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

(21) **PI0609562-3 A2**

BRPI0609562A2

(22) Data de Depósito: 25/04/2006
(43) Data da Publicação: 18/10/2011
(RPI 2128)

(51) Int.Cl.:
H04N 5/783
H04N 7/167

(54) Título: DISPOSITIVO E MÉTODO PARA PROCESSAR UM FLUXO DE DADOS CODIFICADO EM UM SISTEMA CRIPTOGRÁFICO, MEIO LEGÍVEL POR COMPUTADOR E ELEMENTO DE PROGRAMA

(30) Prioridade Unionista: 26/04/2005 EP 05103394.2

(73) Titular(es): KONINKLIJKE PHILIPS ELECTRONICS N. V.

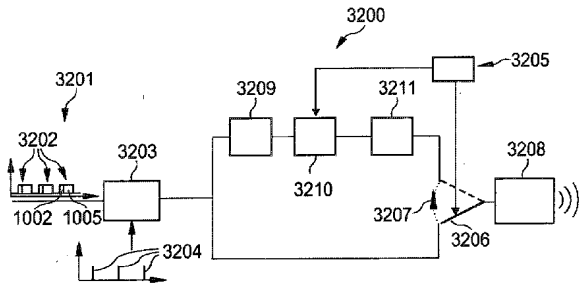
(72) Inventor(es): Albert Maria Arnold Rijckaert, Eric Wilhelmus Josephus Moors, Ronald Peter Jan Mathijs Manders

(74) Procurador(es): Momsen, Leonardos & CIA.

(86) Pedido Internacional: PCT IB2006051278 de 25/04/2006

(87) Publicação Internacional: WO 2006/114760de 02/11/2006

(57) Resumo: DISPOSITIVO E MÉTODO PARA PROCESSAR UM FLUXO DE DADOS CODIFICADO EM UM SISTEMA CRIPTOGRÁFICO, MEIO LEGÍVEL POR COMPUTADOR E ELEMENTO DE PROGRAMA. Um dispositivo (3200) para processar um fluxo de dados codificado (3201) em um sistema criptográfico, no qual dados de decifração (3204) são providos para decifrar cada segmento (3202) do fluxo de dados codificado (3201) para reprodução do fluxo de dados decifrado, em que o dispositivo (3200) inclui uma primeira unidade de determinação (3209) para determinar, no caso de trocar de um primeiro modo de reprodução (1501) de reproduzir o fluxo de dados (3201) para um segundo modo de reprodução (1502) de reproduzir o fluxo de dados (3201), uma posição atual de reprodução dentro do fluxo de dados, e uma segunda unidade de determinação (3210) para determinar uma posição de começo para começar reprodução no segundo modo de reprodução (1502) baseado na posição atual determinada.



"DISPOSITIVO E MÉTODO PARA PROCESSAR UM FLUXO DE DADOS CODIFICADO EM UM SISTEMA CRIPTOGRÁFICO, MEIO LEGÍVEL POR COMPUTADOR E ELEMENTO DE PROGRAMA"

CAMPO DA INVENÇÃO

A invenção relaciona-se a um dispositivo para processar um fluxo de dados codificado em um sistema criptográfico.

Além disto, a invenção relaciona-se a um método de processar um fluxo de dados codificado em um sistema criptográfico.

Além disso, a invenção relaciona-se a um elemento de programa.

Além disso, a invenção relaciona-se a um meio legível por computador.

FUNDAMENTO DA INVENÇÃO

Dispositivos de entretenimento eletrônicos ficam cada vez mais importantes. Particularmente, um número crescente de usuários compra reprodutores de áudio/vídeo baseados em disco rígido e outro equipamento de entretenimento.

Desde que a redução de espaço de armazenamento é um assunto importante no campo de reprodutores de áudio/vídeo, dados de áudio e vídeo são armazenados freqüentemente de uma maneira comprimida, e por razões de segurança de uma maneira codificada.

MPEG2 é um padrão para a codificação genérica de quadros em movimento e áudio associado e cria um fluxo vídeo fora de dados de quadro que pode ser arranjado em uma ordem especificada chamada a estrutura de GOP ("Grupo de Imagens"). Um fluxo de bits de vídeo de MPEG2 é composto de uma série de quadros de dados codificando imagens. Os três modos de codificar uma imagem são intra-codificado (imagem I), preditivo dianteiro (imagem P) e preditivo bidirecional (imagem B). Um quadro intra-codificado (Quadro I) é relacionado a uma imagem particular e

contém os dados correspondentes. Um quadro preditivo dianteiro (Quadro P) precisa de informação de um quadro I ou quadro P precedente. Um quadro preditivo bidirecional (quadro B) é dependente de informação de um quadro I ou quadro P precedente ou subseqüente.

É uma função interessante em um dispositivo de reprodução de mídia trocar de um modo de reprodução normal, no qual conteúdo de mídia é reproduzido em uma velocidade normal, para um modo de reprodução acelerada, no qual conteúdo de mídia é reproduzido de uma maneira modificada, por exemplo com uma velocidade aumentada ("avanço rápido").

WO 2004/071091 A1 expõe a geração de informação de vídeo codificada com um fluxo codificado de informação de vídeo contendo primeiros quadros de vídeo e segundos quadros de vídeo que são acessíveis e não acessíveis durante reprodução acelerada respectivamente. De um fluxo de fonte codificado, quer dizer para decifração de palavras de controle variáveis repetidamente, seções do fluxo são identificadas onde os respectivos primeiros dos quadros ocorrem no fluxo. Palavras de controle para decifração são incluídas no fluxo. Pelo menos parte das palavras de controle é incluída no fluxo a posições selecionadas sincronizadas às seções identificadas.

Para trocar de um modo de reprodução normal para um modo de reprodução acelerada, é desejado que a transição entre os dois modos seja realizada sem um deterioração da qualidade de reprodução.

OBJETIVO E RESUMO DA INVENÇÃO

É um objetivo da invenção trocar de um modo de reprodução para outro modo de reprodução de uma maneira eficiente.

A fim de alcançar o objetivo definido acima, um dispositivo para processar um fluxo de dados codificado em um sistema criptográfico, um método de processar um fluxo de dados codificado em um sistema criptográfico, um elemento de programa e um meio legível por computador de acordo com as reivindicações independentes são providos.

De acordo com uma concretização exemplar da invenção, um dispositivo para processar um fluxo de dados codificado em um sistema criptográfico é provido, no qual dados de decifração são providos para decifrar cada segmento do fluxo de dados codificado para reprodução do fluxo de dados decifrado. O dispositivo pode incluir uma primeira unidade de determinação para determinar, no caso de trocar de um primeiro modo de reprodução de reproduzir os dados fluxos para um segundo modo de reprodução de reproduzir o fluxo de dados, uma posição atual de reprodução dentro do fluxo de dados, e uma segunda unidade de determinação para determinar uma posição de começo par começar reprodução no segundo modo de reprodução baseado na posição atual determinada.

De acordo com outra concretização exemplar da invenção, um método de processar um fluxo de dados codificado em um sistema criptográfico é provido, no qual dados de decifração são providos para decifrar cada segmento dos fluxos de dados codificados para reprodução do fluxo de dados decifrado. O método inclui as etapas de, no caso de trocar de um primeiro modo de reprodução de reproduzir o fluxo de dados para um segundo modo de reprodução de reproduzir o fluxo de dados, determinar uma posição atual de reprodução dentro do fluxo de dados, e determinar uma posição de começo para começar reprodução no segundo modo de reprodução baseado na posição atual determinada.

Além disto, de acordo com outra concretização exemplar da invenção, um meio legível por computador é provido, no qual um programa de computação de processar um fluxo de dados codificado em um sistema criptográfico, no qual dados de decifração são providos para decifrar cada segmento dos fluxos de dados codificados para reprodução do fluxo de dados decifrado, é armazenado, qual programa de computação, ao ser executado por um processador, é adaptado para controlar ou efetuar as etapas de método acima mencionadas.

Além disso, de acordo com ainda outra concretização exemplar da invenção, um elemento de programa de processar um fluxo de dados codificado em um sistema criptográfico é provido, no qual dados de decifração são providos para decifrar cada segmento do fluxo de dados codificado para reprodução do fluxo de dados decifrados, qual elemento de programa, ao ser executado por um processador, é adaptado para controlar ou efetuar as etapas de método acima mencionadas.

Processar dados codificados de acordo com a invenção pode ser realizado por um programa de computação, quer dizer por software, ou usando um ou mais circuitos de otimização eletrônicos especiais, quer dizer em hardware, ou em forma híbrida, quer dizer por meio de componentes de software e componentes de hardware.

O aspectos caracterizadores de acordo com a invenção particularmente têm a vantagem que uma troca de um primeiro modo de reprodução (por exemplo um modo de reprodução normal) de reproduzir um fluxo de dados codificado para um segundo modo de reprodução (por exemplo um modo de reprodução acelerada) é realizado de uma maneira muito eficiente e sem uma deterioração significante da qualidade dos dados reproduzidos. Para alcançar isto, a posição de reprodução atual no primeiro modo de reprodução é determinada, e a posição de começo para começar uma reprodução no segundo modo de reprodução é ajustada baseado neste conhecimento de posição.

Em um cenário particular de um sistema de reprodução para um fluxo de dados codificado sendo dividido em uma pluralidade de segmentos sucessivos, decifração de cada segmento é necessária antes que os dados respectivos possam ser reproduzidos de fato. Desde que pode levar algum tempo para prover dados de decifração para um segmento sucessivo, a posição atual de reprodução dentro do segmento reproduzido atualmente deveria ser levada em conta ao determinar uma posição à qual a reprodução

no novo segundo modo de reprodução começará.

Geralmente, um objetivo de salto em trocar de um primeiro modo de operação (por exemplo um modo de reprodução normal) para um segundo modo de reprodução (por exemplo um modo de reprodução acelerada) pode ser escolhido vantajosamente de acordo com a invenção ou pode ser até mesmo otimizado levando em conta a posição atual de reprodução dentro do segmento reproduzido atualmente. Por exemplo, o tempo deixado para reproduzir o segmento reproduzido atualmente ao fim comparado ao tempo precisado para receber dados de decifração (por exemplo, uma palavra de controle) para decifrar o segmento subseqüente de dados codificados é um critério apropriado para decidir quando é um bom momento para trocar de fato do primeiro modo de reprodução para o segundo modo de reprodução.

A uma transição de uma reprodução normal para uma reprodução acelerada, um possível tempo de transição mais cedo pode ser calculado de tal maneira que o tempo deixado ao momento de trocar ainda seja suficiente para decodificar os dados reproduzidos subseqüentemente.

De acordo com uma concretização exemplar da invenção, um método para otimizar o objetivo de salto ao trocar entre reprodução normal e reprodução acelerada em sistemas de vídeo digitais é provido. Este método pode ser realizado no quadro do padrão de MPEG2. Palavras de controle sucessivas, que podem ser providas em unidades, podem ser requeridas para decifrar segmentos de vídeo. Ao trocar entre reprodução normal e reprodução acelerada, a posição atual pode ser determinada, como também uma posição de começo para processamento de reprodução acelerada baseado na velocidade de reprodução acelerada que pode ser selecionada por um usuário. Esta posição de começo deveria ser tal que uma ECM (mensagem de controle de intitulação) de um período próximo ou prévio seja decifrada antes que este período seja entrado de fato. Se a última posição de reprodução normal estiver

dentro da gama permitida, então essa posição pode ser usada como um objetivo de salto. Se não estiver, uma posição tão perto disto quanto possível pode ser escolhida para trocar de fato de reprodução normal para reprodução acelerada.

De acordo com um aspecto da invenção, um gerador de reprodução acelerada é provido ao decifrar um fluxo a fim de selecionar quadros I de 'plaintext' e construir um fluxo de reprodução acelerada disto. O processo de decifração pode começar o mais cedo possível depois de trocar para o modo de reprodução acelerada.

De acordo com um aspecto da invenção, processamento de reprodução acelerada de um fluxo vídeo ou um fluxo de áudio pode ser executado.

O sistema de acordo com a invenção pode melhorar a velocidade do desempenho de troca, pode realizar um tal desempenho de troca de uma maneira eficiente, e pode alcançar uma qualidade correta de dados reproduzidos até mesmo a um ponto de transição entre um primeiro modo de reprodução e um segundo modo de reprodução.

Campos exemplares de aplicar o sistema de acordo com a invenção são dispositivos de gravação de vídeo digital, tais como combinações de disco rígido, dispositivos de DVD +RW, etc.

De acordo com um aspecto da invenção, um sistema é provido para criar eficientemente reprodução acelerada em um fluxo codificado. Assim, um sistema equilibrado pode ser provido que permite fácil reprodução acelerada dianteira e inversa em um fluxo gravado. De acordo com a invenção, a velocidade de reprodução acelerada maximamente realizável pode ser muito grande, porque um ponto de troca correto é estimado no fluxo para começar a reprodução acelerada levando em consideração as propriedades do sistema criptográfico de radiodifusão de vídeo digital.

Quando um usuário aperta um botão correspondente ou provê

o sistema de outra maneira com o comando que ele pretende trocar de um modo de reprodução normal para um modo de reprodução acelerada, é normalmente desejado que uma transição ocorra tão rápida quanto possível. Por outro lado, a transição deveria ir de mãos dadas com uma qualidade de reprodução correta. Quando uma tal transição ocorre, uma sobreposição de dados reproduzidos antes e depois de troca deveria ser tão pequena quanto possível, e também não deveria haver nenhuma abertura significante de reprodução. Assim, a troca de reprodução normal para reprodução acelerada deve ser sincronizada considerando um tempo de atraso precisado por um cartão inteligente para decifrar dados gerando palavras de controle como informação de decifração.

Se referindo às reivindicações dependentes, concretizações exemplares adicionais da invenção serão descritas.

A seguir, concretizações exemplares do dispositivo para processar um fluxo de dados codificado em um sistema criptográfico serão descritas. Estas concretizações também podem ser aplicadas para o método de processar um fluxo de dados codificado em um sistema criptográfico, para o meio legível por computador e para o elemento de programa.

No dispositivo de acordo com a invenção, a segunda unidade de determinação pode ser adaptada para determinar uma posição de começo para começar reprodução no segundo modo de reprodução baseado nas características (criptográficas) do sistema criptográfico. Ao trocar de um modo de reprodução normal para um modo de reprodução acelerada ou vice-versa, deveria ser levado em conta que o sistema criptográfico pode requerer continuamente informação de decifração para decifrar dados codificados. Desde que esta decifração pode levar algum tempo ou como a provisão de tal informação de decifração pode ser atrasada, esta característica é um critério apropriado para determinar a qual momento uma troca desejada de um primeiro modo de reprodução para um segundo modo de reprodução pode ser

efetuada de fato.

Particularmente, a segunda unidade de determinação pode ser adaptada para determinar uma posição de começo para começar reprodução no segundo modo de reprodução baseado em um atraso com o qual dados de decifração são providos no sistema criptográfico. Por exemplo, quando conteúdo de mídia codificado é transmitido no quadro de um padrão de MPEG2, segmentos subseqüentes dos dados codificados são decifrados com denominadas palavras de controle como informação de decifração, quais palavras de controle podem ser geradas em um cartão inteligente baseado em ECMs previamente transmitidas (mensagem de controle de intitulação). Desde que o cartão inteligente pode precisar de algum tempo de processamento para gerar palavras de controle, os dados correspondentes de um segmento sucessivo só podem ser reproduzidos (no quadro de um modo de reprodução acelerada) depois da decifração. Levando em conta um tal atraso para julgar uma posição de começo correta para o modo de reprodução acelerada permite começar reprodução acelerada sem um tempo de interrupção longo entre o modo de reprodução normal e modo de reprodução acelerada.

A segunda unidade de determinação pode ser adaptada para determinar uma posição de começo para começar reprodução no segundo modo de reprodução baseado em um atraso com o qual dados de decifração para decifrar um segmento sucessivo são providos no sistema criptográfico. Se referindo à explicação precedente, um tal tempo de geração de palavra de controle pode ser de importância quando um tempo correto de transição para um modo de reprodução modificado, por exemplo um modo de reprodução acelerada, é determinado.

A segunda unidade de determinação pode ser adaptada para determinar um começo ou um fim de um segmento precedendo ou sucedendo o segmento atualmente reproduzido como uma posição de começo para

começar reprodução do segundo modo de reprodução. Por exemplo, no caso de um modo de reprodução acelerada dianteira rápida, o sistema pode simplesmente retornar, ao trocar para o modo de reprodução acelerada, à posição de começo do segmento de fato repetido. Isto significa que uma parte dos dados do segmento de dados atualmente reproduzido é repetido duas vezes, isto é anteriormente no modo de reprodução normal e subseqüentemente no modo de reprodução acelerada. Porém, este esquema é muito fácil e seguro e pode ser realizado com baixa carga computacional. De uma maneira semelhante, em um modo de reprodução acelerada inversa rápida, o sistema pode simplesmente saltar ao fim de um segmento atualmente reproduzido.

Particularmente, a segunda unidade de determinação pode ser adaptada para determinar a posição de começo baseado em uma velocidade de reprodução do fluxo de dados de acordo com o segundo modo de reprodução. Esta velocidade (por exemplo duas vezes, três vezes ou quatro vezes de uma velocidade de repetição normal), opcionalmente em combinação com o tempo de atraso e/ou o tempo restante de um segmento atualmente reproduzido é um critério importante adicional para determinar quando trocar do primeiro modo de reprodução para o segundo modo de reprodução é apropriado.

A segunda unidade de determinação pode ser adaptada para determinar a posição de começo de uma maneira que um segmento dos dados codificados que serão reproduzidos a seguir depois de um segmento atualmente reproduzido do fluxo de dados é decifrável por meio dos dados de decifração correspondentes decifrados a um momento antes da reprodução do segmento atualmente reproduzido do fluxo de dados é terminado. Este critério permite evitar tempos de espera entre um modo de reprodução normal e um modo de reprodução acelerada que pode ocorrer desde que os dados tem que ser decodificados. Em outras palavras, só quando os dados de decifração precisados para decifrar o conteúdo de um segmento subseqüente são

decifrados prontamente antes do fim do segmento (que leva algum tempo devido à latência de um cartão inteligente decifrador), será possível continuar reprodução sem uma interrupção.

O dispositivo de acordo com a invenção pode ser adaptado para processar um fluxo de dados de dados de vídeo ou dados de áudio. Porém, tal conteúdo de mídia não é o único tipo de dados que podem ser processados com o esquema de acordo com a invenção. Geração de reprodução acelerada e aplicações semelhantes são um assunto para ambos, processamento de vídeo e processamento de áudio (puro).

O dispositivo de acordo com a invenção pode ser adaptado para processar um fluxo de dados de dados digitais.

Particularmente, o primeiro modo de reprodução pode ser um modo de reprodução normal. O termo "modo de reprodução normal" denota particularmente um modo de reprodução no qual dados relacionados aos segmentos do fluxo de dados são reproduzidos ou repetidos de uma maneira que todos os dados transmitidos são usados. A velocidade de reproduzir os dados não é modificada com respeito à seqüência de dados como transmitidos.

Ademais, o dispositivo pode ser adaptado de uma tal maneira que o segundo modo de reprodução seja um modo de reprodução acelerada. Um usuário pode ajustar um tal "modo de reprodução acelerada" selecionando opções/comandos correspondentes em uma interface de usuário, por exemplo botões de um dispositivo, um teclado, ou um controle remoto. O modo de reprodução acelerada selecionado pelo usuário (que pode ser baseado em informação relativa à posição de quadros I no fluxo de dados) pode ser um do grupo consistindo em um modo de reprodução dianteira rápida, um modo de reprodução inversa rápida, um modo de reprodução de movimento lento, um modo de reprodução de quadro congelado, um modo de reprodução de repetição imediata, e um modo de reprodução inversa. Outros esquemas de

reprodução acelerada, porém, são possíveis. Para reprodução acelerada, normalmente só uma parte de dados deverá ser usada para saída (por exemplo para exibição visual e/ou para saída acústica). Desde que nem todos os dados (quadros P, quadros B) em um fluxo de dados podem ser usados independentemente de outros quadros (quadros I) para gerar estes sinais reprodutíveis, o conhecimento dos dados independentemente utilizáveis (quadros I) pode ser desejado particularmente.

O dispositivo de acordo com a invenção pode incluir uma unidade de geração adaptada para gerar um fluxo de dados decifrado ou um fluxo de dados codificado para reprodução no segundo modo de reprodução do ponto de partida em diante. Tal unidade de geração pode prover os dados de uma maneira a serem produzidos diretamente, e pode incluir por exemplo um dispositivo de exibição e/ou um dispositivo de saída acústica.

O dispositivo de acordo com a invenção pode ser adaptado para processar um fluxo de dados de MPEG2 codificado. MPEG2 é a designação para um grupo de padrões de codificação de áudio e vídeo concordados por MPEG (grupo de peritos em quadros móveis), e publicado como o padrão internacional ISO/IEC13818. MPEG2 pode ser usado para codificar áudio e vídeo para sinais radiodifundidos, incluindo satélite digital e TV a cabo, mas também pode ser usado para DVD. Na estrutura da invenção, troca de reprodução acelerada é habilitada de uma maneira eficiente para um fluxo de dados codificado de MPEG2.

O dispositivo de acordo com a invenção pode ser realizado como pelo menos um do grupo consistindo em um dispositivo de gravação de vídeo digital, um dispositivo habilitado por rede, um sistema de acesso condicional, reprodutor de áudio portátil, um reprodutor de vídeo portátil, um telefone móvel, um reprodutor de DVD, um reprodutor de CD, um reprodutor de mídia baseado em disco rígido, um dispositivo de rádio de Internet, um dispositivo de entretenimento público, e um reprodutor de MP3. Porém, estas

aplicações só são exemplares.

Os aspectos definidos acima e aspectos adicionais da invenção são aparentes dos exemplos de concretização a serem descritos em seguida e são explicados com referência a estes exemplos de concretização.

BREVE DESCRIÇÃO DOS DESENHOS

A invenção será descrita em mais detalhe em seguida com referência a exemplos de concretização, mas aos quais a invenção não está limitada.

Figura 1 ilustra um pacote de fluxo de transporte marcado em tempo.

Figura 2 mostra um grupo de MPEG2 de estrutura de imagem com quadros intra-codificados e quadros preditivos dianteiros.

Figura 3 ilustra um grupo de MPEG2 de estrutura de imagem com quadros intra-codificados, quadros preditivos dianteiros e quadros preditivos bidirecionais.

Figura 4 ilustra uma estrutura de um arquivo de informação de ponto característico e conteúdo de fluxo armazenado.

Figura 5 ilustra um sistema para reprodução acelerada em um fluxo de 'plaintext'.

Figura 6 ilustra compressão de tempo em reprodução acelerada.

Figura 7 ilustra reprodução acelerada com distância fracionária.

Figura 8 ilustra reprodução acelerada de baixa velocidade.

Figura 9 ilustra uma estrutura de sistema de acesso condicional geral.

Figura 10 ilustra um pacote de fluxo de transporte codificado de radiodifusão de vídeo digital.

Figura 11 ilustra um cabeçalho de pacote de fluxo de

transporte do pacote de fluxo de transporte codificado de radiodifusão de vídeo digital da Figura 10.

Figura 12 ilustra um sistema permitindo executar reprodução acelerada em um fluxo completamente codificado.

Figura 13 ilustra um fluxo de transporte completo e um fluxo de transporte parcial.

Figura 14 ilustra um gerador e receptor de reprodução acelerada de acordo com uma concretização exemplar da invenção.

Figura 15 ilustra trocar para reprodução acelerada dianteira no quadro de um esquema de troca cega.

Figura 16 ilustra troca generalizada para reprodução acelerada dianteira no quadro de um esquema de troca cega.

Figura 17 ilustra troca incorreta para reprodução acelerada inversa no quadro de um esquema de troca cega.

Figura 18 ilustra troca generalizada para reprodução acelerada inversa no quadro de um esquema de troca cega.

Figura 19 ilustra troca rápida para reprodução acelerada dianteira para um tipo de fluxo I no quadro de um esquema de troca rápida.

Figura 20 ilustra troca rápida para reprodução acelerada dianteira para um tipo de fluxo II no quadro de um esquema de troca rápida.

Figura 21 ilustra troca rápida para reprodução acelerada dianteira para um tipo de fluxo II perto do fim do período criptográfico atual no quadro de um esquema de troca rápida.

Figura 22 ilustra troca rápida para reprodução acelerada inversa para um tipo de fluxo I no quadro de um esquema de troca rápida.

Figura 23 ilustra troca rápida para reprodução acelerada inversa para um tipo de fluxo II no quadro de um esquema de troca rápida.

Figura 24 ilustra troca rápida para reprodução acelerada inversa para um tipo de fluxo II perto do fim do período criptográfico atual no

quadro de um esquema de troca rápida.

Figura 25 ilustra troca melhorada para reprodução acelerada inversa para um tipo de fluxo II perto do fim do período criptográfico atual no quadro de um esquema de troca rápida.

Figura 26 ilustra troca rápida generalizada para reprodução acelerada no quadro de um esquema de troca rápida.

Figura 27A ilustra um primeiro esquema para otimização de objetivo de salto de acordo com uma concretização exemplar da invenção.

Figura 27B ilustra um segundo esquema para otimização de objetivo de salto de acordo com uma concretização exemplar da invenção.

Figura 27C ilustra um terceiro esquema para ilustrar otimização de objetivo de salto de acordo com uma concretização exemplar da invenção.

Figura 28 mostra uma região de começo para reprodução acelerada dianteira no quadro de um esquema de otimização de salto.

Figura 29 ilustra uma região de começo para reprodução acelerada inversa no quadro de um esquema de otimização de salto.

Figura 30 ilustra um gerador e receptor de reprodução acelerada em uma configuração para um fluxo híbrido de acordo com uma concretização exemplar da invenção.

Figura 31 ilustra troca de reprodução normal para reprodução acelerada para um fluxo híbrido.

Figura 32 ilustra um dispositivo para processar um fluxo de dados codificado em um sistema criptográfico de acordo com uma concretização exemplar da invenção.

DESCRIÇÃO DE CONCRETIZAÇÕES

A ilustração no desenho é descrita esquematicamente. Em desenhos diferentes, elementos semelhantes ou idênticos são providos com os mesmos sinais de referência.

No seguinte, se referindo à Figura 1 à Figura 13, aspectos diferentes de implementação de reprodução acelerada para fluxos de transporte de acordo com concretizações exemplares da invenção serão descritos.

Particularmente, várias possibilidades para executar reprodução acelerada em um fluxo codificado de MPEG2 serão descritas, que podem ser codificadas parcialmente ou totalmente, ou não codificadas. A descrição seguinte visará métodos específicos para o formato de fluxo de transporte de MPEG2. Porém, a invenção não está restringida a este formato.

Experiências foram realmente feitas com uma extensão, o denominado fluxo de transporte marcado em tempo. Isto inclui pacotes de fluxo de transporte, todos dos quais são pré-anexados com um cabeçalho de 4 bytes no qual o tempo de chegada de pacote de fluxo de transporte é colocado. Este tempo pode ser derivado do valor da base de tempo de referência de relógio de programa (PCR) no momento que o primeiro byte do pacote é recebido no dispositivo de gravação. Este é um método correto para armazenar a informação de temporização com o fluxo, de forma que reprodução do fluxo se torne um processo relativamente fácil.

Um problema durante reprodução é assegurar que a memória temporária de decodificador de MPEG2 não transbordará nem esvaziará. Se o fluxo de entrada fosse complacente ao modelo de memória temporária de decodificador, restaurar a temporização relativa assegura que o fluxo de saída também seja complacente. Alguns dos métodos de reprodução acelerada descritos aqui são independentes da marca de tempo e executam igualmente bem em fluxos de transporte com e sem marcas de tempo.

Figura 1 ilustra um pacote de fluxo de transporte marcado em tempo 100 tendo um comprimento total 104 de 188 Bytes e incluindo uma marca de tempo 101 tendo um comprimento 105 de 4 Bytes, um cabeçalho de pacote 102, e uma carga útil de pacote 103 tendo um comprimento de 184

Bytes.

Esta descrição seguinte dará um panorama das possibilidades para criar um fluxo de reprodução acelerada complacente com MPEG/DVB (radiodifusão de vídeo digital) de um fluxo de transporte gravado e pretende cobrir o espectro completo de fluxos gravados daqueles que são completamente 'plaintext', assim todo bit de dados pode ser manipulado, para fluxos que são codificados completamente (por exemplo de acordo com o esquema de DVB), de forma que só cabeçalhos e algumas tabelas possam ser acessíveis para manipulação. A invenção também trata uma solução entre estes extremos, onde só os dados que precisam ser manipulados para gerar o fluxo de reprodução acelerada estão em 'plaintext'.

Ao criar reprodução acelerada para um fluxo de transporte de MPEG/DVB, problemas podem surgir quando o conteúdo é codificado pelo menos parcialmente. Pode não ser possível descer ao nível de fluxo elementar, que é a abordagem usual, ou até mesmo acessar qualquer cabeçalho de fluxo elementar de pacote (PES) antes de decifração. Isto também significa que achar quadros de imagem não é possível. Máquinas de reprodução acelerada conhecidas precisam ser capazes de acessar e processar esta informação.

Na estrutura desta descrição, o termo "ECM" denota uma Mensagem de Controle de Intitulação. Esta mensagem pode incluir particularmente informação de proprietário de provedor secreto e pode, entre outros, conter palavras de controle codificadas (CW) precisadas para decifrar o fluxo de MPEG. Tipicamente, palavras de controle expiram em 10-20 segundos. As ECMs são embutidas em pacotes no fluxo de transporte.

Na estrutura desta descrição, o termo "chaves" denota particularmente dados que podem ser armazenados em um cartão inteligente e podem ser transferidos ao cartão inteligente usando EMMs, quer dizer as denominadas "Mensagens de Administração de Intitulação" que podem ser

embutidas no fluxo de transporte. Estas chaves podem ser usadas pelo cartão inteligente para decifrar as palavras de controle presentes na ECM. Um período de validade exemplar de uma tal chave é um mês.

Na estrutura desta descrição, o termo "palavras de controle" (CW) denota particularmente informação de decifração precisada para decifrar conteúdo atual. Palavras de controle podem ser decifradas pelo cartão inteligente e então armazenadas em uma memória do núcleo de decifração.

No seguinte, alguns aspectos relacionados a reprodução acelerada em fluxos de 'plaintext' serão descritos.

Até mesmo se um fluxo de MPEG2 não estiver codificado (quer dizer 'plaintext'), reprodução acelerada não é trivial. Uma solução fácil é apenas produzir os dados mais rápidos para um decodificador para adquirir um modo dianteiro rápido, mas como MPEG tem informação relacionada à temporização codificada em seus cabeçalhos, isto não pode apenas ser feito com a expectativa de obter um avanço rápido correto. Além disso, pode ser difícil decidir quais quadros suprimir, como este método para executar avanço rápido pode dar uma taxa de quadro mais alta que a taxa de exibição.

Além disso, um tal fluxo não é um fluxo de transporte complacente com MPEG2. Isto pode ser aceitável se o decodificador estiver no dispositivo de armazenamento, mas pode ser problemático se o sinal for transferido por uma interface digital padrão. Além disso, a taxa de bit pode aumentar dramaticamente na cadeia inteira. Se o fluxo de reprodução normal for um fluxo de transporte marcado em tempo de um único programa se originando de radiodifusão de satélite, a taxa de bit para o decodificador em reprodução normal pode ser ao redor de 40 Mbps e pacotes podem estar em posições irregulares com aberturas entre eles (fluxo de transporte parcial). Se o fluxo estiver comprimido com o fator de reprodução acelerada, a taxa de bit pode ser ao redor de 120 Mbps para uma velocidade de reprodução acelerada de 3x. A largura de banda suportada necessária de uma unidade de

acionamento de disco rígido também pode ser aumentada com o fator de reprodução acelerada.

Assim seria apropriado continuar enviando a quantidade correta de quadros, mas aqui um problema pode ocorrer ao usar uma técnica de codificação de vídeo tal como MPEG, que explora a redundância temporal de vídeo para alcançar altas relações de compressão. Quadros não podem mais ser decodificados independentemente.

Uma estrutura de uma pluralidade de grupos de imagens (GOPs) é mostrada na Figura 2.

Particularmente, Figura 2 mostra um fluxo 200 incluindo várias estruturas de GOP de MPEG2 com uma seqüência de quadros I 201 e quadros P 202. O tamanho de GOP é denotado com numeral de referência 203. O tamanho de GOP 203 está fixado a 12 quadros, e só quadros I 201 e quadros P 202 são mostrados aqui.

Em MPEG, uma estrutura de GOP pode ser usada na qual só o primeiro quadro é codificado independentemente de outros quadros. Isto é o denominado quadro I ou intra-codificado 201. Os quadros preditivos ou quadros P 202 são codificados com uma predição unidirecional, significando que eles só se confiam no quadro I prévio 201 ou quadro P 202 como indicado por setas 204 na Figura 2.

Uma tal estrutura de GOP tipicamente tem um tamanho de 12 ou 16 quadros 201, 202. É assumido que uma velocidade de reprodução acelerada de 2x adiante é desejada. Assim, por exemplo, todo segundo quadro deveria ser saltado. Isto não é possível no domínio comprimido devido à independência do quadro prévio reconstruído durante decodificação. Assim, apenas suprimir alguns quadros comprimidos e fixar a informação de temporização não é uma opção.

A alternativa é decodificar o fluxo inteiro primeiro, então saltar todo segundo quadro e finalmente codificar os quadros restantes

novamente. Isto pode conduzir a uma complexidade inaceitável dos circuitos ou software de reprodução acelerada. Assim no melhor caso, alguns quadros podem ser saltados do GOP, no qual nenhum outro quadro se confia. Para o exemplo de uma velocidade de reprodução acelerada de 2x com um tamanho de GOP de 12 quadros, só os últimos 6 quadros P podem ser saltados. Neste caso, as imagens exibidas tendem a ser de uma natureza "saltadora", onde um período de velocidade normal curto é obtido, seguido por um salto súbito em tempo. Especialmente a velocidades de reprodução acelerada mais altas isto pode ser desagradável e não dá ao espectador a aparência e sensação de reprodução acelerada usual.

Outra estrutura 300 de uma pluralidade de grupos de imagens (GOP) é mostrada na Figura 3.

Particularmente, Figura 3 mostra a estrutura de GOP de MPEG2 com uma seqüência de quadros I 201, quadros P 202 e quadros B 301. O tamanho de GOP é denotado novamente com numeral de referência 203.

É possível usar uma estrutura de GOP contendo também quadros preditivos de modo bidirecional ou quadros B 301 como mostrado na Figura 3. Um tamanho de GOP 203 de 12 quadros é escolhido para o exemplo. Os quadros B 301 são codificados com uma predição bidirecional, significando que eles se confiam em um quadro I ou P prévio e seguinte 201, 202 como indicado para alguns quadros B 301 por setas curvadas 204. A ordem de transmissão dos quadros comprimidos pode não ser a mesma como a ordem na qual eles são exibidos.

Para decodificar um quadro B 301, ambos os quadros de referência antes e depois do quadro B 301 (em ordem de exibição) são precisados. Para minimizar a demanda de memória temporária em um decodificador, os quadros comprimidos podem ser reordenados. Assim em transmissão, os quadros de referência podem vir primeiro. O fluxo

reordenado, como é transmitido, também é mostrado na Figura 3, parte inferior. A reordenação é indicada por setas retas 302. Um fluxo contendo quadros B 301 pode dar uma imagem de reprodução acelerada de boa aparência se todos os quadros B 301 forem saltados. Para o presente exemplo, isto conduz a uma velocidade de reprodução acelerada de 3x adiante.

Qualquer estrutura que o fluxo tenha, as soluções descritas até agora podem dar uma forma aceitável de reprodução acelerada para um modo dianteiro rápido. Para inverso, os quadros teriam que ser reordenados em tempo, mas devido ao fato que MPEG usa a correlação temporal entre quadros sucessivos para alcançar uma alta relação de compressão, a ordem na qual os quadros têm que ser decodificados é fixa. Portanto, um GOP primeiro tem que ser decodificado em direção dianteira. A ordem dos GOPs enviados ao decodificador pode ser invertida, e GOPs podem ser saltados para velocidades de reprodução acelerada inversa mais altas. Reduzir os GOPs saltando quadros P ou quadros B como descrito acima também é possível neste caso. De qualquer maneira, pode resultar em uma seqüência exibida de reprodução dianteira e saltos para trás. Portanto, os quadros de reprodução acelerada têm que ser selecionados do GOP decodificado e invertidos em ordem, depois do que os quadros são re-codificados. Então, o GOP prévio é buscado e processado e assim por diante. Embora possível, a complexidade de tal procedimento pode ser alta.

Uma conclusão das considerações precedentes é que usar só os quadros I na geração de reprodução acelerada pode ser uma solução correta, porque estes quadros podem ser decodificados independentemente. Como resultado, a geração de reprodução acelerada pode ser mais fácil especialmente para inverso. Adicionalmente, o uso só de quadros I já permite velocidades de reprodução acelerada até 3x ou 4x. Para velocidades de reprodução acelerada realmente baixas, as técnicas mais complexas mencionadas acima podem ser implementadas.

No seguinte, alguns aspectos relacionados a um arquivo de CPI ("informação de ponto característico") serão descritos.

Achar quadros I em um fluxo requer normalmente analisar o fluxo, para achar os cabeçalhos de quadro. Localizar as posições onde o quadro I começa pode ser feito enquanto a gravação está sendo feita, ou fora de linha depois que a gravação está completada, ou semi em linha, na realidade sendo fora de linha, mas com um pequeno atraso com respeito ao momento de gravação. O fim de quadro I pode ser achado detectando o começo do próximo quadro P ou quadro B. Os metadados derivados deste modo podem ser armazenados em um arquivo separado, mas acoplado que pode ser denotado como arquivo de informação de ponto característico ou arquivo de CPI. Este arquivo pode conter ponteiros ao começo e eventualmente fim de cada quadro I no arquivo de fluxo de transporte. Cada gravação individual pode ter seu próprio arquivo de CPI.

A estrutura de um arquivo de informação de ponto característico 400 é visualizada na Figura 4.

À parte do arquivo de CPI 400, informação armazenada 401 é mostrada. O arquivo de CPI 400 também pode conter alguns outros dados que não são discutidos aqui.

Com os dados do arquivo de CPI 400 é possível saltar ao começo de qualquer quadro I 201 no fluxo. Se o arquivo de CPI 400 também contiver o fim dos quadros I 201, a quantidade de dados para ler do arquivo de fluxo de transporte é conhecida exatamente para obter um quadro I 201 completo. Se por alguma razão o fim de quadro I não for conhecido, o GOP inteiro ou pelo menos uma grande parte dos dados de GOP é para ser lida para estar seguro que o quadro I 201 inteiro é lido. O fim do GOP é dado pelo começo do próximo quadro I 201. É conhecido de medições que a quantidade de dados de quadro I pode ser 40% ou mais dos dados de GOP totais.

Com os quadros I 201 recuperados um novo fluxo de

reprodução acelerada que obedece ao formato de fluxo de transporte de MPEG-2 pode ser construído. Tudo que é precisado é que os quadros para o fluxo de reprodução acelerada sejam re-multiplexados corretamente, de tal maneira que nenhum problema de memória temporária para o decodificador de MPEG ocorrerá. Embora isto pareça ser uma solução direta, não é uma solução trivial como se tornará claro no seguinte.

A seguir, alguns aspectos relacionados a como construir um fluxo de reprodução acelerada serão descritos.

Com a ajuda do arquivo de CPI, descrevendo a qual posição de pacote um quadro I 201 começa, como também onde o quadro I 201 termina, acesso é provido a todos os quadros I 201 do fluxo original. Mas apenas concatenar quadros I 201 adequadamente escolhidos em um fluxo grande de só quadros I 201 não resulta em um fluxo de MPEG válido, como se tornará claro do seguinte.

O primeiro ponto a investigar é a taxa de bit do fluxo de reprodução acelerada. Por exemplo, o fluxo original tem uma taxa de bit de vídeo média de 4 Mbps e um tamanho de GOP 203 de 12 quadros. A taxa de bit pode ser extraída de uma medição em um fluxo radiodifundido real. É assumido que o fluxo de reprodução acelerada consiste em quadros I 201 só que são exibidos cada um uma vez por quadro, conduzindo a uma taxa de renovação do fluxo de reprodução acelerada igual à reprodução normal. É lembrado que a quantidade de dados de quadro I 201 poderia ser 40% dos dados de GOP. Este número se origina de uma medição, onde a média estava ao redor de 25%. Assim, em média 25% dos dados têm que ser comprimidos em 1/12 do tempo, conduzindo a uma taxa de bit 3 vezes mais alta. Assim, a taxa de bit de reprodução acelerada média seria 12 Mbps com picos até ao redor de 20 Mbps. Este exemplo simples é pretendido para provê algum sentimento para o efeito de taxa de bit e sua origem.

Na realidade, os tamanhos dos quadros I 201 são conhecidos

ou são deriváveis da medição. Portanto, a taxa de bit para um quadro I 201 só para fluxo de reprodução acelerada como uma função de tempo pode facilmente ser calculada precisamente. A taxa de bit de reprodução acelerada pode ser 2 a 3 vezes mais alta que a taxa de bit de reprodução normal e às vezes pode ser mais alta que permitido pelo padrão de MPEG2. Levando em conta que este é um exemplo com um fluxo de taxa de bit moderada e que fluxos com taxas de bit mais altas serão encontrados seguramente, está claro que alguma forma de redução de taxa de bit tem que ser aplicada. Por exemplo, a taxa de bit de reprodução acelerada pode ser comparável à taxa de bit de reprodução normal. Isto é especialmente importante se os fluxos forem enviados a um decodificador por uma interface digital. Demanda adicional em largura de banda da interface devido à reprodução acelerada deveria ser evitada. Uma primeira opção é reduzir o tamanho dos quadros I 201. Porém, isto pode adicionar complexidade e limitações em relação à reprodução acelerada para fluxos codificados.

Uma opção, que pode ser apropriada para aplicações particulares, é reduzir a taxa de renovação de imagem de reprodução acelerada exibindo cada quadro I 201 várias vezes. A taxa de bit será reduzida por conseguinte. Isto pode ser alcançado adicionando os denominados quadros P 202 vazios entre os quadros I 201. Tal quadro P 202 vazio não está realmente vazio, mas pode conter dados instruindo o decodificador para repetir o quadro prévio. Isto tem um custo de bit limitado, que pode em muitos casos ser desprezado comparado a um quadro I 201. De experiências é conhecido que estruturas de GOP de reprodução acelerada como IPP ou IPPP podem ser aceitáveis para a qualidade de imagem de reprodução acelerada até mesmo vantajoso a altas velocidades de reprodução acelerada. A taxa de bit de reprodução acelerada resultante é da mesma ordem como a taxa de bit de reprodução normal. Também é mencionado que estas estruturas podem reduzir a largura de banda suportada requerida do dispositivo de

armazenamento.

No seguinte, alguns aspectos relacionados a assuntos de temporização e construção de fluxo serão descritos.

Um sistema de reprodução acelerada 500 é descrito esquematicamente na Figura 5.

O sistema de reprodução acelerada 500 inclui uma unidade de gravação 501, uma unidade de seleção de quadro I 502, um bloco de geração de reprodução acelerada 503 e um decodificador de MPEG2 504. O bloco de geração de reprodução acelerada 503 inclui uma unidade analisadora 505, uma unidade somadora 506, uma unidade empacotadora 507, uma unidade de memória de tabela 508 e um multiplexador 509.

A unidade de gravação 501 provê a unidade de seleção de quadro I 502 com dados de MPEG2 de 'plaintext' 510. O multiplexer 509 provê o decodificador de MPEG2 504 com um fluxo de transporte complacente com MPEG2 DVB 511.

O seletor de quadro I 502 lê quadros I 201 específicos do dispositivo de armazenamento 501. Quais quadros I 201 são escolhidos depende da velocidade de reprodução acelerada como será descrito abaixo. Os quadros I 201 recuperados são usados para construir um fluxo de reprodução acelerada complacente com MPEG-2/DVB que é então enviado ao decodificador de MPEG-2 504 para decodificar e representação.

A posição dos pacotes de quadro I no fluxo de reprodução acelerada não pode ser acoplada à temporização relativa do fluxo de transporte original. Em reprodução acelerada, o eixo de tempo pode ser comprimido com o fator de velocidade e adicionalmente invertido para reprodução acelerada inversa. Portanto, as marcas de tempo do fluxo de transporte marcado em tempo original podem não ser adequadas para geração de reprodução acelerada. Além disso, a base de tempo de PCR original pode ser perturbadora para reprodução acelerada. Em primeiro lugar, não está

garantido que um PCR estará disponível dentro do quadro I 201 selecionado. Mas até mesmo mais importante, é que a freqüência da base de tempo de PCR seria mudada. De acordo com a especificação de MPEG2, esta freqüência deveria estar dentro de 30 ppm de 27 MHz. A base de tempo de PCR original satisfaz este requisito, mas se usada para reprodução acelerada seria multiplicada pelo fator de velocidade de reprodução acelerada. Para reprodução acelerada inversa, isto conduz até mesmo a uma base de tempo correndo na direção errada. Portanto, a base de tempo de PCR antiga tem que ser removida e uma nova adicionada ao fluxo de reprodução acelerada.

Finalmente, quadros I 201 normalmente contêm duas marcas de tempo que contam para o decodificador 504 quando começar a decodificar o quadro (marca de tempo de decodificação, DTS) e quando começar apresentação, por exemplo exibindo-o (marca de tempo de apresentação, PTS). Decodificação e apresentação podem ser começadas quando DTS respectivamente PTS são iguais à base de tempo de PCR, que é reconstruída no decodificador 504 por meio dos PCRs no fluxo. A distância entre, por exemplo, os valores de PTS de 2 quadros I 201 corresponde a sua distância nominal em tempo de exibição. Em reprodução acelerada, esta distância de tempo é comprimida com o fator de velocidade. Desde que uma nova base de tempo de PCR é usada em reprodução acelerada, e porque a distância para DTS e PTS não é mais correta, o DTS e PTS originais do quadro I 201 têm que ser substituídos.

Para resolver as complicações acima mencionadas, o quadro I 201 pode primeiro ser analisado em um fluxo elementar na unidade analisadora 505. Então os quadros P vazios 202 são adicionados em nível de fluxo elementar. A reprodução acelerada obtida, GOP é mapeada em um pacote de PES e empacotada a pacotes de fluxo de transporte. Então tabelas corrigidas como PAT, PMT, etc., são adicionadas. Nesta fase, uma nova base de tempo de PCR junto com DTS e PTS são incluídas. Os pacotes de fluxo de

transporte são pré-anexados com uma marca de tempo de 4 bytes que é acoplada à base de tempo de PCR tal que o fluxo de reprodução acelerada possa ser operado pelos mesmos circuitos de saída como usados para reprodução normal.

No seguinte, alguns aspectos relacionados a velocidades de reprodução acelerados serão descritos.

Neste contexto, primeiramente, velocidades de reprodução acelerada fixas serão discutidas.

Como mencionado antes, uma estrutura de GOP de reprodução acelerada como IPP pode ser usada na qual dois (2) quadros P vazios 202 seguem o quadro I 201. É assumido que o GOP original tem um tamanho de GOP 203 de 12 quadros e que todos os quadros I 201 originais são usados para reprodução acelerada. Isto significa que os quadros I 201 no fluxo de reprodução normal têm uma distância de 12 quadros e os mesmos quadros I 201 no fluxo de reprodução acelerada uma distância de 3 quadros. Isto conduz a uma velocidade de reprodução acelerada de 12/3 = 4x. Se denotar o tamanho de GOP original 203 em quadros por G, o tamanho de GOP de reprodução acelerada em quadros por T e o fator de velocidade de reprodução acelerada por N_b, então a velocidade de reprodução acelerada é em geral dada por:

$$N_b = G/T \quad (1)$$

N_b também será denotado como a velocidade básica. Velocidades mais altas podem ser realizadas saltando quadros I 201 do fluxo original. Se todo segundo quadro I 201 for tomado, a velocidade de reprodução acelerada é dobrada, se todo terceiro quadro I 201 for tomado, a velocidade de reprodução acelerada é triplicada e assim por diante. Em outras palavras, a distância entre os quadros I 201 usados do fluxo original é 2, 3 e assim por diante. Esta distância pode ser sempre um número inteiro. Se denotar a distância entre os quadros I 201 usados para geração de reprodução

acelerada por D (D = 1 significando que todo quadro I 201 é usado), então o fator de velocidade de reprodução acelerada geral N é dado por:

$$N = D*G/T \quad (2)$$

Isto significa que todos os múltiplos inteiros da velocidade básica podem ser realizados, conduzindo a um conjunto aceitável de velocidades. Deveria ser notado que D é negativo para reprodução acelerada inversa e que D = 0 resulta em uma imagem parada. Dados só podem ser lidos em uma direção dianteira. Portanto, em reprodução acelerada inversa, dados são lidos adiante e saltos são feitos para trás para recuperar o quadro I 201 precedente dado por D. Também deveria ser notado que um tamanho de GOP de reprodução acelerada maior T resulta em uma velocidade básica mais baixa. Por exemplo, IPPP conduz a um conjunto granulado mais fino de velocidades que IPP.

No seguinte, se referindo à Figura 6, compressão de tempo em reprodução acelerada será explicada.

Figura 6 mostra a situação para T = 3 (IPP) e G = 12. Para D = 2, um tempo de exibição original de 24 quadros é comprimido em um tempo de exibição de reprodução acelerada de 3 quadros resultando em N = 8. No exemplo dado, a velocidade básica é um inteiro mas isto não é necessariamente o caso. Para G = 16 e T = 3, a velocidade básica é 16/3 = 5 1/3, que não resulta em um conjunto de velocidades de reprodução acelerada inteiras. Portanto, a estrutura de IPPP (T = A) é melhor adequada para um tamanho de GOP de 16 resultando em uma velocidade básica de 4x. Se uma única estrutura de reprodução acelerada for desejada que se ajusta aos tamanhos de GOP mais comuns de 12 e 16, IPPP pode ser escolhido.

Em segundo lugar, velocidades de reprodução acelerada arbitrárias serão discutidas.

Em alguns casos, o conjunto de velocidades de reprodução acelerada resultando do método descrito acima é satisfatório, em alguns casos

não. No caso de G = 16 e T = 3, alguém provavelmente ainda preferiria fatores de velocidade de reprodução acelerada inteiros. Até mesmo no caso de G = 12 e T = 4, poderia ser preferido ter uma velocidade não disponível no conjunto como por exemplo 7x. Agora, a fórmula de velocidade de reprodução acelerada será invertida e a distância D será calculada que é dado por:

$$D = N*T/G \quad (3)$$

Usando o exemplo acima com G = 12, T = 4 e N = 7 resulta em D = 2 1/3. Em vez de saltar um número fixo de quadros I 201, um algoritmo de salto adaptável poderia ser usado que escolhe o próximo quadro I 201 baseado no fato de qual quadro I 201 melhor casa com a velocidade requerida. Para escolher o melhor quadro I 201 de casamento, o próximo ponto ideal Ip com a distância D pode ser calculado e um dos quadros I 201 pode ser escolhido mais perto a este ponto ideal para construir um GOP de reprodução acelerada. Na etapa seguinte, novamente o próximo ponto ideal pode ser calculado aumentando o último ponto ideal por D.

Como visualizado na Figura 7 ilustrando reprodução acelerada com distâncias fracionárias, há três possibilidades particularmente para escolher o quadro I 201:

A. O quadro I mais perto ao ponto ideal; I = arredondado (Ip)

B. O último quadro I antes do ponto ideal; I = int (Ip)

C. O primeiro quadro I depois do ponto ideal; I = int (Ip)+1

Como pode ser visto claramente, a distância atual é variada entre int (D) e int (D) +1, a relação entre as ocorrências dos dois sendo dependente da fração de D, tal que a distância média seja igual a D. Isto significa que a velocidade de reprodução acelerada média é igual a N, mas que o quadro realmente usado tem uma pequena instabilidade com respeito ao quadro ideal. Várias experiências foram executadas com isto, e embora a velocidade de reprodução acelerada possa variar localmente, isto não é

visualmente perturbador. Normalmente, não é mesmo notável especialmente a velocidades de reprodução acelerada um pouco mais altas. Também está claro da Figura 7 que não faz diferença se escolher o método A, B ou C.

Com este método, a velocidade de reprodução acelerada N não precisa ser um inteiro, mas pode ser qualquer número acima da velocidade básica N_b. Também velocidades abaixo deste mínimo podem ser escolhidas, mas então a taxa de renovação de imagem pode ser abaixada localmente porque o tamanho de GOP efetivo de reprodução acelerada T é dobrado ou a velocidades ainda mais baixas até triplicada ou mais. Isto é devido a uma repetição dos GOPs de reprodução acelerada, como o algoritmo escolherá o mesmo quadro I 201 mais de uma vez.

Figura 8 mostra um exemplo para D = 2/3 que é equivalente a N = 2/3 N_b. Aqui, a função redonda é usada para selecionar os quadros I 201 e como pode ser visto, quadros 2 e 4 são selecionados duas vezes.

De qualquer maneira, o método descrito permitirá uma velocidade de reprodução acelerada continuamente variável. Para reprodução acelerada inversa, um valor negativo é escolhido para N. Para o exemplo da Figura 7, isto simplesmente significa que as setas 700 estão apontando na outra direção. O método descrito também incluirá os conjuntos de velocidades de reprodução acelerada fixas mencionados mais cedo e eles terão a mesma qualidade, especialmente se a função redonda for usada. Portanto, poderia ser apropriado que o método flexível descrito nesta seção sempre deveria ser implementado seja qual for a escolha das velocidades.

No seguinte, alguns aspectos relacionados à taxa de renovação da imagem de reprodução acelerada serão discutidos.

O termo "taxa de renovação" denota particularmente a freqüência com a qual imagens novas são exibidas. Embora não dependente de velocidade, será discutido brevemente aqui porque pode influenciar a escolha de T. Se a taxa de renovação da imagem original for denotada por R

(25Hz ou 30Hz), a taxa de renovação da imagem de reprodução acelerada (R_t) é dada por:

$$R_t = R/T \quad (4)$$

Com uma estrutura de GOP de reprodução acelerada de IPP (T = 3) ou IPPP (T = 4), a taxa de renovação R_t é 8 1/3 Hz respectivamente 6 1/4 Hz para a Europa e 10 Hz respectivamente 7 1/2 Hz para os E.U.A.

Embora o julgamento de qualidade de imagem de reprodução acelerada seja uma questão algo subjetiva, há sugestões claras de experiências que estas taxas de renovação são aceitáveis para velocidades baixas e até mesmo vantajosas a velocidades mais altas.

No seguinte, alguns aspectos relacionados a ambientes de fluxo codificados serão descritos.

No seguinte, alguma informação sobre fluxos de transporte codificados é apresentada como uma base para a descrição de reprodução acelerada em fluxos codificados. É focalizado no Sistema de Acesso Condicional usado para radiodifusão.

Figura 9 ilustra um sistema de acesso condicional 900, que será descrito no seguinte.

No sistema de acesso condicional 900, conteúdo 901 pode ser provido a uma unidade de criptografia de conteúdo 902. Depois de ter codificado o conteúdo 901, a unidade de criptografia de conteúdo 902 provê uma unidade de decifração de conteúdo 904 com conteúdo codificado 903.

Uma palavra de controle 906 pode ser provida à unidade de criptografia de conteúdo 902 e a uma unidade de geração de ECM 907. A unidade de geração de ECM 907 gera uma ECM e provê a mesma a uma unidade de decodificação de ECM 908 de um cartão inteligente 905. A unidade de decodificação de ECM 908 gera da ECM uma palavra de controle, quer dizer informação de decifração que é precisada e provida à unidade de criptografia de conteúdo 904 para decifrar o conteúdo codificado 903.

Além disso, uma chave de autorização 910 é provida à unidade de geração de ECM 907 e a uma unidade de geração de KMM 911, em que a última gera uma KMM e provê a mesma a uma unidade de decodificação de KMM 912 do cartão inteligente 905. A unidade de decodificação de KMM 912 provê um sinal de saída à unidade de decodificação de ECM 908.

Além disso, uma chave de grupo 914 pode ser provida à unidade de geração de KMM 911 e a uma unidade de geração de GKM 915, que pode ser ademais provida com uma chave de usuário 918. A unidade de geração de GKM 915 gera um sinal de GKM e provê o mesmo a uma unidade de decodificação de GKM 916 do cartão inteligente 905, em que a unidade de decodificação de GKM 916 obtém como uma entrada adicional uma chave de usuário 917.

Além disso, intitulações 919 podem ser providas a uma unidade de geração de EMM 920, que gera um sinal de EMM e provê o mesmo a uma unidade de decodificação de EMM 921. A unidade de decodificação de EMM 921 localizada no cartão inteligente 905 está acoplada com uma unidade de lista de intitulação 913, que provê a unidade de decodificação de ECM 908 com informação de controle correspondente.

ECM denota Mensagens de Controle de Intitulação, KMM denota Mensagens de Administração de Chave, GKM denota Mensagens de Chave de Grupo e EMM denota Mensagens de Administração de Intitulação.

Em muitos casos, provedores de conteúdo e provedores de serviço querem controlar acesso a certos itens de conteúdo por um sistema de acesso condicional (CA).

Para alcançar isto, o conteúdo radiodifundido 901 é codificado sob o controle do sistema de CA 900. No receptor, conteúdo é decifrado antes de decodificação e representação se acesso for concedido pelo sistema de CA 900.

O sistema de CA 900 usa uma hierarquia em camadas (veja

Figura 9). O sistema de CA 900 transfere a chave de decifração de conteúdo (palavra de controle CW 906, 909) de servidor para cliente na forma de uma mensagem codificada, chamada ECM (Mensagem de Controle de Intitulação). ECMs são codificadas usando uma chave de autorização (AK) 910. Por razões de segurança, o servidor de CA 900 pode renovar a chave de autorização 910 emitindo uma KMM (Mensagem de Administração de Chave). Uma KMM é na realidade um tipo especial de EMM (Mensagem de Administração de Intitulação), mas para clareza, o termo KMM pode ser usado. KMMs também são codificadas usando uma chave que por exemplo pode ser uma chave de grupo (GK) 914, que é renovada enviando uma GKM (Mensagem de Chave de Grupo), que é novamente um tipo especial de EMM. GKMs são então codificadas com a chave de usuário (UK) 917, 918, que é uma chave única fixa embutida no cartão inteligente 905 e conhecida só pelo sistema de CA 900 do provedor. Chaves de autorização e chaves de grupo são armazenadas no cartão inteligente 905 do receptor.

Intitulações 919 (por exemplo direitos de visão) são enviadas para clientes individuais na forma de uma EMM (Mensagem de Administração de Intitulação) e armazenadas localmente em um dispositivo seguro (cartão inteligente 905). Intitulações 919 são acopladas a um programa específico. Uma lista de intitulações 913 dá acesso a um grupo de programas dependendo do tipo de assinatura. ECMs só são processadas em chaves (palavras de controle) pelo cartão inteligente 905 se uma intitulação 919 estiver disponível para o programa específico. EMMs de Intitulação estão sujeitas a uma estrutura em camadas idêntica como as KMMs (não descritas na Figura 9). Em um sistema de MPEG2, conteúdo codificado, ECMs e EMMs (incluindo a KMM e tipos de GKM) são todos multiplexados em um único fluxo de transporte de MPEG2.

A descrição anterior é uma visão generalizada do sistema de CA 900. Em radiodifusão de vídeo digital, só o algoritmo de criptografia, a

estrutura de palavra de controle impar/par, a estrutura global de ECMs e EMMs e sua referência são definidas. A estrutura detalhada do sistema de CA 900 e o modo que as cargas úteis de ECMs e EMMs são codificadas e usadas são específicos de provedor. Também o cartão inteligente é específico de provedor. Porém, de experiência é conhecido que muitos provedores seguem essencialmente a estrutura da visão generalizada da Figura 9.

No seguinte, tópicos de Criptografia/Decifração de DVB serão discutidos.

O algoritmo de criptografia aplicada e decifração é definido pela organização de padronização de DVB. Em princípio, duas possibilidades de criptografia são definidas a saber criptografia de nível de PES e criptografia de nível de TS. Porém, na vida real principalmente o método de criptografia de nível de TS é usado. Criptografia e decifração dos pacotes de fluxo de transporte são feitas baseado em pacote. Isto significa que o algoritmo de criptografia e decifração é reiniciado toda vez que um novo pacote de fluxo de transporte é recebido. Portanto, pacotes podem ser codificados ou decifrados individualmente. No fluxo de transporte, pacotes codificados e de 'plaintext' são misturados porque algumas partes de fluxo são codificadas (por exemplo áudio/vídeo) e outras não são (por exemplo, tabelas). Até mesmo dentro de uma parte de fluxo (por exemplo vídeo) pacotes codificados e de 'plaintext' podem ser misturados.

No seguinte, se referindo à Figura 10, um pacote de fluxo de transporte codificado de DVB 1000 será descrito.

O pacote de fluxo 1000 tem um comprimento 1001 de 188 Bytes e inclui três porções. Um cabeçalho de pacote 1002 tem um tamanho 1003 de 4 Bytes. Subseqüente ao cabeçalho de pacote 1002, um campo de adaptação 1004 pode ser incluído no pacote de fluxo 1000. Depois disso, uma carga útil de pacote codificada de DVB 1005 pode ser enviada.

Figura 11 ilustra uma estrutura detalhada do cabeçalho de

pacote de fluxo de transporte 1002 da Figura 10.

O cabeçalho de pacote de fluxo de transporte 1002 inclui uma unidade de sincronização (SYNC) 1010, um indicador de erro de transporte (TEI) 1011, que pode indicar erros de transporte em um pacote, um indicador de começo de unidade de carga útil (PLUSI) 1012, que pode indicar particularmente um possível começo de um pacote de PES na carga útil subseqüente 1005, uma unidade de prioridade de transporte (TPI) 1017 indicando prioridade do transporte, um identificador de pacote (PID) 1013 usado para determinar a designação do pacote, um controle de mistura de transporte (SCB) 1014 para selecionar a CW que é precisada para decifrar o pacote de fluxo de transporte, um controle de campo de adaptação (AFLD) 1015, e um contador de continuidade (CC) 1016.

Assim, Figura 10 e Figura 11 mostram o pacote de fluxo de transporte de MPEG2 1000 que foi codificado e que inclui partes diferentes:

Cabeçalho de pacote 1002 está em 'plaintext'. Serve para obter informação importante tal como um número de identificador de pacote (PID), presença de um campo de adaptação, bits de controle de mistura, etc.

Campo de adaptação 1004 também está em 'plaintext'. Pode conter informação de temporização importante tal como o PCR.

Carga Útil de Pacote Codificada de DVB 1005 contém o conteúdo de programa atual que pode ter sido codificado usando o algoritmo de DVB.

A fim de selecionar a CW correta que é precisada para decifrar o programa radiodifundido é necessário analisar o cabeçalho de pacote de fluxo de transporte. Um panorama esquemático deste cabeçalho é dado na Figura 11. Um campo importante para a decifração do programa radiodifundido é o campo de bits de controle de mistura (SCB) 1014. Este campo de SCB 1014 indica qual CW o decifrador deve usar para decifrar o programa radiodifundido. Além disso, indica se a carga útil do pacote está

codificada ou em 'plaintext'. Para todo novo pacote de fluxo de transporte, este SCB 1014 deve ser analisado desde que muda com tempo e pode mudar de pacote para pacote.

No seguinte, alguns aspectos relacionados à reprodução acelerada em fluxos completamente codificados serão descritos.

A primeira razão por que isto é que um tópico interessante é que reprodução acelerada em fluxos de 'plaintext' e completamente codificados são os dois extremos de uma gama de possibilidades. Outra razão é que existem aplicações nas quais pode ser necessário gravar fluxos completamente codificados. Assim, seria útil ter uma técnica à mão para executar reprodução acelerada em um fluxo completamente codificado.

Um princípio básico é ler um bloco suficientemente grande de dados do dispositivo de armazenamento, decifra-lo, selecionar um quadro I no bloco e construir um fluxo de reprodução acelerada com ele.

Tal sistema 1200 é descrito na Figura 12.

Figura 12 mostra o princípio básico de reprodução acelerada em um fluxo completamente codificado. Para este propósito, dados armazenados em um disco rígido 1201 são providos como um fluxo de transporte 1202 para um decifrador 1203. Ademais, o disco rígido 1201 provê um cartão inteligente 1204 com uma ECM, em que o cartão inteligente 1204 gera palavras de controle desta ECM e envia as mesmas ao decifrador 1203.

Usando as palavras de controle, o decifrador 1203 decifra o fluxo de transporte codificado 1202 e envia os dados decifrados a um detector de quadro I e filtro 1205. De lá, os dados são providos a uma unidade de quadro P vazia de inserção 1206 que leva os dados a uma caixa de topo fixa 1207. De lá, os dados são providos a uma televisão 1208.

No seguinte, alguns aspectos serão mencionados com respeito à questão qual uma gravação contém.

Fazendo uma gravação de um único canal, a gravação deve

conter todos os dados requeridos para reproduzir a gravação do canal a uma fase posterior. Alguém pode recorrer a apenas gravar tudo em um certo transponder, mas deste modo alguém gravaria muito mais que precisa para reproduzir o programa pretendido gravar. Isto significa que ambos largura de banda e espaço de armazenamento seriam desperdiçados. Assim, em vez disto, só os pacotes realmente precisados deveriam ser gravados. Para cada programa isto significa que alguém deve gravar todos os pacotes obrigatórios de MPEG2 como PAT (tabela de associação de programa), CAT (tabela de acesso condicional), e obviamente para cada programa os pacotes de vídeo e áudio como também a PMT (tabela de mapa de programa) que descreve quais pacotes pertencem a um programa. Além disso, a CAT/PMT pode descrever pacotes de CA (ECMs) precisados para decifração do fluxo. A menos que a gravação seja feita em 'plaintext' depois de decifração, esses pacotes de ECM têm que ser gravados igualmente.

Se a gravação feita não consistir em todos os pacotes do multiplex completo, a gravação se torna um denominado fluxo de transporte parcial 1300 (veja Figura 13). Ademais, Figura 13 ilustra um fluxo de transporte completo 1301. O padrão de DVB requer que se um fluxo de transporte parcial 1300 for reproduzido, todas as tabelas obrigatórias de DVB normais como NIT (tabela de informação de rede), BAT (tabela de associação de buquê), etc., sejam removidas. Em vez destas tabelas, o fluxo parcial deveria ter as tabelas de SIT (tabela de informação de seleção) e DIT (tabela de informação de descontinuidade) inseridas.

No seguinte, se referindo à Figura 14 à Figura 32, sistemas serão descritos que são capazes de processar um fluxo de dados codificado em um sistema criptográfico de acordo com concretizações exemplares da invenção.

É enfatizado que os sistemas descritos no seguinte podem ser implementados na estrutura e em combinação com quaisquer dos sistemas

descritos se referindo à Figura 1 à Figura 13.

No seguinte, alguns aspectos relacionados à troca de reprodução normal para reprodução acelerada serão descritos.

A troca de reprodução normal para reprodução acelerada pode resultar em alguns efeitos especiais. A influência de memórias temporárias em outras partes da cadeia de reprodução não será o aspecto primário das considerações seguintes. Também é assumido que números de PID (identificador de pacote) em um fluxo de reprodução acelerada são idênticos a um fluxo de reprodução normal para evitar os efeitos de números de PID divergentes.

A seção seguinte se concentra particularmente nos efeitos de troca do processo de decifração, uma interrupção de qual aumentaria o tempo de transição para reprodução acelerada. Comportamento atual pode depender da disponibilidade de palavras de controle (CWs) e portanto da manipulação e processamento de ECMs (mensagens de controle de intitulação).

Se referindo à Figura 14, um sistema de reprodução acelerada 1400 será descrito.

O sistema de reprodução acelerada 1400 inclui um dispositivo de armazenamento 1403, um gerador de reprodução acelerada 1401 e um receptor 1402.

O dispositivo de armazenamento 1403 armazena dados a serem reproduzidos que são providos como um fluxo de transporte 1405 para uma unidade de decifrador 1406 e a uma unidade de chave 1408 do gerador de reprodução acelerada 1401. A unidade de chave 1408 pode trocar entre um modo de reprodução normal (NP) e um modo de reprodução acelerada (TP). Por uma unidade de controle 1409, a velocidade de uma reprodução acelerada desejada pode ser introduzida seletivamente como também o fato se uma reprodução normal ou uma reprodução acelerada é desejada. Esta informação é provida da unidade de controle 1409 ao dispositivo de armazenamento

1403. A unidade de controle 1403 é, por exemplo, controlada por um usuário por uma interface de usuário. Ademais, a unidade de controle 1409 provê os dados ou comandos entrados a uma unidade de construção de fluxo de reprodução acelerada 1407 e a uma unidade de memória de ECM 1412.

O dispositivo de armazenamento 1403 transmite o fluxo de transporte não só à unidade de decifrador 1406 e à unidade de chave 1408, mas também provê dados de ECM armazenados em um arquivo de ECM 1404 a uma unidade de memória de ECM 1412. A unidade de memória de ECM 1412, que também recebe os parâmetros da unidade de controle 1409, provê a unidade de construção de fluxo de reprodução acelerada 1407 e uma unidade de interface de cartão inteligente 1411 com dados de ECM. Ademais, a unidade de interface de cartão inteligente 1411 é adaptada para se comunicar com um cartão inteligente 1410.

O cartão inteligente 1410 gera palavras de controle (CW) e provê as palavras de controle pela unidade de interface de cartão inteligente 1411 à unidade de decifrador 1406.

Em um modo de reprodução normal, a posição da chave da unidade de chave 1408 é como mostrado na Figura 14. Neste modo de operação, o fluxo de transporte 1405 é provido diretamente à unidade de receptor 1412. Porém, quando um modo de reprodução acelerada é selecionado, a chave irá para a outra posição como mostrado na Figura 14, de forma que o fluxo de transporte 1405 será processado pela unidade de construção de fluxo de reprodução acelerada 1407, que proverá dados de reprodução acelerada ao receptor 1402, mais particularmente a uma unidade de decifrador 1413 do receptor 1402 e a uma unidade de extrator de ECM 1416 do receptor 1402.

Uma unidade de extrator de ECM 1416 proverá ECMs a uma interface de cartão inteligente 1417 que está acoplada comunicativamente ao cartão inteligente 1418. Com respeito às ECMs, a interface de cartão

inteligente 1417 provê a unidade de decifrador 1413 com palavras de controle como informação de decifração. Depois de ter passado a unidade de decifrador 1413, os dados são passados a uma unidade de decodificador/representador 1414, donde os dados podem ser transmitidos a uma unidade de exibição 1415.

Como descrito na Figura 14, há particularmente dois aspectos que têm que ser considerados. O primeiro é o efeito no receptor 1402 que pode decifrar, decodificar e representar um sinal que é trocado entre reprodução normal e reprodução acelerada. O segundo é o efeito da troca em relação ao gerador de reprodução acelerada 1401.

No seguinte, a unidade de receptor 1402 será descrita ademais.

O fluxo de reprodução acelerada gerado de acordo com as técnicas descritas aqui pode ser um fluxo de 'plaintext'. Neste caso, nenhuma decifração do fluxo de reprodução acelerada é necessária no receptor 1402 e a decodificação de MPEG pode começar imediatamente depois da troca para reprodução acelerada.

No seguinte, o gerador de reprodução acelerada 1401 será descrito ademais.

O gerador de reprodução acelerada 1401 pode decifrar o fluxo a fim de selecionar os quadros I de 'plaintext' e construir um fluxo de reprodução acelerada disto. Este processo de decifração deveria começar o mais cedo possível depois de trocar para reprodução acelerada. Entre outros, o número de CWs por ECM influencia este processo de decifração. Esta informação é considerada como sendo conhecida (por exemplo do arquivo de CPI, veja Figura 4 e descrição correspondente), porque também é necessária para a geração de reprodução acelerada contínua. Os efeitos de troca são descritos daqui por diante.

Primeiro, a denominada "troca cega" será descrita. Isto significa basicamente que o estado de decifrador é desconhecido e poderia

assim estar errado. Porém, este esquema pode permitir troca de reprodução acelerada com baixa carga computacional.

Então, "troca rápida" será descrita. Neste caso, o estado de decifrador é assumido ser dado por história e pode ser usado para melhorar a velocidade de troca.

Finalmente, otimização da posição de troca será descrita.

No seguinte, "troca cega" será descrita.

Primeiramente, uma situação será considerada na qual não há nenhum conhecimento sobre o estado dos registradores de decifrador, ou que eles poderiam conter CWs totalmente erradas. Assim, uma certa iniciação pode ser executada a um começo. Para isto, é necessário conhecer onde o processamento de reprodução acelerada começa. Pode ser assumido que o fluxo de reprodução acelerada começa no local do fluxo de reprodução normal no momento de troca. Isto implica que a CW para decifrar o período atual é precisada primeiro. Assim, o esquema pode começar enviando a ECM do período atual ao cartão inteligente. Deveria ser assegurado que esta ECM seja processada. Isto não é garantido por uma mudança em ID de tabela porque a história é assumida ser desconhecida. Ao invés, o extrator de ECM do gerador de reprodução acelerada pode ser reiniciado durante reprodução normal trazendo-o no mesmo estado como depois da inserção de um cartão inteligente. O efeito é que a primeira ECM encontrada depois desta reiniciação sempre será enviada ao cartão inteligente independente de seu ID de tabela. Depois da latência do cartão inteligente, o processamento de reprodução acelerada pode ser começado. O método exato depende de se reprodução dianteira ou reprodução inversa deverá ser executada e de se uma ou duas CWs por ECM são providas. Os mesmos parâmetros também podem pedir etapas de iniciação adicionais no instante que o processamento de reprodução acelerada é começado.

Particularmente, dois cenários diferentes ou tipos de fluxo

podem ser distinguidos:

De acordo com um tipo de fluxo I, duas palavras de controle (CWs) são providas por Mensagem de Controle de Intitulação (ECM).

De acordo com um tipo de fluxo II, uma palavra de controle (CW) é provida por Mensagem de Controle de Intitulação (ECM). Para tipo de fluxo II, troca de reprodução normal para reprodução acelerada pode ocorrer mais tarde a uma certa distância, por exemplo 600 ms, antes do fim de um período particular.

Os efeitos e suas conseqüências são descritos daqui por diante para cada situação.

Um primeiro cenário pode ser denotado como "dianteiro e duas CWs".

No caso de reprodução acelerada dianteira, a próxima CW precisada para geração de reprodução acelerada é a CW do próximo período. A ECM enviada ao cartão inteligente na iniciação também continha esta CW.

Nenhuma etapa adicional é necessária. A primeira ECM enviada automaticamente pelo gerador de reprodução acelerada é a do próximo período.

Figura 15 mostra uma seqüência de períodos de um fluxo de dados. Um primeiro período é denotado como B, um segundo período é denotado como C, um terceiro período é denotado como D, um quarto período é denotado como E, e um quinto período é denotado como F. Figura 15 ademais ilustra uma troca de um modo de reprodução normal 1501 para um modo de reprodução acelerada 1502, em que o ponto de troca de tempo é denotado com numeral de referência 1503. A tempo 1503, um ID 0x80 de tabela de ECM C é enviado. No modo de reprodução normal 1501, o fluxo de dados inteiro é reproduzido continuamente. No modo de reprodução acelerada 1502, o fluxo de dados inteiro não é repetido, mas só algumas porções, em que setas 1504 indicam saltos entre porções exibidas através de porções não

exibidas do fluxo de dados.

Se referindo a tipo de fluxo I; a um ponto de tempo 1505, uma ECM D é enviada com ID de tabela 0x81. No ponto de tempo 1506, uma ECM E é enviada com ID de tabela 0x80.

Outro cenário pode ser denotado como "dianteiro e uma CW".

Esta situação também é descrita na Figura 15 para tipo de fluxo II.

Para o caso de tipo de fluxo II, uma ECM E com ID de tabela 0x80 é enviada no ponto de tempo 1505. No ponto de tempo 1506, uma ECM F é enviada com ID de tabela 0x81.

Troca ocorre durante período C. Neste caso, a CW para o próximo período D não está presente em ECM C. A primeira ECM que é enviada automaticamente pelo gerador de reprodução acelerada é a de período E. A palavra "automaticamente" pode se referir particularmente ao modo que ECMs são enviadas em reprodução acelerada contínua. Como esta ECM E tem um ID de tabela idêntico à ECM C enviada na iniciação, ela não será processada. Assim dois períodos completos são perdidos, isto é D e E. Isto pode ser corrigido do modo seguinte, como também pode ser tirado da Figura 16. A máquina de reprodução acelerada assume que o período atual C foi entrado há pouco e começa a geração de reprodução acelerada no começo deste período em vez de na última posição de reprodução normal. Então também envia a ECM do próximo período D para o cartão inteligente. Como esta ECM tem uma tabela diferente (ID 0x81) de ECM C enviada na iniciação (ID 0x80), ela será processada corretamente. Um período completo C está disponível agora para decifração de ECM D. Isto assegura que a CW decifrada D esteja disponível em tempo até mesmo na velocidade de reprodução acelerada mais alta. Isto também significa que as primeiras imagens de reprodução acelerada podem ser uma repetição das últimas imagens de reprodução normal. Experiências mostraram este efeito que é em

muitos casos aceitável.

Outro cenário pode ser denotado como "troca generalizada para reprodução acelerada dianteira" e será explicado no seguinte, também se referindo à Figura 16.

No cenário mostrado, um ponto de tempo 1600 é indicado a qual uma ECM C é enviada. Uma troca para reprodução acelerada ocorre depois que o sistema esperou por latência de cartão inteligente 1601.

O método alternativo também pode ser usado no caso de duas CWs por ECM. Neste caso, a primeira ECM enviada pelo gerador de reprodução acelerada é idêntica a enviada na iniciação. A ECM repetida não é então processada, que não é nenhum problema. Assim, uma abordagem generalizada para troca de reprodução normal para reprodução acelerada dianteira como descrito na Figura 16 pode ser como segue:

Durante reprodução normal 1501, o extrator de ECM no gerador de reprodução acelerada é reiniciado;

No momento de troca, a ECM do período atual é enviada primeiro; isso é o período no qual a última posição de reprodução normal está localizada;

Depois da latência 1601 do cartão inteligente, o processo de reprodução acelerada é começado, o primeiro bloco de reprodução acelerada sendo lido do começo do período atual;

O gerador de reprodução acelerada assume que o período atual foi entrado há pouco e envia uma ECM por conseguinte a um ponto de tempo 1602 (dependendo de uma ou duas CWs). Para tipo de fluxo I, uma ECM C é enviada aqui. Para tipo de fluxo II, uma ECM D é enviada aqui.

Outro cenário pode ser denotado como "inverso e duas CWs".

Novamente, a suposição é feita que reprodução acelerada começa na última posição de reprodução normal. Na Figura 17 é indicado que troca ocorre a um ponto de tempo 1700 durante período E a qual momento

ECM E (ID de Tabela 0x80) é enviada ao cartão inteligente. Em reprodução acelerada inversa, a CW precisada depois da uma para o período atual E é a do período prévio D. A ECM E enviada na iniciação não contém esta CW D. A primeira ECM enviada automaticamente pelo gerador de reprodução acelerada é ECM C a um ponto de tempo 1701. Esta ECM contém CW D, mas porque esta ECM C tem a mesma tabela (ID 0x80) como a ECM E enviada na iniciação, ela não será processada. A primeira ECM processada corretamente será a ECM B enviada a um ponto de tempo 1702 que contém CWs B e C. ECM A é enviada a um ponto de tempo 1703.

CW D não estará disponível no decifrador. Como conseqüência, entre um e dois períodos estarão perdidos, isto é período D completamente e período C parcialmente. Quanto de período C é perdido depende da velocidade de reprodução acelerada e da latência de cartão inteligente. Isto interromperá o fluxo de reprodução acelerada.

Este problema pode ser resolvido enviando na iniciação a ECM D do período prévio em vez da ECM E do período atual. Isto carregará as CWs necessárias D e E do período prévio e atual nos registradores de decifrador. Também a primeira ECM enviada automaticamente pelo gerador de reprodução acelerada sendo ECM C pode ser processada agora corretamente.

Outro cenário pode ser denotado como "inversa e uma CW".

A mesma situação inicial ou de começo como para "inversa e duas CWs" é considerada (veja Figura 17 novamente). Assim, ECM E é enviada na iniciação 1700 e a primeira ECM processada corretamente é ECM B. Mas neste caso, as ECMs só contêm uma CW. Assim ECM B só contém CW B e não CW C. Como uma conseqüência, dois períodos são perdidos.

Porém, a correção seguinte pode ser executada. Como já mencionado, ECM E do período atual é enviada na iniciação 1700. Mas então, depois da latência do cartão inteligente, o processamento de reprodução

acelerada começará no fim do período atual E em vez de na última posição de reprodução normal. Isto significa saltar a uma posição correspondendo ao fim do período atual E menos o tamanho de bloco. A máquina de reprodução acelerada então ademais assume que o período atual E foi entrado há pouco e envia (automaticamente) a ECM D do período prévio no fluxo de reprodução normal. Esta ECM D será processada corretamente porque ECM E e D têm IDs de tabela diferentes e o cartão inteligente já terminou o processamento de ECM E. Saltar ao fim do período assegura uma decifração oportuna desta ECM D até mesmo na velocidade de reprodução acelerada mais alta. Então, o processamento de reprodução acelerada normal pode ser continuado. Certamente, a próxima ECM C também pode ser processada agora corretamente.

Outro cenário pode ser denotado como "troca generalizada para reprodução acelerada inversa'

O método descrito para "inversa e uma CW" também pode ser usado para "inversa e duas CWs". O envio na iniciação da ECM do período atual garante a decifração correta dos dados neste período para ambos os casos. Depois do envio e processamento da segunda ECM, sendo a ECM do período de reprodução normal prévio, o conteúdo dos registradores de decifrador se tornou idêntico para ambas as situações.

Assim, uma troca generalizada de reprodução normal para reprodução acelerada inversa, como descrito na Figura 18, é como segue:

Durante reprodução normal 1501, o extrator de ECM no gerador de reprodução acelerada é reiniciado;

No momento de troca, a ECM do período atual é enviada primeiro; isso é o período no qual a última posição de reprodução normal está localizada;

Depois da latência 1601 do cartão inteligente, o processamento de reprodução acelerada 1502 é começado, o primeiro bloco de reprodução

acelerada sendo lido do fim do período atual;

O gerador de reprodução acelerada assume que o período atual foi entrado há pouco e envia uma ECM por conseguinte (a ECM do período prévio D a um ponto de tempo 1801).

No seguinte, "troca rápida" será descrita.

No caso descrito previamente de troca cega, foi assumido que não há nenhum conhecimento sobre o estado dos registradores de decifrador. Como uma conseqüência, uma ECM de iniciação tem que ser enviada primeiro, e o processamento de reprodução acelerada só pode começar depois que esta ECM foi decifrada pelo cartão inteligente. Isto introduz um atraso adicional igual à latência do cartão inteligente. Porém, este atraso adicional pode ser evitado se os registradores do decifrador já contiverem CWs úteis. Se este é o caso ou não depende da configuração de sistema.

Será assumido para um momento que o gerador de reprodução acelerada 1401 e receptor 1402 estão em uma e a mesma caixa e que eles compartilham o uso do decifrador. Não há nenhuma violação de compartilhamento neste caso porque o receptor 1402 só usa o decifrador em reprodução normal 1501 e o gerador de reprodução acelerada 1401 só em reprodução acelerada 1502.

O estado do decifrador no momento de troca nesta configuração de sistema é de interesse. Está claro que a CW precisada para decifrar o período atual já deveria estar no registrador do decifrador comum porque estava sendo usada para decifrar este período em reprodução normal. Este fato omite a necessidade para enviar uma ECM de iniciação, assim evitando o atraso adicional. Processamento de reprodução acelerada pode começar imediatamente. O decifrador também conterá a ECM do período prévio ou seguinte dependendo da situação de uma/duas CWs por ECM. Isto realmente não importa para a decifração do período atual, que é a primeira etapa de processamento de reprodução acelerada, mas pode influenciar a

continuação do processo de geração de reprodução acelerada. O processamento de reprodução acelerada poderia ser interrompido se a primeira ECM enviada pelo gerador de reprodução acelerada não estiver processada porque tem o mesmo ID de tabela como a última ECM de reprodução normal. Isto pode ser avaliado para cada caso individual. Também deveria ser considerado que tipo de fluxo II começa enviando ECMs para um novo período ao redor de um período de tempo predeterminado antes que seja entrado. Este período de tempo predeterminado pode ser definido pela distância de tempo entre a troca de ID de tabela atual da ECM e a troca de SCB dos pacotes de fluxo de transporte de dados codificados. Esta distância deveria ser maior que a latência máxima do cartão inteligente. Por exemplo, cartões inteligentes atuais têm uma latência de aproximadamente 600 ms.

Um cenário discutido no seguinte pode ser denotado como "dianteiro e tipo de fluxo I".

Ao trocar durante período B, processamento de reprodução acelerada é começado no começo de período B. A última ECM de reprodução normal é ECM B. A primeira ECM enviada pelo gerador de reprodução acelerada também é ECM B. Assim, ela não será processada uma segunda vez, que certamente não é nenhum problema.

O cenário anterior é ilustrado na Figura 19.

Uma porção 1901 de reprodução normal 1501 em período A relaciona-se a ID de Tabela 0x80. A porção 1902 de reprodução normal 1501 em período B relaciona-se a ID de Tabela 0x81. A um ponto de tempo 1900, ECM B (CW B e CW C) é enviada.

Um cenário discutido no seguinte pode ser denotado como "dianteiro e tipo de fluxo II, mas não em um intervalo de tempo predeterminado antes do fim do período atual", por exemplo os últimos 600 ms.

Neste caso, uma troca é executada durante período B, mas não

no intervalo de tempo predeterminado antes do fim do período atual. A última ECM de reprodução normal é ECM B. A primeira ECM enviada pelo gerador de reprodução acelerada é ECM C, que tem um ID de tabela diferente. Assim, ela será processada corretamente.

O cenário anterior é ilustrado na Figura 20.

Uma porção 2000 de reprodução normal 1501 relaciona-se a ID de Tabela 0x80. Uma porção 2001 de reprodução normal 1501 relaciona-se a ID de Tabela 0x81. A um ponto de tempo 2002, ECM C (CW C) é enviada.

Um cenário discutido no seguinte pode ser denotado como "dianteiro e tipo de fluxo II dentro do intervalo de tempo predeterminado antes do fim do período atual".

Aqui, a troca ocorre quando o intervalo de tempo predeterminado antes do fim de período B chegou. A última ECM de reprodução normal é agora ECM C. A primeira ECM enviada pelo gerador de reprodução acelerada também é a ECM C. Assim, ela não será processada uma segunda vez, que certamente não é nenhum problema.

O cenário anterior é ilustrado na Figura 21.

As porções 2100 e 2102 de reprodução normal 1501 relacionam-se a ID de Tabela 0x80. A porção 2101 de reprodução normal 1501 relaciona-se a ID de Tabela 0x81. A ponto de tempo 2103, ECM C (CW C) é enviada.

Um cenário discutido no seguinte pode ser denotado como "inverso e tipo de fluxo I".

Ao trocar durante período B, processamento de reprodução acelerada é começado com um bloco ao fim de período B. A última ECM de reprodução normal é ECM B. A primeira ECM enviada pelo gerador de reprodução acelerada é ECM A, que tem um ID de tabela diferente. Assim, ela será processada corretamente.

O cenário anterior é ilustrado na Figura 22.

A porção 2200 de reprodução normal 1501 em período A relaciona-se a Tabela ID de 0x80. A porção 2201 de reprodução normal 1501 em período B relaciona-se a Tabela ID de 0x81. A ponto de tempo 2202, ECM A (CW A + CW B) é enviada.

Outro cenário discutido no seguinte pode ser denotado como "inverso e tipo de fluxo II, mas não no intervalo de tempo predeterminado antes do fim do período atual".

Neste caso, troca ocorre durante período B, mas não no intervalo de tempo predeterminado antes do fim do período atual. A última ECM de reprodução normal é ECM B. A primeira ECM enviada pelo gerador de reprodução acelerada é ECM A, que tem um ID de tabela diferente. Assim, ela será processada corretamente.

O cenário anterior é ilustrado na Figura 23.

Uma porção 2300 de reprodução normal 1501 em período A relaciona-se a Tabela ID de 0x80. Uma porção 2301 de reprodução normal 1501 em período B relaciona-se a ID de Tabela 0x81. A um ponto de tempo 2302, ECM A (CW A) é enviada.

Outro cenário discutido no seguinte pode ser denotado como "inverso e tipo de fluxo II dentro do intervalo de tempo predeterminado antes do fim do período atual".

Aqui, a troca ocorre na chegada no intervalo de tempo predeterminado antes do fim de período B. Este cenário é ilustrado na Figura 24.

Porções 2400 e 2402 de reprodução normal 1501 relacionam-se a ID de Tabela 0x80. Uma porção 2401 de reprodução normal 1501 relaciona-se a Tabela ID de 0x81. A um ponto de tempo 2403, ECM A (CW A) é enviada.

A última ECM de reprodução normal é agora ECM C. A

primeira ECM enviada pelo gerador de reprodução acelerada é ECM A, que tem o mesmo ID de tabela. Assim, ela não será processada, embora seu conteúdo seja precisado para evitar uma interrupção do fluxo de reprodução acelerada.

Assim, a única situação que pode causar problemas é, ao trocar de reprodução normal 1501 para reprodução acelerada inversa 1502 para tipo de fluxo II, se o momento de troca estiver no intervalo de tempo predeterminado antes do fim de um período. Isto pode ser detectado observando as trocas do ID de tabela e SCB no fluxo de reprodução normal. Esta situação especial pode estar presente ao fim do período depois que a troca do ID de tabela é alcançada, mas antes da troca no SCB que indica o começo do próximo período.

O problema pode ser resolvido facilmente. Reprodução normal 1501 apenas será continuada neste caso até que o próximo período seja alcançado. Isto é descrito na Figura 25. A um ponto de tempo 2500, uma ECM B (CW B) é enviada.

A seqüência correta de ECMs já foi verificada. Ademais, disponibilidade do cartão inteligente tem que ser assegurada. Se estiver ocupado com o processamento de uma ECM, ele não pode receber e começar o processamento de uma nova ECM. Esta ECM poderia então ser perdida e portanto tal situação deveria ser evitada. Verificando todas as situações novamente revela que este problema só ocorre para tipo de fluxo I inverso no começo de um período. Neste caso, reprodução normal é continuada até que o cartão inteligente esteja novamente disponível.

Figura 26 ilustra "troca generalizada rápida" como segue:

Se necessário, reprodução normal 1501 será continuada até que um ponto de troca válido seja alcançado. Então, o processamento de reprodução acelerada é começado imediatamente. Esta reprodução acelerada pode ser iniciada trocando para um modo dianteiro rápido 2600 ou trocando

para um modo inverso rápido 2601. No seguinte, numeral de referência 2600 pode denotar não só um ponto de tempo ao qual troca para um modo dianteiro rápido ocorre, mas também pode ser usado para denotar o modo dianteiro rápido. Por conseguinte, numeral de referência 2601 pode denotar não só um ponto de tempo ao qual troca para um modo inverso rápido ocorre, mas também pode ser usado para denotar o modo inverso rápido.

No caso de trocar para o modo dianteiro rápido 2600, uma ECM B (tipo de fluxo I) ou uma ECM C (tipo de fluxo II) será enviada a um ponto de tempo 2602.

No caso de uma troca para o modo inverso rápido 2601, uma ECM B (CW B) será enviada a um ponto de tempo 2603.

O primeiro bloco de reprodução acelerada é lido do começo (dianteiro) ou fim (inverso) do período atual. O gerador de reprodução acelerada assume que o período atual foi entrado há pouco e envia uma ECM por conseguinte.

Este método de troca rápida pode ser usado não só no caso de um decifrador comum, mas também se o receptor e gerador de reprodução acelerada estiverem em caixas separadas com decifradores individuais. Embora o sistema de reprodução acelerada esteja inativo durante reprodução normal 1501, enviar as ECMs do fluxo de reprodução normal também ao sistema de reprodução acelerada sincroniza seu decifrador, assim habilitando a troca rápida. Para este propósito, um extrator de ECM conectado à entrada de fluxo de transporte e uma chave de ECM é adicionada ao gerador de reprodução acelerada na Figura 14.

No seguinte, vários aspectos relativos à otimização do objetivo de salto quando troca ou salto entre um primeiro modo de reprodução (por exemplo, reprodução normal) e um segundo modo de reprodução (por exemplo, reprodução acelerada) de acordo com uma concretização exemplar da invenção, serão descritos.

Foi indicado que pode ser melhor começar processamento de reprodução acelerada ao começo (dianteiro) ou ao fim (inverso) do período ou segmento atual. Isto garantirá que a ECM enviada neste mesmo instante possa ser processada pelo cartão inteligente a tempo até mesmo na velocidade de reprodução acelerada mais alta dada pelo processamento máximo do cartão inteligente. A velocidades mais baixas porém, o processamento de reprodução acelerada poderia ser começado a uma posição mais perto à última posição de reprodução normal. Assim, uma versão otimizada deste método pode ser não saltar ao começo ou fim do período atual, mas para uma posição neste período que depende da velocidade de reprodução acelerada. Esta posição pode ser então tal que seja garantido que a ECM do período próximo ou prévio seja decifrada antes que este período seja entrado. Se a última posição de reprodução normal estiver dentro da gama permitida, ela pode ser usada como objetivo de salto. Caso contrário, uma posição tão perto dela quanto possível poderia ser escolhida.

Tal situação é descrita na Figura 27A à Figura 27C para três pontos de troca diferentes para reprodução acelerada dianteira.

No seguinte, as três situações de saltar entre um modo de reprodução normal 1501 e uma reprodução acelerada 1502 serão descritas se referindo à Figura 27A à Figura 27C.

Figura 27A mostra uma primeira situação na qual o primeiro segmento 2700 de um fluxo de dados, isto é um período B, e um segundo segmento 2701, isto é um período C, são mostrados. A fronteira entre o primeiro segmento 2700 e o segundo segmento 2701 é denotada com numeral de referência 2704. Em cada uma da Figura 27A à Figura 27C, um ponto de tempo 2702 é mostrado ao qual um usuário opera uma interface de usuário de tal maneira a executar uma troca do modo de reprodução normal 1501 para o modo de reprodução acelerada 1502. Também descrito na Figura 27A à Figura 27C é um atraso de tempo de cartão inteligente 2703, quer dizer um

tempo que um cartão inteligente precisa para recuperar palavras de controle de uma ECM.

No cenário mostrado na Figura 27A, a troca para o modo de reprodução acelerada 1502 ocorre a um ponto de tempo relativamente cedo 2702 dentro de período B, de forma ainda haja bastante tempo deixado para decifrar a ECM, desde que o tempo restante no primeiro período 2700 é maior do que o tempo de atraso de cartão inteligente 2703. Conseqüentemente, o modo de reprodução acelerada 1502 começa imediatamente depois de um comando de troca correspondente de um usuário. Não há nenhuma necessidade para processar uma nova ECM porque a CW precisada para decifrar os dados em seção 2700 já está presente. Além disso, há bastante tempo disponível para processar a próxima ECM para obter a CW precisada na seção 2701. Figura 27B mostra um segundo cenário que é em algum sentido um tipo de cenário fronteiriço. Neste cenário, o ponto de tempo 2702 é selecionado por um usuário de tal maneira que coincida essencialmente com um tempo intervalo 2703 antes da fronteira 2704. Aqui, ainda é possível trocar imediatamente em um modo de reprodução acelerada (de uma maneira "vertical", veja Figura 27B), desde que o tempo restante no primeiro segmento 2700 é apenas suficiente para decifrar a ECM subseqüente para decifrar dados do segundo segmento 2701.

Porém, Figura 27C mostra uma terceira situação, na qual o usuário seleciona uma troca da reprodução normal 1501 para a reprodução acelerada 1502 tão tarde, que o intervalo de tempo restante do primeiro segmento 2700 não é suficiente para decifrar a ECM para o segmento subseqüente 2701 antes de entrar no segmento subseqüente 2701. No cenário como mostrado na Figura 27C, se o sistema trocasse para a reprodução acelerada de uma maneira "vertical" como mostrado na Figura 27A, 27B, haveria problemas na região de fronteira 2704. Portanto, o sistema salta atrás para uma tal porção dentro do primeiro segmento 2700, que o tempo é suficiente para decifrar a ECM do segundo segmento 2701 levando em conta o atraso de cartão inteligente 2703. Em

outras palavras, uma porção do primeiro segmento 2700 que foi previamente reproduzido em modo normal 1501 será reproduzido agora em modo de reprodução acelerada 1502.

Embora o salto não seja necessariamente ao começo ou fim do período atual, ainda tem que ser assumido que este período foi entrado há pouco e enviada uma ECM por conseguinte.

Porém, pode haver um fator complicador com o método descrito. Normalmente, a posição de tempo de pacotes na gravação não é usada, mas a latência do cartão inteligente é um atraso de tempo. Assim, pelo menos uma suposição adequada da temporização dentro de um período criptográfico deveria ser usada.

No seguinte, será investigado como os dados são lidos em reprodução acelerada. O tempo para ler um bloco de dados do dispositivo de armazenamento é freqüentemente desconhecido porque os dados são lidos a uma velocidade mais alta que tempo real. A velocidade atual pode depender do dispositivo de armazenamento e das atividades que executa mais ou menos simultaneamente. O que pode ser conhecido porém no sistema é a distância de tempo entre os começos de ler blocos subseqüentes, porque isto é igual ao tempo de um GOP de reprodução acelerada. Este tempo t depende do tamanho de GOP de reprodução acelerada em quadros T e da taxa de quadro R e é dado por:

$$t = T/R \quad (5)$$

O que pode ser concluído é que o número destas distâncias de tempo n precisadas para compensar a latência de cartão inteligente L deveria obedecer a fórmula seguinte:

$$n*t > L \quad (6)$$

Alguém só pode estar seguro sobre a temporização se n for um número inteiro. Isto resulta em:

$$n = \text{int}\{L/t\}+1 \quad (7)$$

Assumindo T = 3 (IPP) e R = 25 Hz resulta em t = 120 ms.

Assumindo uma latência razoável maior L ao redor de 800 ms resulta em n = 7. Certamente poderia ser tentado monitorar a latência do cartão inteligente e usar isto no cálculo, mas caso contrário uma suposição educada pode ser feita no lado seguro.

A distância entre objetivos de salto subseqüentes pode ser calculada em bytes D_B ou em pacotes D_P como uma função da velocidade de reprodução acelerada. Isto significa que n*t segundos é equivalente a uma distância de bytes de $n*D_B$ ou $n*D_P$ pacotes.

Da Figura 28, para reprodução acelerada dianteira, pode ser visto que a distância mínima do objetivo de salto ao fim do período atual deveria ser $(n-1)*D_P+B$ pacotes, em que B é o bloco tamanho em pacotes. O valor resultante poderia às vezes ser maior que o tamanho de período devido ao arredondamento ao inteiro mais alto mais próximo n e uma latência superestimada L. Neste caso, o objetivo de salto é igual ao começo do período atual. Caso contrário, o objetivo de salto está entre o começo do período atual e o ponto calculado, tão perto quanto possível à última posição de reprodução normal. Uma região de começo permitida 2800 é ilustrada na Figura 28.

Da Figura 29 para reprodução acelerada inversa, pode ser visto que a distância mínima do objetivo de salto ao começo do período atual deveria ser (n-1)*DP pacotes. Novamente, este valor poderia ser maior que o tamanho de período, em qual caso nenhuma otimização é possível. O objetivo de salto é então um bloco antes do fim do período atual. Caso contrário, o objetivo de salto é escolhido entre a posição calculada e uma posição um bloco antes do fim do período atual, tão perto quanto possível à última posição de reprodução normal. Uma região de começo permitida 2900 é ilustrada na Figura 29.

Como um refinamento adicional, é possível aumentar a região de começo permitida escolhendo um valor de D_P menor para o período atual e então trocar ao valor de D_P nominal quando no próximo período é entrado. Valores de D_P menores resultam em velocidades mais baixas de reprodução acelerada.

Assim, é possível começar com uma velocidade mais baixa de reprodução acelerada se necessário e então trocar para a velocidade desejada é possível no cruzamento ao próximo período. Isto pode até resultar em um casamento até mesmo melhor entre a posição de começo de reprodução acelerada e a posição de reprodução normal atual.

No seguinte, vários aspectos adicionais relacionados à troca de reprodução normal para reprodução acelerada e vice-versa, serão explicados.

Várias configurações de sistema são possíveis no caso de fluxos híbridos. Fluxos de dados híbridos podem denotar particularmente fluxos com uma mistura de porções codificadas e não codificadas. A configuração da Figura 14 também é aplicável no caso que o fluxo híbrido é construído no lado de reprodução do dispositivo de armazenamento.

Normalmente, só um fluxo de reprodução acelerada híbrido seria gerado. A geração de um fluxo de reprodução normal híbrido ao lado de reprodução do dispositivo de armazenamento 1403 também seria possível com uma configuração um pouco diferente. Neste caso, o fluxo de transporte 1405 sempre será alimentado pela unidade de construção de fluxo de reprodução acelerada 1407, que então também gera um fluxo de reprodução normal híbrido.

Para a situação com um fluxo híbrido gravado, a configuração é um pouco diferente, como é descrito na Figura 30.

Figura 30 mostra um sistema modificado 3000 em uma configuração para um fluxo híbrido. O sistema 3000 inclui um gerador de reprodução acelerada 3001 e um receptor 1402. O anterior pode ser constituído semelhante como na Figura 14.

Nenhuma decifração é precisada no gerador de reprodução acelerada 3001 neste caso. Inserção de ECM é executada porém para habilitar a decifração do fluxo de reprodução acelerada no receptor 1402. Em qualquer caso, está claro que o decifrador 1413 no receptor 1402 decifrará ambos, isso é o fluxo de reprodução normal e reprodução acelerada. Em uma configuração, há um

decifrador adicional no gerador de reprodução acelerada 3001. Ambos os decifradores podem ser sincronizados automaticamente pelo uso das mesmas ECMs no mesmo momento relativo.

Para trocar de reprodução normal para reprodução acelerada, ações para receptor 1402 e gerador de reprodução acelerada 3001 podem ser invertidas, porque a decifração do fluxo de reprodução acelerada acontece agora no receptor 1402. Além disso, está claro que há um decifrador comum para reprodução acelerada e reprodução normal (no receptor 1402), e possivelmente um decifrador sincronizado adicional para reprodução acelerada no gerador de reprodução acelerada 3001. Esta configuração é idêntica à situação de troca rápida descrita acima. Também a otimização do objetivo de salto é válida aqui. Assim, referência é feita às partes anteriores correspondentes desta descrição. O método de troca para um fluxo híbrido é idêntico ao que é descrito lá.

Se referindo à Figura 31, reprodução normal 1501 será continuada até que um ponto de troca apropriado seja alcançado. Então, o processamento de reprodução acelerada é começado. Esta reprodução acelerada 1502 pode ser um modo dianteiro rápido 2600 ou um modo inverso rápido 2601. No caso de um modo dianteiro rápido 2600, uma ECM B (tipo de fluxo I) ou uma ECM C (tipo de fluxo II) será enviada a um ponto de tempo 3102. No caso de um modo inverso rápido 2601, uma ECM A será enviada a um ponto de tempo 3103. Uma região de começo permitida correspondente é denotada com numeral de referência 3100 e 3101.

A troca de reprodução normal para reprodução acelerada como descrito na Figura 31 pode ser como segue:

Se necessário, continuar reprodução normal 1501 até que um ponto de troca válido seja alcançado;

Então o processamento de reprodução acelerada é começado imediatamente. O primeiro bloco de reprodução acelerada é lido desde o começo (adiante) ou fim (inverso) do período atual ou pelo menos de uma posição de

começo dentro da região de começo permitida;

O gerador de reprodução acelerada assume que o período atual foi entrado há pouco e envia uma ECM por conseguinte.

No seguinte, se referindo à Figura 32, um dispositivo 3200 para processar um fluxo de dados codificado 3201 em um sistema criptográfico de acordo com uma concretização exemplar da invenção será descrito.

Como pode ser tirado da Figura 32, um fluxo de dados codificado 3201 incluindo uma pluralidade de segmentos 3202 é provido a uma entrada de uma unidade decifradora 3203. Cada um dos segmentos 3202 inclui uma unidade de cabeçalho 1002 e uma unidade de carga útil 1005. Palavras de controle 3204 são providas ao decifrador 3203, que permitem decifrar porções codificadas dos segmentos 3202. Assim, na saída do decifrador 3203, um fluxo de dados decifrado é provido.

Ademais, uma interface de usuário 3205 é provida por qual um usuário pode prover o sistema 3200 com comandos de controle para processar seletivamente dados em um modo de reprodução normal ou em um modo de reprodução acelerada. Por estes comandos de controle, uma chave 3206 é controlada entre uma primeira posição de chave (veja Figura 32) e uma segunda posição de chave (não mostrada), que pode ser obtida trocando a chave 3206 ao longo de uma seta 3207.

Quando a chave 3206 está na posição mostrada na Figura 32, os dados decifrados pelo decifrador 3203 são providos diretamente a uma unidade de reprodução 3208 (por exemplo, um monitor para exibir informação visual e/ou um alto-falante para reproduzir informação audível).

Porém, quando o usuário opera a interface de usuário 3205 (por exemplo, um botão) de uma maneira para fixar a segunda posição de chave não mostrada na Figura 32, um modo de reprodução acelerada será iniciado, como será explicado no seguinte.

Uma primeira unidade de determinação 3209 é provida no

caminho de sinal de modo de reprodução acelerada para determinar, no caso de trocar do modo de reprodução normal para o modo de reprodução de reprodução acelerada, uma posição atual de reprodução dentro do fluxo de dados. Ademais, uma segunda unidade de determinação 3210 (que pode ser controlada opcionalmente por um usuário pela interface de usuário 3205) é provida para determinar uma posição de começo para começar reprodução em um segundo modo de reprodução baseado na posição atual determinada provida pela primeira unidade de determinação 3209. Para determinar uma posição de começo, a segunda unidade de determinação 3210 leva em conta características do sistema criptográfico. Particularmente, a posição de começo é determinada baseado em um atraso com o qual as palavras de controle 3204 para decifrar segmentos diferentes 3202 do fluxo de dados codificado 3201 são providas no sistema criptográfico.

Além disso, uma unidade de geração de reprodução acelerada 3211 é provida para reprodução no modo de reprodução acelerada da posição de começo em diante.

De acordo com a Figura 32, a chave 3206 é provida ao término da cadeia, quer dizer depois das unidades 3209 a 3211, de forma que as unidades de determinação 3209, 3210 possam executar suas tarefas de determinação continuamente a fim de trocar tão rápido quanto possível sem interromper o fluxo de saída à unidade de reprodução 3208.

Deveria ser notado que o termo "incluindo" não exclui outros elementos ou etapas e o "um" ou "uma" não excluem uma pluralidade. Também elementos descritos em associação com concretizações diferentes podem ser combinados.

Também deveria ser notado que sinais de referência nas reivindicações não deverão ser interpretados como limitando a extensão das reivindicações.

REIVINDICAÇÕES

1. Dispositivo (3200) para processar um fluxo de dados codificado (3201) em um sistema criptográfico, no qual dados de decifração (3204) são providos para decifrar cada segmento (3202) do fluxo de dados codificado (3201) para reprodução do fluxo de dados decifrado,

o dispositivo (3200) caracterizado pelo fato de que inclui:

uma primeira unidade de determinação (3209) para determinar, no caso de troca de um primeiro modo de reprodução (1501) de reproduzir o fluxo de dados (3201) para um segundo modo de reprodução (1502) de reproduzir o fluxo de dados (3201), uma posição atual de reprodução dentro do fluxo de dados (3201);

uma segunda unidade de determinação (3210) para determinar uma posição de começo para começar reprodução no segundo modo de reprodução (1502) baseado na posição atual determinada.

2. Dispositivo (3200) de acordo com reivindicação 1, caracterizado pelo fato de que a segunda unidade de determinação (3210) é adaptada para determinar uma posição de começo para começar reprodução no segundo modo de reprodução (1502) baseado em características do sistema criptográfico.

3. Dispositivo (3200) de acordo com reivindicação 1, caracterizado pelo fato de que a segunda unidade de determinação (3210) é adaptada para determinar uma posição de começo para começar reprodução no segundo modo de reprodução (1502) baseado em um atraso (2703) com o qual dados de decifração (3204) são providos no sistema criptográfico.

4. Dispositivo (3200) de acordo com reivindicação 1, caracterizado pelo fato de que a segunda unidade de determinação (3210) é adaptada para determinar uma posição de começo para começar reprodução no segundo modo de reprodução (1502) baseado em um atraso (2703) com o qual dados de decifração (3204) para decifrar um segmento sucessivo são

providos no sistema criptográfico.

5. Dispositivo (3200) de acordo com reivindicação 1, caracterizado pelo fato de que a segunda unidade de determinação (3210) é adaptada para determinar um começo ou um fim de um segmento precedendo ou sucedendo o segmento atualmente reproduzido como uma posição de começo para começar reprodução no segundo modo de reprodução (1502).

6. Dispositivo (3200) de acordo com reivindicação 1, caracterizado pelo fato de que a segunda unidade de determinação (3210) é adaptada para determinar a posição de começo baseado em uma velocidade de reprodução do fluxo de dados (3201) de acordo com o segundo modo de reprodução (1502).

7. Dispositivo (3200) de acordo com reivindicação 1, caracterizado pelo fato de que a segunda unidade de determinação (3210) é adaptada para determinar a posição de começo de tal maneira que um segmento do fluxo de dados codificado (3201) que é para ser reproduzido logo depois que um segmento reproduzido atualmente do fluxo de dados é decifrável por meio dos dados de decifração correspondentes (3204) decifrados a um momento antes da reprodução do segmento reproduzido atualmente do fluxo de dados (3201) seja terminado.

8. Dispositivo (3200) de acordo com reivindicação 1, caracterizado pelo fato de que é adaptado para processar um fluxo de dados codificado (3201) de dados de vídeo ou dados de áudio.

9. Dispositivo (3200) de acordo com reivindicação 1, caracterizado pelo fato de que é adaptado para processar um fluxo de dados codificado (3201) de dados digitais.

10. Dispositivo (3200) de acordo com reivindicação 1, caracterizado pelo fato de que o primeiro modo de reprodução é um modo de reprodução normal (1501).

11. Dispositivo (3200) de acordo com reivindicação 1,

caracterizado pelo fato de que o segundo modo de reprodução é um modo de reprodução acelerada (1502).

12. Dispositivo (3200) de acordo com reivindicação 11, caracterizado pelo fato de que o modo de reprodução acelerada (1502) é um do grupo consistindo em um modo de reprodução dianteira rápida (2600), um modo de reprodução inversa rápida (2601), um modo de reprodução de movimento lento, um modo de reprodução de quadro congelado, um modo de reprodução de repetição, e um modo de reprodução inversa.

13. Dispositivo (3200) de acordo com reivindicação 1, caracterizado pelo fato de que compreende uma unidade de geração (3211) adaptada para gerar um fluxo de dados decifrado ou um fluxo de dados codificado para reprodução no segundo modo de reprodução (1502) da posição de começo em diante.

14. Dispositivo (3200) de acordo com reivindicação 1, caracterizado pelo fato de que é adaptado para processar um fluxo de dados de MPEG2 codificado.

15. Dispositivo (3200) de acordo com reivindicação 1, caracterizado pelo fato de que é realizado como pelo menos um do grupo consistindo em um dispositivo de gravação de vídeo digital e um dispositivo habilitado por rede e um sistema de acesso condicional e reprodutor de áudio portátil e reprodutor de vídeo portátil e um telefone móvel e reprodutor de DVD e um reprodutor de CD, um reprodutor de mídia baseada em disco rígido e um dispositivo de rádio de Internet e um dispositivo de entretenimento público e um reprodutor de MP3.

16. Método para processar um fluxo de dados codificado (3201) em um sistema criptográfico, no qual dados de decifração (3204) são providos para decifrar cada segmento (3202) do fluxo de dados codificado (3201) para reprodução do fluxo de dados decifrado, o método caracterizado pelo fato de que compreende as etapas de:

determinar, no caso de trocar de um primeiro modo de reprodução (1501) de reproduzir o fluxo de dados (3201) para um segundo modo de reprodução (1502) de reproduzir o fluxo de dados (3201), uma posição atual de reprodução dentro do fluxo de dados (3201);

determinar uma posição de começo para começar reprodução no segundo modo de reprodução (1502) baseado na posição atual determinada.

17. Meio legível por computador, caracterizado pelo fato de que um programa de computação de processar um fluxo de dados codificado (3201) em um sistema criptográfico, no qual dados de decifração (3204) são providos para decifrar cada segmento (3202) do fluxo de dados codificado (3201) para reprodução do fluxo de dados decifrado (3201), é armazenado, qual programa de computação, ao ser executado por um processador, é adaptado para controlar ou efetuar as etapas de método seguintes:

determinar, no caso de trocar de um primeiro modo de reprodução (1501) de reproduzir o fluxo de dados (3201) para um segundo modo de reprodução (1502) de reproduzir o fluxo de dados, uma posição atual de reprodução dentro do fluxo de dados (3201);

determinar uma posição de começo para começar reprodução no segundo modo de reprodução (1502) baseado na posição atual determinada.

18. Elemento de programa de processar um fluxo de dados codificado (3201) em um sistema criptográfico, caracterizado pelo fato de que dados de decifração (3204) são providos para decifrar cada segmento (3202) do fluxo de dados codificado (3201) para reprodução do fluxo de dados decifrado, qual elemento de programa, ao ser executado por um processador, é adaptado para controlar ou efetuar as etapas de método de:

determinar, no caso de trocar de um primeiro modo de reprodução (1501) de reproduzir o fluxo de dados (3201) para um segundo

modo de reprodução (1502) de reproduzir o fluxo de dados (3201), uma posição atual de reprodução dentro do fluxo de dados (3201);

determinar uma posição de começo para começar reprodução no segundo modo de reprodução (1502) baseado na posição atual determinada.

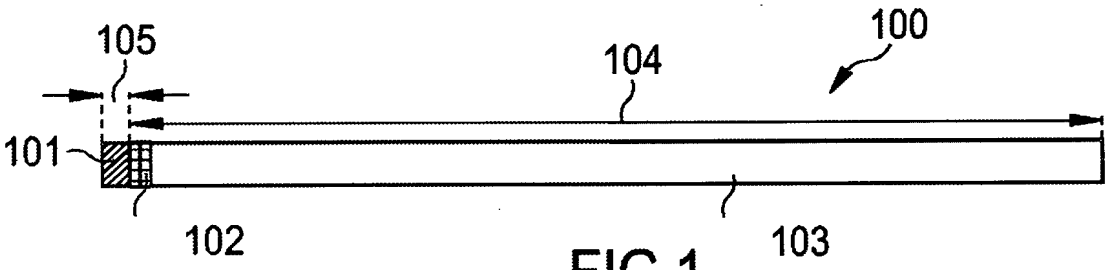


FIG 1

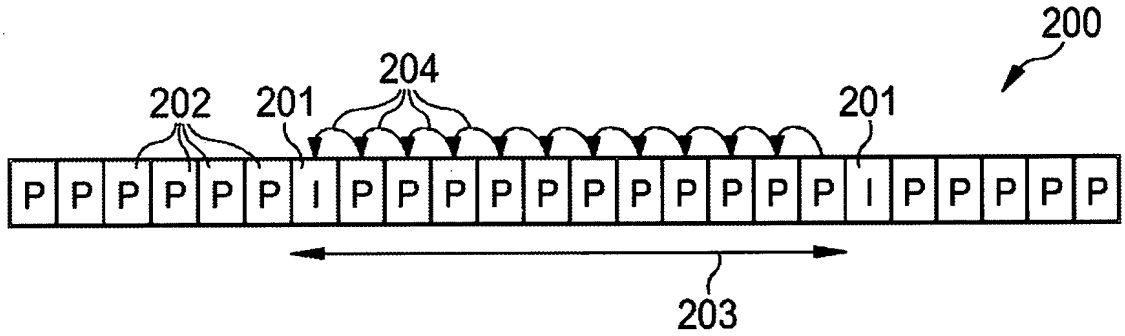


FIG 2

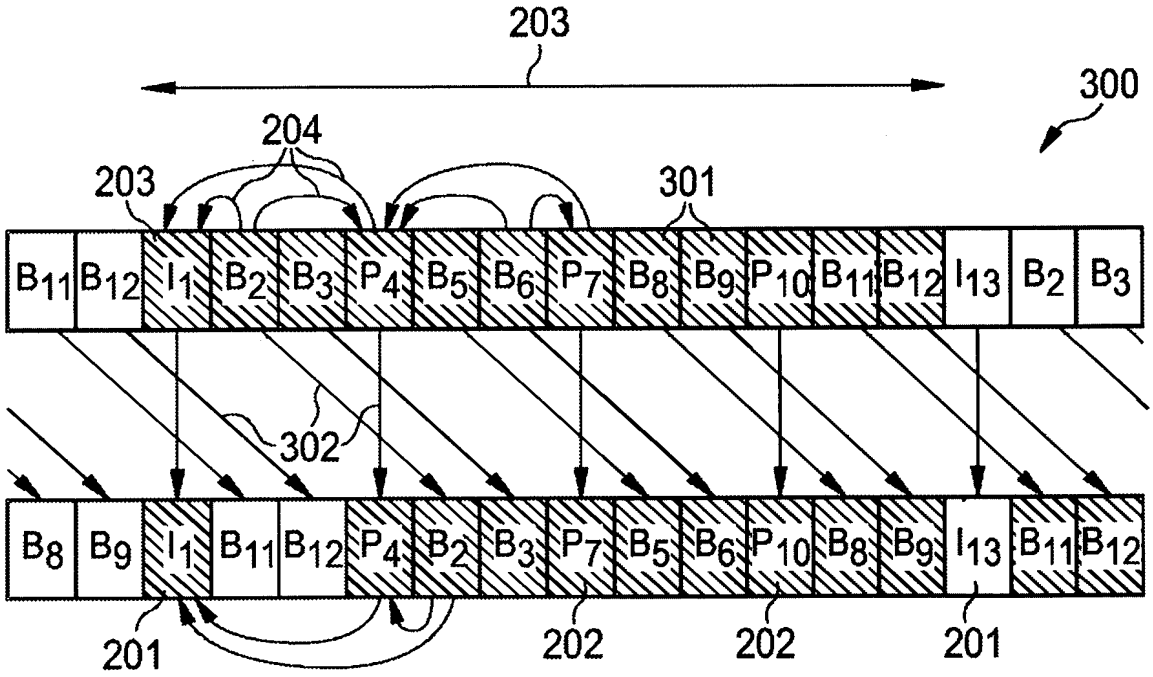


FIG 3

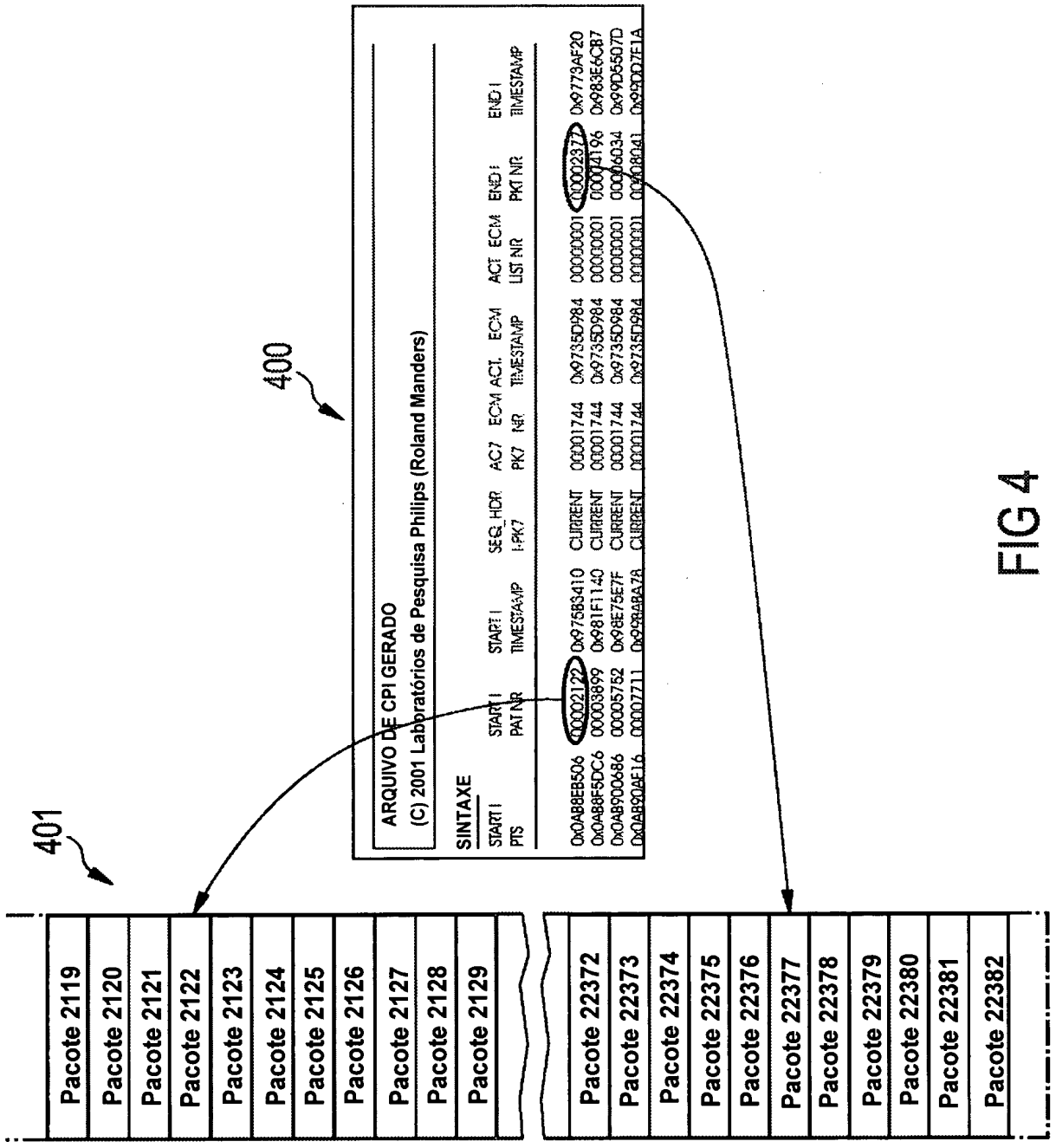

401
400
Pacote 2119
Pacote 2120
Pacote 2121
Pacote 2122
Pacote 2123
Pacote 2124
Pacote 2125
Pacote 2126
Pacote 2127
Pacote 2128
Pacote 2129
Pacote 22372
Pacote 22373
Pacote 22374
Pacote 22375
Pacote 22376
Pacote 22377
Pacote 22378
Pacote 22379
Pacote 22380
Pacote 22381
Pacote 22382
ARQUIVO DE CPI GERADO
(C) 2001 Labpratórios de Pesquisa Philips (Roland Manders)
SINTAXE
START I
PTS
START I
PAT NR
START I
TIMESTAMP
SEQ_HDR
I-PK7
AC7
PK7
ECM
NR
ACT. ECM
TIMESTAMP
ACT. ECM
LIST NR
END I
PKT NR
END I
TIMESTAMP
0x0AB8EB5D6 00002122 0x97563410 CURRENT 00001744 0x9735D984 00000001 00002377 0x9779AF20
0x0AB8F5DC6 00003899 0x981F1140 CURRENT 00001744 0x9735D984 00000001 00004196 0x983E4CB7
0x0AB900686 00005752 0x98E75E7F CURRENT 00001744 0x9735D984 00000001 00006034 0x99D5507D
0x0AB90AE16 00007711 0x99848A7A CURRENT 00001744 0x9735D984 00000001 00008041 0x99D7EF1A

FIG 4

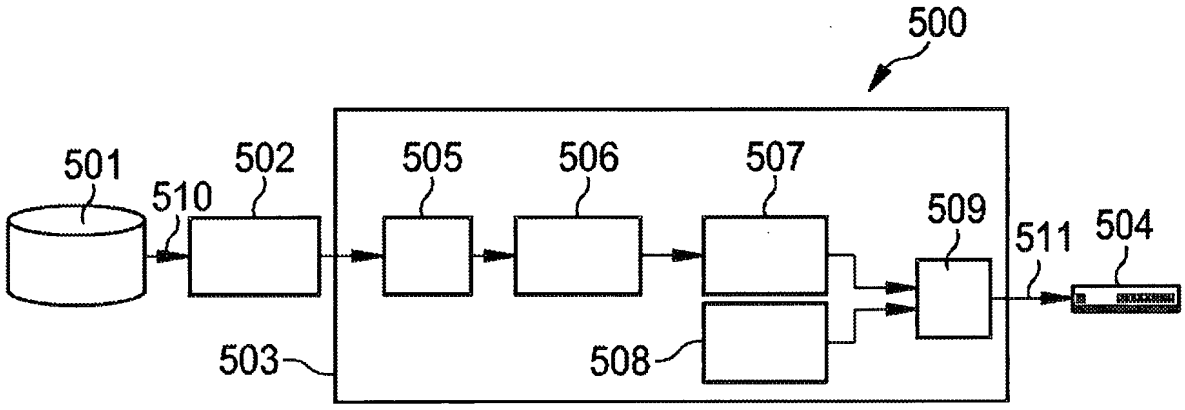

500
501
502
505
506
507
509
511
504
510
503
508

FIG 5

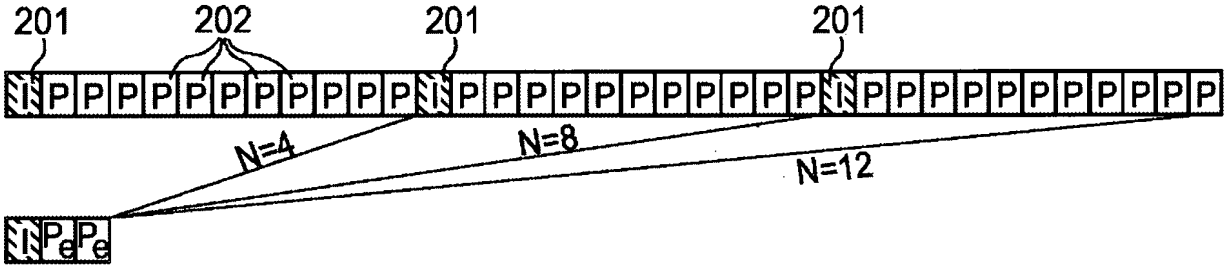

201
202
201
201
N=4
N=8
N=12

FIG 6

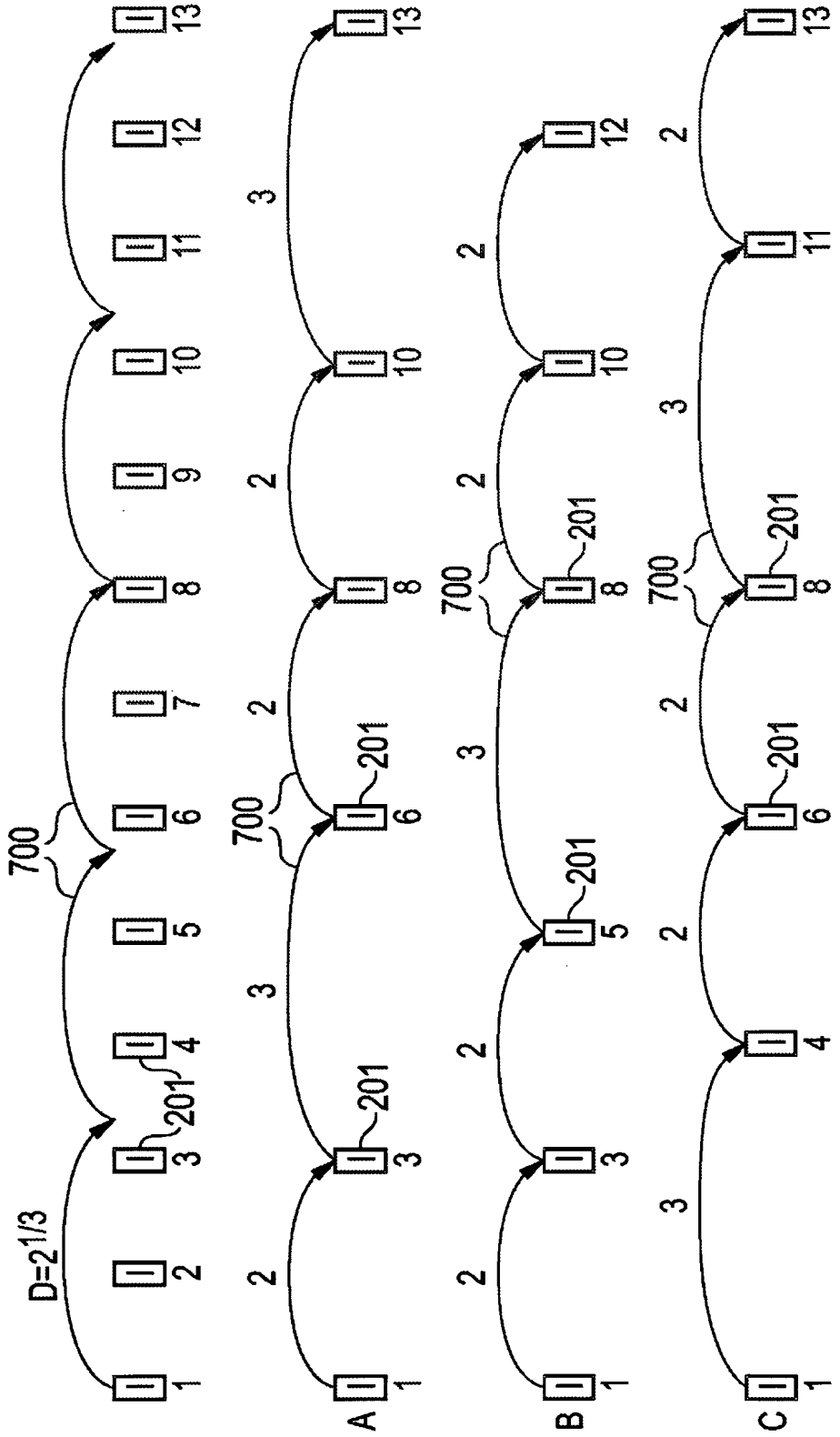


FIG 7

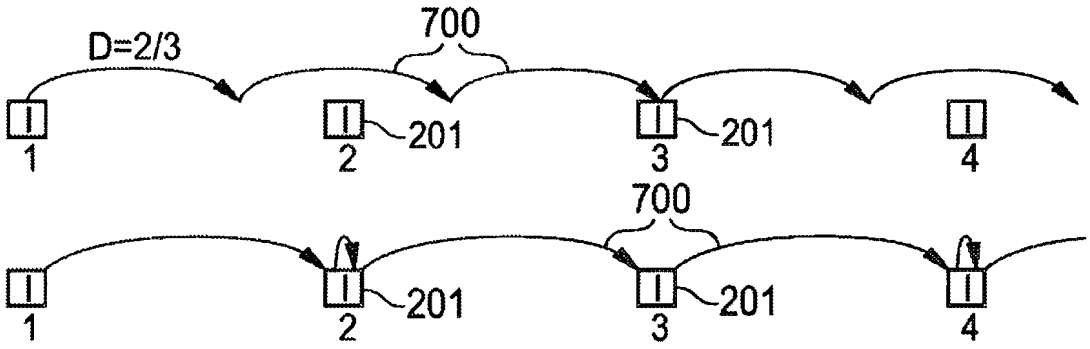

D=2/3
700
1
2
201
3
201
4
700
1
2
201
3
201
4

FIG 8

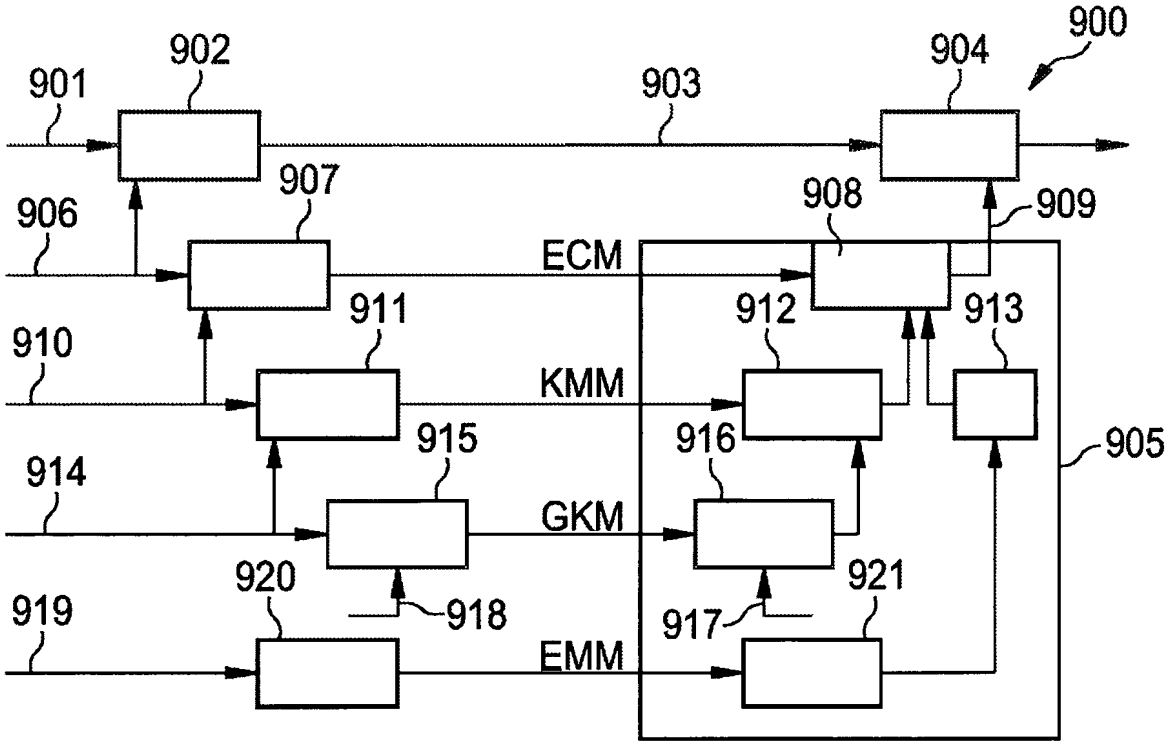

900
901
902
903
904
906
907
908
909
ECM
910
911
912
913
KMM
914
915
916
905
GKM
919
920
918
917
921
EMM

FIG 9

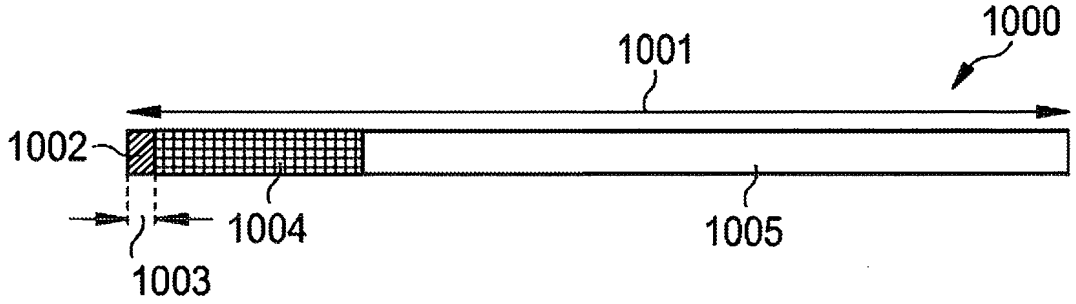


FIG 10

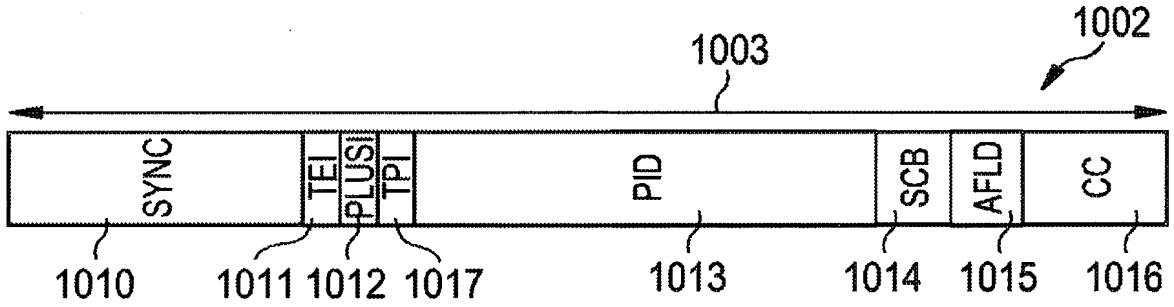


FIG 11

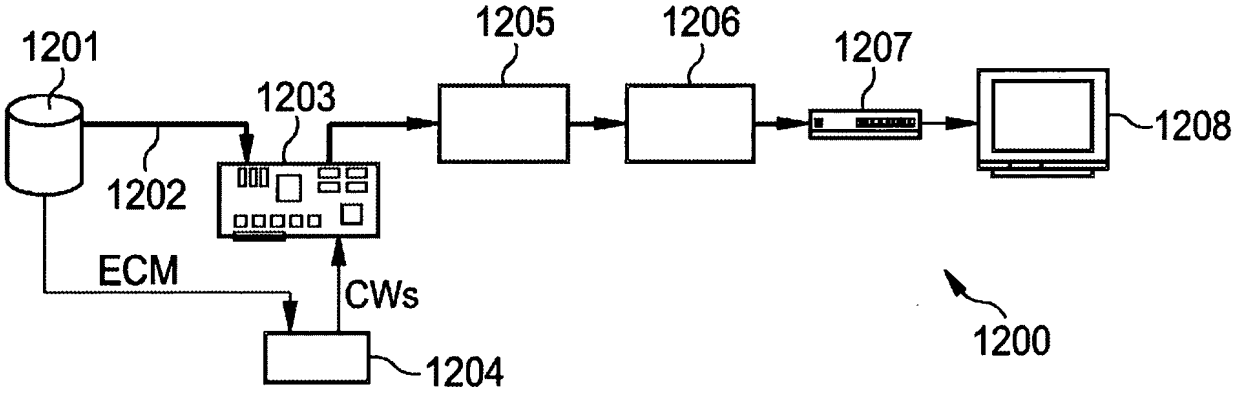


FIG 12

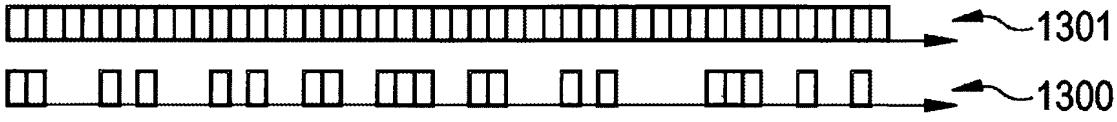


FIG 13

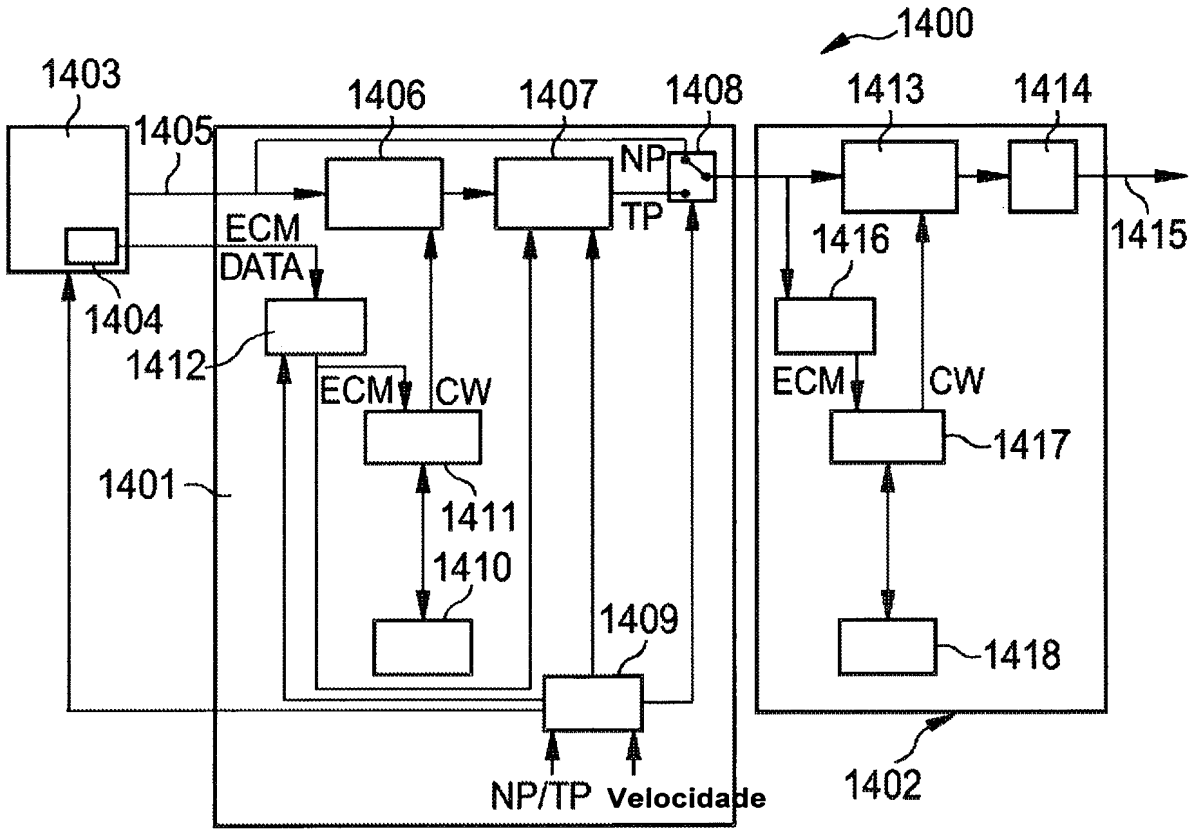


FIG 14

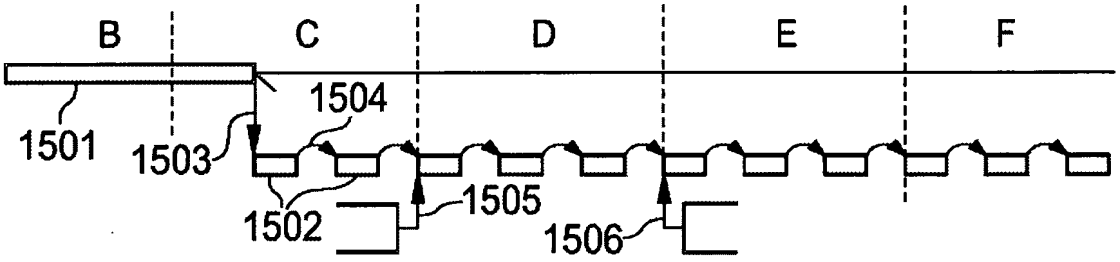


FIG 15

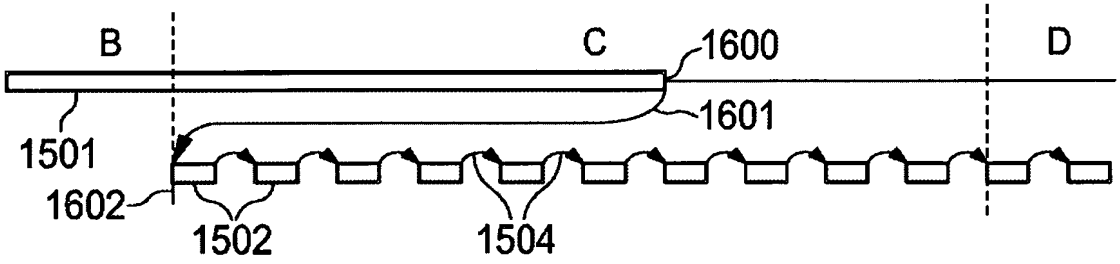


FIG 16

ECM	CW	
	S. I	S. II
A	A&B	A
B	B&C	B
C	C&D	C
E	E&F	E

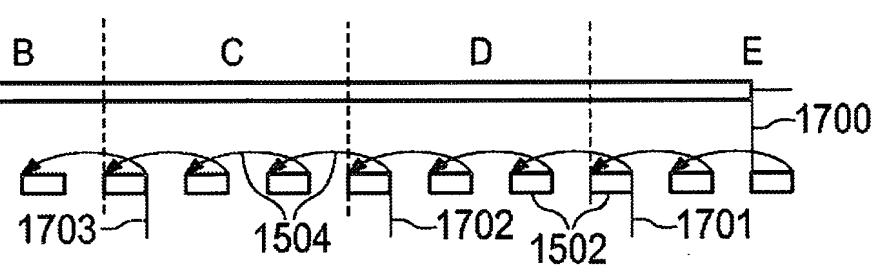


FIG 17

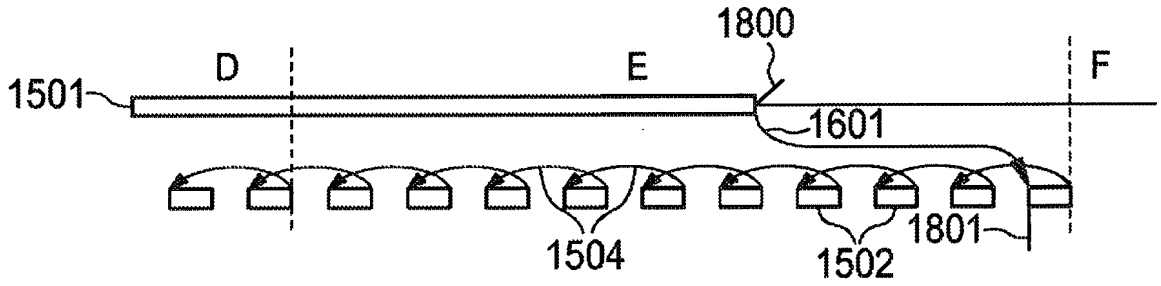


FIG 18

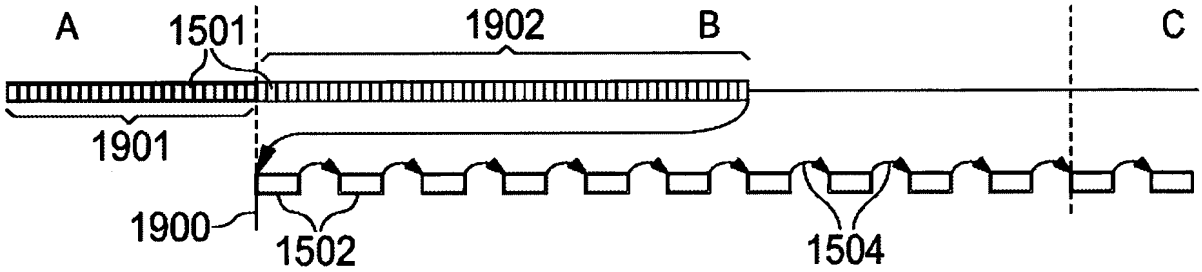


FIG 19

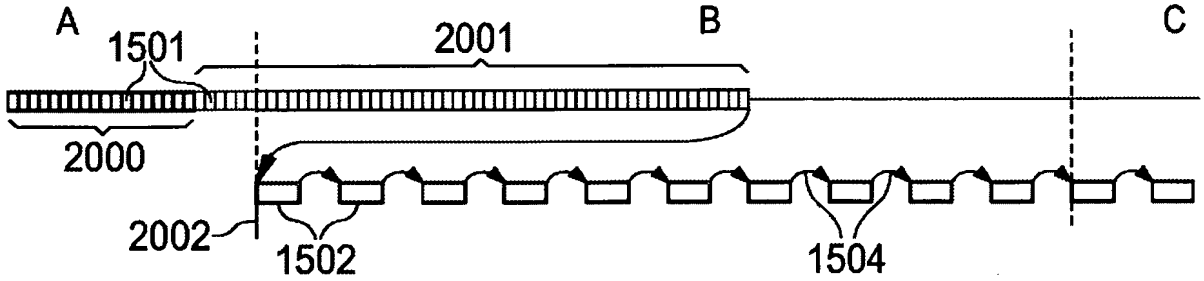


FIG 20

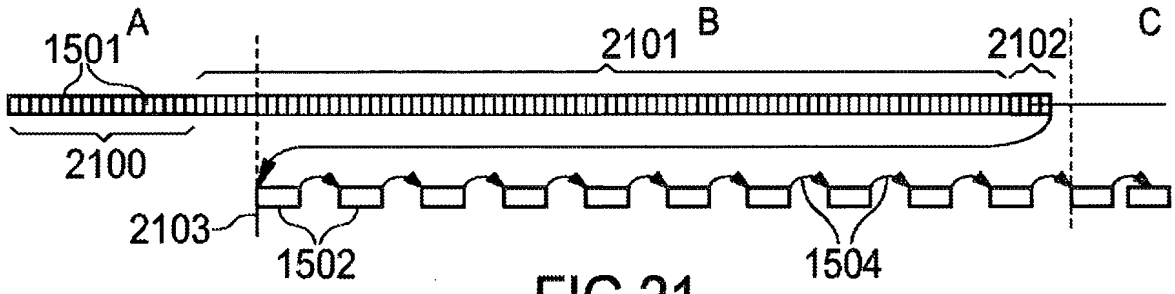


FIG 21

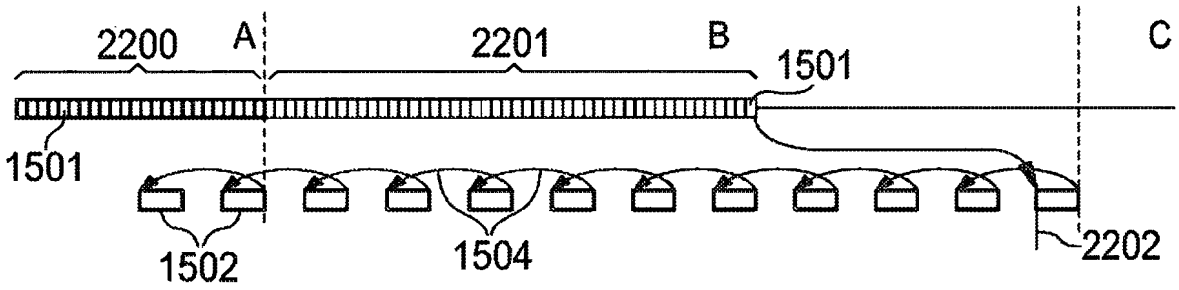


FIG 22

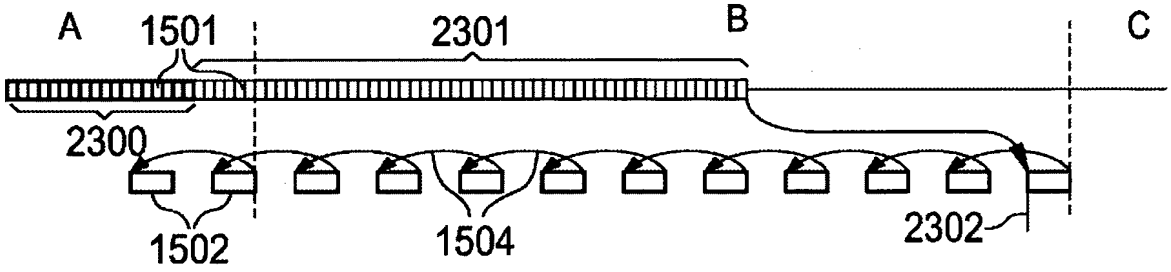


FIG 23

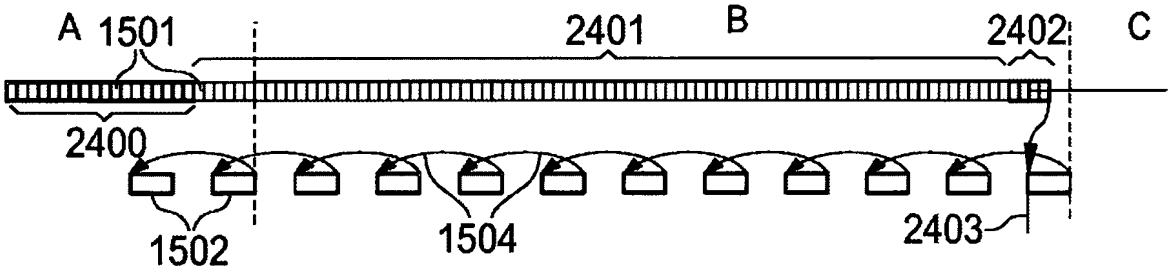


FIG 24

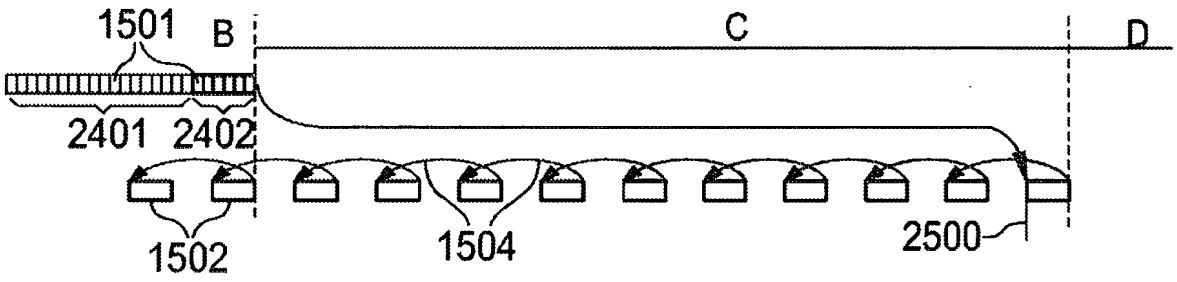


FIG 25

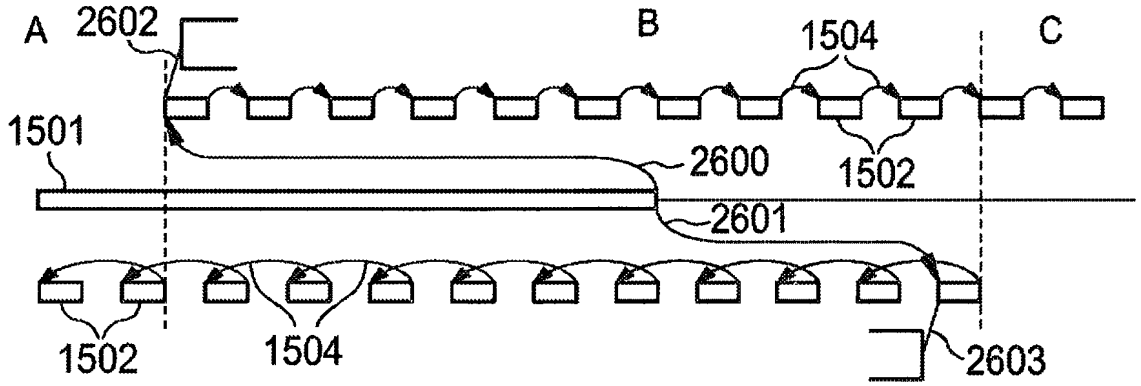


FIG 26

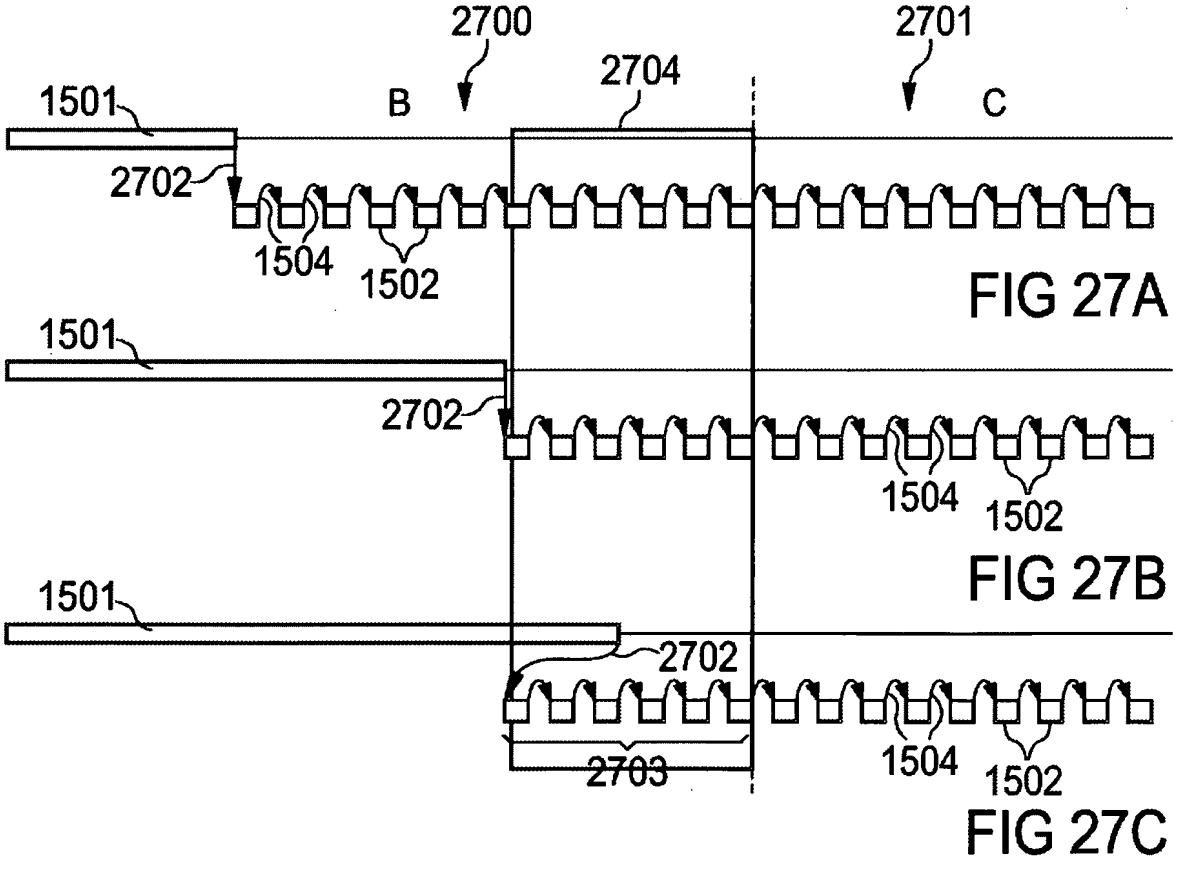


FIG 27A

FIG 27B

FIG 27C

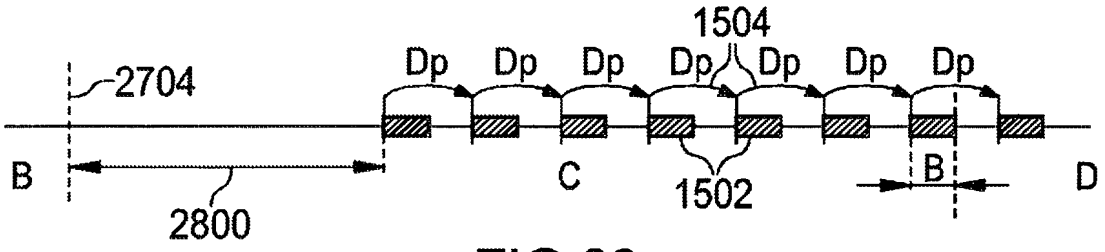


FIG 28

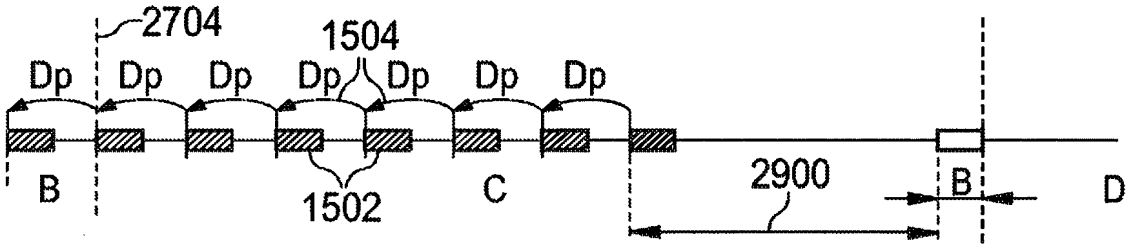


FIG 29

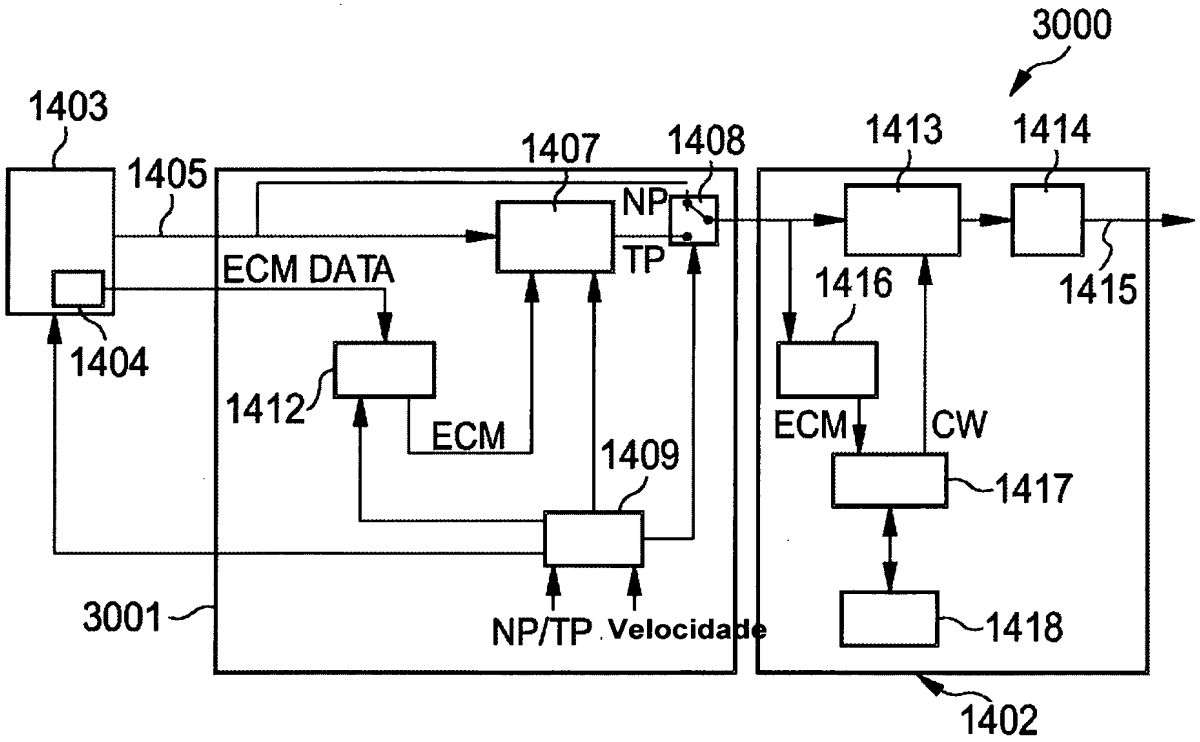


FIG 30

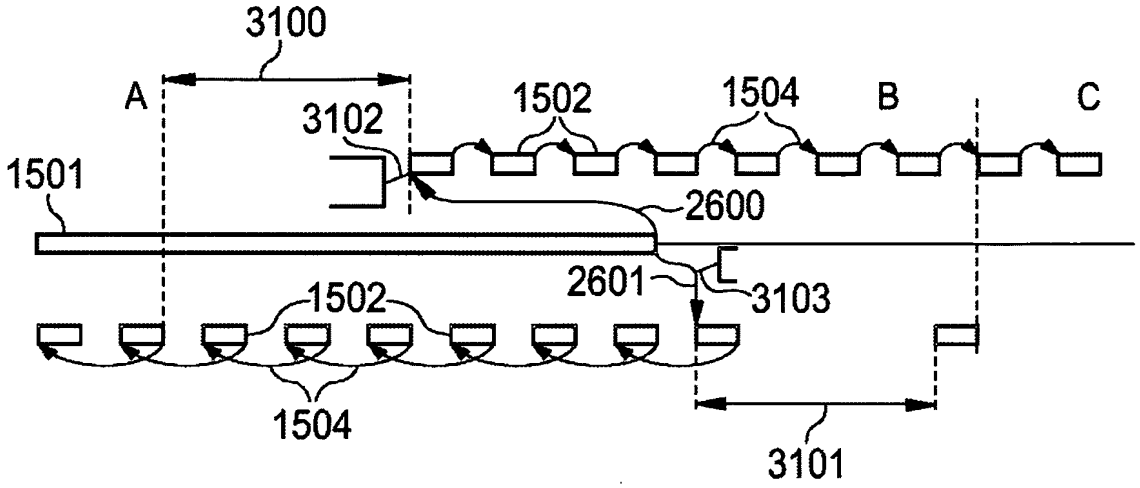

3100
A
3102
1502
1504
B
C
1501
2600
2601
3103
1502
1504
3101

FIG 31

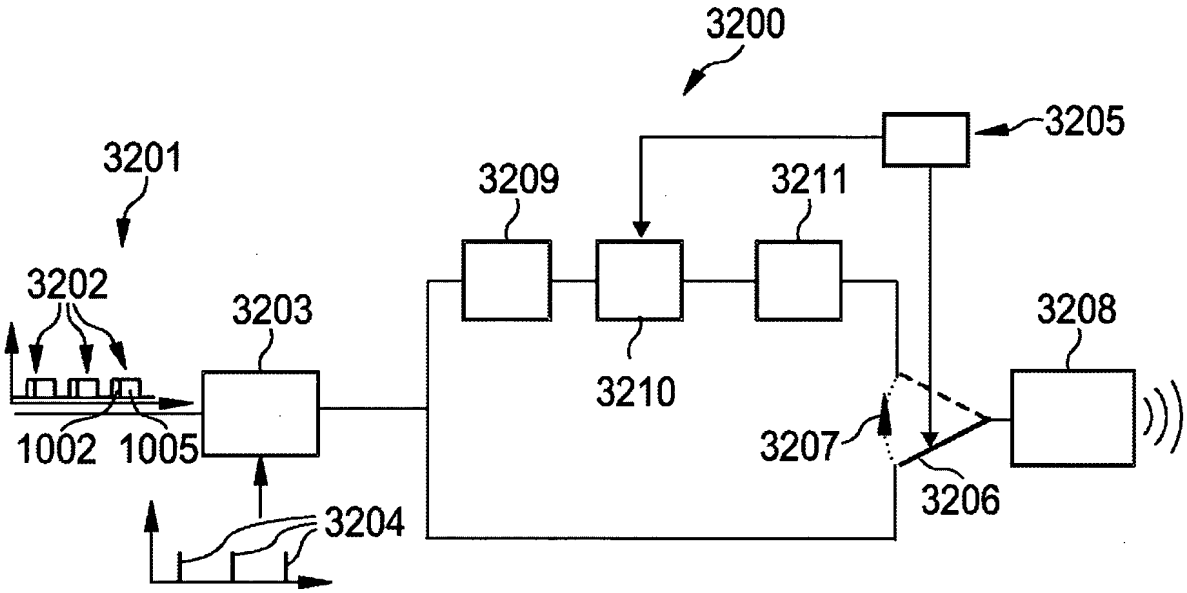

3200
3205
3201
3209
3211
3202
3203
3208
3210
3207
1002
1005
3206
3204

FIG 32

PI0609562-3

RESUMO

"DISPOSITIVO E MÉTODO PARA PROCESSAR UM FLUXO DE DADOS CODIFICADO EM UM SISTEMA CRIPTOGRÁFICO, MEIO LEGÍVEL POR COMPUTADOR E ELEMENTO DE PROGRAMA"

Um dispositivo (3200) para processar um fluxo de dados codificado (3201) em um sistema criptográfico, no qual dados de decifração (3204) são providos para decifrar cada segmento (3202) do fluxo de dados codificado (3201) para reprodução do fluxo de dados decifrado, em que o dispositivo (3200) inclui uma primeira unidade de determinação (3209) para determinar, no caso de trocar de um primeiro modo de reprodução (1501) de reproduzir o fluxo de dados (3201) para um segundo modo de reprodução (1502) de reproduzir o fluxo de dados (3201), uma posição atual de reprodução dentro do fluxo de dados, e uma segunda unidade de determinação (3210) para determinar uma posição de começo para começar reprodução no segundo modo de reprodução (1502) baseado na posição atual determinada.

A requerente apresenta novas vias das reivindicações para melhor esclarecer e definir o invento descrito no presente pedido.

REIVINDICAÇÕES

1. Dispositivo (3200) para processar um fluxo de dados codificado (3201) em um sistema criptográfico, no qual dados de decifração (3204) são providos para decifrar cada segmento (3202) do fluxo de dados codificado (3201) para reprodução do fluxo de dados decifrado,

o dispositivo (3200) caracterizado pelo fato de que inclui:

uma primeira unidade de determinação (3209) para determinar, no caso de troca de um primeiro modo de reprodução (1501) de reproduzir o fluxo de dados (3201) para um segundo modo de reprodução (1502) de reproduzir o fluxo de dados (3201), uma posição atual de reprodução dentro do fluxo de dados (3201);

uma segunda unidade de determinação (3210) para determinar uma posição de começo para começar reprodução no segundo modo de reprodução (1502) baseado na posição atual determinada e em que a segunda unidade de determinação (3210) é adaptada para determinar uma posição de começo para começar reprodução no segundo modo de reprodução (1502) baseado em um atraso (2703) com o qual dados de decifração (3204) são providos no sistema criptográfico.

2. Dispositivo (3200) de acordo com reivindicação 1, caracterizado pelo fato de que a segunda unidade de determinação (3210) é adaptada para determinar uma posição de começo para começar reprodução no segundo modo de reprodução (1502) baseado em características do sistema criptográfico.

3. Dispositivo (3200) de acordo com reivindicação 1, caracterizado pelo fato de que a segunda unidade de determinação (3210) é adaptada para determinar uma posição de começo para começar reprodução no segundo modo de reprodução (1502) baseado em um atraso (2703) com o qual dados de decifração (3204) para decifrar um segmento sucessivo são providos no sistema criptográfico.

4. Dispositivo (3200) de acordo com reivindicação 1, caracterizado pelo fato de que a segunda unidade de determinação (3210) é adaptada para determinar um começo ou um fim de um segmento precedendo ou sucedendo o segmento atualmente reproduzido como uma posição de começo para começar reprodução no segundo modo de reprodução (1502).

5. Dispositivo (3200) de acordo com reivindicação 1, caracterizado pelo fato de que a segunda unidade de determinação (3210) é adaptada para determinar a posição de começo baseado em uma velocidade de reprodução do fluxo de dados (3201) de acordo com o segundo modo de reprodução (1502).

6. Dispositivo (3200) de acordo com reivindicação 1, caracterizado pelo fato de que a segunda unidade de determinação (3210) é adaptada para determinar a posição de começo de tal maneira que um segmento do fluxo de dados codificado (3201) que é para ser reproduzido logo depois que um segmento reproduzido atualmente do fluxo de dados é decifrável por meio dos dados de decifração correspondentes (3204) decifrados a um momento antes da reprodução do segmento reproduzido atualmente do fluxo de dados (3201) seja terminado.

7. Dispositivo (3200) de acordo com reivindicação 1, caracterizado pelo fato de que é adaptado para processar um fluxo de dados codificado (3201) de dados de vídeo ou dados de áudio.

8. Dispositivo (3200) de acordo com reivindicação 1, caracterizado pelo fato de que é adaptado para processar um fluxo de dados codificado (3201) de dados digitais.

9. Dispositivo (3200) de acordo com reivindicação 1, caracterizado pelo fato de que o primeiro modo de reprodução é um modo de reprodução normal (1501).

10. Dispositivo (3200) de acordo com reivindicação 1, caracterizado pelo fato de que o segundo modo de reprodução é um modo de

reprodução acelerada (1502).

11. Dispositivo (3200) de acordo com reivindicação 10, caracterizado pelo fato de que o modo de reprodução acelerada (1502) é um do grupo consistindo em um modo de reprodução dianteira rápida (2600), um modo de reprodução inversa rápida (2601), um modo de reprodução de movimento lento, um modo de reprodução de quadro congelado, um modo de reprodução de repetição, e um modo de reprodução inversa.

12. Dispositivo (3200) de acordo com reivindicação 1, caracterizado pelo fato de que compreende uma unidade de geração (3211) adaptada para gerar um fluxo de dados decifrado ou um fluxo de dados codificado para reprodução no segundo modo de reprodução (1502) da posição de começo em diante.

13. Dispositivo (3200) de acordo com reivindicação 1, caracterizado pelo fato de que é adaptado para processar um fluxo de dados de MPEG2 codificado.

14. Dispositivo (3200) de acordo com reivindicação 1, caracterizado pelo fato de que é realizado como pelo menos um do grupo consistindo em um dispositivo de gravação de vídeo digital e um dispositivo habilitado por rede e um sistema de acesso condicional e reprodutor de áudio portátil e reprodutor de vídeo portátil e um telefone móvel e reprodutor de DVD e um reprodutor de CD, um reprodutor de mídia baseada em disco rígido e um dispositivo de rádio de Internet e um dispositivo de entretenimento público e um reprodutor de MP3.

15. Método para processar um fluxo de dados codificado (3201) em um sistema criptográfico, no qual dados de decifração (3204) são providos para decifrar cada segmento (3202) do fluxo de dados codificado (3201) para reprodução do fluxo de dados decifrado, o método caracterizado pelo fato de que compreende as etapas de:

determinar, no caso de trocar de um primeiro modo de

reprodução (1501) de reproduzir o fluxo de dados (3201) para um segundo modo de reprodução (1502) de reproduzir o fluxo de dados (3201), uma posição atual de reprodução dentro do fluxo de dados (3201);

determinar uma posição de começo para começar reprodução no segundo modo de reprodução (1502) baseado na posição atual determinada e um retardo (2703) com o qual dados de descriptpgrafação (3204) são fornecidos no sistema criptográfico.

16. Meio legível por computador, caracterizado pelo fato de que um programa de computação de processar um fluxo de dados codificado (3201) em um sistema criptográfico, no qual dados de decifração (3204) são providos para decifrar cada segmento (3202) do fluxo de dados codificado (3201) para reprodução do fluxo de dados decifrado (3201), é armazenado, qual programa de computação, ao ser executado por um processador, é adaptado para controlar ou efetuar as etapas de método seguintes:

determinar, no caso de trocar de um primeiro modo de reprodução (1501) de reproduzir o fluxo de dados (3201) para um segundo modo de reprodução (1502) de reproduzir o fluxo de dados, uma posição atual de reprodução dentro do fluxo de dados (3201);

determinar uma posição de começo para começar reprodução no segundo modo de reprodução (1502) baseado na posição atual determinada e um retardo (2703) com o qual dados de descriptpgrafação (3204) são fornecidos no sistema criptográfico.

17. Elemento de programa de processar um fluxo de dados codificado (3201) em um sistema criptográfico, caracterizado pelo fato de que dados de decifração (3204) são providos para decifrar cada segmento (3202) do fluxo de dados codificado (3201) para reprodução do fluxo de dados decifrado, qual elemento de programa, ao ser executado por um processador, é adaptado para controlar ou efetuar as etapas de método de:

determinar, no caso de trocar de um primeiro modo de

reprodução (1501) de reproduzir o fluxo de dados (3201) para um segundo modo de reprodução (1502) de reproduzir o fluxo de dados (3201), uma posição atual de reprodução dentro do fluxo de dados (3201);

determinar uma posição de começo para começar reprodução no segundo modo de reprodução (1502) baseado na posição atual determinada e um retardo (2703) com o qual dados de descriptpgrafação (3204_ são fornecidos no sistema criptográfico.