DE IDENTIFICAÇÃO [Ad2]
INFORMAÇÃO DE IDENTIFICAÇÃO [Ad3]
INFORMAÇÃO DE IDENTIFICAÇÃO [Adc]
IDENTIFICADOR DE INFORMAÇÃO DE IDENTIFICAÇÃO [ADID1]
IDENTIFICADOR DE INFORMAÇÃO DE IDENTIFICAÇÃO [ADID2]
IDENTIFICADOR DE INFORMAÇÃO DE IDENTIFICAÇÃO [ADID3]
IDENTIFICADOR DE INFORMAÇÃO DE IDENTIFICAÇÃO [ADIDc]
SELECIONA k PEDAÇOS DENTRE OS c PEDAÇOS

FIG.48

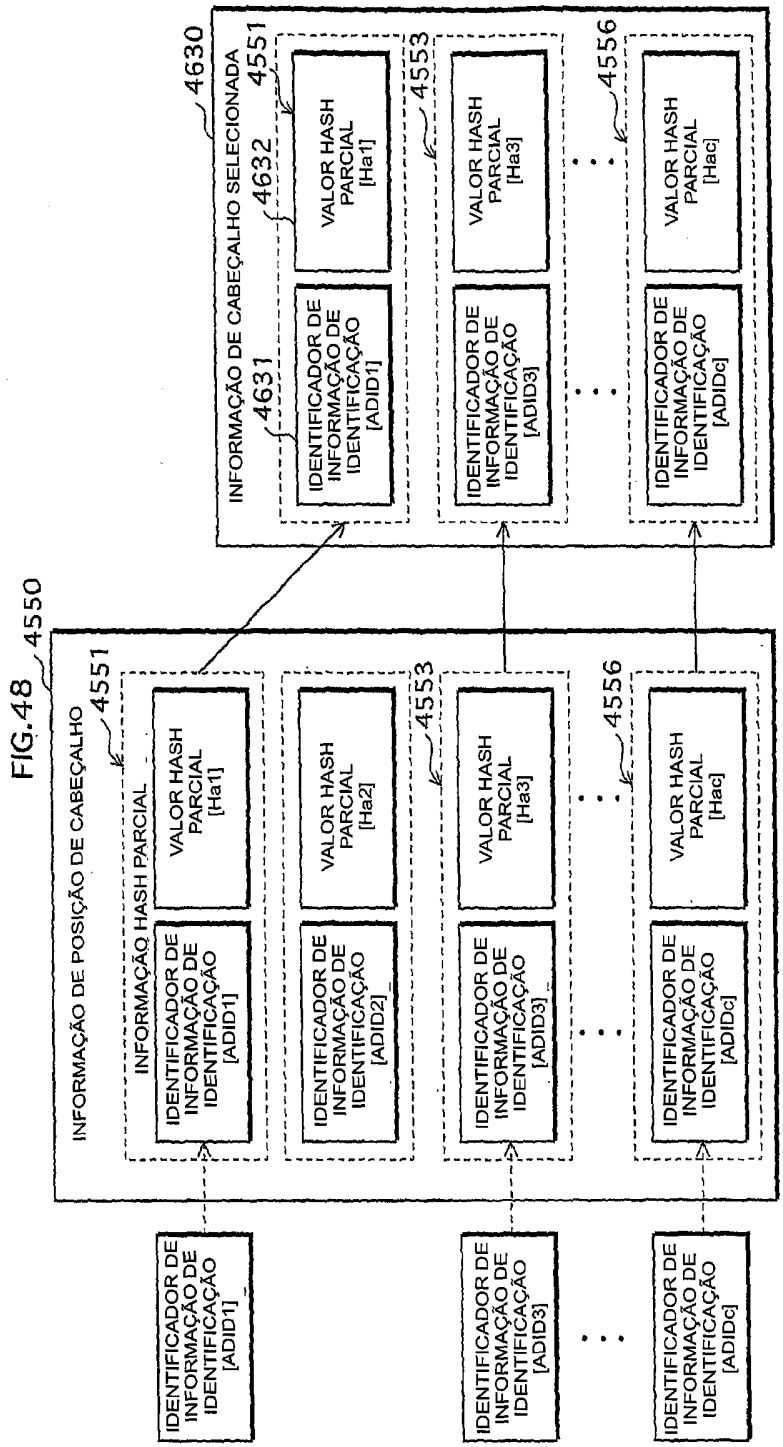

4550
INFORMAÇÃO DE POSIÇÃO DE CABEÇALHO
4551
INFORMAÇÃO HASH PARCIAL
IDENTIFICADOR DE INFORMAÇÃO DE IDENTIFICAÇÃO [ADID1]
VALOR HASH PARCIAL [Ha1]
4553
IDENTIFICADOR DE INFORMAÇÃO DE IDENTIFICAÇÃO [ADID2]
VALOR HASH PARCIAL [Ha2]
IDENTIFICADOR DE INFORMAÇÃO DE IDENTIFICAÇÃO [ADID3]
VALOR HASH PARCIAL [Ha3]
4556
IDENTIFICADOR DE INFORMAÇÃO DE IDENTIFICAÇÃO [ADIDc]
VALOR HASH PARCIAL [Hac]
4630
INFORMAÇÃO DE CABEÇALHO SELECIONADA
4551
4631
4632
IDENTIFICADOR DE INFORMAÇÃO DE IDENTIFICAÇÃO [ADID1]
VALOR HASH PARCIAL [Ha1]
4553
IDENTIFICADOR DE INFORMAÇÃO DE IDENTIFICAÇÃO [ADID3]
VALOR HASH PARCIAL [Ha3]
4556
IDENTIFICADOR DE INFORMAÇÃO DE IDENTIFICAÇÃO [ADIDc]
VALOR HASH PARCIAL [Hac]
IDENTIFICADOR DE INFORMAÇÃO DE IDENTIFICAÇÃO [ADID1]
IDENTIFICADOR DE INFORMAÇÃO DE IDENTIFICAÇÃO [ADID3]
IDENTIFICADOR DE INFORMAÇÃO DE IDENTIFICAÇÃO [ADIDc]

FIG.49

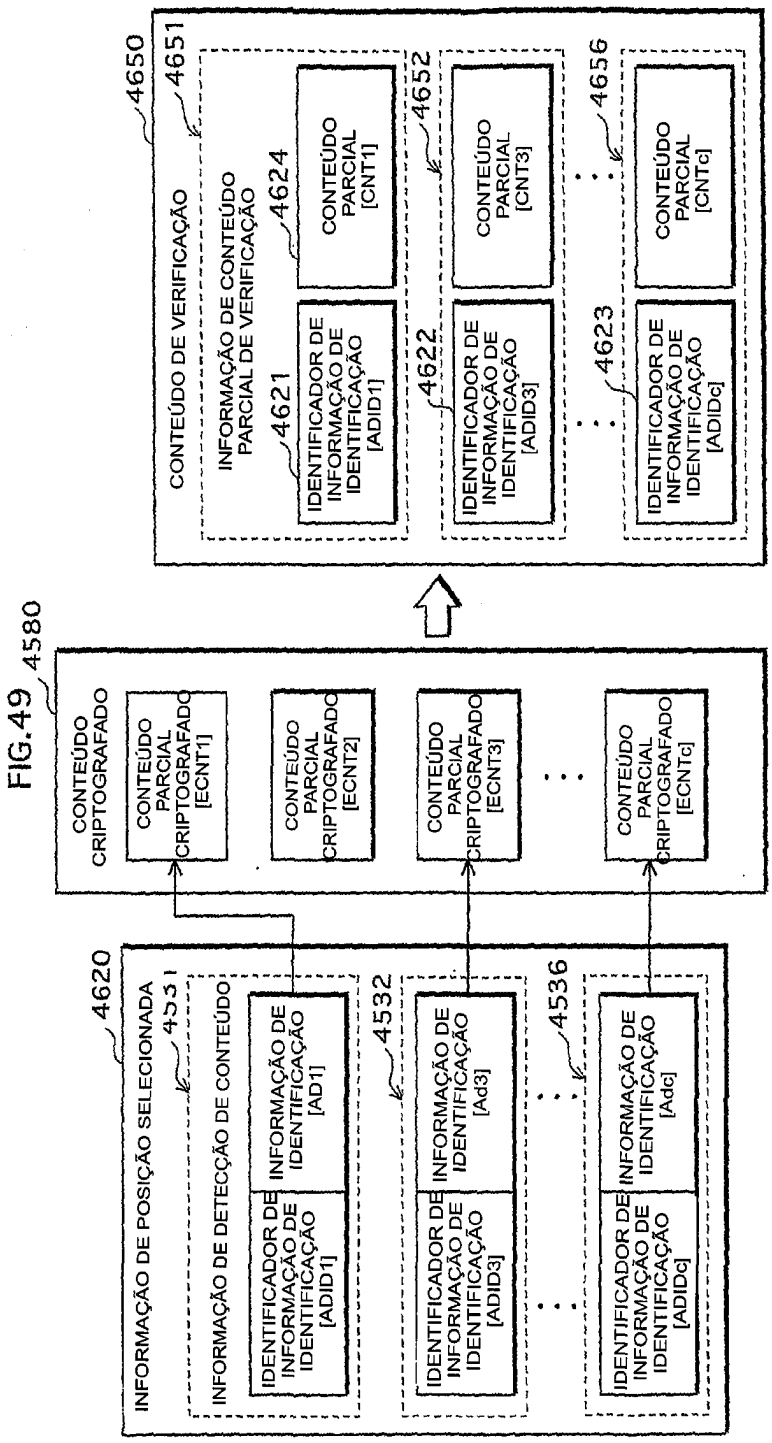

4620
INFORMAÇÃO DE POSIÇÃO SELECIONADA
4531
INFORMAÇÃO DE DETECÇÃO DE CONTEÚDO
IDENTIFICADOR DE INFORMAÇÃO DE IDENTIFICAÇÃO [ADID1]
INFORMAÇÃO DE IDENTIFICAÇÃO [AD1]
4532
IDENTIFICADOR DE INFORMAÇÃO DE IDENTIFICAÇÃO [ADID3]
INFORMAÇÃO DE IDENTIFICAÇÃO [Ad3]
4536
IDENTIFICADOR DE INFORMAÇÃO DE IDENTIFICAÇÃO [ADIDc]
INFORMAÇÃO DE IDENTIFICAÇÃO [Adc]
4580
CONTEÚDO CRIPTOGRAFADO
CONTEÚDO PARCIAL CRIPTOGRAFADO [ECNT1]
CONTEÚDO PARCIAL CRIPTOGRAFADO [ECNT2]
CONTEÚDO PARCIAL CRIPTOGRAFADO [ECNT3]
CONTEÚDO PARCIAL CRIPTOGRAFADO [ECNTc]
4650
CONTEÚDO DE VERIFICAÇÃO
4651
INFORMAÇÃO DE CONTEÚDO PARCIAL DE VERIFICAÇÃO
4621
IDENTIFICADOR DE INFORMAÇÃO DE IDENTIFICAÇÃO [ADID1]
4624
CONTEÚDO PARCIAL [CNT1]
4622
IDENTIFICADOR DE INFORMAÇÃO DE IDENTIFICAÇÃO [ADID3]
4652
CONTEÚDO PARCIAL [CNT3]
4623
IDENTIFICADOR DE INFORMAÇÃO DE IDENTIFICAÇÃO [ADIDc]
4656
CONTEÚDO PARCIAL [CNTc]

FIG.50

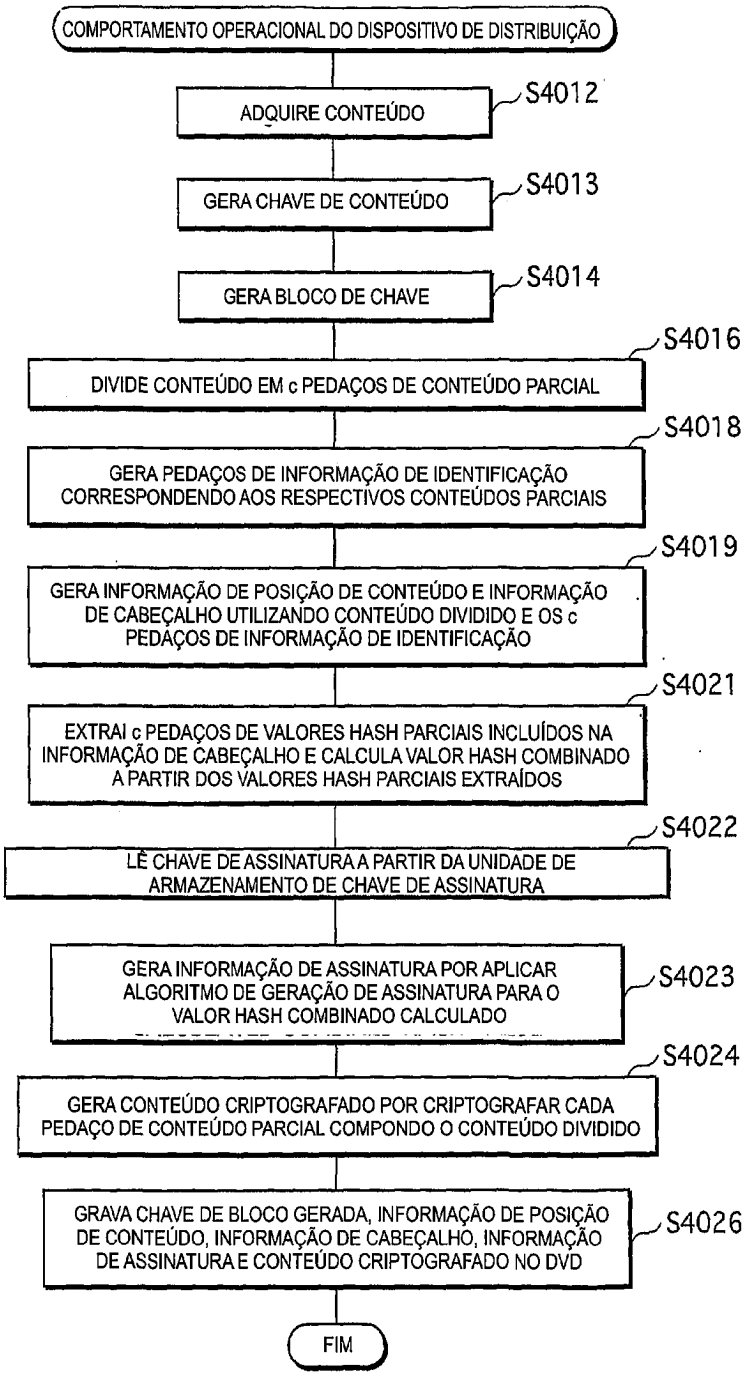

COMPORTAMENTO OPERACIONAL DO DISPOSITIVO DE DISTRIBUIÇÃO
ADQUIRE CONTEÚDO
S4012
GERA CHAVE DE CONTEÚDO
S4013
GERA BLOCO DE CHAVE
S4014
DIVIDE CONTEÚDO EM c PEDAÇOS DE CONTEÚDO PARCIAL
S4016
GERA PEDAÇOS DE INFORMAÇÃO DE IDENTIFICAÇÃO CORRESPONDENDO AOS RESPECTIVOS CONTEÚDOS PARCIAIS
S4018
GERA INFORMAÇÃO DE POSIÇÃO DE CONTEÚDO E INFORMAÇÃO DE CABEÇALHO UTILIZANDO CONTEÚDO DIVIDIDO E OS c PEDAÇOS DE INFORMAÇÃO DE IDENTIFICAÇÃO
S4019
EXTRAI c PEDAÇOS DE VALORES HASH PARCIAIS INCLUÍDOS NA INFORMAÇÃO DE CABEÇALHO E CALCULA VALOR HASH COMBINADO A PARTIR DOS VALORES HASH PARCIAIS EXTRAÍDOS
S4021
LÊ CHAVE DE ASSINATURA A PARTIR DA UNIDADE DE ARMAZENAMENTO DE CHAVE DE ASSINATURA
S4022
GERA INFORMAÇÃO DE ASSINATURA POR APLICAR ALGORITMO DE GERAÇÃO DE ASSINATURA PARA O VALOR HASH COMBINADO CALCULADO
S4023
GERA CONTEÚDO CRIPTOGRAFADO POR CRIPTOGRAFAR CADA PEDAÇO DE CONTEÚDO PARCIAL COMPONDO O CONTEÚDO DIVIDIDO
S4024
GRAVA CHAVE DE BLOCO GERADA, INFORMAÇÃO DE POSIÇÃO DE CONTEÚDO, INFORMAÇÃO DE CABEÇALHO, INFORMAÇÃO DE ASSINATURA E CONTEÚDO CRIPTOGRAFADO NO DVD
S4026
FIM

FIG.51

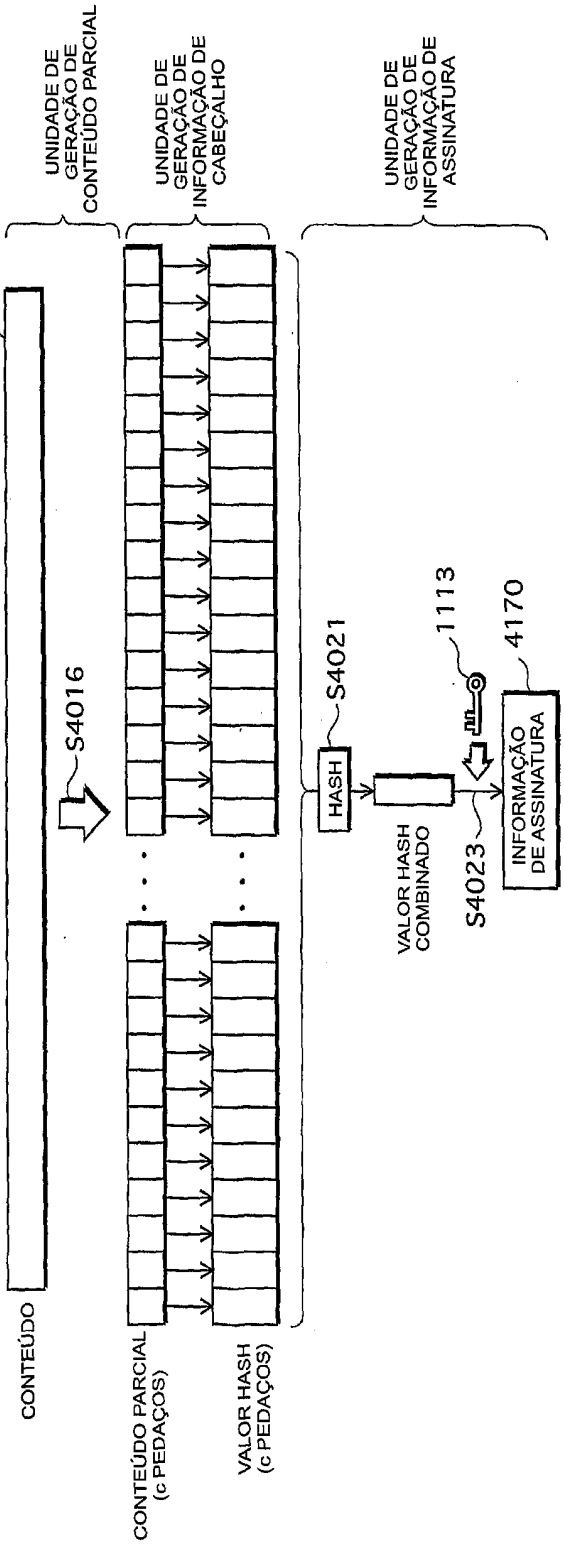

UNIDADE DE GERAÇÃO DE CONTEÚDO PARCIAL
UNIDADE DE GERAÇÃO DE INFORMAÇÃO DE CABEÇALHO
UNIDADE DE GERAÇÃO DE INFORMAÇÃO DE ASSINATURA
4119
S4016
CONTEÚDO
CONTEÚDO PARCIAL (c PEDAÇOS)
VALOR HASH (c PEDAÇOS)
HASH
S4021
VALOR HASH COMBINADO
1113
S4023
4170
INFORMAÇÃO DE ASSINATURA

FIG.52

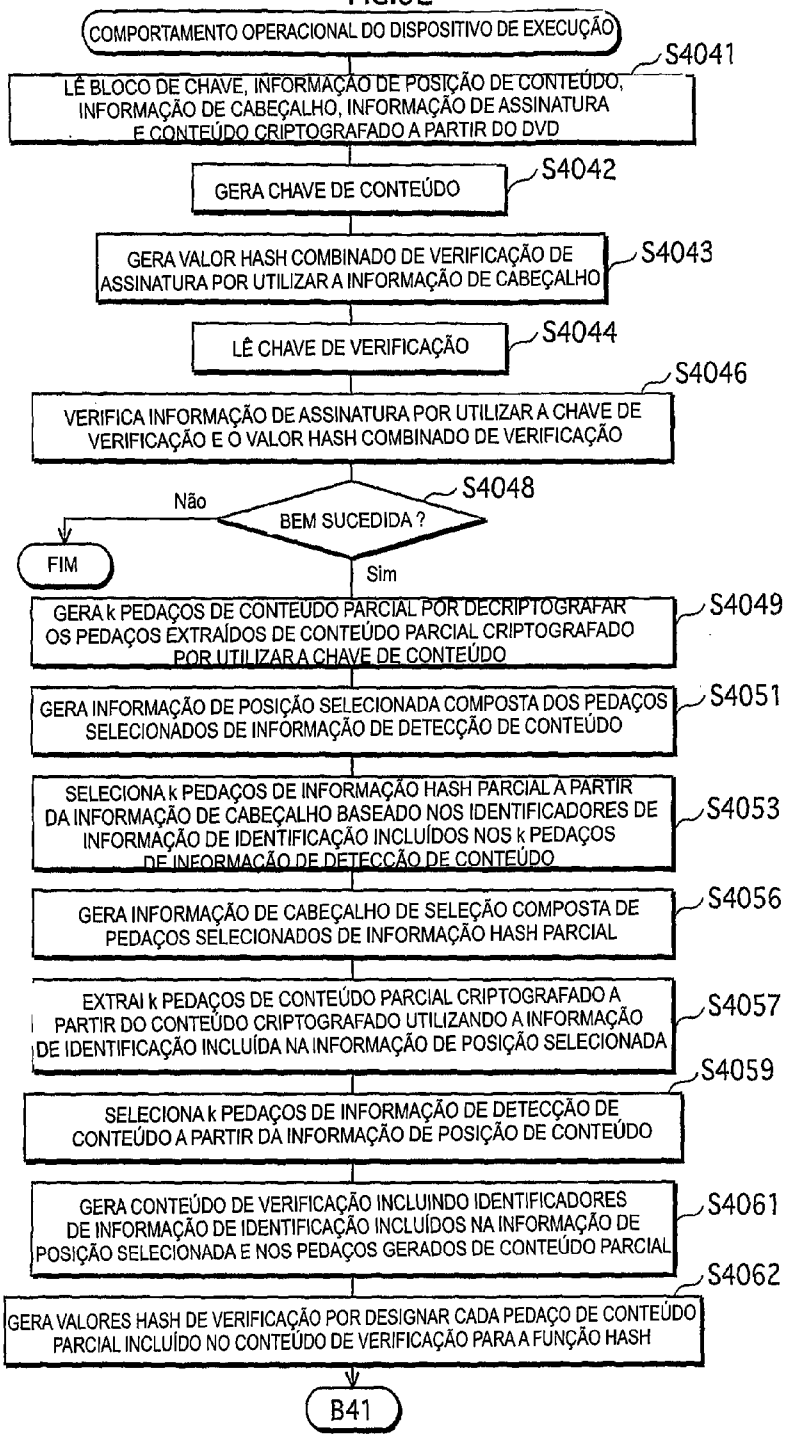
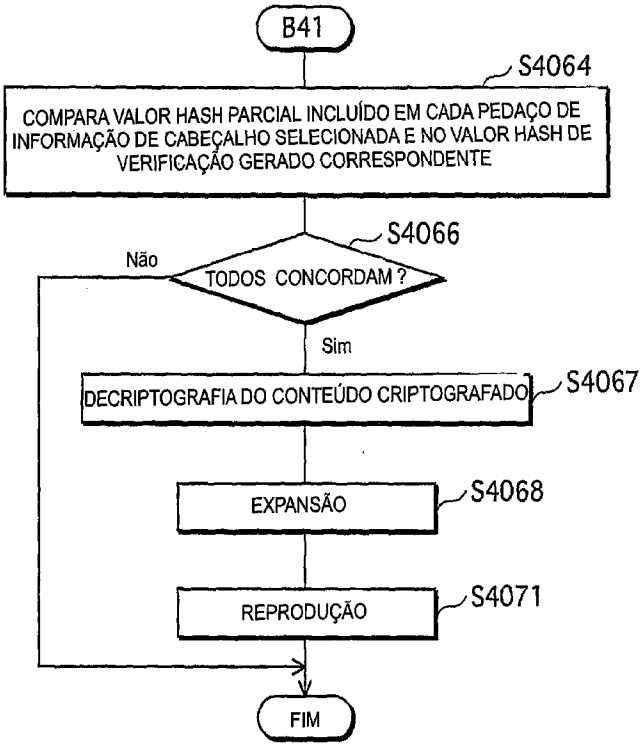

COMPORTAMENTO OPERACIONAL DO DISPOSITIVO DE EXECUÇÃO
S4041
LÊ BLOCO DE CHAVE, INFORMAÇÃO DE POSIÇÃO DE CONTEÚDO, INFORMAÇÃO DE CABEÇALHO, INFORMAÇÃO DE ASSINATURA E CONTEÚDO CRIPTOGRAFADO A PARTIR DO DVD
S4042
GERA CHAVE DE CONTEÚDO
S4043
GERA VALOR HASH COMBINADO DE VERIFICAÇÃO DE ASSINATURA POR UTILIZAR A INFORMAÇÃO DE CABEÇALHO
S4044
LÊ CHAVE DE VERIFICAÇÃO
S4046
VERIFICA INFORMAÇÃO DE ASSINATURA POR UTILIZAR A CHAVE DE VERIFICAÇÃO E O VALOR HASH COMBINADO DE VERIFICAÇÃO
S4048
BEM SUCEDIDA ?
Não
FIM
Sim
S4049
GERA k PEDAÇOS DE CONTEÚDO PARCIAL POR DECRIPTOGRAFAR OS PEDAÇOS EXTRAÍDOS DE CONTEÚDO PARCIAL CRIPTOGRAFADO POR UTILIZAR A CHAVE DE CONTEÚDO
S4051
GERA INFORMAÇÃO DE POSIÇÃO SELECIONADA COMPOSTA DOS PEDAÇOS SELECIONADOS DE INFORMAÇÃO DE DETECÇÃO DE CONTEÚDO
S4053
SELECIONA k PEDAÇOS DE INFORMAÇÃO HASH PARCIAL A PARTIR DA INFORMAÇÃO DE CABEÇALHO BASEADO NOS IDENTIFICADORES DE INFORMAÇÃO DE IDENTIFICAÇÃO INCLUÍDOS NOS k PEDAÇOS DE INFORMAÇÃO DE DETECÇÃO DE CONTEÚDO
S4056
GERA INFORMAÇÃO DE CABEÇALHO DE SELEÇÃO COMPOSTA DE PEDAÇOS SELECIONADOS DE INFORMAÇÃO HASH PARCIAL
S4057
EXTRAI k PEDAÇOS DE CONTEÚDO PARCIAL CRIPTOGRAFADO A PARTIR DO CONTEÚDO CRIPTOGRAFADO UTILIZANDO A INFORMAÇÃO DE IDENTIFICAÇÃO INCLUÍDA NA INFORMAÇÃO DE POSIÇÃO SELECIONADA
S4059
SELECIONA k PEDAÇOS DE INFORMAÇÃO DE DETECÇÃO DE CONTEÚDO A PARTIR DA INFORMAÇÃO DE POSIÇÃO DE CONTEÚDO
S4061
GERA CONTEÚDO DE VERIFICAÇÃO INCLUINDO IDENTIFICADORES DE INFORMAÇÃO DE IDENTIFICAÇÃO INCLUÍDOS NA INFORMAÇÃO DE POSIÇÃO SELECIONADA E NOS PEDAÇOS GERADOS DE CONTEÚDO PARCIAL
S4062
GERA VALORES HASH DE VERIFICAÇÃO POR DESIGNAR CADA PEDAÇO DE CONTEÚDO PARCIAL INCLUÍDO NO CONTEÚDO DE VERIFICAÇÃO PARA A FUNÇÃO HASH
B41

FIG.53


B41
S4064
COMPARA VALOR HASH PARCIAL INCLUÍDO EM CADA PEDAÇO DE INFORMAÇÃO DE CABEÇALHO SELECIONADA E NO VALOR HASH DE VERIFICAÇÃO GERADO CORRESPONDENTE
S4066
Não
TODOS CONCORDAM ?
Sim
DECRIPTOGRAFIA DO CONTEÚDO CRIPTOGRAFADO
S4067
EXPANSÃO
S4068
REPRODUÇÃO
S4071
FIM

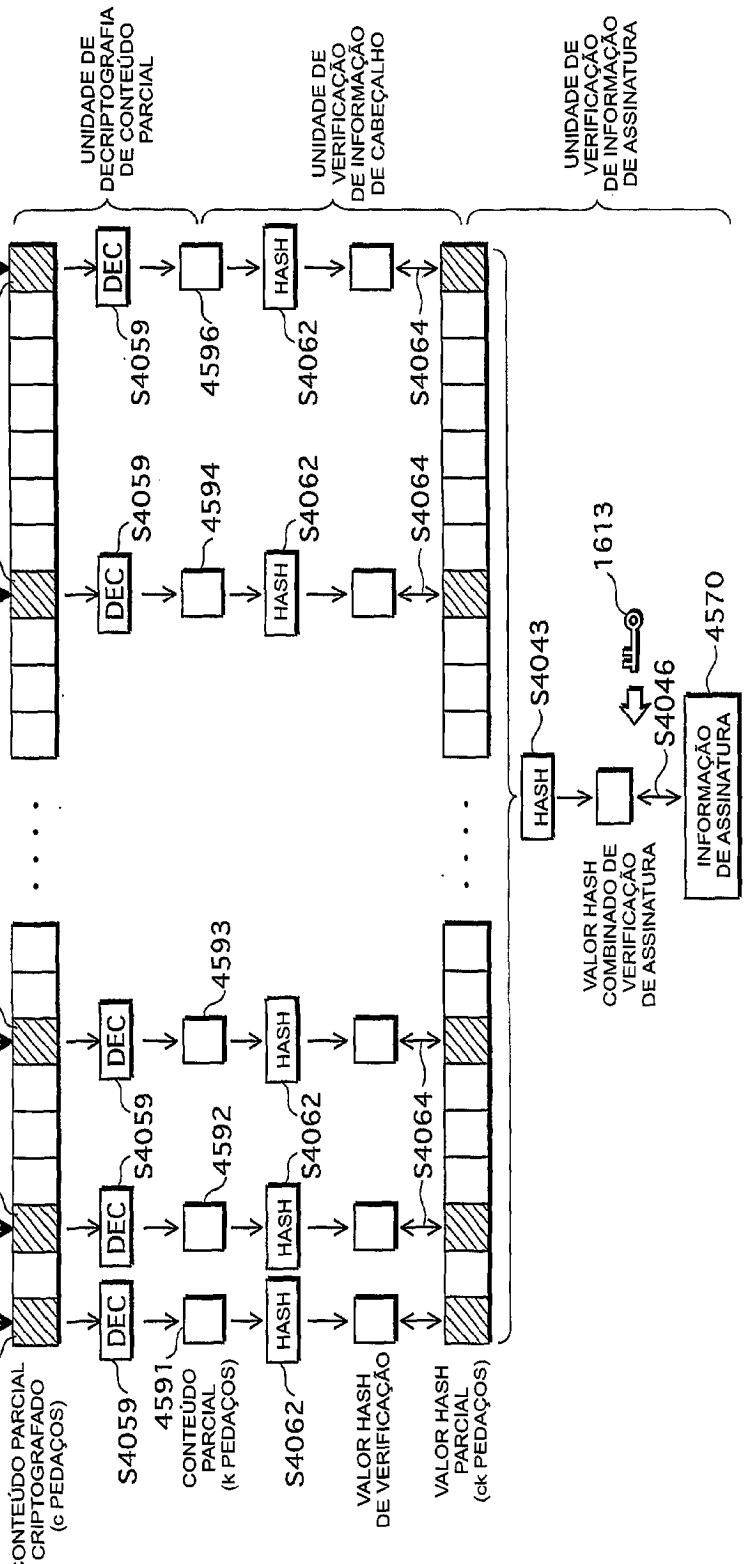


FIG.54
UNIDADE DE DECRIPTOGRAFIA DE CONTEÚDO PARCIAL
UNIDADE DE VERIFICAÇÃO DE INFORMAÇÃO DE CABEÇALHO
UNIDADE DE VERIFICAÇÃO DE INFORMAÇÃO DE ASSINATURA
S4057
4581
4582
4583
4584
4586
CONTEÚDO PARCIAL CRIPTOGRAFADO (c PEDAÇOS)
DEC
S4059
4591
4592
4593
4594
4596
CONTEÚDO PARCIAL (k PEDAÇOS)
HASH
S4062
VALOR HASH DE VERIFICAÇÃO
S4064
VALOR HASH PARCIAL (ck PEDAÇOS)
S4043
VALOR HASH COMBINADO DE VERIFICAÇÃO DE ASSINATURA
1613
S4046
INFORMAÇÃO DE ASSINATURA
4570

FIG.55

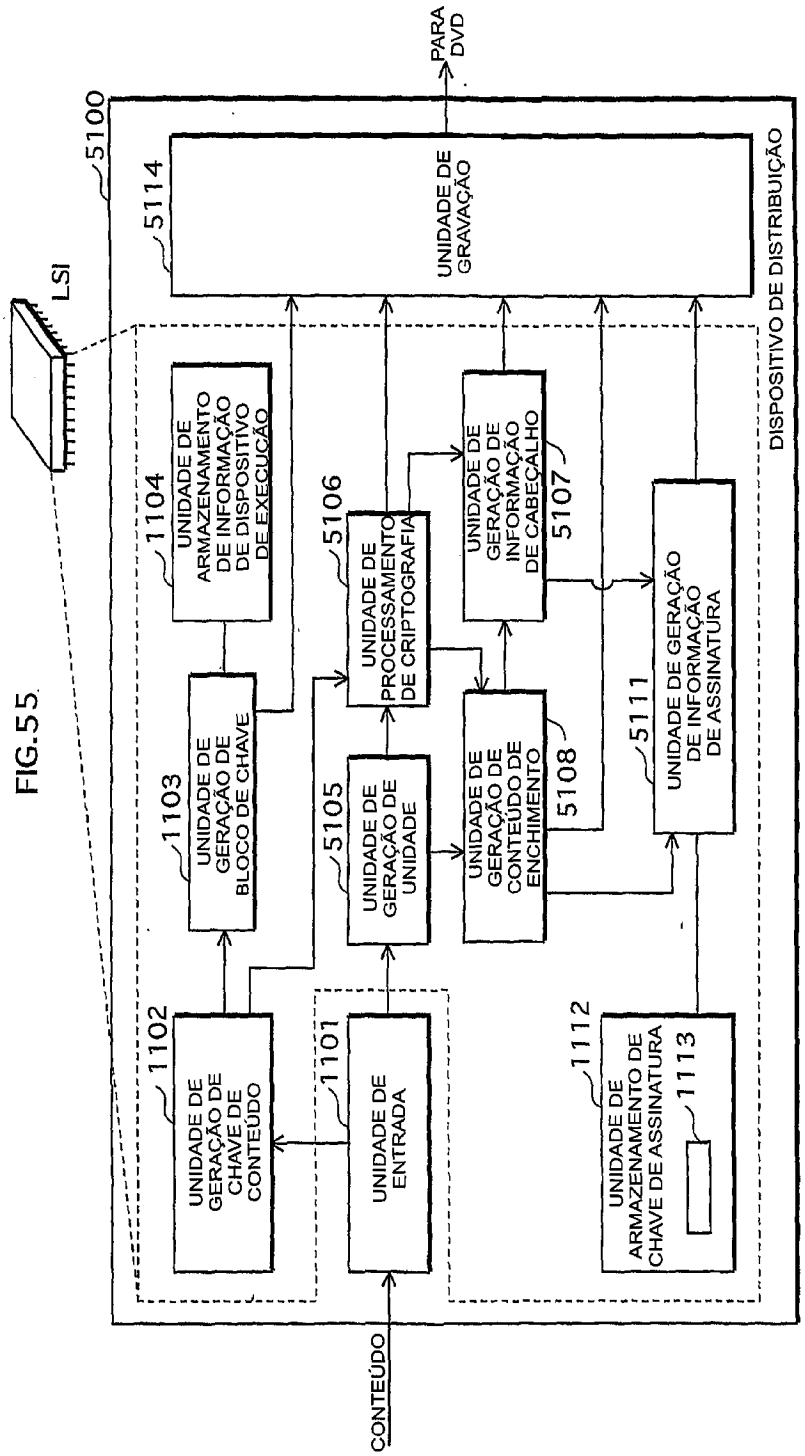

PARA DVD
5100
DISPOSITIVO DE DISTRIBUIÇÃO
LSI
5114
UNIDADE DE GRAVAÇÃO
1104
UNIDADE DE ARMAZENAMENTO DE INFORMAÇÃO DE DISPOSITIVO DE EXECUÇÃO
5106
UNIDADE DE PROCESSAMENTO DE CRIPTOGRAFIA
5107
UNIDADE DE GERAÇÃO DE INFORMAÇÃO DE CABEÇALHO
1103
UNIDADE DE GERAÇÃO DE BLOCO DE CHAVE
5105
UNIDADE DE GERAÇÃO DE UNIDADE
5108
UNIDADE DE GERAÇÃO DE CONTEÚDO DE ENCHIMENTO
5111
UNIDADE DE GERAÇÃO DE INFORMAÇÃO DE ASSINATURA
1102
UNIDADE DE GERAÇÃO DE CHAVE DE CONTEÚDO
1101
UNIDADE DE ENTRADA
1112
UNIDADE DE ARMAZENAMENTO DE CHAVE DE ASSINATURA
1113
CONTEÚDO

FIG.56

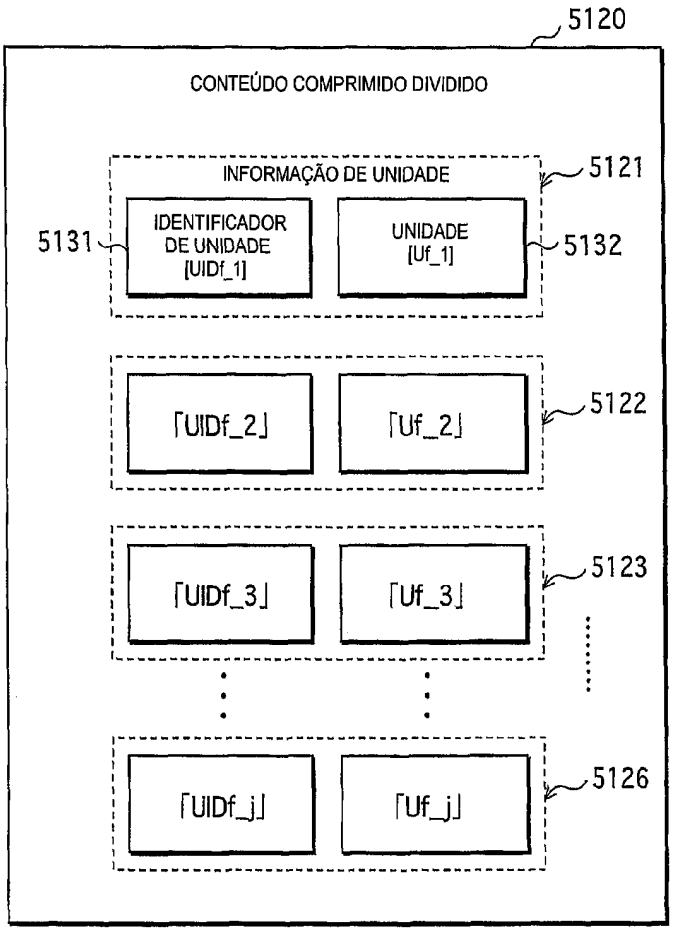

5120
CONTEÚDO COMPRIMIDO DIVIDIDO
INFORMAÇÃO DE UNIDADE
5121
5131
IDENTIFICADOR DE UNIDADE [UIDf_1]
UNIDADE [Uf_1]
5132
5122
⌈UIDf_2⌋
⌈Uf_2⌋
5123
⌈UIDf_3⌋
⌈Uf_3⌋
5126
⌈UIDf_j⌋
⌈Uf_j⌋

FIG.57

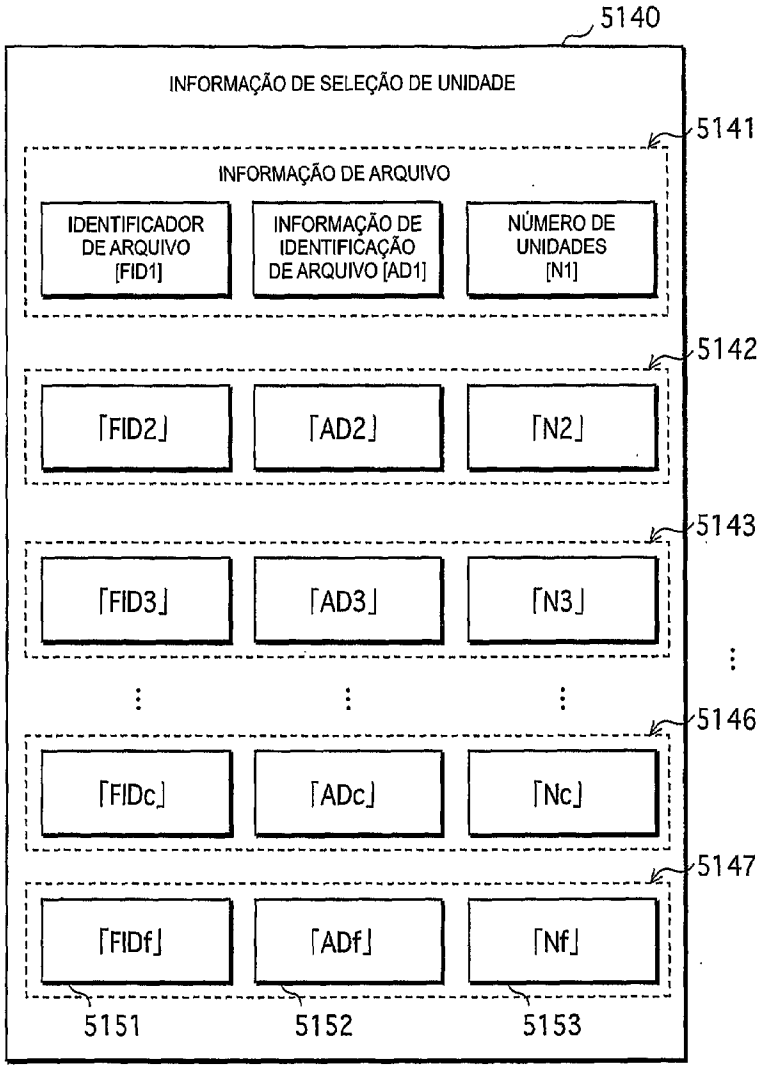

5140
INFORMAÇÃO DE SELEÇÃO DE UNIDADE
5141
INFORMAÇÃO DE ARQUIVO
IDENTIFICADOR DE ARQUIVO [FID1]
INFORMAÇÃO DE IDENTIFICAÇÃO DE ARQUIVO [AD1]
NÚMERO DE UNIDADES [N1]
5142
⌈FID2⌋
⌈AD2⌋
⌈N2⌋
5143
⌈FID3⌋
⌈AD3⌋
⌈N3⌋
5146
⌈FIDc⌋
⌈ADc⌋
⌈Nc⌋
5147
⌈FIDf⌋
⌈ADf⌋
⌈Nf⌋
5151
5152
5153

FIG.58

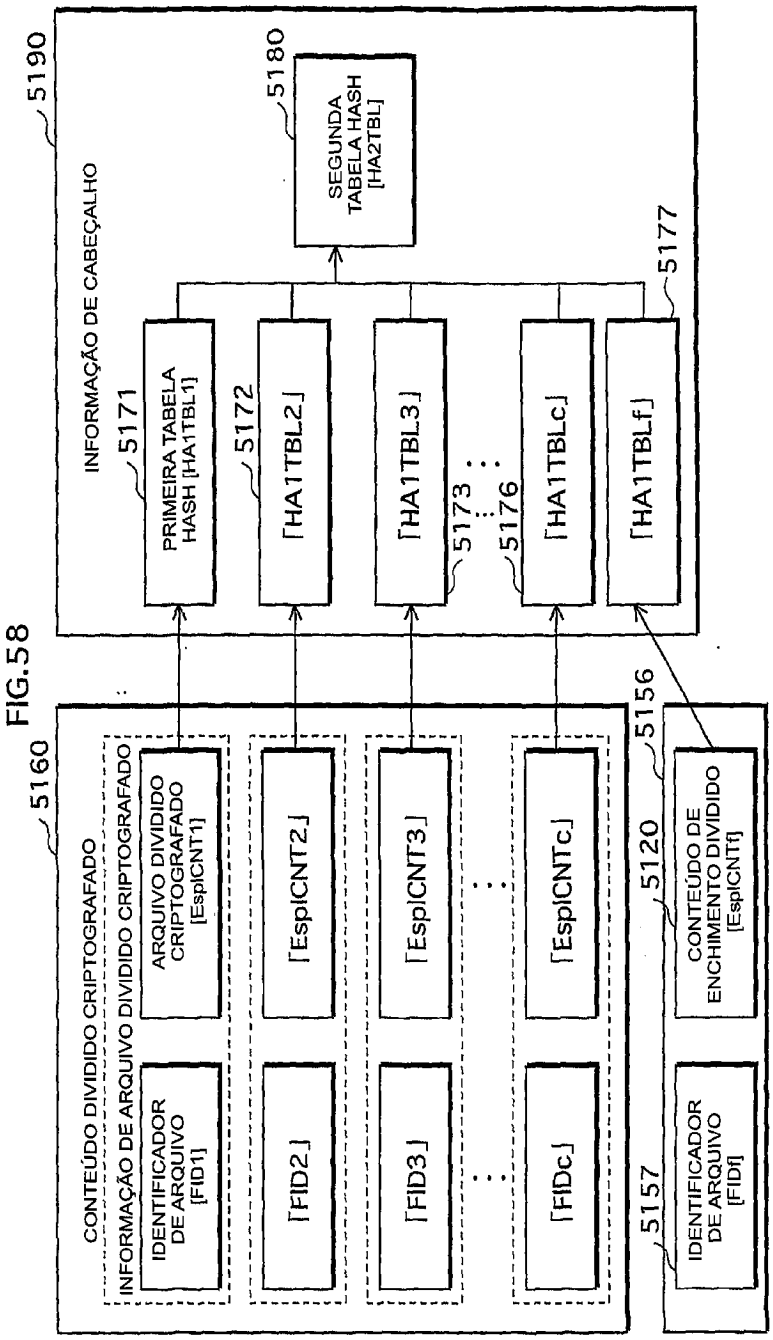

5190
INFORMAÇÃO DE CABEÇALHO
5180
SEGUNDA TABELA HASH [HA2TBL]
5171
PRIMEIRA TABELA HASH [HA1TBL1]
5172
「HA1TBL2」
「HA1TBL3」
5173
5176
「HA1TBLc」
「HA1TBLf」
5177
5160
CONTEÚDO DIVIDIDO CRIPTOGRAFADO
INFORMAÇÃO DE ARQUIVO DIVIDIDO CRIPTOGRAFADO
IDENTIFICADOR DE ARQUIVO [FID1]
ARQUIVO DIVIDIDO CRIPTOGRAFADO [EsplCNT1]
「FID2」
「EsplCNT2」
「FID3」
「EsplCNT3」
「FIDc」
「EsplCNTc」
5156
5120
CONTEÚDO DE ENCHIMENTO DIVIDIDO [EsplCNTf]
5157
IDENTIFICADOR DE ARQUIVO [FIDf]

FIG.59

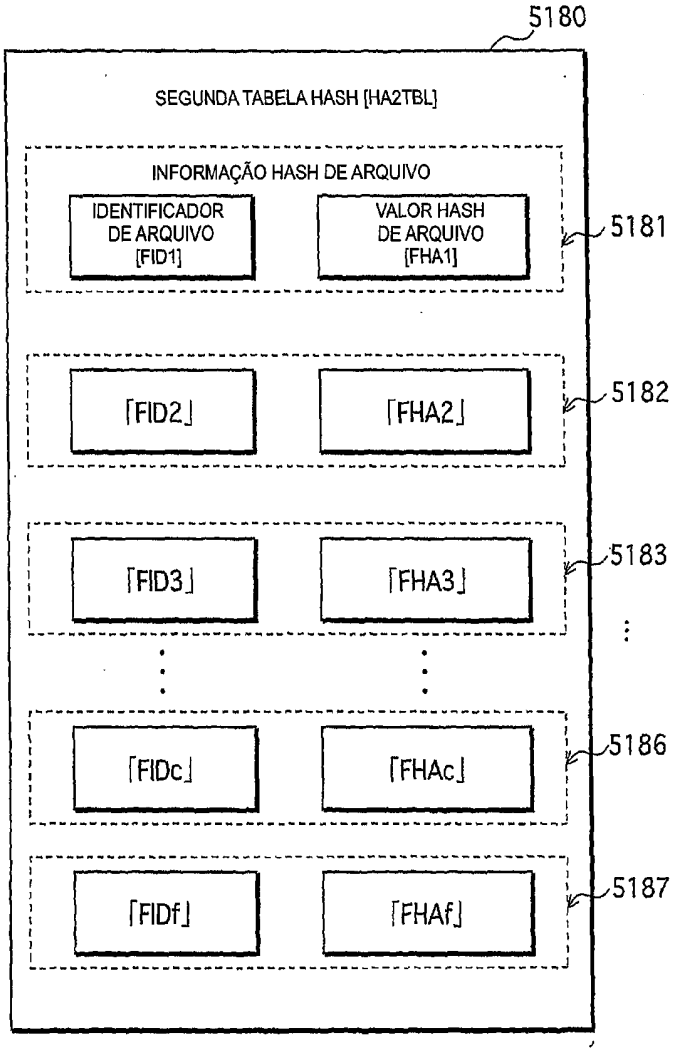

5180
SEGUNDA TABELA HASH [HA2TBL]
INFORMAÇÃO HASH DE ARQUIVO
IDENTIFICADOR DE ARQUIVO [FID1]
VALOR HASH DE ARQUIVO [FHA1]
5181
「FID2」
「FHA2」
5182
「FID3」
「FHA3」
5183
「FIDc」
「FHAc」
5186
「FIDf」
「FHAf」
5187

FIG.60

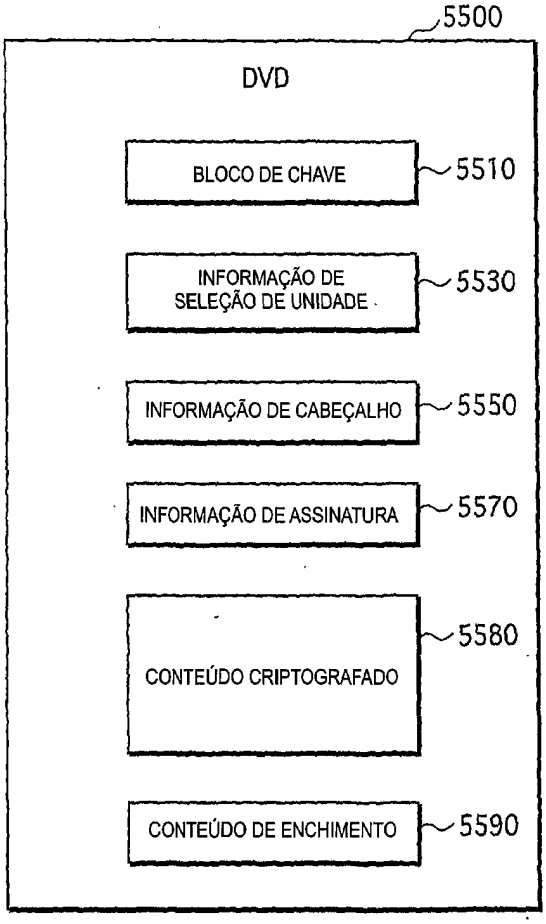

5500
DVD
BLOCO DE CHAVE
5510
INFORMAÇÃO DE SELEÇÃO DE UNIDADE
5530
INFORMAÇÃO DE CABEÇALHO
5550
INFORMAÇÃO DE ASSINATURA
5570
CONTEÚDO CRIPTOGRAFADO
5580
CONTEÚDO DE ENCHIMENTO
5590

FIG.61

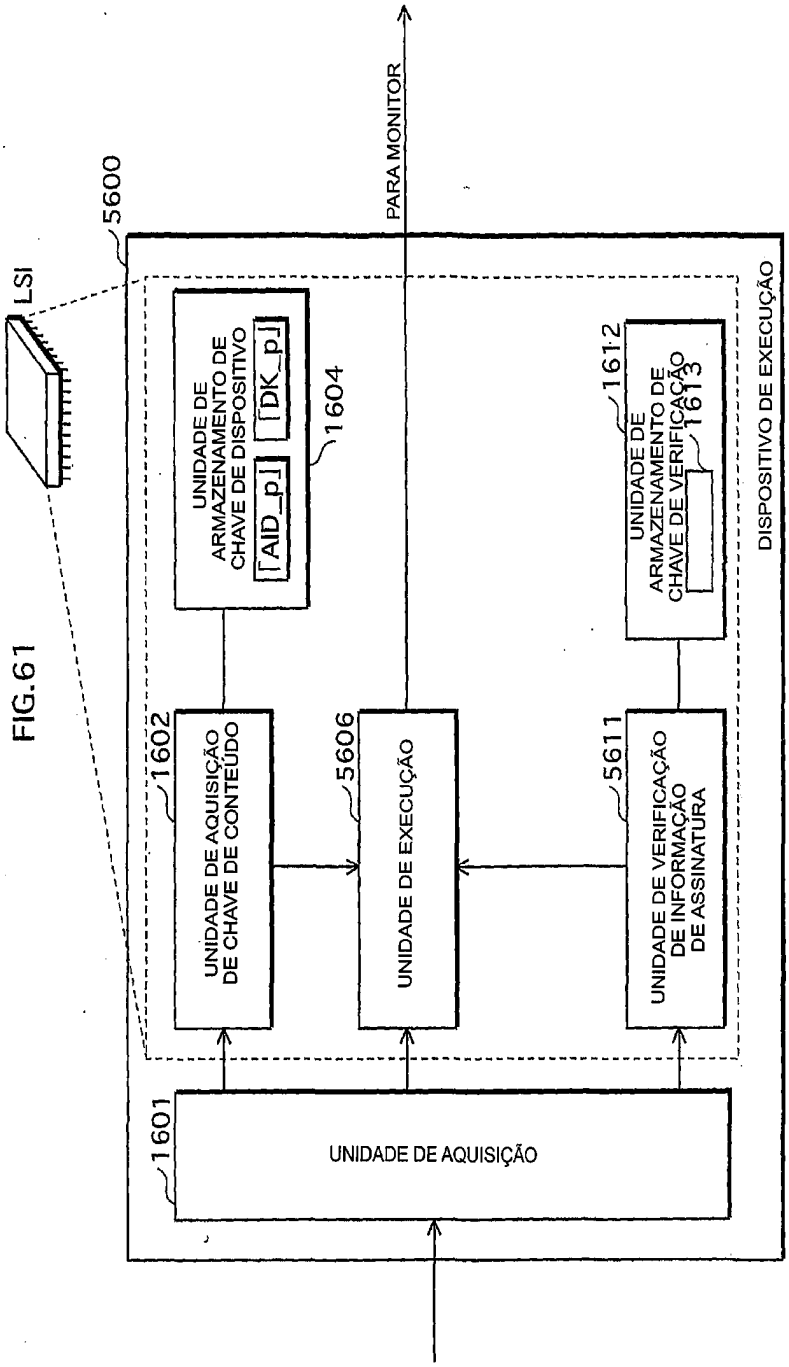

LSI
5600
PARA MONITOR
DISPOSITIVO DE EXECUÇÃO
UNIDADE DE ARMAZENAMENTO DE CHAVE DE DISPOSITIVO
「AID_pJ」
「DK_pJ」
1604
1612
UNIDADE DE ARMAZENAMENTO DE CHAVE DE VERIFICAÇÃO
1613
1602
UNIDADE DE AQUISIÇÃO DE CHAVE DE CONTEÚDO
5606
UNIDADE DE EXECUÇÃO
5611
UNIDADE DE VERIFICAÇÃO DE INFORMAÇÃO DE ASSINATURA
1601
UNIDADE DE AQUISIÇÃO

FIG.62

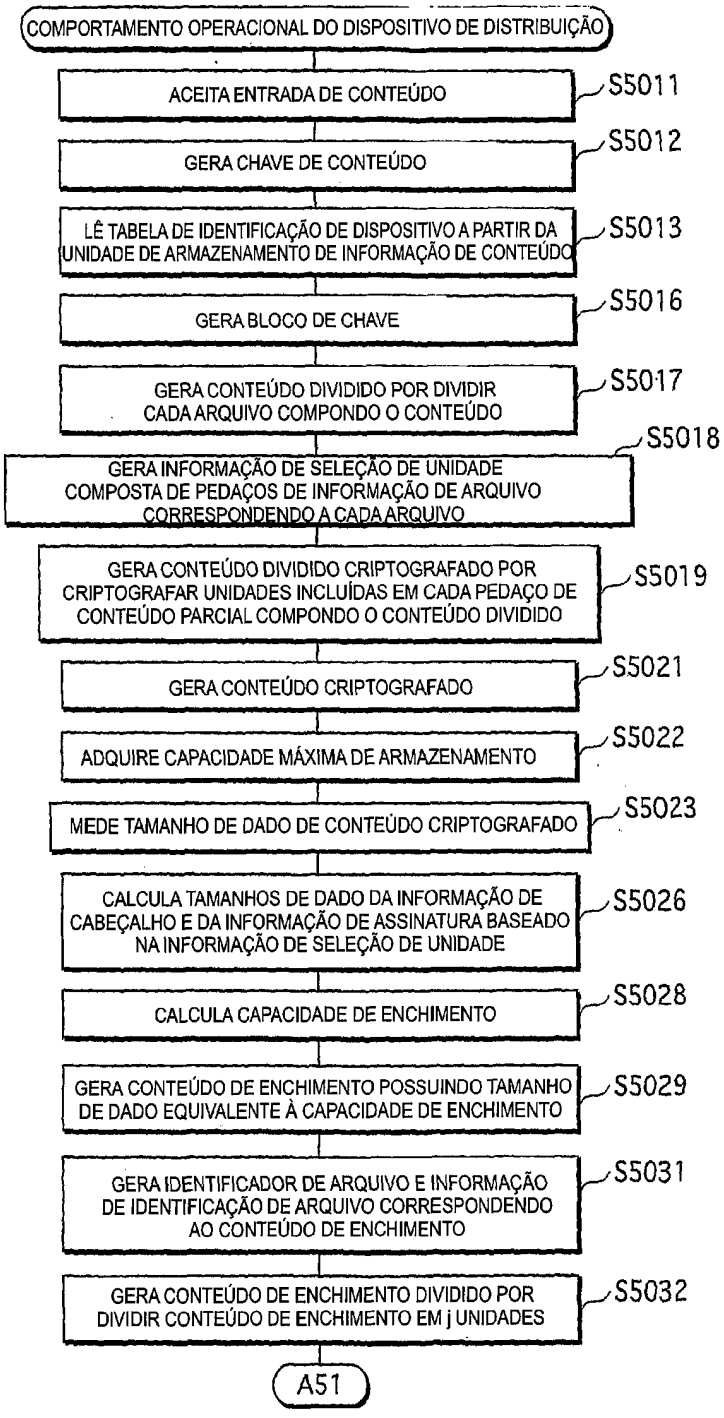

COMPORTAMENTO OPERACIONAL DO DISPOSITIVO DE DISTRIBUIÇÃO
ACEITA ENTRADA DE CONTEÚDO
S5011
GERA CHAVE DE CONTEÚDO
S5012
LÊ TABELA DE IDENTIFICAÇÃO DE DISPOSITIVO A PARTIR DA UNIDADE DE ARMAZENAMENTO DE INFORMAÇÃO DE CONTEÚDO
S5013
GERA BLOCO DE CHAVE
S5016
GERA CONTEÚDO DIVIDIDO POR DIVIDIR CADA ARQUIVO COMPONDO O CONTEÚDO
S5017
GERA INFORMAÇÃO DE SELEÇÃO DE UNIDADE COMPOSTA DE PEDAÇOS DE INFORMAÇÃO DE ARQUIVO CORRESPONDENDO A CADA ARQUIVO
S5018
GERA CONTEÚDO DIVIDIDO CRIPTOGRAFADO POR CRIPTOGRAFAR UNIDADES INCLUÍDAS EM CADA PEDAÇO DE CONTEÚDO PARCIAL COMPONDO O CONTEÚDO DIVIDIDO
S5019
GERA CONTEÚDO CRIPTOGRAFADO
S5021
ADQUIRE CAPACIDADE MÁXIMA DE ARMAZENAMENTO
S5022
MEDE TAMANHO DE DADO DE CONTEÚDO CRIPTOGRAFADO
S5023
CALCULA TAMANHOS DE DADO DA INFORMAÇÃO DE CABEÇALHO E DA INFORMAÇÃO DE ASSINATURA BASEADO NA INFORMAÇÃO DE SELEÇÃO DE UNIDADE
S5026
CALCULA CAPACIDADE DE ENCHIMENTO
S5028
GERA CONTEÚDO DE ENCHIMENTO POSSUINDO TAMANHO DE DADO EQUIVALENTE À CAPACIDADE DE ENCHIMENTO
S5029
GERA IDENTIFICADOR DE ARQUIVO E INFORMAÇÃO DE IDENTIFICAÇÃO DE ARQUIVO CORRESPONDENDO AO CONTEÚDO DE ENCHIMENTO
S5031
GERA CONTEÚDO DE ENCHIMENTO DIVIDIDO POR DIVIDIR CONTEÚDO DE ENCHIMENTO EM j UNIDADES
S5032
A51

FIG.63

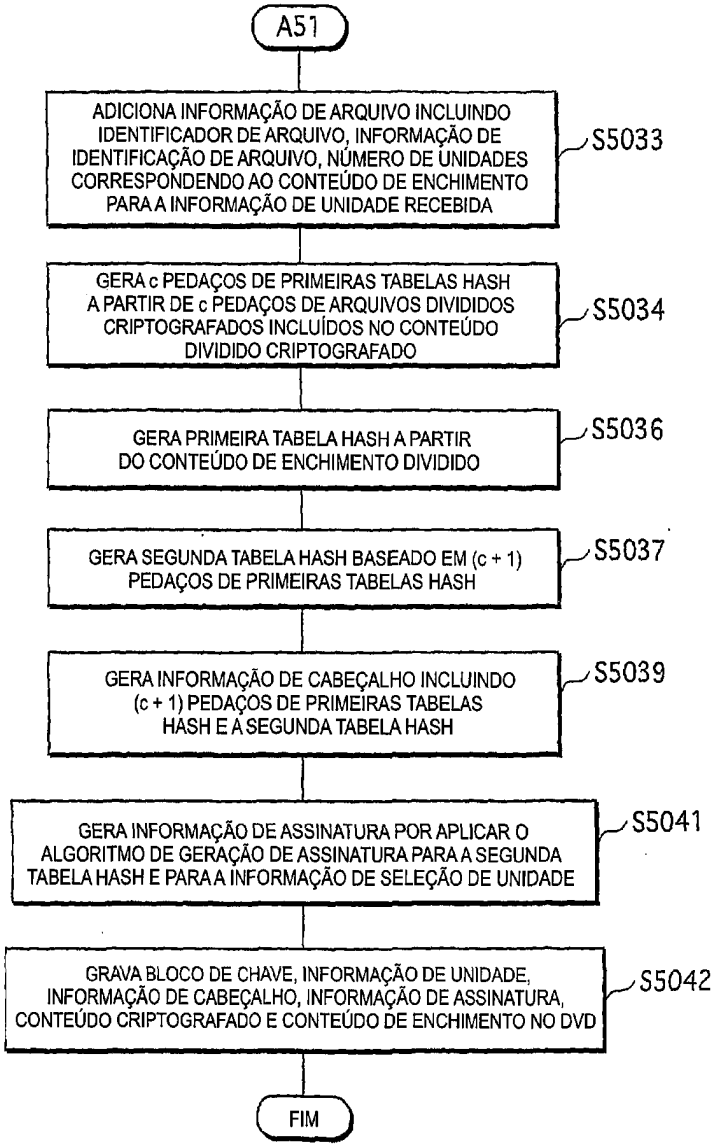

A51
ADICIONA INFORMAÇÃO DE ARQUIVO INCLUINDO IDENTIFICADOR DE ARQUIVO, INFORMAÇÃO DE IDENTIFICAÇÃO DE ARQUIVO, NÚMERO DE UNIDADES CORRESPONDENDO AO CONTEÚDO DE ENCHIMENTO PARA A INFORMAÇÃO DE UNIDADE RECEBIDA
S5033
GERA c PEDAÇOS DE PRIMEIRAS TABELAS HASH A PARTIR DE c PEDAÇOS DE ARQUIVOS DIVIDIDOS CRIPTOGRAFADOS INCLUÍDOS NO CONTEÚDO DIVIDIDO CRIPTOGRAFADO
S5034
GERA PRIMEIRA TABELA HASH A PARTIR DO CONTEÚDO DE ENCHIMENTO DIVIDIDO
S5036
GERA SEGUNDA TABELA HASH BASEADO EM (c + 1) PEDAÇOS DE PRIMEIRAS TABELAS HASH
S5037
GERA INFORMAÇÃO DE CABEÇALHO INCLUINDO (c + 1) PEDAÇOS DE PRIMEIRAS TABELAS HASH E A SEGUNDA TABELA HASH
S5039
GERA INFORMAÇÃO DE ASSINATURA POR APLICAR O ALGORITMO DE GERAÇÃO DE ASSINATURA PARA A SEGUNDA TABELA HASH E PARA A INFORMAÇÃO DE SELEÇÃO DE UNIDADE
S5041
GRAVA BLOCO DE CHAVE, INFORMAÇÃO DE UNIDADE, INFORMAÇÃO DE CABEÇALHO, INFORMAÇÃO DE ASSINATURA, CONTEÚDO CRIPTOGRAFADO E CONTEÚDO DE ENCHIMENTO NO DVD
S5042
FIM

FIG.64

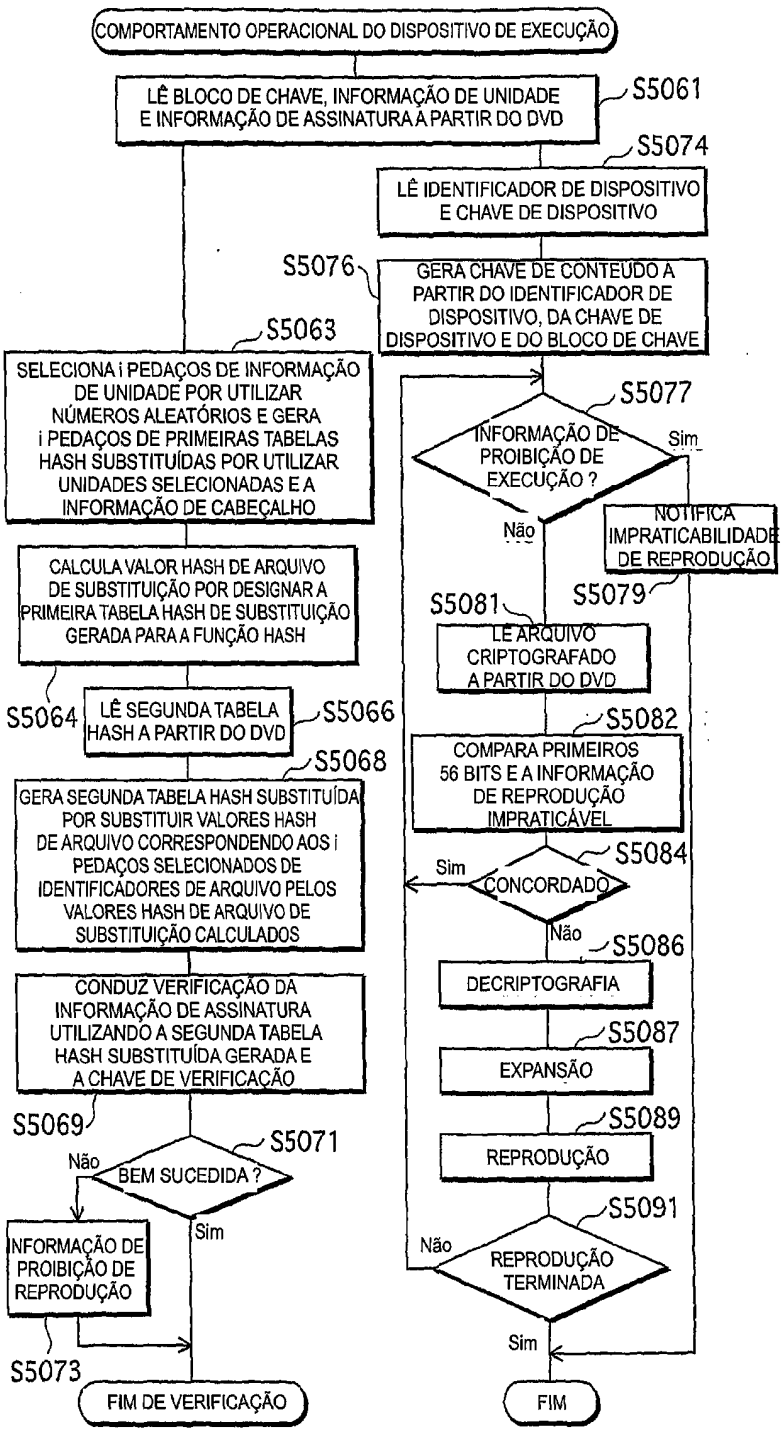

COMPORTAMENTO OPERACIONAL DO DISPOSITIVO DE EXECUÇÃO
LÊ BLOCO DE CHAVE, INFORMAÇÃO DE UNIDADE E INFORMAÇÃO DE ASSINATURA A PARTIR DO DVD
S5061
S5074
LÊ IDENTIFICADOR DE DISPOSITIVO E CHAVE DE DISPOSITIVO
S5076
GERA CHAVE DE CONTEÚDO A PARTIR DO IDENTIFICADOR DE DISPOSITIVO, DA CHAVE DE DISPOSITIVO E DO BLOCO DE CHAVE
S5063
SELECIONA i PEDAÇOS DE INFORMAÇÃO DE UNIDADE POR UTILIZAR NÚMEROS ALEATÓRIOS E GERA i PEDAÇOS DE PRIMEIRAS TABELAS HASH SUBSTITUÍDAS POR UTILIZAR UNIDADES SELECIONADAS E A INFORMAÇÃO DE CABEÇALHO
CALCULA VALOR HASH DE ARQUIVO DE SUBSTITUIÇÃO POR DESIGNAR A PRIMEIRA TABELA HASH DE SUBSTITUIÇÃO GERADA PARA A FUNÇÃO HASH
S5064
LÊ SEGUNDA TABELA HASH A PARTIR DO DVD
S5066
S5068
GERA SEGUNDA TABELA HASH SUBSTITUÍDA POR SUBSTITUIR VALORES HASH DE ARQUIVO CORRESPONDENDO AOS i PEDAÇOS SELECIONADOS DE IDENTIFICADORES DE ARQUIVO PELOS VALORES HASH DE ARQUIVO DE SUBSTITUIÇÃO CALCULADOS
CONDUZ VERIFICAÇÃO DA INFORMAÇÃO DE ASSINATURA UTILIZANDO A SEGUNDA TABELA HASH SUBSTITUÍDA GERADA E A CHAVE DE VERIFICAÇÃO
S5069
S5071
Não
BEM SUCEDIDA ?
Sim
INFORMAÇÃO DE PROIBIÇÃO DE REPRODUÇÃO
S5073
FIM DE VERIFICAÇÃO
S5077
INFORMAÇÃO DE PROIBIÇÃO DE EXECUÇÃO ?
Sim
Não
NOTIFICA IMPRATICABILIDADE DE REPRODUÇÃO
S5079
S5081
LÊ ARQUIVO CRIPTOGRAFADO A PARTIR DO DVD
S5082
COMPARA PRIMEIROS 56 BITS E A INFORMAÇÃO DE REPRODUÇÃO IMPRATICÁVEL
S5084
Sim
CONCORDADO
Não
S5086
DECRIPTOGRAFIA
S5087
EXPANSÃO
S5089
REPRODUÇÃO
S5091
Não
REPRODUÇÃO TERMINADA
Sim
FIM

FIG.65

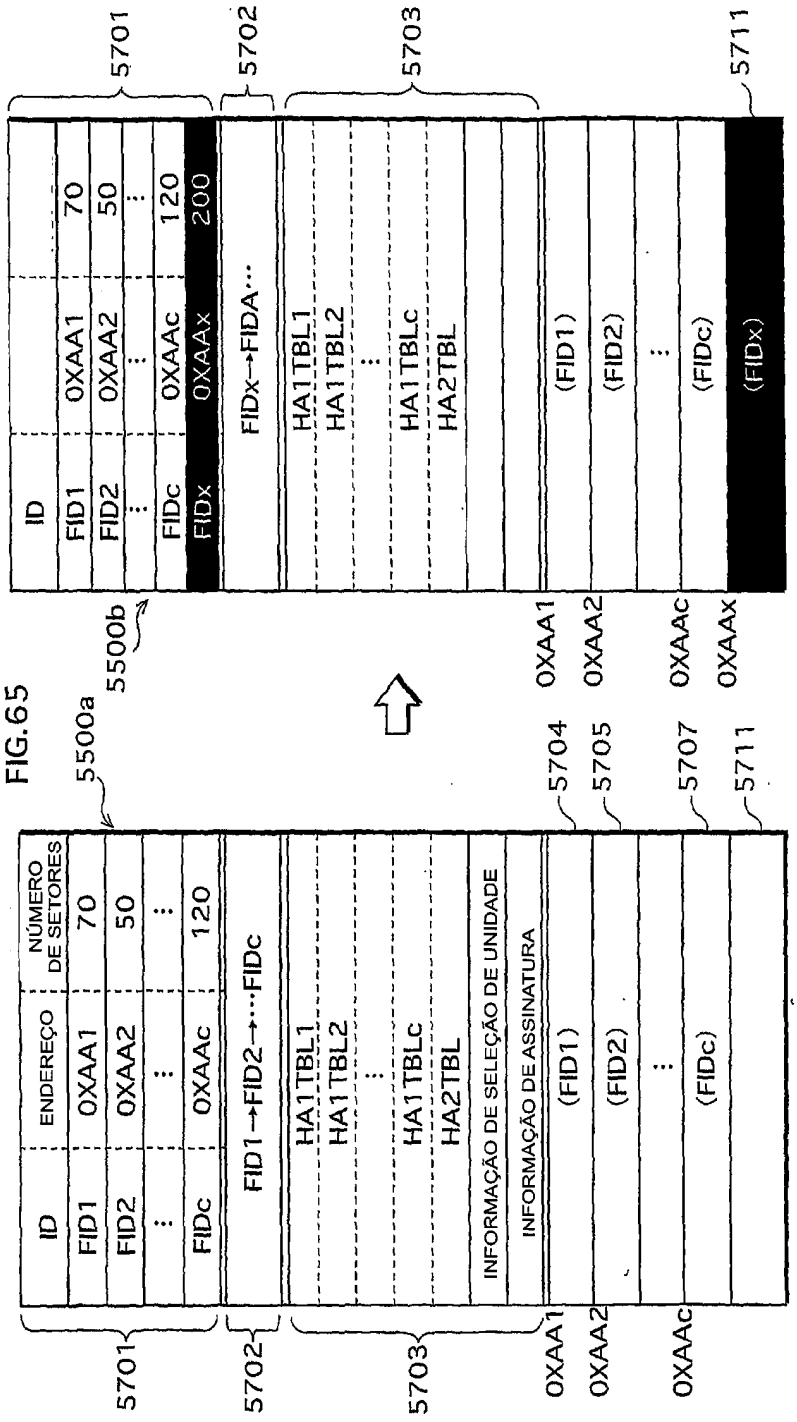

ID
ENDEREÇO
NÚMERO DE SETORES
FID1
FID2
FIDc
0XAA1
0XAA2
0XAAc
70
50
120
200
FIDx
0XAAx
FID1→FID2→…FIDc
FIDx→FIDA…
HA1TBL1
HA1TBL2
HA1TBLc
HA2TBL
INFORMAÇÃO DE SELEÇÃO DE UNIDADE
INFORMAÇÃO DE ASSINATURA
(FID1)
(FID2)
(FIDc)
(FIDx)
5500a
5500b
5701
5702
5703
5704
5705
5707
5711
0XAA1
0XAA2
0XAAc
0XAAx

FIG.66

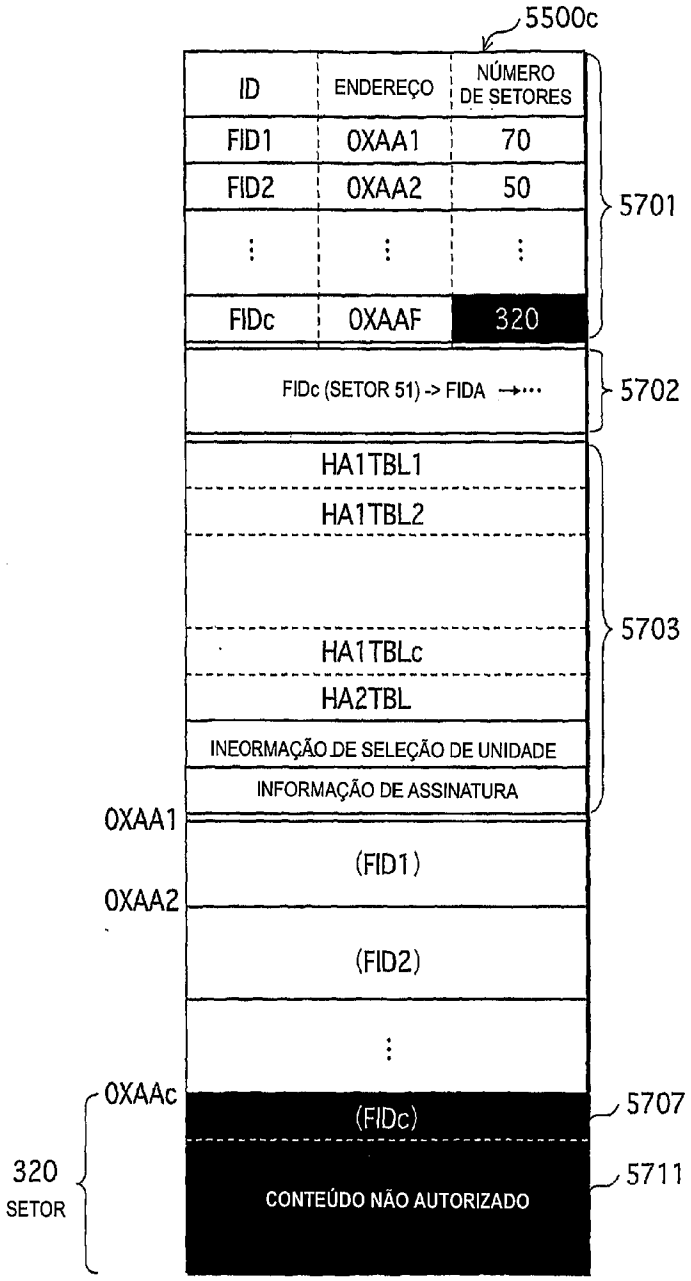

5500c
ID
ENDEREÇO
NÚMERO DE SETORES
FID1
0XAA1
70
FID2
0XAA2
50
FIDc
0XAAF
320
5701
FIDc (SETOR 51) -> FIDA
5702
HA1TBL1
HA1TBL2
HA1TBLc
HA2TBL
INEORMAÇÃO DE SELEÇÃO DE UNIDADE
INFORMAÇÃO DE ASSINATURA
5703
0XAA1
(FID1)
0XAA2
(FID2)
0XAAc
(FIDc)
5707
320
SETOR
CONTEÚDO NÃO AUTORIZADO
5711

FIG.67

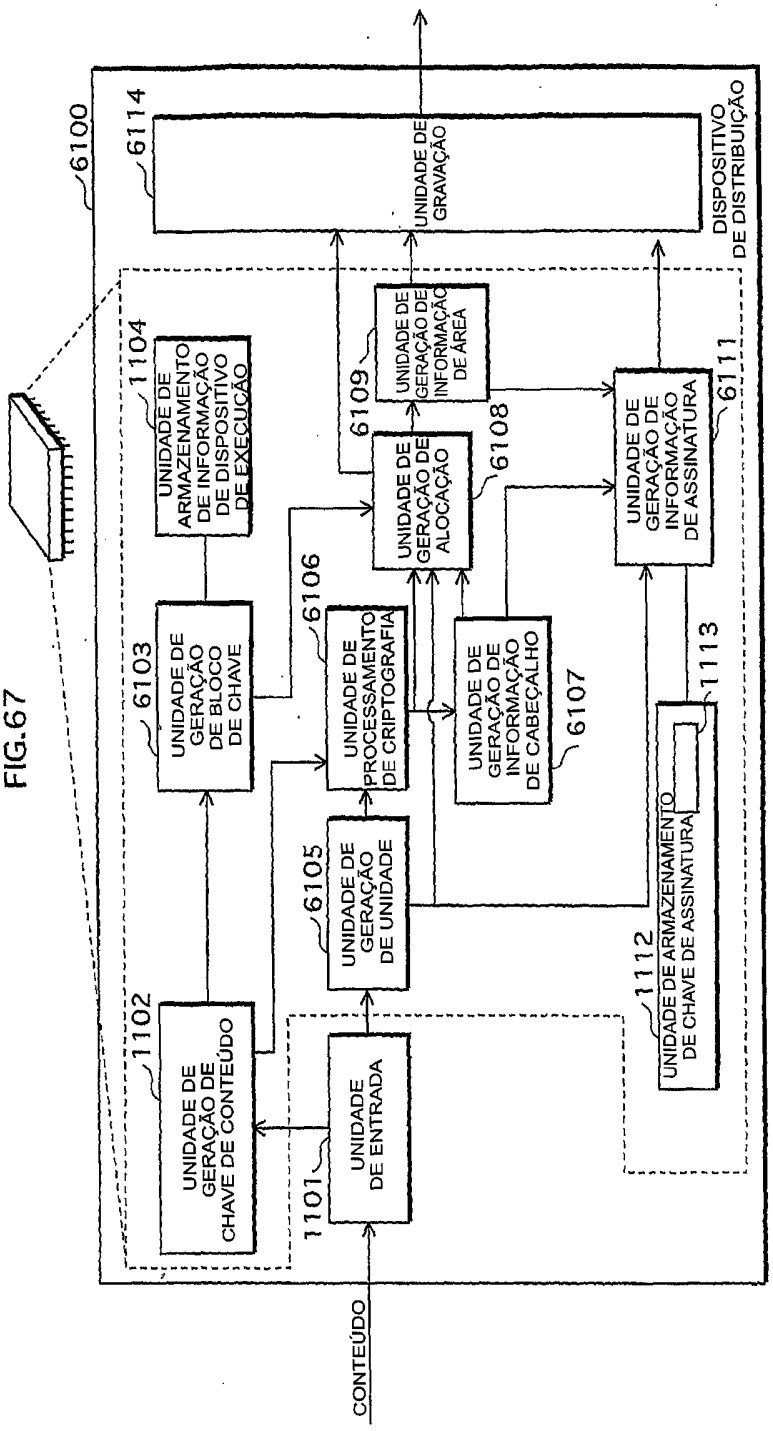

6100
6114
UNIDADE DE GRAVAÇÃO
DISPOSITIVO DE DISTRIBUIÇÃO
1104
UNIDADE DE ARMAZENAMENTO DE INFORMAÇÃO DE DISPOSITIVO DE EXECUÇÃO
6109
UNIDADE DE GERAÇÃO DE INFORMAÇÃO DE ÁREA
6108
UNIDADE DE GERAÇÃO DE ALOCAÇÃO
6111
UNIDADE DE GERAÇÃO DE INFORMAÇÃO DE ASSINATURA
6103
UNIDADE DE GERAÇÃO DE BLOCO DE CHAVE
6106
UNIDADE DE PROCESSAMENTO DE CRIPTOGRAFIA
6107
UNIDADE DE GERAÇÃO DE INFORMAÇÃO DE CABEÇALHO
1113
6105
UNIDADE DE GERAÇÃO DE UNIDADE
1112
UNIDADE DE ARMAZENAMENTO DE CHAVE DE ASSINATURA
1102
UNIDADE DE GERAÇÃO DE CHAVE DE CONTEÚDO
1101
UNIDADE DE ENTRADA
CONTEÚDO

FIG.68

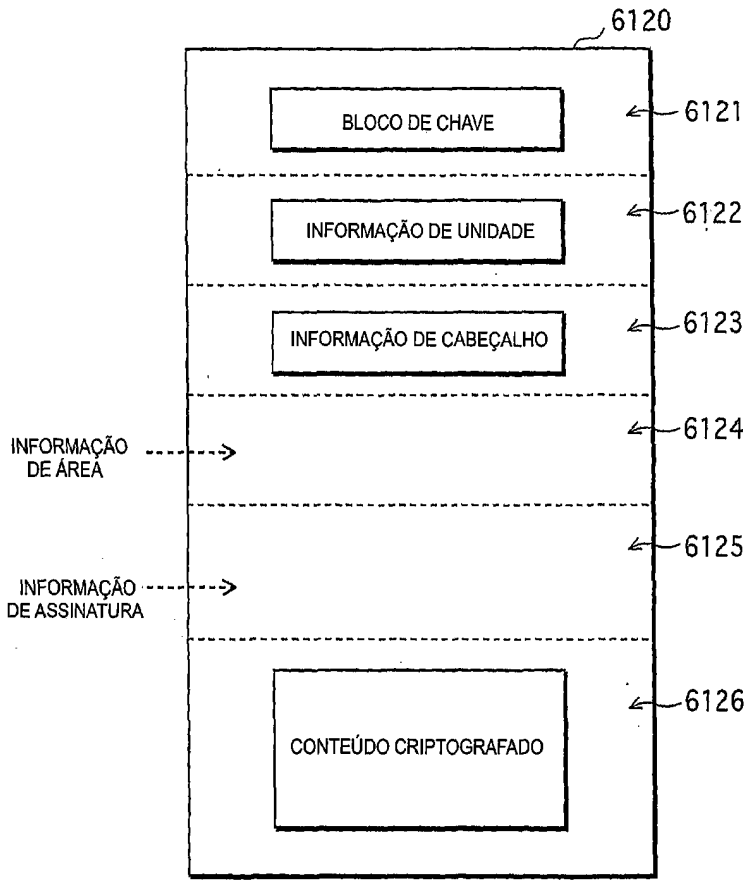

6120
BLOCO DE CHAVE
6121
INFORMAÇÃO DE UNIDADE
6122
INFORMAÇÃO DE CABEÇALHO
6123
6124
INFORMAÇÃO DE ÁREA
6125
INFORMAÇÃO DE ASSINATURA
CONTEÚDO CRIPTOGRAFADO
6126

FIG.69

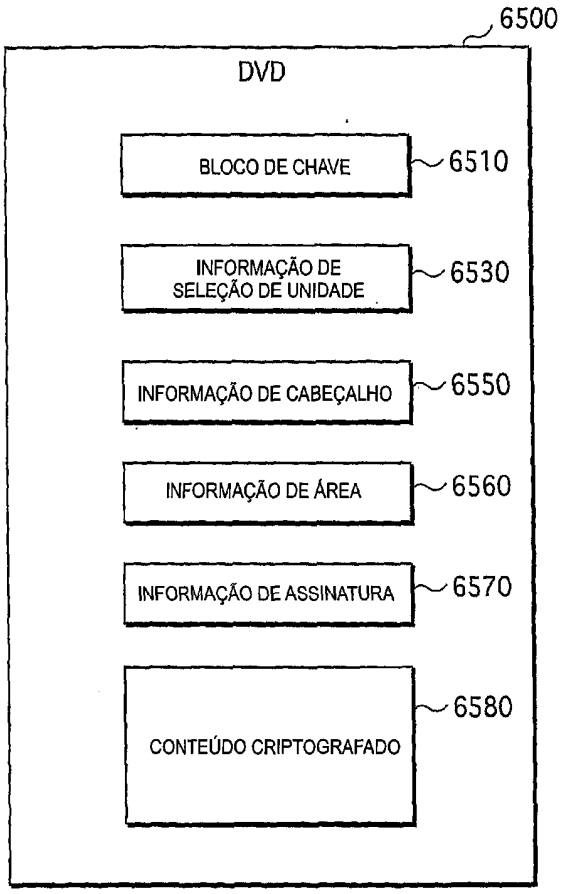
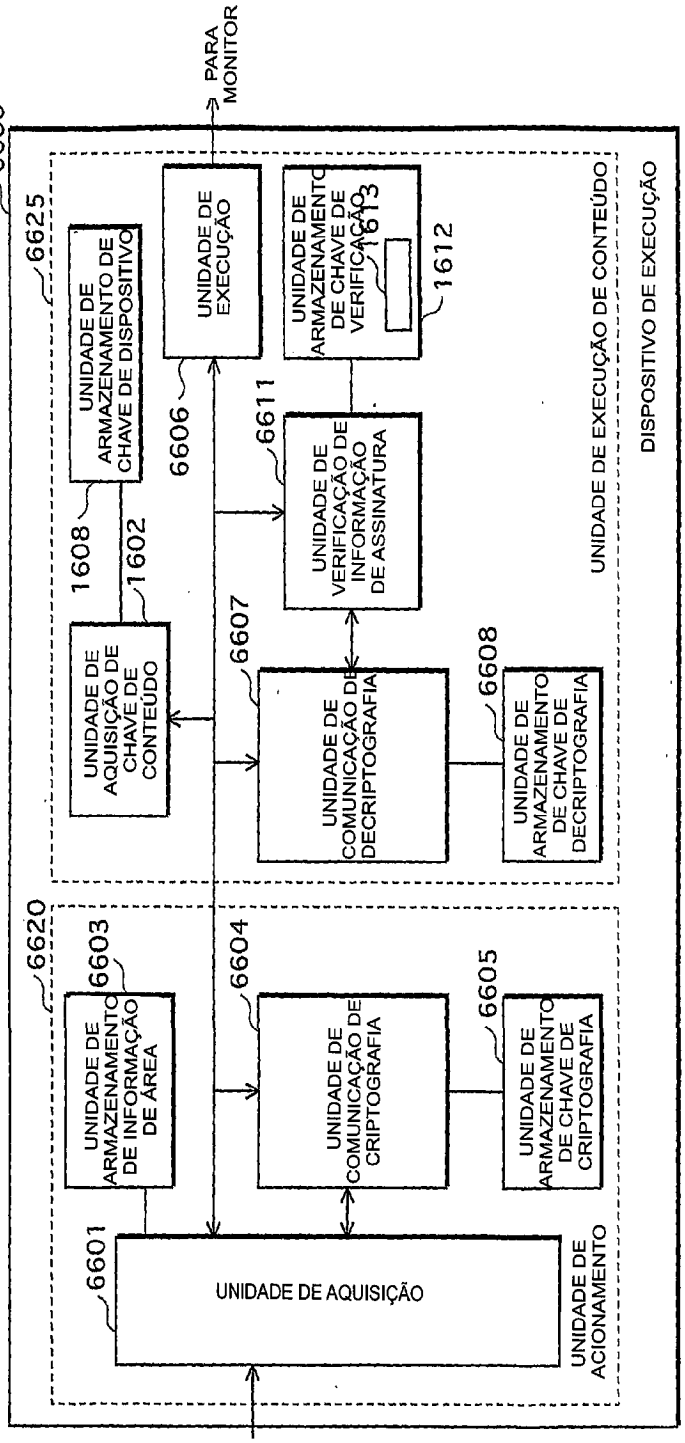
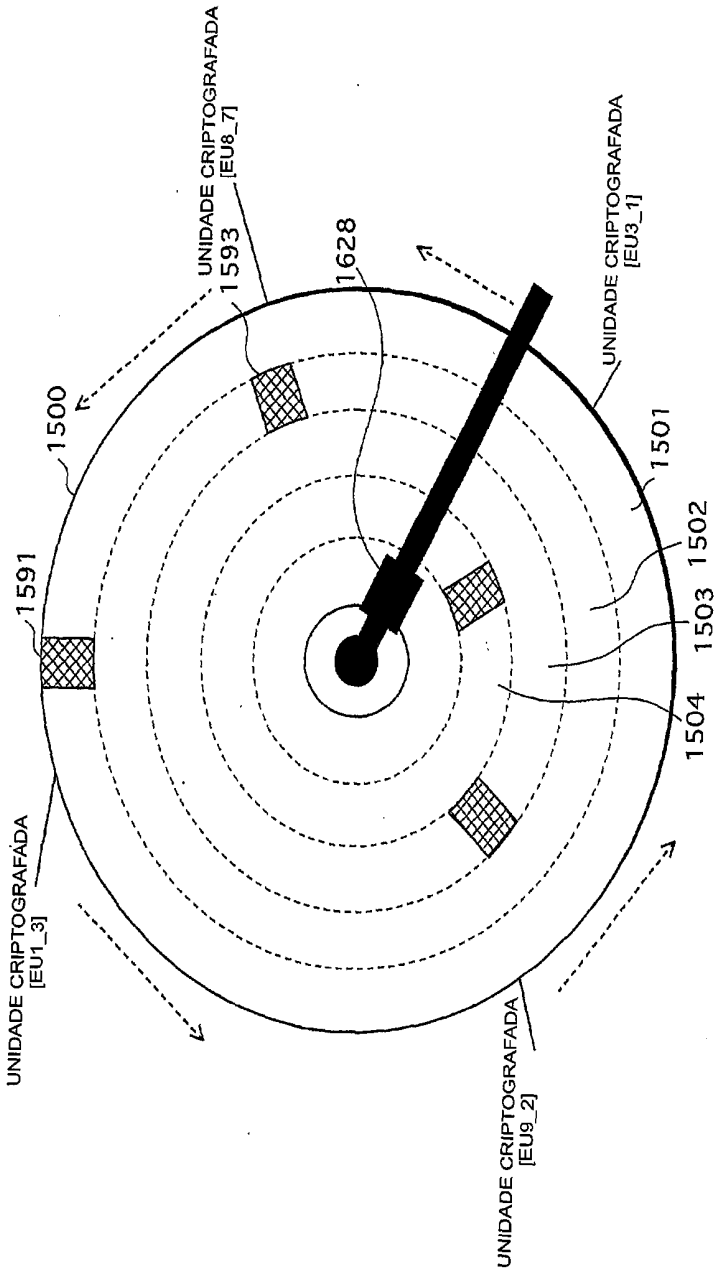

6500
DVD
BLOCO DE CHAVE
6510
INFORMAÇÃO DE SELEÇÃO DE UNIDADE
6530
INFORMAÇÃO DE CABEÇALHO
6550
INFORMAÇÃO DE ÁREA
6560
INFORMAÇÃO DE ASSINATURA
6570
CONTEÚDO CRIPTOGRAFADO
6580

FIG.70



6605 UNIDADE DE ARMAZENAMENTO DE CHAVE DE CRIPTOGRAFIA
1612 UNIDADE DE ARMAZENAMENTO DE CHAVE DE VERIFICAÇÃO

FIG.71


UNIDADE CRIPTOGRAFADA [EU8_7]
1593
1628
UNIDADE CRIPTOGRAFADA [EU3_1]
1500
1501
1502
1503
1504
1591
UNIDADE CRIPTOGRAFADA [EU1_3]
UNIDADE CRIPTOGRAFADA [EU9_2]