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

(21) **PI0613730-0 A2**

BRPI0613730A2

(22) Data de Depósito: 12/07/2006
(43) Data da Publicação: 01/02/2011
(RPI 2091)

(51) Int.Cl.:
H04N 7/24
H04N 7/16

(54) Título: **MÉTODO E APARELHO PARA CRIPTOGRAFAR/DECRIPTOGRAFAR CONTEÚDO DE MULTIMÍDIA PARA PERMITIR O ACESSO ALEATÓRIO**

(30) Prioridade Unionista: 14/07/2005 US 11/182,088

(73) Titular(es): QUALCOMM INCORPORATED

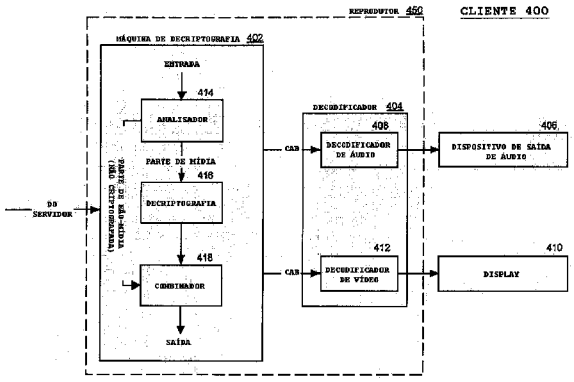
(72) Inventor(es): CHRISTOPHER WINGERT, POOJA AGGARWAL

(74) Procurador(es): Montaury Pimenta, Machado & Lioce S/C Ltda

(86) Pedido Internacional: PCT US2006027461 de 12/07/2006

(87) Publicação Internacional: WO 2007/011766de 25/01/2007

(57) Resumo: MÉTODO E APARELHO PARA CRIPTOGRAFAR/DECRIPTOGRAFAR CONTEUDO DE MULTIMÍDIA PARA PERMITIR ACESSO ALEATÓRIO. Um método é descrito para criptografar um arquivo de multimídia que inclui analisar o arquivo de multimídia para identificar uma parte de dados de mídia; criptografar a parte de dados de mídia; e combinar a parte de dados de midia criptografada com uma parte de dados não-criptografada e de não-midia. Um método é também descrito para reproduzir um arquivo de multimidia que inclui analisar o arquivo de multimídia para identificar uma parte de metadados não-criptografada; usar a parte de metadados não-criptografada para localizar uma posição de interesse no arquivo de mídia, a posição de interesse possuindo uma parte de dados de mídia criptografada associada; e decriptografar a parte de dados de mídia criptografada associada. Um aparelho para executar os métodos é também descrito aqui.



"MÉTODO E APARELHO PARA CRIPTOGRAFAR/DECRIPTOGRAFAR CONTEÚDO DE MULTIMÍDIA PARA PERMITIR ACESSO ALEATÓRIO".

Campo da Invenção

As modalidades da invenção referem, de modo geral, à criptografia e decriptografia de arquivos de multimídia e, mais particularmente, a um método e aparelho para criptografar/decriptografar conteúdo de multimídia para permitir acesso aleatório.

Descrição da Técnica Anterior

À medida que as redes 3G e outras redes celulares são desenvolvidas, surgem novos serviços baseados em dados de pacote IP. Uma das áreas de serviço mais desafiadoras que os operadores estão procurando explorar envolve a distribuição de conteúdo de vídeo para o mercado de massa. O vídeo de alta qualidade constitui o tipo de conteúdo mais intenso em termos de dados. Simultaneamente, a experiência dos consumidores com as opções atuais de apresentação doméstica apresenta aos operadores e provedores de conteúdo de mercados alvo que mantêm idéias consolidadas sobre o que deve constituir a experiência dos usuários. A combinação das expectativas dos consumidores e da mobilidade apresenta desafios fundamentais para os operadores de rede e provedores de conteúdo. Em suma, modelos de negócios atraentes, controle e gerenciamento de redes, controle de acesso, capacidades dos dispositivos e uma experiência atraente para o usuário combinam para apresentar um complexo de desafios independentes que ainda não foram completamente atendidos na indústria sem fio.

Um desafio que surgiu reside na necessidade de prover proteção do conteúdo que deve ser distribuído. Como exemplo, o conteúdo distribuído deve tipicamente ser protegido contra cópias não autorizadas. Além disso, os provedores de conteúdo também desejam controlar, direta ou indiretamente, a distribuição do conteúdo. Dessa forma, os

provedores de conteúdo requerem tipicamente que qualquer sistema de distribuição de conteúdo usado pelos provedores de serviço possua a capacidade de prover gerenciamento dos direitos digitais (DRM - Digital Rights Management), o que refere a quaisquer dentre vários arranjos técnicos que provêem controle sobre como o material distribuído pode ser usado em qualquer dispositivo eletrônico com tais medidas instaladas. Um componente subjacente crítico para todos os sistemas de distribuição de conteúdo para dar suporte ao DRM, de forma a proteger os direitos de propriedade intelectual dos provedores de conteúdo, consiste no recurso de criptografia/decriptografia da mídia durante a transmissão/recepção. Além disso, há freqüentemente uma exigência para armazenar a mídia em uma forma criptografada, nos servidores no centro de distribuição ou no dispositivo de reprodução. Adicionalmente, a criptografia freqüentemente deve dar suporte a características de "controle", tais como a capacidade de ver o conteúdo durante a reprodução rápida para frente ou em reverso ("fast-forward" e "rewind"). É desejável que a solução de criptografia da mídia possa prover a criptografia com um mínimo de modificações da interface de codificação de vídeo.

Resumo da Invenção

As modalidades aqui descritas propiciam métodos e aparelhos para criptografar apenas os dados de vídeo de qualquer fluxo de transporte do codec e deixando intacto o meta-conteúdo. Dessa forma, qualquer erro, expansão ou contração de bytes dos dados será minimizada de modo a afetar uma pequena parte da reprodução de multimídia.

Em uma modalidade, um método é descrito para criptografar um arquivo de multimídia, o método compreendendo analisar o arquivo de multimídia para identificar uma parte de dados de mídia; criptografar a parte de dados de mídia; e combinar a parte de dados de

mídia criptografada com uma parte de dados não-criptografada e de não-mídia. Um método para reproduzir um arquivo de multimídia é também fornecido para analisar o arquivo de multimídia para identificar uma parte de metadados não-criptografada; usar a parte de metadados não-criptografada para localizar uma posição de interesse no arquivo de mídia, a posição de interesse possuindo uma parte de dados de mídia criptografada associada; e decriptografar a parte de dados de mídia criptografada associada.

Em outra modalidade, um processador configurado para implementar um método para criptografar um arquivo de multimídia é descrito aqui, o método compreendendo analisar o arquivo de multimídia para identificar uma parte de dados de mídia; criptografar a parte de dados de mídia; e combinar a parte de dados de mídia criptografada com uma parte de dados não-criptografada e de não-mídia. Em tal modalidade, um processador configurado para implementar um método para reproduzir um arquivo de multimídia é também fornecido aqui, o método compreendendo analisar o arquivo de multimídia para identificar uma parte de metadados não-criptografada; usar a parte de metadados não-criptografada para localizar uma posição de interesse no arquivo de mídia, a posição de interesse possuindo uma parte de dados de mídia criptografada associada; e decriptografar a parte de dados de mídia criptografada associada.

Em ainda outra modalidade, um meio legível por computador é descrito aqui possuindo instruções armazenadas neste, as instruções armazenadas, quando executadas por um processador, fazem com que o processador execute um método para criptografar um arquivo de multimídia, o método compreende analisar o arquivo de multimídia para identificar uma parte de dados de mídia; criptografar a parte de dados de mídia; e combinar a parte de dados de mídia criptografada com a parte de dados não-criptografada

e de não-mídia. Em tal modalidade, um meio legível por computador é também fornecido possuindo instruções armazenadas neste, as instruções armazenadas, quando executadas por um processador, fazem com que o processador execute um método para reproduzir um arquivo de multimídia, o método compreendendo analisar o arquivo de multimídia para identificar uma parte de metadados não-criptografada; usar a parte de metadados não-criptografada para localizar uma posição de interesse no arquivo de mídia, a posição de interesse possuindo uma parte de dados de mídia criptografada associada; e decriptografar a parte de dados de mídia criptografada associada.

Em ainda outra modalidade, um aparelho para criptografar um arquivo de multimídia é descrito aqui, o aparelho compreendendo mecanismos para analisar o arquivo de multimídia para identificar uma parte de dados de mídia; mecanismos para criptografar a parte de dados de mídia; e mecanismos para combinar a parte de dados de mídia criptografada com uma parte de dados não-criptografada e de não-mídia. Em tal modalidade, um aparelho para reproduzir um arquivo de multimídia é também descrito aqui possuindo mecanismos para analisar o arquivo de multimídia para identificar uma parte de metadados não-criptografada; mecanismos para usar a parte de metadados não-criptografada para localizar uma posição de interesse no arquivo de mídia, a posição de interesse possuindo uma parte de dados de mídia criptografada associada; e mecanismos para decriptografar a parte de dados de mídia criptografada associada.

Outros objetivos, características e vantagens ficarão evidentes para os versados na técnica através da descrição detalhada a seguir. No entanto, deve ficar claro que a descrição detalhada e os exemplos específicos, apesar de descreverem modalidades exemplares, são apresentados apenas como ilustração e não limitação. Várias alterações e

modificações dentro do escopo da descrição a seguir podem ser efetuadas sem se afastar de seu conceito inventivo, e devendo a descrição ser considerada como incluindo todas estas modificações.

Breve Descrição das Figuras

A invenção poderá ser mais prontamente entendida por referência aos desenhos anexos, nos quais:

Figura 1 - ilustra uma organização de um fluxo de bits de vídeo exemplar tal como definido por um codec padrão;

Figura 2 - ilustra um exemplo de uma organização de amostras de vídeo e áudio em blocos e os deslocamentos dos blocos;

Figura 3 - é um diagrama em blocos de um servidor com uma máquina de criptografia configurada para criptografar somente uma parte de mídia de um conteúdo de multimídia;

Figura 4 - é um diagrama em blocos de um cliente com um reprodutor para decriptografar e reproduzir a parte de mídia criptografada do conteúdo de multimídia;

Figura 5 - é um fluxograma de uma operação da máquina de criptografia; e

Figura 6 - é um diagrama em blocos de um ponto de acesso e um terminal de acesso que podem ser usados para implementar as características descritas aqui.

As referências numéricas similares referem a partes semelhantes em todas as vistas dos desenhos.

Descrição Detalhada da Invenção

As modalidades aqui descritas provêem um método para criptografar apenas a parte do "conteúdo" dos dados de qualquer fluxo de transporte do codec e separando o meta-conteúdo intacto, o qual é usado para localizar e reproduzir o conteúdo. Como exemplo, em uma modalidade, apenas a parte de conteúdo de vídeo é criptografada. Como resultado, os efeitos de quaisquer erros ou

expansão/contração de bytes de dados devem ser minimizados, desse modo, afetando uma pequena parte da reprodução da multimídia.

A descrição a seguir presume que o codec usado para armazenar o conteúdo de multimídia está de acordo com o padrão MPEG4 como divulgado pelo Grupo de Peritos em Imagem em Movimento (MPEG), um grupo de trabalho da Organização de Padronização Internacional/Comissão Eletrotécnica Internacional, e Comitê de Conjunto Técnico 1(ISO/IEC JTC1). Os padrões ISO/IEC são denotados como MPEG-x (por exemplo, MPEG-1, MPEG-2 e MPEG-3) e o padrão MPEG-4 é descrito na ISO/IEC 14496-2.

Um arquivo MPEG4 consiste em átomos hierárquicos, incluindo metadados e átomos de mídia. Cada átomo em si pode ser composto por outros átomos. Os metadados e átomos de dados de mídia podem estar presentes em qualquer ponto no arquivo. De modo geral, o átomo de metadados (**moov**) não é essencial e pode estar localizado antes ou após os átomos de dados de mídia no arquivo. Os metadados constituem tipicamente menos de 5 a 10 % de um arquivo MPEG4.

Cada átomo em si possui um tipo e um campo de tamanho para ele designados, a partir dos quais um mapa do conteúdo do arquivo pode ser gerado. Isto permite ao analisador do reprodutor de multimídia pular rapidamente de um átomo para outro. Cada fluxo elementar, tal como o fluxo de áudio ou o fluxo de vídeo, terão seu próprio átomo **mdat** (dados de mídia). Dentro do átomo **mdat**, os dados de mídia são organizados na forma de blocos, que são uma coleção de amostras correlacionadas. Como exemplo, um bloco de dados de vídeo pode incluir os primeiros três quadros de vídeo de uma seqüência de vídeo (por exemplo, os quadros 1, 2 e 3), enquanto um bloco de dados de áudio poderia ter uma ou mais amostras de áudio neste. Tais blocos de dados de mídia são interpostos por todo o arquivo.

O átomo de metadados contém informações a respeito da mídia no arquivo, dos quadros e de seus deslocamentos. Especificamente, existe um **stbl** ou átomo de tabela de amostras presente dentro do átomo **moov**. Tal átomo **stbl** é também composto dos átomos de tabela a seguir:

stts: Mapeia tempo para números de amostras;
stsz: Especifica o tamanho das amostras;
stsc: Mapeia amostras para blocos (indica basicamente qual amostra ocorre em qual bloco);
stco: Provê o deslocamento do bloco dentro do arquivo;
stsd: Tabela de descrição de amostra que contém informações de configuração (cabeçalhos VOL, etc.).

Em conjunto, tais átomos provêem os metadados essenciais exigidos para analisar o quadro apropriado ou amostra de áudio para apresentá-los para reprodução, como será também descrito mais adiante.

Vários reprodutores de multimídia são baseados em arquivos, de tal forma que eles tomam como entrada um nome de arquivo (filename) ou um buffer contendo um arquivo de multimídia. O reprodutor realiza uma varredura dos metadados do arquivo para carregar uma tabela interna com os deslocamentos de quadros e informações de temporização. Os quadros brutos são alimentados ao codec (por exemplo, um codec MPEG-4) para decodificar e a seguir apresentados no display pelo reprodutor. A tabela interna é usada para realizar funções tais como buscas "rápidas" a uma posição apropriada no arquivo durante uma reprodução em avanço rápido (fast-forward) ou recuo rápido (rewind), ou de "acesso aleatório" a partir de qualquer ponto no arquivo. Tais recursos são coletivamente referenciados aqui como recursos de "controle de leitura" (trick play).

Para manter compactas as tabelas internas, uma variedade de técnicas é usada. Uma delas, usada para compactar as informações de localização e tamanho, se baseia na observação de que as várias amostras provenientes da mesma trilha são freqüentemente armazenadas de forma contígua, mesmo quando dados provenientes de várias trilhas são intercalados. Tal seqüência de amostras contíguas provenientes de uma trilha específica é denominada como um bloco. A tabela de amostras-para-blocos dentro do átomo "stsc" obrigatório provê o mapeamento de números de amostras para índices de blocos. A posição (absoluta) de cada bloco é gravada dentro do átomo "stco" obrigatório, como um deslocamento de bloco (usando 32 ou 64 bits), que é medido do início do arquivo no qual o bloco reside. O comprimento, em bytes, de cada amostra é também gravado na tabela de tamanhos de amostras dentro do átomo "stsz" obrigatório. Portanto, ao usar:

1. a referência de dados da trilha;
2. o mapeamento de amostras-para-blocos;
3. o deslocamento do bloco; e
4. os tamanhos das amostras precedentes no mesmo bloco,

é possível encontrar:

1. o arquivo de dados contendo a amostra, o qual pode ser um arquivo designado pela URL proveniente do próprio arquivo MP4;
2. o bloco (e seu deslocamento) dentro deste arquivo;
3. o deslocamento da amostra dentro do bloco (a partir dos tamanhos das amostras precedentes no mesmo bloco); e
4. o tamanho da própria amostra.

A Figura 2 ilustra um exemplo simples relacionado a tal processo. Note que os tamanhos do quadro de vídeo e do quadro de áudio (amostra) são também conhecidos,

quaisquer limites de amostras de vídeo ou áudio podem ser facilmente calculados como deslocamentos absolutos. Em tal reprodutor, a estrutura de tabela pré-construída não permite uma alimentação de arquivos criptografados para o reprodutor. A entrada do reprodutor está na forma de um nome de arquivo (char*) ou de um buffer que presume que todo o arquivo reside no formato não-criptografado no buffer. Nenhuma destas interfaces permite ao reprodutor decriptografar o arquivo de uma sessão "streaming" (isto é, efetuar a decriptografia enquanto reproduz o arquivo).

Em uma modalidade, a funcionalidade streaming pode ser adicionada se o sistema de criptografia/decriptografia for modificado de forma que a criptografia ocorra em nível de quadro ou fatia em um arquivo, deixando os metadados visíveis para dar suporte ao controle de leitura. Tal método de "criptografia inteligente" permite ao sistema de criptografia (por exemplo, o servidor) ficar informado do formato de mídia, enquanto criptografa o conteúdo atual e deixando os metadados essenciais e os dados de cabeçalho visíveis. De forma similar, no sistema de decriptografia (por exemplo, o cliente), os metadados podem ser utilizados para realizar características tais como o controle de leitura sem processamento adicional visto que estes não estão criptografados, e apenas a parte de conteúdo do fluxo ou arquivo devendo ser decriptografada.

Deve ser observado que apesar de cada parte do esquema de criptografia estar aqui descrita especificamente em termos da parte de mídia sendo separada da parte que não é mídia (por exemplo, os metadados), e então criptografada, em uma modalidade, o sistema de criptografia irá analisar o arquivo/fluxo de mídia e, enquanto analisa o arquivo/fluxo de mídia, criptografará apenas as partes de dados de mídia e deixará os metadados como estão. Dessa forma, em uma modalidade, a parte de mídia não necessita ser separada dos

metadados, criptografada e a seguir ser novamente agrupada (isto é, multiplexada) com os metadados. Em outra modalidade, a parte de mídia pode ser separada para processamento e requerer multiplexação. Em qualquer dos casos, para sistemas e processos externos ao sistema de criptografia, ambas as modalidades também se aplicam na parte de decriptografia do esquema.

A Figura 3 ilustra um servidor 300 com uma máquina de criptografia 302 que inclui um analisador 308 que analisa os dados entrantes provenientes de uma fonte de multimídia 332, os quais podem ser de um fluxo ou um arquivo, em partes de mídia e de não-mídia. Enquanto o analisador 308 está analisando os dados entrantes, um processador de criptografia 306 então criptografa apenas as partes de mídia usando informações provenientes de um servidor DRM 322. Um combinador 304 combinará a parte de não-mídia (que não está criptografada) e a parte de mídia criptografada e as enviará para um pós-processador 352 para transmissão para um cliente 400, tal como mostrado na Figura 4.

A criptografia inteligente exige que a máquina de criptografia 302 esteja informada sobre os vários formatos de mídia a serem suportados pelo sistema, de forma que este apenas criptografe os dados de quadros, deixando os cabeçalhos visíveis. Como exemplo, no caso do MPEG4, tal como ilustrado na Figura 1, o sistema criptografará somente os dados VOP e deixará os cabeçalhos VOP e GOV visíveis. Além disso, presumindo-se que o fluxo de bits de vídeo seja um arquivo MP4 padrão, em que o átomo de metadados **stbl** é compulsório, a máquina de criptografia não necessitará analisar os códigos de início de amostra de áudio ou quadro para obter os dados de mídia. Em lugar disto, a máquina de criptografia usará as informações no átomo de metadados

stbl para analisar a posição apropriada no arquivo para obter os dados de amostra de áudio ou quadro.

A Figura 4 ilustra um cliente 400 que recebe o arquivo de multimídia a partir do servidor 300 e decriptografa as partes relevantes do arquivo recebido para apresentação e reprodução. Um reprodutor 450 poderá construir uma tabela interna sem qualquer decriptografia, pois as informações de cabeçalho do arquivo estão todas visíveis. O reprodutor 450 inclui uma máquina de decriptografia 402, e um analisador 414 na máquina de decriptografia 402 passará a parte do arquivo que está criptografada para uma unidade de decriptografia 416, juntamente com a chave para decriptografia antes de enviar os quadros para o codec MP4. Especificamente, o analisador 414 extrai os dados para os quadros criptografados e os envia para a unidade de decriptografia 416. A parte de não-mídia, que não foi criptografada pelo servidor 300, será enviada diretamente para um combinador 418 para combinação com a parte de mídia decriptografada. Um decodificador 404, que inclui um decodificador de áudio 408 e um decodificador de vídeo 412, decodificará o fluxo de bits de áudio (CAB) e o fluxo de bits de vídeo codificado (CVB) para apresentação em um dispositivo de saída de áudio 406 e em um display 410, respectivamente. Deve ser observado, que o reprodutor 450 pode possuir mais componentes do que os ilustrados na Figura 4.

Na modalidade acima, o arquivo parecerá um arquivo MPEG4 normal para o reprodutor 450, pois os cabeçalhos não estão criptografados. A criação da tabela interna não irá requerer que ocorra qualquer decriptografia, portanto a decriptografia ocorrerá somente quando os quadros estiverem sendo alimentados ao codec. Naturalmente, as máquinas de criptografia/decriptografia devem estar informadas sobre o formato do arquivo para reconhecer o cabeçalho. Dessa forma, serão necessárias

alterações para cada formato de mídia adicional que o sistema deve suportar. Além disso, haverá uma carga adicional de processamento na máquina de criptografia para permitir a criptografia no nível de quadro - análise de átomos **stbl**, buscando por dados de mídia, etc.

A Figura 5 ilustra um fluxograma de uma modalidade exemplar da operação do processo de criptografia/decriptografia 500, onde, no bloco 502, o analisador 308 da máquina de criptografia 302 determina se os dados estão sendo recebidos a partir de um arquivo ou de um fluxo que pertencem a uma parte de mídia ou a uma parte de não-mídia. Se sim, então a operação continua com o bloco 504, onde a unidade de criptografia 306 criptografa a parte de mídia. Caso contrário, a operação passa ao bloco 508, onde a parte de não-mídia dos dados não é criptografada (ou seja, é deixada visível). No bloco 506, as partes de mídia e de não-mídia são combinadas e lidas para a localização de armazenamento do arquivo (tal como uma unidade de armazenamento no servidor 300), ou em streaming para o cliente 400. Se o fluxo ou o arquivo completo não tiver sido processado, então a operação retorna ao bloco 502. Caso contrário, os dados são transmitidos para o cliente 400.

Uma vez que os dados tenham sido transmitidos para o cliente 400, seja em um arquivo ou como parte de um fluxo, durante a reprodução, o cliente 400 pode ler a parte de metadados no bloco 512 e, no bloco 514, determinar se foi encontrada a localização da reprodução. Se sim, a operação continua com o bloco 516, onde a parte de mídia é lida e decriptografada. A parte decriptografada é a seguir apresentada ao decodificador 404 para reprodução, tal como acima descrito.

A Figura 6 mostra um diagrama em blocos de um ponto de acesso 604x e um terminal de acesso 602x que podem ser utilizados, respectivamente, para transmitir e receber

dados criptografados usando os métodos e aparelhos descritos aqui. Como descrito aqui, um "terminal de acesso" refere a um dispositivo que provê conectividade de voz e/ou dados para um usuário. O terminal de acesso pode ser conectado a um dispositivo de computação, tal como um computador laptop ou um computador de mesa (desktop), ou pode ser um dispositivo autônomo, tal como um assistente digital pessoal. Um terminal de acesso pode também ser denominado como uma unidade de assinante, estação móvel, móvel, estação remota, terminal remoto, terminal de usuário, agente de usuário, ou equipamento de usuário. Um terminal de acesso pode ser uma estação de assinante, dispositivo sem fio, telefone celular, telefone PCS, um telefone sem fio convencional, um telefone de Protocolo de Iniciação de Sessão (SIP), uma estação de um sistema de loop local sem fio (WLL), um assistente digital pessoal (PDA), um dispositivo portátil possuindo capacidade de conexão sem fio, ou outro dispositivo de processamento conectado a um modem sem fio. Além disso, um "ponto de acesso", tal como aqui utilizado refere a um dispositivo em uma rede de acesso que comunica através da interface aérea, através de um ou mais setores, com os terminais de acesso. O ponto de acesso atua como um roteador entre o terminal de acesso e o restante da rede de acesso, a qual pode incluir uma rede IP, por conversão de quadros da interface aérea recebidos para pacotes IP. O ponto de acesso também coordena o gerenciamento de atributos para a interface aérea.

Para o link reverso, no terminal de acesso 602x, um processador de dados de transmissão (TX) 614 recebe dados de tráfego provenientes de um buffer de dados 612, processa (por exemplo, codifica, intercala, e mapeia em símbolos) cada pacote de dados com base em um esquema de codificação e modulação selecionado, e provê símbolos de dados. Um símbolo de dados consiste em um símbolo de

modulação para dados, e um símbolo piloto consiste em um símbolo de modulação para piloto (o qual é conhecido *a priori*). Um modulador 616 recebe os símbolos de dados, os símbolos piloto e, possivelmente, sinalização para o link reverso, realiza modulação (por exemplo, por OFDM) e/ou outro processamento como especificado pelo sistema, e provê um fluxo de chips de saída. Uma unidade transmissora (TMTR) 618 processa (por exemplo, converte para analógico, filtra, amplifica e converte ascendentemente em freqüência) o fluxo de chips de saída e gera um sinal modulado, o qual é transmitido a partir de uma antena 620.

No ponto de acesso 604x, os sinais modulados transmitidos pelo terminal de acesso 602x e outros terminais em comunicação com o ponto de acesso 604x são recebidos por uma antena 652. Uma unidade receptora (RCVR) 654 processa (por exemplo, condiciona e digitaliza) o sinal recebido a partir da antena 652 e provê amostras recebidas. Um demodulador (DEMOD) 656 processa (por exemplo, demodula e detecta) as amostras recebidas e provê símbolos de dados detectados, os quais são uma estimativa ruidosa dos símbolos de dados transmitidos pelos terminais para o ponto de acesso 604x. Um processador de dados de recepção (RX) 658 processa (por exemplo, demapeia em símbolos, deintercala, e decodifica) os símbolos de dados detectados para cada terminal e provê dados decodificados para tal terminal.

Para o link direto, no ponto de acesso 604x, os dados de tráfego são processados por um processador de dados TX 660 para gerar símbolos de dados. Um modulador 662 recebe os símbolos de dados, símbolos piloto, e sinalização para o link direto, realiza a modulação (por exemplo, por OFDM) e/ou outro processamento pertinente, e provê um fluxo de chips de saída, o qual é adicionalmente condicionado por uma unidade transmissora 664 e transmitido a partir da antena 652. A sinalização de link direto pode incluir

comandos de controle de potência gerados por um controlador 670 para todos os terminais transmitindo através do link reverso para o ponto de acesso 604x. No terminal de acesso 602x, o sinal modulado transmitido pelo ponto de acesso 604x é recebido pela antena 620, condicionado e digitalizado por uma unidade receptora 622, e processado por um demodulador 624 para obter símbolos de dados detectados. Um processador de dados RX 1026 processa os símbolos de dados detectados e provê dados decodificados para o terminal e para a sinalização de link direto. O controlador 630 recebe os comandos de controle de potência, e controla a transmissão de dados e a potência de transmissão no link reverso para o ponto de acesso 604x. Os controladores 630 e 670 direcionam a operação do terminal de acesso 602x e do ponto de acesso 604x, respectivamente. As unidades de memória 632 e 672 armazenam códigos de programa e dados usados pelos controladores 630 e 670, respectivamente.

As modalidades descritas podem ser aplicadas a qualquer uma ou a combinações das seguintes tecnologias: sistemas de Acesso Múltiplo por Divisão de Código (CDMA), CDMA com Múltiplas Portadoras (MC-CDMA), CDMA de Banda Larga (W-CDMA), Acesso de Pacotes em Downlink de Alta Velocidade (HSDPA), sistemas de Acesso Múltiplo por Divisão de Tempo (TDMA), sistemas de Acesso Múltiplo por Divisão de Freqüência (FDMA), e sistemas de Acesso Múltiplo por Divisão de Freqüência Ortogonal (OFDMA).

As etapas de um método ou algoritmo descritas em conexão com as modalidades apresentadas aqui podem ser incorporadas diretamente em hardware, em um módulo de software executado por um processador, ou em uma combinação de ambos. Um módulo de software pode residir em uma memória RAM, memória flash, memória ROM, memória EPROM, memória EEPROM, registradores, em um disco rígido, em um disco removível, em um CD-ROM, ou em qualquer outra forma de meio

de armazenamento conhecido pelos versados na técnica. Um meio de armazenamento exemplar é acoplado ao processador, de tal forma que o processador possa ler e gravar informações no meio de armazenamento. Como alternativa, o meio de armazenamento pode estar acoplado ao processador. O processador e o meio de armazenamento podem residir em um ASIC. O ASIC pode residir em um terminal de usuário. Como alternativa, o processador e o meio de armazenamento podem residir como componentes individuais em um terminal de usuário.

Deve ser observado que os métodos aqui descritos podem ser implementados em uma diversidade de processadores, hardware e sistemas conhecidos pelos versados na técnica. Como exemplo, a exigência geral para que o cliente opere tal como descrito aqui consiste em que o cliente possua um display para a apresentação de conteúdo e informações, um processador para controlar a operação do cliente e uma memória para armazenar dados e programas relacionados à operação do cliente. Em uma modalidade, o cliente é um telefone celular. Em outra modalidade, o cliente é um computador portátil possuindo capacidades de comunicação. Em ainda outra modalidade, o cliente é um computador pessoal possuindo capacidades de comunicação. Além disso, hardware, tal como um receptor GPS, podem ser incorporados ao cliente quando necessário para implementar as várias modalidades descritas aqui. Os vários blocos lógicos, módulos, lógicas e circuitos descritos em conexão com as modalidades descritas aqui podem ser implementados ou realizados com um processador de propósito geral, um processador de sinal digital (DSP), um circuito integrado de aplicação específica (ASIC), uma matriz de porta programável em campo (FPGA), ou outro dispositivo lógico programável, porta ou lógica de transistor discreto, componentes de hardware discretos, ou qualquer combinação destes projetada para realizar as funções descritas aqui.

Um processador de propósito geral pode ser um microprocessador, porém como alternativa, o processador pode ser qualquer processador, controlador, microcontrolador ou máquina de estado convencionais. Um processador pode ser também implementado como uma combinação de dispositivos de computação, por exemplo, uma combinação de um DSP e um microprocessador, uma pluralidade de microprocessadores, um ou mais microprocessadores em conjunto com um núcleo DSP, ou qualquer outra configuração similar.

Os vários exemplos de lógicas, blocos lógicos, módulos e circuitos descritos em conexão com as modalidades descritas aqui podem ser implementados ou realizados com um processador de propósito geral, um processador de sinal digital (DSP), um circuito integrado de aplicação específica (ASIC), uma matriz de porta programável em campo (FPGA) ou outro dispositivo de lógica programável, porta discreta, ou lógica de transistor, componentes de hardware discretos, ou qualquer combinação destes projetada para realizar as funções descritas. Um processador de propósito geral pode ser um microprocessador, porém como alternativa, o processador pode ser qualquer processador, controlador, microcontrolador ou máquina de estado convencionais. Um processador pode também ser implementado como uma combinação de dispositivos de computação, por exemplo, uma combinação de um DSP e um microprocessador, uma pluralidade de microprocessadores, um ou mais microprocessadores em conjunto com um núcleo DSP, ou qualquer outra configuração similar.

As modalidades acima descritas constituem modalidades exemplares. Os versados na técnica poderão efetuar vários usos e derivações das modalidades acima descritas sem se afastar dos conceitos da invenção descritos aqui. Várias modificações a estas modalidades ficarão prontamente claras para os técnicos na área, e os

princípios genéricos aqui definidos podem ser aplicados a outras modalidades, por exemplo, em um serviço de mensagens instantâneas ou quaisquer aplicações gerais de comunicação de dados sem fio, sem constituir um afastamento do conceito inventivo ou escopo dos novos aspectos aqui descritos. Dessa forma, o escopo da invenção não deve ficar limitado às modalidades aqui apresentadas, devendo receber o escopo mais amplo, consistente com os princípios e as novas características aqui descritos. O termo "exemplar" é aqui usado exclusivamente com o significado de "servindo como exemplo, caso, ou ilustração". Qualquer modalidade aqui descrita como "exemplar" não deve ser necessariamente considerada como preferida ou vantajosa em relação a outras modalidades.

REIVINDICAÇÕES

1. Método para criptografar um arquivo de multimídia, compreendendo:

- analisar o arquivo de multimídia para identificar uma parte de dados de mídia;

- criptografar a parte de dados de mídia; e

- combinar a parte de dados de mídia criptografada com uma parte de dados não-criptografada e de não-mídia.

2. Método, de acordo com a reivindicação 1, no qual analisar o arquivo de multimídia para identificar a parte de dados de mídia compreende:

- determinar um formato de arquivo do arquivo de multimídia; e

- com base no formato de arquivo determinado, identificar as partes de dados de mídia do arquivo de multimídia.

3. Método, de acordo com a reivindicação 1, no qual a parte de dados de mídia inclui uma pluralidade de quadros de vídeo, e criptografar a parte de dados de mídia compreende criptografar a parte de dados de mídia com base em quadro de vídeo a quadro de vídeo.

4. Método, de acordo com a reivindicação 1, no qual a parte de dados de mídia inclui uma pluralidade de amostras de áudio, e criptografar a parte de dados de mídia compreende criptografar a parte de dados de mídia com base em amostra de áudio a amostra de áudio.

5. Método para reproduzir um arquivo de multimídia, compreendendo:

- analisar o arquivo de multimídia para identificar uma parte de metadados não-criptografada;

- usar a parte de metadados não-criptografada para localizar uma posição de interesse no arquivo de mídia, a posição de interesse possuindo uma parte de dados de mídia criptografada associada; e

- decriptografar a parte de dados de mídia criptografada associada.

6. Método, de acordo com a reivindicação 5, no qual analisar o arquivo de multimídia para identificar a parte de metadados compreende:

- determinar um formato de arquivo do arquivo de multimídia; e

- com base no formato de arquivo determinado, identificar uma parte não-criptografada e de não-mídia do arquivo de multimídia.

7. Método, de acordo com a reivindicação 5, no qual usar a parte de metadados não-criptografada para localizar a posição de interesse no arquivo de mídia compreende:

- montar uma tabela de deslocamentos de quadros de vídeo e informações de temporização; e

- determinar a localização de uma amostra no arquivo de dados.

8. Método, de acordo com a reivindicação 7, no qual determinar a localização de uma amostra no arquivo de dados compreende:

- mapear a amostra para um bloco; e

- determinar um deslocamento da amostra dentro do bloco.

9. Pelo menos um processador configurado para implementar um método para criptografar um arquivo de multimídia, o método compreendendo:

- analisar o arquivo de multimídia para identificar uma parte de dados de mídia;

- criptografar a parte de dados de mídia; e

- combinar a parte de dados de mídia criptografada com uma parte de dados não-criptografada e de não-mídia.

10. Pelo menos um processador, de acordo com a reivindicação 9, no qual analisar o arquivo de multimídia para identificar a parte de dados de mídia compreende:

- determinar um formato de arquivo do arquivo de multimídia; e

- com base no formato de arquivo determinado, identificar as partes de dados de mídia do arquivo de multimídia.

11. Pelo menos um processador, de acordo com a reivindicação 9, no qual a parte de dados de mídia inclui uma pluralidade de quadros de vídeo, e criptografar a parte de dados de mídia compreende criptografar a parte de dados de mídia com base em quadro de vídeo a quadro de vídeo.

12. Pelo menos um processador, de acordo com a reivindicação 9, no qual a parte de dados de mídia inclui uma pluralidade de amostras de áudio, e criptografar a parte de dados de mídia compreende criptografar a parte de dados de mídia com base em amostra de áudio a amostra de áudio.

13. Pelo menos um processador configurado para implementar um método para reproduzir um arquivo de multimídia, o método compreendendo:

- analisar o arquivo de multimídia para identificar uma parte de metadados não-criptografada;

- usar a parte de metadados não-criptografada para localizar uma posição de interesse no arquivo de mídia, a posição de interesse possuindo uma parte de dados de mídia criptografada associada; e

- decriptografar a parte de dados de mídia criptografada associada.

14. Pelo menos um processador, de acordo com a reivindicação 13, no qual analisar o arquivo de multimídia para identificar a parte de metadados compreende:

- determinar um formato de arquivo do arquivo de multimídia; e

- com base no formato de arquivo determinado, identificar uma parte não-criptografada e de não-mídia do arquivo de multimídia.

15. Pelo menos um processador, de acordo com a reivindicação 13, no qual usar a parte de metadados não-criptografada para localizar a posição de interesse no arquivo de mídia compreende:

- montar uma tabela de deslocamentos de quadros de vídeo e informações de temporização; e

- determinar a localização de uma amostra no arquivo de dados.

16. Pelo menos um processador, de acordo com a reivindicação 15, no qual determinar a localização de uma amostra no arquivo de dados compreende:

- mapear a amostra para um bloco; e

- determinar um deslocamento da amostra dentro do bloco.

17. Meio legível por computador possuindo instruções armazenadas neste, as instruções armazenadas, quando executadas por um processador, fazem com que o processador execute um método para criptografar um arquivo de multimídia, o método compreendendo:

- analisar o arquivo de multimídia para identificar uma parte de dados de mídia;

- criptografar a parte de dados de mídia; e

- combinar a parte de dados de mídia criptografada com uma parte de dados não-criptografada e de não-mídia.

18. Meio legível por computador, de acordo com a reivindicação 17, no qual analisar o arquivo de multimídia para identificar a parte de dados de mídia compreende:

- determinar um formato de arquivo do arquivo de multimídia; e

- com base no formato de arquivo determinado, identificar as partes de dados de mídia do arquivo de multimídia.

19. Meio legível por computador, de acordo com a reivindicação 17, no qual a parte de dados de mídia inclui uma pluralidade de quadros de vídeo, e criptografar a parte de dados de mídia compreende criptografar a parte de dados de mídia com base em quadro de vídeo a quadro de vídeo.

20. Meio legível por computador, de acordo com a reivindicação 17, no qual a parte de dados de mídia inclui uma pluralidade de amostras de áudio, e criptografar a parte de dados de mídia compreende criptografar a parte de dados de mídia com base em amostra de áudio a amostra de áudio.

21. Meio legível por computador possuindo instruções armazenadas neste, as instruções armazenadas, quando executadas por um processador, fazem com que o processador execute um método para reproduzir um arquivo de multimídia, o método compreendendo:

- analisar o arquivo de multimídia para identificar uma parte de metadados não-criptografada;

- usar a parte de metadados não-criptografada para localizar uma posição de interesse no arquivo de mídia, a posição de interesse possuindo uma parte de dados de mídia criptografada associada; e

- decriptografar a parte de dados de mídia criptografada associada.

22. Meio legível por computador, de acordo com a reivindicação 21, no qual analisar o arquivo de multimídia para identificar a parte de metadados compreende:

- determinar um formato de arquivo do arquivo de multimídia; e

- com base no formato de arquivo determinado, identificar uma parte não-criptografada e de não-mídia do arquivo de multimídia.

23. Meio legível por computador, de acordo com a reivindicação 21, no qual usar a parte de metadados não-criptografada para localizar a posição de interesse no arquivo de mídia compreende:

- montar uma tabela de deslocamentos de quadros de vídeo e informações de temporização; e

- determinar a localização de uma amostra no arquivo de dados.

24. Meio legível por computador, de acordo com a reivindicação 23, no qual determinar a localização de uma amostra no arquivo de dados compreende:

- mapear a amostra para um bloco; e

- determinar um deslocamento da amostra dentro do bloco.

25. Aparelho para criptografar um arquivo de multimídia, compreendendo:

- mecanismos para analisar o arquivo de multimídia para identificar uma parte de dados de mídia;

- mecanismos para criptografar a parte de dados de mídia; e

- mecanismos para combinar a parte de dados de mídia com uma parte de dados não-criptografada e de não-mídia.

26. Aparelho, de acordo com a reivindicação 25, no qual os mecanismos para analisar o arquivo de multimídia para identificar a parte de dados de mídia compreendem:

- mecanismos para determinar um formato de arquivo do arquivo de multimídia; e

- mecanismos para, com base no formato de arquivo determinado, identificar as partes de dados de mídia do arquivo de multimídia.

27. Aparelho, de acordo com a reivindicação 25, no qual a parte de dados de mídia inclui uma pluralidade de quadros de vídeo, e os mecanismos para criptografar a parte de dados de mídia compreendem mecanismos para criptografar

a parte de dados de mídia com base em quadro de vídeo a quadro de vídeo.

28. Aparelho, de acordo com a reivindicação 25, no qual a parte de dados de mídia inclui uma pluralidade de amostras de áudio, e os mecanismos para criptografar a parte de dados de mídia compreendem mecanismos para criptografar a parte de dados de mídia com base em amostra de áudio a amostra de áudio.

29. Aparelho para reproduzir um arquivo de multimídia, compreendendo:

- mecanismos para analisar o arquivo de multimídia para identificar uma parte de metadados não-criptografada;

- mecanismos para usar a parte de metadados não-criptografada para localizar uma posição de interesse no arquivo de mídia, a posição de interesse possuindo uma parte de dados de mídia criptografada associada; e

- mecanismos para decriptografar a parte criptografada de dados de mídia associada.

30. Aparelho, de acordo com a reivindicação 29, no qual os mecanismos para analisar o arquivo de multimídia para identificar a parte de metadados compreendem:

- mecanismos para determinar um formato de arquivo do arquivo de multimídia; e

- mecanismos para identificar uma parte não-criptografada e de não-mídia do arquivo de multimídia com base no formato de arquivo determinado.

31. Aparelho, de acordo com a reivindicação 29, no qual os mecanismos para usar a parte de metadados não-criptografada para localizar a posição de interesse no arquivo de mídia compreendem:

- mecanismos para montar uma tabela de deslocamentos de quadros de vídeo e informações de temporização; e

- mecanismos para determinar a localização de uma amostra no arquivo de dados.

32. Aparelho, de acordo com a reivindicação 31, no qual os mecanismos para determinar a localização de uma amostra no arquivo de dados compreendem:

- mecanismos para mapear a amostra para um bloco; e

- mecanismos para determinar um deslocamento da amostra dentro do bloco.

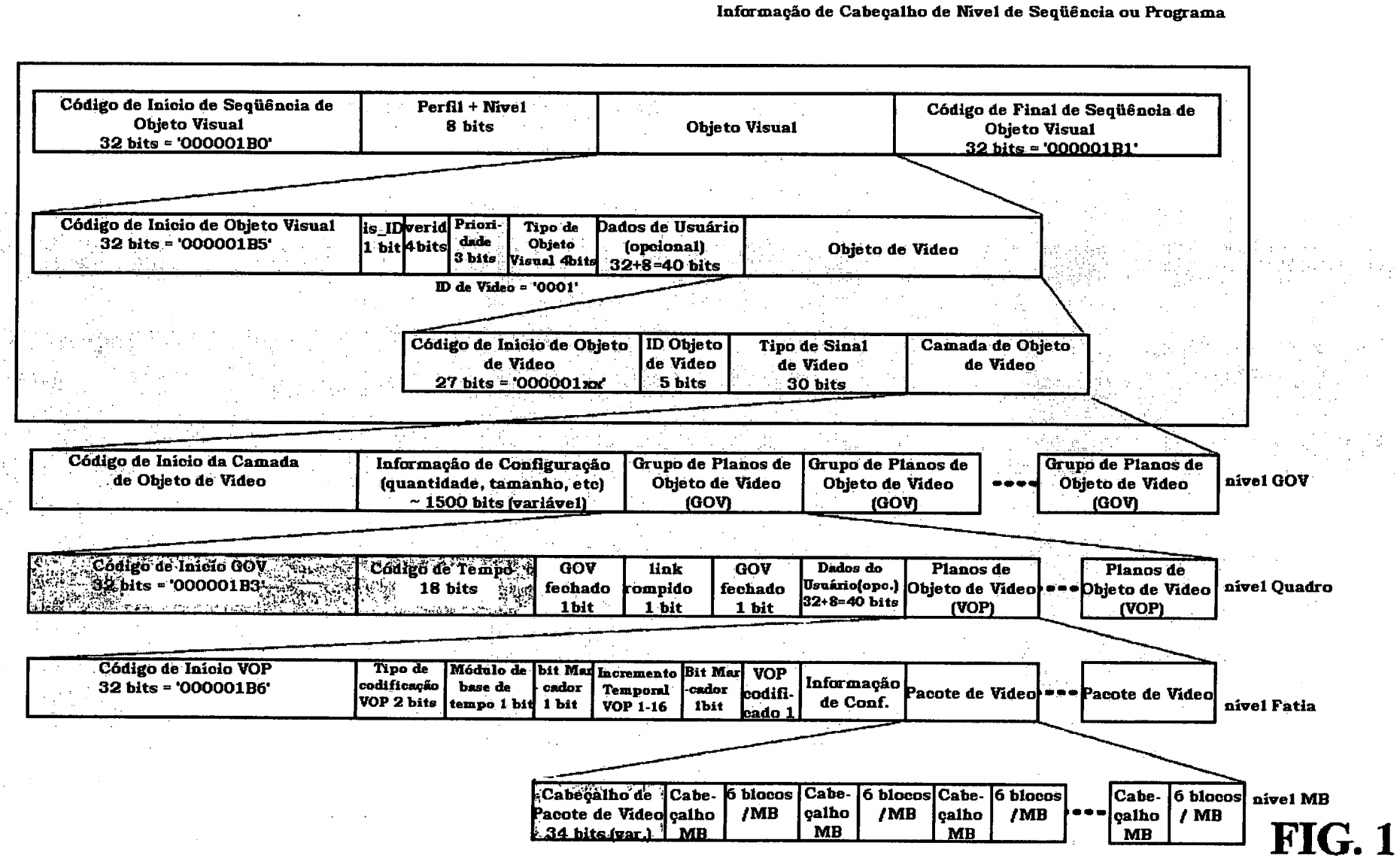

Informação de Cabeçalho de Nível de Seqüência ou Programa
Código de Início de Seqüência de Objeto Visual 32 bits = '000001B0'
Perfil + Nível 8 bits
Objeto Visual
Código de Final de Seqüência de Objeto Visual 32 bits = '000001B1'
Código de Início de Objeto Visual 32 bits = '000001B5'
is_ID 1 bit
verid 4bits
Priori-dade 3 bits
Tipo de Objeto Visual 4bits
Dados de Usuário (opcional) 32+8=40 bits
Objeto de Vídeo
ID de Vídeo = '0001'
Código de Início de Objeto de Vídeo 27 bits = '000001xx'
ID Objeto de Vídeo 5 bits
Tipo de Sinal de Vídeo 30 bits
Camada de Objeto de Vídeo
Código de Início da Camada de Objeto de Vídeo
Informação de Configuração (quantidade, tamanho, etc) ~ 1500 bits (variável)
Grupo de Planos de Objeto de Vídeo (GOV)
Grupo de Planos de Objeto de Vídeo (GOV)
Grupo de Planos de Objeto de Vídeo (GOV)
nível GOV
Código de Início GOV 32 bits = '000001B3'
Código de Tempo 18 bits
GOV fechado 1bit
link rompido 1 bit
GOV fechado 1 bit
Dados do Usuário(opc.) 32+8=40 bits
Planos de Objeto de Vídeo (VOP)
Planos de Objeto de Vídeo (VOP)
nível Quadro
Código de Início VOP 32 bits = '000001B6'
Tipo de codificação VOP 2 bits
Módulo de base de tempo 1 bit
bit Mar cador 1 bit
Incremento Temporal VOP 1-16
Bit Mar -cador 1bit
VOP codifi-cado 1
Informação de Conf.
Pacote de Vídeo
Pacote de Vídeo
nível Fatia
Cabeçalho de Pacote de Vídeo 34 bits (var.)
Cabe-çalho MB
6 blocos /MB
Cabe-çalho MB
6 blocos /MB
Cabe-çalho MB
6 blocos /MB
Cabe-çalho MB
6 blocos / MB
nível MB

FIG. 1

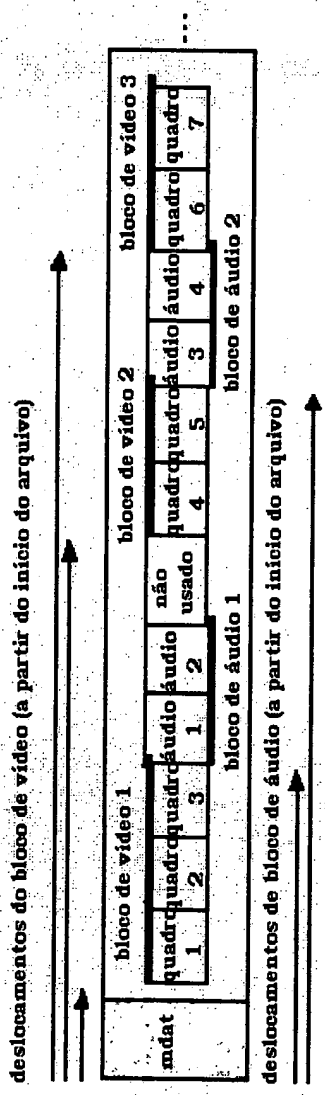

deslocamentos do bloco de vídeo (a partir do início do arquivo)
mdat
bloco de vídeo 1
quadro 1
quadro 2
quadro 3
áudio 1
áudio 2
não usado
bloco de vídeo 2
quadro 4
quadro 5
áudio 3
áudio 4
bloco de vídeo 3
quadro 6
quadro 7
...
bloco de áudio 1
bloco de áudio 2
deslocamentos de bloco de áudio (a partir do início do arquivo)

FIG. 2

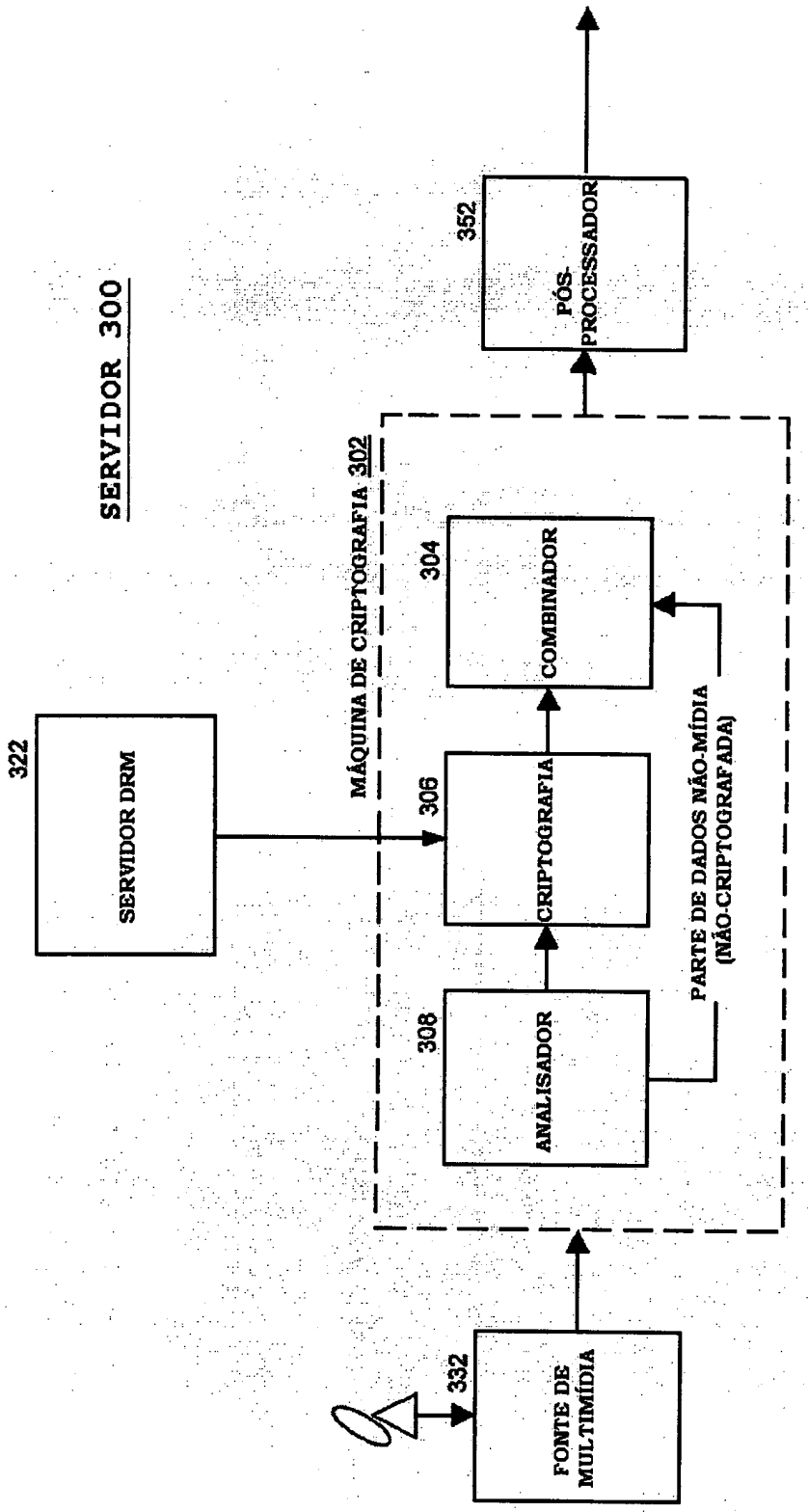

SERVIDOR 300
MÁQUINA DE CRIPTOGRAFIA 302
322
SERVIDOR DRM
306
CRIPTOGRAFIA
304
COMBINADOR
352
PÓS-PROCESSADOR
308
ANALISADOR
PARTE DE DADOS NÃO-MÍDIA (NÃO-CRIPTOGRAFADA)
332
FONTE DE MULTIMÍDIA

FIG. 3

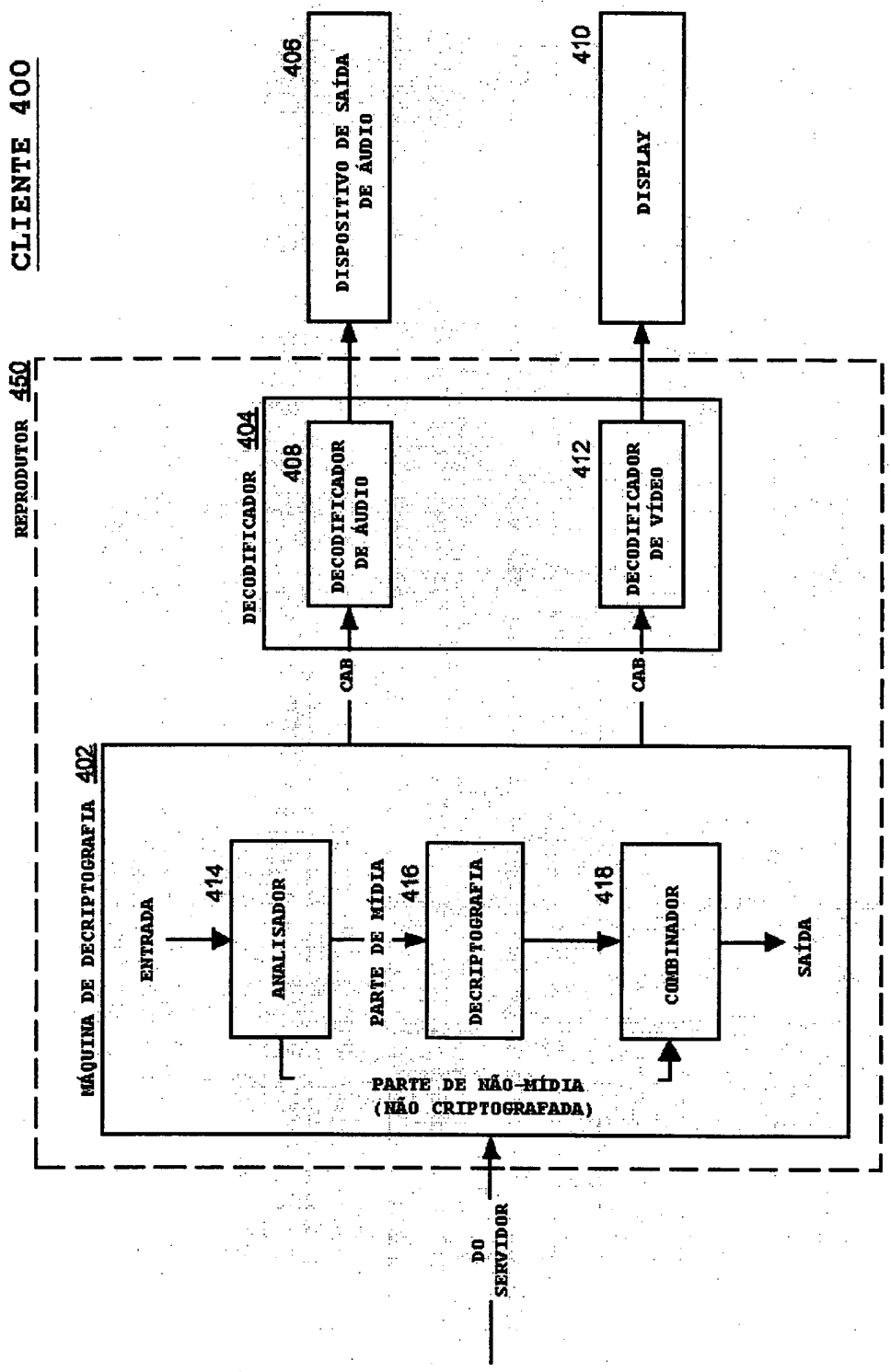

CLIENTE 400
REPRODUTOR 450
406
DISPOSITIVO DE SAÍDA DE ÁUDIO
410
DISPLAY
DECODIFICADOR 404
408
DECODIFICADOR DE ÁUDIO
412
DECODIFICADOR DE VÍDEO
CAB
CAB
MÁQUINA DE DECRIPTOGRAFIA 402
ENTRADA
414
ANALISADOR
PARTE DE MÍDIA
416
DECRIPTOGRAFIA
418
COMBINADOR
SAÍDA
PARTE DE NÃO-MÍDIA
(NÃO CRIPTOGRAFADA)
DO SERVIDOR

FIG. 4

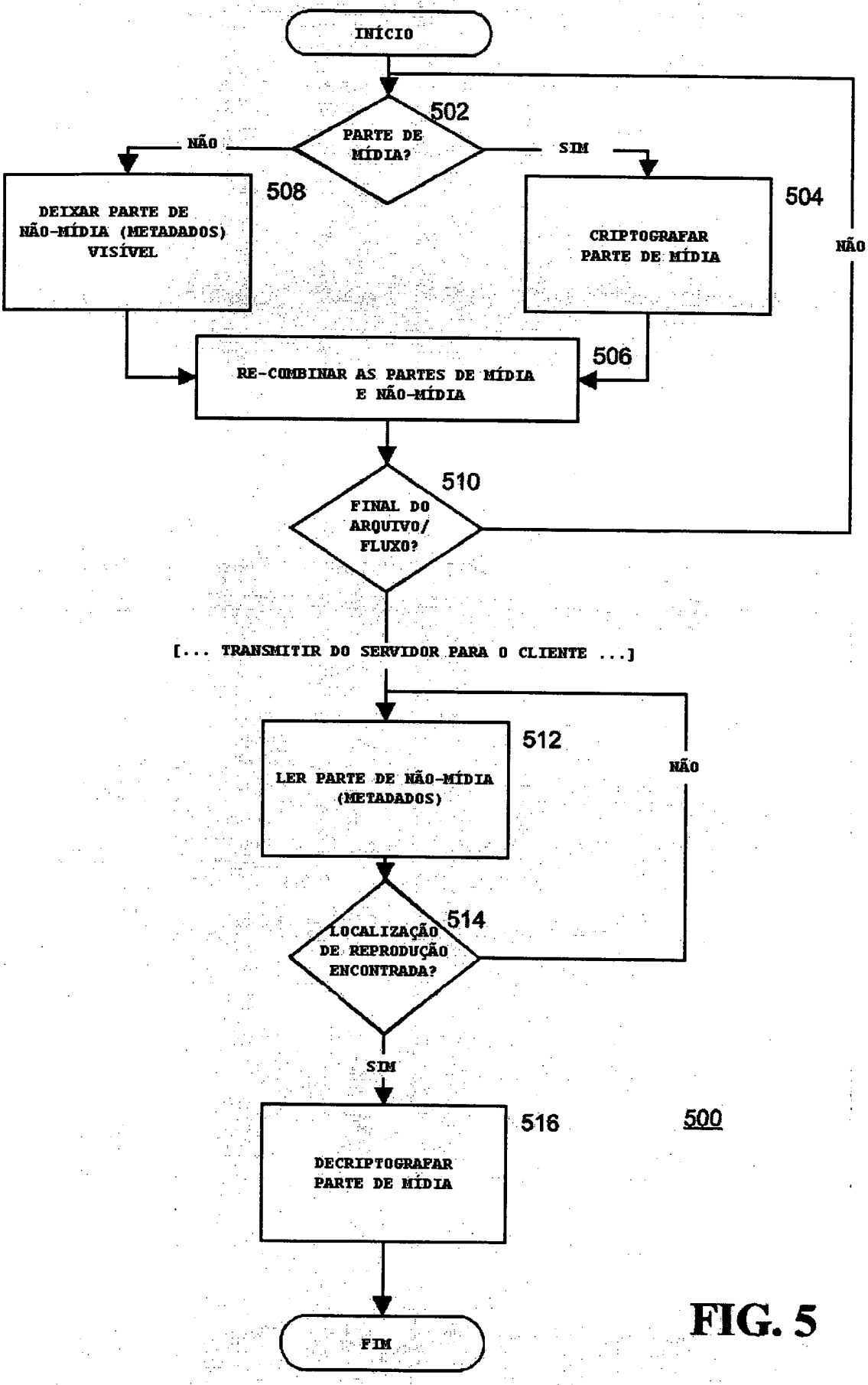

INÍCIO
502
PARTE DE MÍDIA?
NÃO
SIM
508
DEIXAR PARTE DE NÃO-MÍDIA (METADADOS) VISÍVEL
504
CRIPTOGRAFAR PARTE DE MÍDIA
NÃO
506
RE-COMBINAR AS PARTES DE MÍDIA E NÃO-MÍDIA
510
FINAL DO ARQUIVO/ FLUXO?
[... TRANSMITIR DO SERVIDOR PARA O CLIENTE ...]
512
LER PARTE DE NÃO-MÍDIA (METADADOS)
NÃO
514
LOCALIZAÇÃO DE REPRODUÇÃO ENCONTRADA?
SIM
516
DECRIPTOGRAFAR PARTE DE MÍDIA
500
FIM

FIG. 5

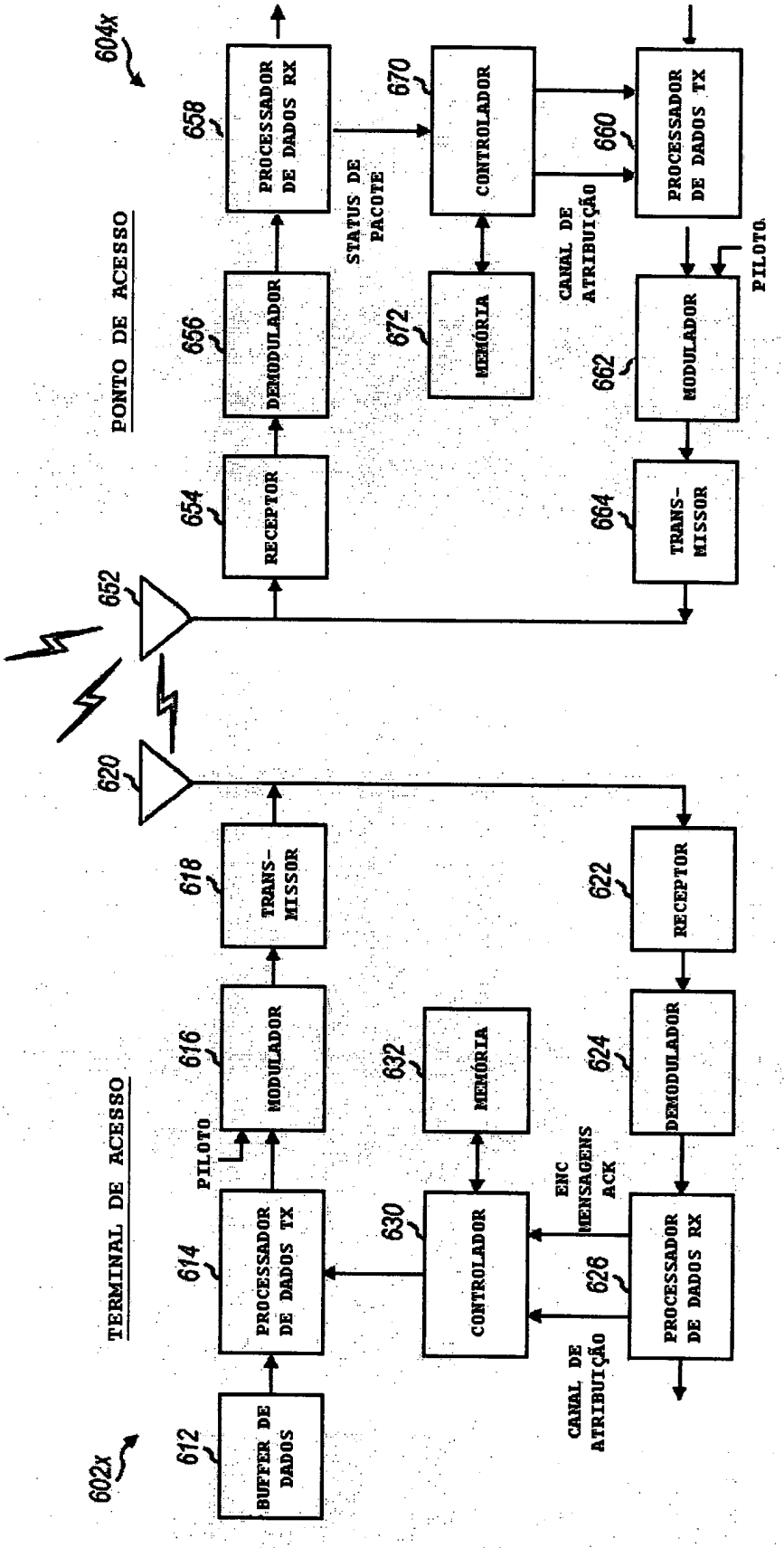

602x
TERMINAL DE ACESSO
612
BUFFER DE DADOS
614
PROCESSADOR DE DADOS TX
616
MODULADOR
618
TRANS-MISSOR
620
652
654
RECEPTOR
656
DEMODULADOR
658
PROCESSADOR DE DADOS RX
604x
PONTO DE ACESSO
630
CONTROLADOR
632
MEMÓRIA
626
622
RECEPTOR
624
DEMODULADOR
PROCESSADOR DE DADOS RX
PILOTO
ENC MENSAGENS ACK
CANAL DE ATRIBUIÇÃO
670
CONTROLADOR
672
MEMÓRIA
660
PROCESSADOR DE DADOS TX
662
MODULADOR
664
TRANS-MISSOR
STATUS DE PACOTE
CANAL DE ATRIBUIÇÃO
PILOTO

FIG. 6

PI0613730-0

RESUMO

"MÉTODO E APARELHO PARA CRIPTOGRAFAR/DECRIPTOGRAFAR CONTEÚDO DE MULTIMÍDIA PARA PERMITIR ACESSO ALEATÓRIO".

Um método é descrito para criptografar um arquivo de multimídia que inclui analisar o arquivo de multimídia para identificar uma parte de dados de mídia; criptografar a parte de dados de mídia; e combinar a parte de dados de mídia criptografada com uma parte de dados não-criptografada e de não-mídia. Um método é também descrito para reproduzir um arquivo de multimídia que inclui analisar o arquivo de multimídia para identificar uma parte de metadados não-criptografada; usar a parte de metadados não-criptografada para localizar uma posição de interesse no arquivo de mídia, a posição de interesse possuindo uma parte de dados de mídia criptografada associada; e decriptografar a parte de dados de mídia criptografada associada. Um aparelho para executar os métodos é também descrito aqui.