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

(21) PI 0718817-0 A2

(22) Data de Depósito: 06/11/2007
(43) Data da Publicação: 03/12/2013
(RPI 2239)

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

(54) Título: MÉTODO E DISPOSITIVO PARA GERENCIAR UMA TRANSMISSÃO DE CHAVES.

(57) Resumo:

(30) Prioridade Unionista: 09/11/2006 EP 06301141.5

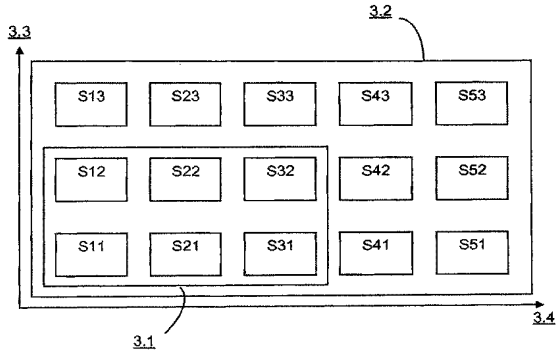
(73) Titular(es): Thomson Licensing

(72) Inventor(es): Alain Durand, Mohamed Karroumi, Stephane Onno

(74) Procurador(es): Nellie Anne Daniel-Shores

(86) Pedido Internacional: PCT EP2007061934 de 06/11/2007

(87) Publicação Internacional: WO 2008/055900de 15/05/2008



"MÉTODO E DISPOSITIVO PARA GERENCIAR UMA TRANSMISSÃO DE CHAVES"

A presente invenção diz respeito a um método para gerenciar uma transmissão de chaves.

A técnica de Escalabilidade de Grão Fino é definida nos padrões MPEG-4 parte 2 e MPEG-2 parte 10. É mencionado daqui por diante MPEG-4 FGS. Ela define um método onde um fluxo de dados é compactado em duas camadas: uma camada de base, a parte não escalável, e uma camada de enriquecimento, a parte escalável. Um receptor do fluxo compactado pode decodificar somente a camada de base ou a camada de base e a camada de enriquecimento. Se somente a camada de base for decodificada, isto resulta em versão de baixa qualidade do conteúdo original. Se uma parte da camada de enriquecimento for decodificada e combinada com a camada de base, isto produz uma qualidade melhorada do conteúdo, proporcional à parte de enriquecimento decodificada. Além disso, a camada de enriquecimento suporta escalabilidade de Relação Sinal de Pico para Ruído, mencionado PSNR, e escalabilidade temporal. Assim, o MPEG-4 FGS fornece flexibilidade em suportar escalabilidade temporal ao aumentar somente a taxa de bits, ou escalabilidade de PSNR enquanto mantendo a mesma taxa de bits, ou ambas as escalabilidades de PSNR e temporal. Escalabilidade de Grão Fino é oferecida pela camada de enriquecimento. A Relação Sinal de Pico para Ruído é uma métrica de qualidade de vídeo de objetivo usada para comparar duas imagens, a qual pode ser computada automaticamente pelo receptor de um vídeo. A taxa de bits é a taxa de bits disponível no receptor para receber o vídeo.

A Criptografia FGS de Múltiplas Camadas Escaláveis, mencionado SMLFE, é um esquema de controle de acesso em camadas que suporta ambas as escalabilidades de PSNR e de taxa de bits simultaneamente para a codificação MPEG-4 FGS. Na SMLFE, a camada de enriquecimento é criptografada em um único fluxo com múltiplos níveis de qualidade divididos de acordo com valores de PSNR e de taxas de bits. Níveis de qualidade mais baixos podem ser acessados e reutilizados por um nível de qualidade mais alto de um mesmo tipo de escalabilidade. A camada de enriquecimento é então composta de diversos segmentos diferentes. Uma chave é gerada por segmento para criptografar cada segmento.

Para acessar o conteúdo compactado MPEG-4 FGS um consumidor necessita das chaves para descriptografar todos os segmentos exigidos. O número de chaves pode ser significativo. Consequentemente, enviar todas as chaves para o consumidor pode ser trabalhoso e acrescentar significativo baixo desempenho ao conteúdo transmitido. É então desejável fornecer um esquema de gerenciamento de chave eficiente.

A presente invenção diz respeito a um método para gerenciar as chaves de criptografia e capacitar um receptor para descriptografar todos os segmentos na camada de enriquecimento correspondendo à qualidade exigida enquanto todos os outros segmentos ficam

ainda inacessíveis para o consumidor. Ela focaliza o sistema de gerenciamento de chave visando criptografar e descriptografar de forma eficiente fluxos complementares.

Ela se aplica notavelmente ao campo de MPEG-4 FGS, mas também de uma maneira mais geral a outros campos onde quadros codificados criptografados são transmitidos.

Com esta finalidade, a invenção diz respeito a um método para criptografar um quadro de aperfeiçoamento escalável codificado enviado por um emissor para um receptor, o quadro de aperfeiçoamento compreendendo uma pluralidade de fluxos complementares ordenados em termo de nível de qualidade, cada fluxo complementar correspondendo a uma combinação de mais de um tipo de escalabilidade, onde um fluxo complementar de um nível de qualidade mais baixo corresponde a uma qualidade mais baixa em cada tipo de escalabilidade, compreendendo no nível do emissor as etapas de gerar uma chave por fluxo complementar para criptografar o fluxo complementar de uma tal maneira que todos os tipos de escalabilidade podem ser usados simultaneamente ou de forma individual, as ditas chaves sendo geradas de uma tal maneira que somente as chaves dos fluxos complementares de níveis de qualidade mais baixos do que o nível de qualidade de um fluxo complementar podem ser obtidas a partir da chave do dito fluxo complementar, e enviar a chave de um fluxo complementar correspondendo a um nível de qualidade para o receptor, a chave permitindo a um receptor gerar somente as chaves dos fluxos complementares dos níveis de qualidade mais baixos.

Recursos desejados tais como alta segurança, baixa complexidade e pouco baixo desempenho de dados são fornecidos. Ter alta segurança para um esquema de criptografia e para o seu sistema de gerenciamento de chave relacionado é essencial, entretanto, isto é feito de uma maneira geral com um custo de complexidade e de baixo desempenho de dados. Um método de baixa complexidade é um método que usa tão poucas chaves quanto possível, tamanhos de chaves pequenos e ainda trabalha com dispositivos de potência de computação limitada. Pouco baixo desempenho de dados significa um método que não acrescenta baixo desempenho significativo com os fluxos misturados. O processo de geração de chave permite gerar todas as chaves subsequentes a partir de uma única chave. O servidor somente necessita enviar uma chave para o receptor de maneira que o receptor deduz as chaves permitidas. Isto exige pouco baixo desempenho de dados.

De acordo com uma modalidade, antes de enviar a chave de um fluxo complementar correspondendo a um nível de qualidade, o método compreende a etapa de receber uma solicitação de um receptor para a dita recepção de nível de qualidade do fluxo.

De acordo com uma modalidade, a etapa de gerar uma chave por fluxo complementar compreende as etapas de gerar uma chave aleatória do fluxo complementar do nível de qualidade mais alto, e obter as chaves dos fluxos complementares dos níveis de qualidade mais baixos ao aplicar sucessivamente pelo menos um algoritmo de permutação unidire-

cional à chave aleatória.

Uma única função permite gerar todas as chaves subsequentes. Isto exige poucos recursos computacionais.

Particularmente, em uma combinação de dois tipos de escalabilidade, uma primeira escalabilidade e uma segunda escalabilidade, a etapa de obter a chave do fluxo complementar de um nível de qualidade mais baixo, para um dado primeiro nível de escalabilidade, compreende a etapa de dividir a chave de um nível em uma parte esquerda e uma parte direita, aplicar o algoritmo de permutação unidirecional à parte direita da chave, e concatenar a parte esquerda da chave com a parte direita obtida para obter a chave do nível de qualidade mais baixo.

De forma similar, em uma combinação de dois tipos de escalabilidade, uma primeira escalabilidade e uma segunda escalabilidade, a etapa de obter a chave do fluxo complementar de um nível de qualidade mais baixo para um dado segundo nível de escalabilidade compreende a etapa de dividir a chave de um nível em uma parte esquerda e uma parte direita, aplicar o algoritmo de permutação unidirecional à parte esquerda da chave, e concatenar a parte direita obtida com a parte esquerda da chave para obter a chave do nível de qualidade mais baixo.

A invenção também diz respeito a um método para calcular chaves de descriptografia pretendidas para descriptografar um quadro de aperfeiçoamento escalável codificado, o quadro de aperfeiçoamento compreendendo uma pluralidade de fluxos complementares ordenados em termos de nível de qualidade, cada fluxo complementar correspondendo a uma combinação de mais de um tipo de escalabilidade, onde um fluxo complementar de um nível de qualidade mais baixo corresponde a uma qualidade mais baixa em cada tipo de escalabilidade, compreendendo no nível do receptor as etapas de receber a chave do fluxo complementar correspondendo a um nível de qualidade exigido e gerar, a partir da chave recebida, as chaves subsequentes somente dos fluxos complementares correspondendo aos níveis de qualidade mais baixos.

O receptor não necessita receber todas as chaves para todos os fluxos complementares. Ele recebe uma única chave que permite gerar somente as chaves autorizadas.

De acordo com uma modalidade, o método compreende a etapa de receber a chave do fluxo complementar, e compreende a etapa de indicar a dita recepção de nível de qualidade exigido do fluxo.

De acordo com uma modalidade, a etapa de gerar as chaves subsequentes compreende uma etapa de aplicar sucessivamente um algoritmo de permutação unidirecional à chave recebida.

A invenção também diz respeito a um dispositivo para criptografar um quadro de aperfeiçoamento escalável codificado compreendendo uma pluralidade de fluxos comple-

complementares ordenados em termos de nível de qualidade, cada fluxo complementar correspondendo a uma combinação de mais de um tipo de escalabilidade, onde um fluxo complementar de um nível de qualidade mais baixo corresponde a uma qualidade mais baixa em cada tipo de escalabilidade, o dispositivo compreendendo dispositivo de criptografia para gerar uma chave aleatória do fluxo complementar do nível de qualidade mais alto, para gerar as chaves dos fluxos complementares dos níveis de qualidade mais baixos ao aplicar sucessivamente pelo menos um algoritmo de permutação unidirecional à chave aleatória.

A invenção também diz respeito a um dispositivo para descriptografar um quadro de aperfeiçoamento escalável codificado compreendendo uma pluralidade de fluxos complementares ordenados em termos de nível de qualidade, cada fluxo complementar correspondendo a uma combinação de mais de um tipo de escalabilidade, onde um fluxo complementar de um nível de qualidade mais baixo corresponde a uma qualidade mais baixa em cada tipo de escalabilidade, o dispositivo compreendendo dispositivo de descriptografia para gerar, a partir de uma chave recebida, as chaves subsequentes somente dos fluxos complementares correspondendo aos níveis de qualidade mais baixos.

Um outro objetivo da invenção é um produto de programa de computador compreendendo instruções de código de programa para executar as etapas dos processos de acordo com a invenção, quando esse programa é executado em um computador. Por "produto de programa de computador" é pretendido significar um suporte de programa de computador, o qual pode consistir não somente de um espaço de armazenamento contendo o programa, tal como um disquete ou um cassete, mas também de um sinal, tal como um sinal elétrico ou ótico.

A invenção será mais bem entendida e ilustrada por meio da modalidade e exemplos de execução seguintes, em nenhum modo limitativos, com referência às figuras anexas, nas quais:

- A figura 1 representa um fluxo dividido em um fluxo de base e dois fluxos complementares;

- A figura 2 mostra a criptografia dos fluxos complementares codificados escaláveis;

- A figura 3 é um diagrama de blocos que representa uma camada de enriquecimento escalável;

- A figura 4 ilustra os diferentes modos para usar escalabilidade na camada de enriquecimento;

- A figura 5 é um fluxograma do método para criptografar e descriptografar; e

- A figura 6 representa o sistema da modalidade.

Na figura 6, os blocos representados são puramente entidades funcionais, os quais não correspondem necessariamente a entidades separadas fisicamente. Isto é, eles podem ser desenvolvidos na forma de software, ou serem implementados em um ou em diversos

circuitos integrados.

A modalidade exemplar ocorre dentro da estrutura do MPEG-4 FGS, mas a invenção não está limitada a este ambiente particular e pode ser aplicada dentro de outras estruturas onde um conjunto de quadros codificados criptografados é transmitido.

Existem múltiplos modos de separar um serviço digital transmitido como componentes distintos, estes componentes sendo transmitidos por meio de um fluxo particular de cliente. Por exemplo, é possível usar codificadores incrementais que codificam um serviço, ou um componente do último tal como o vídeo, na forma de um primeiro fluxo de pequena largura de banda, chamado de fluxo de base, e de fluxos complementares. O fluxo de base é de uma maneira geral suficiente para permitir a restituição do serviço em um modo de transmissão degradado. Ele pode ser sempre decodificado independentemente. No que diz respeito a vídeo, este serviço de base pode conter uma versão de baixa definição do vídeo. O mesmo é possível com relação ao áudio. Os fluxos complementares enviam a informação perdida pelo fluxo de base tornando possível restaurar o serviço em um modo não degradado. Um fluxo complementar somente pode ser decodificado juntamente com o fluxo mais baixo.

Um serviço como este, ou pelo menos seu componente de vídeo, está representado na figura 1. O vídeo completo 1 está decomposto em um primeiro fluxo de base 1.1 e uma camada de enriquecimento escalável, compreendendo os dois fluxos complementares referenciados como 1.2 e 1.3. O fluxo de base torna possível reconstituir o vídeo em uma primeira resolução baixa. A decodificação do fluxo de base e do fluxo complementar 1 torna possível restaurar um vídeo para uma resolução intermediária. A decodificação dos três fluxos torna possível restaurar o vídeo completo na sua melhor resolução.

De fato, codificação de fluxos complementares é escalável enquanto que a codificação de fluxo de base em geral não é escalável. Em termos de criptografia, uma chave é suficiente para criptografar a camada de base e um esquema de gerenciamento de chave não é necessário para o fluxo de base. Diversas chaves são necessárias para criptografar os fluxos complementares e um esquema de gerenciamento de chave é usualmente necessário. A criptografia dos fluxos complementares codificados escaláveis está ilustrada pela figura 2. A modalidade propõe um esquema que permite criptografar os fluxos complementares codificados escaláveis 2.1 em fluxos complementares criptografados 2.2 onde estes fluxos criptografados permanecem escaláveis. A criptografia 2.3 é aplicada à parte de vídeo clara 2.1 para fornecer uma parte de vídeo criptografada.

Codificação MPEG-4 FGS é definida no padrão MPEG-4 parte 2 ISO/IEC 14496-2:2003. Em FGS, fluxo de dados é codificado e compactado em duas camadas, uma camada de base, a parte não escalável, e a camada de enriquecimento, a parte escalável. Se somente a camada de base for decodificada, isto resulta em versão de baixa qualidade do

conteúdo original. Se, entretanto, uma parte da camada de enriquecimento for decodificada, combinada com a camada de base, isto produz uma qualidade melhorada do conteúdo, proporcional à parte de enriquecimento decodificada. Além disso, a camada de enriquecimento suporta tanto escalabilidade de PSNR quanto temporal. A figura 3 é um diagrama de blocos que representa um serviço como este, onde o vídeo completo é decomposto em uma camada de base não representada e na camada de enriquecimento escalável 3.2, a qual compreende múltiplos fluxos complementares baseados em duas escalabilidades, a de PNSR 3.3 e a de taxa de bits 3.4. Cada camada de enriquecimento é particionada em T níveis de PSNR e M níveis de taxa de bits independentemente. Uma camada de enriquecimento é então composta de M*T segmentos diferentes, ou fluxos complementares. Na figura 3, T=3 e M=5, e cada segmento $S_{m,t}$, onde m pertence a {1,..,M} e t a {1,..,T}, é na interseção de um nível de PSNR e um nível de taxa de bits.

Uma qualidade de conteúdo MPEG-4 FGS pode depender tanto de taxa de bits de escalabilidade temporal quanto de escalabilidade de PSNR. Para uma qualidade solicitada, um provedor de conteúdo pode dar acesso a uma certa camada de nível usando somente camadas de taxa de bits, usando somente camadas de PSNR enquanto mantendo o mesmo nível para a taxa de bits ou pelo uso de ambas as camadas de PSNR e de taxa de bits simultaneamente. Assim, existem três modos para obter a mesma qualidade de conteúdo. Isto está ilustrado pela figura 4 que representa os mesmos tipos de diagrama de blocos tais como o diagrama indicado na figura 3. Em 4.1 somente a escalabilidade de taxa de bits é usada enquanto mantendo o mesmo nível para a PSNR. Em 4.2 somente a escalabilidade de PSNR é usada enquanto mantendo o mesmo nível para a taxa de bits. Em 4.3 ambas as escalabilidades são usadas simultaneamente. O uso de ambas as escalabilidades permite dar para um usuário acesso a somente alguns segmentos em uma fileira ou em uma coluna sem necessariamente dar acesso a todos os segmentos nessa fileira ou coluna. De fato, o provedor de conteúdo pode dar acesso aos segmentos S1,1, S2,1, S3,1, S1,2, S2,2, S3,2 enquanto mantendo, por exemplo, S4,1, S5,1, S4,2, S5,2 inacessíveis para o consumidor. Em 4.1 e 4.2 quando somente um tipo de escalabilidade é usado, se o consumidor tiver o direito de acessar um segmento em uma camada de um dado tipo de qualidade, então ele tem o direito de acessar todos os segmentos nessa camada. Em 4.1 o consumidor tem o direito de acessar a taxa de bits de nível 2, e consequentemente qualquer segmento na camada com uma taxa de bits de nível 2 e abaixo, tal como indicado em 4.1.1. Em 4.2 o consumidor tem o direito de acessar a PSNR de nível 2, e consequentemente qualquer segmento na camada com um PSNR de nível 2 e abaixo, tal como indicado em 4.2.1.

O esquema de criptografia da modalidade permite usar estes três modos para acessar camada de enriquecimento criptografada. Ele permite manter a escalabilidade com segmentos criptografados. Ele não exige descriptografar qualquer segmento da camada de

enriquecimento para ser capaz de usar a escalabilidade. O gerenciamento de chave é então flexível e a escalabilidade MPEG 4 FGS pode ser inteiramente explorada com o conteúdo criptografado. Todos os tipos de escalabilidade podem ser usados simultaneamente ou de forma individual.

O esquema de controle de acesso por camada de Criptografia FGS de Múltiplas Camadas Escaláveis, anotado SMLFE, suporta ambas as escalabilidades de PSNR e de taxa de bits simultaneamente para a codificação MPEG-4 FGS. SMLFE está definida no documento, de C. Yuan, B. B. Zhu, M. Su, X. Wang, S. Li, e Y. Zhong, "Layered Access Control for MPEG-4 FGS Video", IEEE Int. Conf. Image Processing, Barcelona, Espanha, setembro de 2003, vol. 1, pp. 517 - 520. Em SMLFE, a camada de enriquecimento é criptografada em um único fluxo com múltiplos níveis de qualidade divididos de acordo com valores de PSNR e de taxas de bits. Níveis de qualidade mais baixos podem ser acessados e reutilizados por um nível de qualidade mais alto do mesmo tipo de escalabilidade, mas não vice-versa. A proteção dos dois diferentes tipos de escalabilidade é ortogonal, isto é, um direito de acessar um nível de um tipo de escalabilidade não torna os níveis do outro tipo de escalabilidade também acessíveis.

Cada segmento da figura 3 é criptografado com uma chave de segmento correspondente, $K_{m,t}$, não representada. Em tal caso, M*T chaves são geradas aleatoriamente para criptografar todos os segmentos pelo transmissor do vídeo. Estas chaves têm que ser gerenciadas e enviadas para o receptor do vídeo para acessar o conteúdo compactado MPEG-4 FGS.

O método para criptografar e descriptografar os segmentos assim como o método para gerar as chaves de criptografia de acordo com a modalidade é agora descrito. A codificação e criptografia são executadas no servidor, ou no transmissor. A decodificação e descriptografia são executadas no cliente, ou no receptor do vídeo.

Tal como no contexto de SMLFE, a camada de enriquecimento é composta de M*T segmentos diferentes. Cada chave $K_{m,t}$ diferente é usada para criptografar um segmento $S_{m,t}$ onde m pertence a {1,..,M} e t a {1,..,T}. $S_{M,T}$ é o segmento de qualidade mais alta para ambos os tipos de escalabilidade.

No servidor, uma chave é primeiramente gerada de forma aleatória. Ela corresponde à chave $K_{M,T}$ do segmento de qualidade mais alta $S_{M,T}$. Esta chave é dividida em duas metades, um lado esquerdo e um lado direito. Consequentemente, a chave associada a um segmento de qualidade de PSNR mais baixa é obtida ao concatenar o lado esquerdo da chave $K_{M,T}$ com o resultado de lado direito da chave $K_{M,T}$ por meio de uma permutação unidirecional. E a chave associada a um segmento de qualidade de taxa de bits mais baixa é obtida ao concatenar o resultado da chave $K_{M,T}$ de lado esquerdo, por meio de uma permutação unidirecional, com a chave $K_{M,T}$ de lado direito. Pela repetição do processo da mesma

maneira, até computar $K_{1,1}$ a chave de criptografia do segmento de qualidade mais baixa $S_{1,1}$, todas as chaves $K_{m,t}$ para m = 1,..,M e t = 1,..,T são assim obtidas.

Explicitamente, deixamos h ser uma permutação unidirecional. Dada uma chave K, $h^n(K)$ indica o resultado depois de aplicar n vezes a permutação unidirecional h a K. Deixamos $K_{M,T}$ ser a chave de criptografia de um dado segmento $S_{m,t}$ na camada de enriquecimento, cuja chave é gerada respeitando o seguinte procedimento:

- Gerar aleatoriamente $K_{M,T} = (LK_{M,T} \,||\, RK_{M,T})$ onde $LK_{M,T}$ representa o valor de chave de lado esquerdo, $RK_{M,T}$ o valor de chave de lado direito e o símbolo $||$ representa a concatenação.

- Computar as diferenças M-m = x, e T-t = y.

- Produzir as chaves $K_{m,t}$ usando a seguinte equação de geração de chave: $K_{m,t} = (h^x(LK_{M,T}) \,||\, h^y(RK_{M,T}))$.

Na modalidade, as chaves $Km_{,t}$ são longas de 128 bits, com $h^x(LK_{M,T})$ e $h^y(RK_{M,T})$ sendo longas de 64 bits.

Para evitar ter a mesma chave de segmento para segmentos diferentes, o valor de metade direita de $K_{M,T}$ será diferente do valor de metade esquerda. De outro modo a chave $K_{M,T}$ é regenerada até obter uma chave bem apropriada.

De volta aos segmentos indicados na figura 3, $S_{5,3}$ é o segmento de qualidade mais alta para ambas as escalabilidades de PSNR e de taxa de bits.

Primeiro, a chave de segmento associada $K_{5,3}$ é gerada aleatoriamente.

A seguir, esta chave é dividida em duas metades $K_{5,3} = (LK_{5,3} \,||\, RK_{5,3})$ e processada usando uma permutação unidirecional h, para obter todas as outras chaves.

A Tabela 1 mostra como todas as outras chaves de segmento são obtidas com a equação de geração de chave definida anteriormente.

Tabela 1

Nível	t = 1	t = 2	t = 3
m = 1	$K_{1,1} = \left(h^4\left(L_{K5,3}\right) \middle\| h^2\left(R_{K5,3}\right)\right)$	$K_{1,2} = \left(h^4\left(L_{K5,3}\right) \middle\| h\left(R_{K5,3}\right)\right)$	$K_{1,3} = \left(h^4\left(L_{K5,3}\right) \middle\| R_{K5,3}\right)$
m = 2	$K_{2,1} = \left(h^3\left(L_{K5,3}\right) \middle\| h^2\left(R_{K5,3}\right)\right)$	$K_{2,2} = \left(h^3\left(L_{K5,3}\right) \middle\| h\left(R_{K5,3}\right)\right)$	$K_{2,3} = \left(h^3\left(L_{K5,3}\right) \middle\| R_{K5,3}\right)$
m = 3	$K_{3,1} = \left(h^2\left(L_{K5,3}\right) \middle\| h^2\left(R_{K5,3}\right)\right)$	$K_{3,2} = \left(h^2\left(L_{K5,3}\right) \middle\| h\left(R_{K5,3}\right)\right)$	$K_{3,3} = \left(h^2\left(L_{K5,3}\right) \middle\| R_{K5,3}\right)$
m = 4	$K_{4,1} = \left(h\left(L_{K5,3}\right) \middle\| h^2\left(R_{K5,3}\right)\right)$	$K_{4,2} = \left(h\left(L_{K5,3}\right) \middle\| h\left(R_{K5,3}\right)\right)$	$K_{4,3} = \left(h\left(L_{K5,3}\right) \middle\| R_{K5,3}\right)$
m = 5	$K_{5,1} = \left(L_{K5,3} \middle\| h^2\left(R_{K5,3}\right)\right)$	$K_{5,2} = \left(L_{K5,3} \middle\| h\left(R_{K5,3}\right)\right)$	$K_{5,3} = \left(L_{K5,3} \middle\| R_{K5,3}\right)$

Quando um receptor adquire direitos para conteúdo com uma certa qualidade, a chave associada ao segmento de qualidade mais alta da qualidade solicitada é computada pelo transmissor e enviada para o receptor. Vamos considerar que este segmento de quali-

dade mais alta é $S_{3,2}$ com $K_{3,2}$ a sua chave associada. As diferenças M - m = 5 - 3 e T - t = 3 - 2 são respectivamente iguais a 2 e 1. $K_{3,2} = (h^2(LK_{5,3}) \,||\, h(RK_{5,3}))$ é a chave de segmento computada de $K_{5,3}$ pelo transmissor usando a equação de geração de chave definida anteriormente e um algoritmo de permutação unidirecional. $K_{3,2}$ é enviada para o receptor. No receptor, os segmentos acessíveis são $S_{3,2}$, $S_{3,1}$, $S_{2,2}$, $S_{2,1}$, $S_{1,2}$ e $S_{1,1}$, tal como indicado em 3.1 na figura 3. Isto é, se o segmento de qualidade mais alta for $S_{m,t}$, os segmentos acessíveis serão $S_{u,v}$, onde $1 \leq u \leq m$ e $1 \leq v \leq t$.

$K_{3,2}$ é recebida pelo receptor e é dividida em duas metades $LK_{3,2}$ e $RK_{3,2}$. As chaves de segmento $K_{3,1}$, $K_{2,2}$, $K_{2,1}$, $K_{1,2}$ e $K_{1,1}$ são então obtidas pela dispersão e concatenação de $LK_{3,2}$ e $RK_{3,2}$. Isto é feito usando o mesmo algoritmo de permutação unidirecional tal como o algoritmo usado pelo transmissor. O processo é repetido até computar todas as chaves de segmento. As chaves computadas são obtidas de $K_{3,2}$ tal como indicado na tabela 2.

Tabela 2

Nível	t = 1	t = 2
m = 1	$K_{1,1}=(h(LK_{2,2})\|\|h(RK_{2,2}))=(h^2(LK_{3,2})\|\|h(RK_{3,2}))$	$K_{1,2}=(h(LK_{2,2})\|\|RK_{2,2})=(h^2(LK_{3,2})\|\|h(RK_{3,2}))$
m = 2	$K_{2,1}=(h(LK_{3,2})\|\|h(RK_{3,2}))$	$K_{2,2}=(h(LK_{3,2})\|\|(RK_{3,2}))$
m = 3	$K_{3,1}=(LK_{3,2}\|\|h(RK_{3,2}))$	$K_{3,2}$

Um direito de acessar um nível de qualidade fornece também o direito de acessar níveis de qualidade mais baixos para as diferentes escalabilidades de PSNR ou de taxa de bits ao dispersar respectivamente lado direito ou esquerdo da chave de segmento. Graças ao critério unidirecional da função de dispersão, e ao fato de que uma função de dispersão não é injectiva, níveis de qualidade mais altos não são acessíveis. Se o segmento de qualidade mais alta for $S_{m,t}$, os segmentos $S_{u,v}$, onde $m < u$ ou $t < v$. A segurança do esquema de gerenciamento de chave conta essencialmente com a escolha e robustez da função de dispersão.

O método para criptografar e descriptografar está resumido na figura 5.

Etapa S1. O servidor gera uma chave aleatória, e chaves subsequentes a partir da chave aleatória.

Etapa S2. O receptor envia uma solicitação para a recepção do conteúdo em um nível de qualidade. O servidor recebe a solicitação e deduz o segmento de comparação da qualidade mais alta.

Etapa S3. O servidor envia a chave correspondendo ao segmento de comparação da qualidade mais alta para o receptor.

Etapa S4. O receptor recebe a chave e gera as chaves correspondentes aos segmentos acessíveis.

Tal como descrito anteriormente, uma função de permutação unidirecional exclusiva é usada em cada lado. Em vez de uma permutação unidirecional diferente ser usada para o lado direito e para o lado esquerdo. A equação para geração de chave seria então, com as funções h1 e h2: $K_{m,t} = (h1^{x}(LK_{M,T})||h2^{y}(RK_{M,T}))$.

Na modalidade, $K_{M,T}$ é obtida com a concatenação de $LK_{M,T}$ e $RK_{M,T}$, onde $LK_{M,T}$ representa o valor de chave de lado esquerdo e $RK_{M,T}$ o valor de chave de lado direito. Alternativamente, $LK_{M,T}$ pode representar o bits pares e $RK_{M,T}$ os bits ímpares de $LK_{M,T}$.

Uma permutação unidirecional é uma função que é muito mais fácil de computar em uma direção do que na direção inversa; isto é, se uma saída for obtida com uma permutação unidirecional em uma entrada, é desconfortável obter a entrada de volta dada a saída. Pode ser possível, por exemplo, computar a função na direção para frente em segundos, mas para computar seu inverso pode levar meses ou anos, se possível de algum modo. Vários algoritmos de permutação unidirecional que podem ser usados:

- Funções de dispersão bem conhecidas na técnica, tais como MD5, RIPEMD-160 ou SHA1.

- Geradores de números pseudoaleatórios, mencionado PRNG, bem conhecidos na técnica, tais como Mersenne Twister, ISAAC... Uma chave de segmento, ou a parte da chave de segmento, é usada como uma semente para o PRNG, h(K) = PRNG (K). A saída pode ser truncada para ajustar um tamanho predefinido.

- Cifradores simétricos: cifrador de bloco ou cifrador de fluxo, tal como DES ou RC4. Cifradores simétricos exigem duas entradas, uma mensagem e chave, mas quando usados como uma permutação unidirecional as duas entradas podem ser idênticas. Na nossa invenção, quando um cifrador simétrico é aplicado a uma chave de segmento K, K é usada tanto como a mensagem para criptografar quanto a chave usada para criptografia. Nesse caso $h(K) = E_{\{K\}}(K)$.

- Logaritmo Discreto ou algoritmo de criptografia de chave pública RSA:

- Com referência a Logaritmo Discreto, um gerador g de um grupo multiplicativo Z^{*}_{p} é escolhido, onde p é um número primo grande. Uma chave de segmento associada a um segmento de qualidade mais baixa é obtida pela exponenciação de g (módulo p) com o valor da chave de segmento de qualidade mais alta. Nesse caso $h(K) = g^{K}$ mód p.

Com referência a RSA, valores públicos (e, n) são gerados, onde n é produto de dois números primos e "e" o expoente público (a chave privada é descartada). Uma chave de segmento associada a um segmento de qualidade mais baixa é obtida pela exponenciação do valor da chave de segmento de qualidade mais alta K pelo expoente público "e" (módulo n). Nesse caso $h(K) = K^{e}$ mód n.

A propriedade necessária para a permutação é somente o critério unidirecional. O fato de que existem algumas colisões, tal como para MD5, por exemplo, não tem conse-

quências na segurança.

A modalidade diz respeito a uma camada de enriquecimento que suporta ambas as escalabilidades de PSNR e de taxa de bits. De fato é aplicável a mais de duas escalabilidades. Com N escalabilidades a chave transmitida $K_{M,T}$ é dividida em N partes, e chaves subsequentes são geradas usando uma permutação unidirecional em cada parte sucessivamente.

A figura 6 representa o sistema da modalidade, compreendendo um servidor 5.1, também chamado de remetente, um cliente 5.2, também chamado de receptor, conectado ao servidor através de uma rede 5.3. O servidor envia o conteúdo de vídeo criptografado para o cliente. A rede é, por exemplo, a Internet. O servidor é o transmissor do vídeo. O cliente é o receptor do vídeo.

O servidor compreende o dispositivo de compactação 5.1.5 para compactar o fluxo e gerar a camada de base e as camadas de enriquecimento subsequentes de acordo com a modalidade. Ele também compreende dispositivo de criptografia 5.1.2 para gerar chaves de criptografia de acordo com a modalidade e criptografar os segmentos. Ele compreende o dispositivo de comunicação 5.1.3 para enviar o fluxo através da rede para os clientes. O servidor compreende o dispositivo de processamento 5.1.1 e o dispositivo de armazenamento 5.1.4 para armazenar programas que executam algoritmos de compressão e algoritmos de criptografia. O servidor compreende um barramento interno 5.1.6 para transmitir os dados internamente.

O cliente compreende o dispositivo de descompactação 5.2.5 para descompactar o fluxo. Ele compreende o dispositivo de descriptografia 5.2.2 para gerar as chaves de criptografia de acordo com a modalidade e descriptografar os segmentos criptografados. Ele compreende o dispositivo de comunicação 5.2.3 para receber o fluxo do servidor através da rede. O servidor compreende o dispositivo de processamento 5.2.1 e o dispositivo de armazenamento 5.2.4 para armazenar programas que executam algoritmos de descompressão e algoritmos de descriptografia. O cliente compreende um barramento interno 5.2.6 para transmitir os dados internamente.

REIVINDICAÇÕES

1. Método para criptografar um quadro de aperfeiçoamento escalável codificado (3.2) enviado por um emissor (5.1) para um receptor (5.2), o dito quadro de aperfeiçoamento compreendendo uma pluralidade de fluxos complementares ordenados em termos de nível de qualidade, cada fluxo complementar correspondendo a uma combinação de mais de um tipo de escalabilidade, onde um fluxo complementar de um nível de qualidade mais baixo corresponde a uma qualidade mais baixa em cada tipo de escalabilidade, o dito método sendo **CARACTERIZADO** pelo fato de que compreende, no nível do emissor (5.1), as etapas de:

- Gerar uma chave aleatória ($K_{M,T}$) correspondendo à chave do fluxo complementar do nível de qualidade mais alto ($S_{M,T}$);

- Obter as chaves ($K_{I,J}$) dos fluxos complementares dos níveis de qualidade mais baixos ($S_{I,J}$) ao aplicar sucessivamente uma função unidirecional (h) à chave aleatória ($K_{M,T}$), onde a saída de função unidirecional é diferente de cada tipo de escalabilidade; e

- Enviar (S3) a chave ($K_{m,t}$) de um fluxo complementar correspondendo a um nível de qualidade para o receptor, a dita chave permitindo a um receptor gerar somente as chaves dos fluxos complementares dos níveis de qualidade mais baixos.

2. Método, de acordo com a reivindicação anterior, **CARACTERIZADO** pelo fato de que na etapa de obter a chave, a chave aleatória ($K_{M,T}$) é separada em um número de partes ($L_{KM,T}$, $R_{KM,T}$) correspondendo ao número de tipos de escalabilidade, e uma chave subsequente ($K_{M-I,\ T-J}$) é gerada utilizando a função unidirecional em cada parte sucessivamente ($h^{M-I}(L_{KM,\ T})||h^{T-J}(R_{KM,\ T})$).

3. Método, de acordo com a reivindicação 1 ou 2, **CARACTERIZADO** pelo fato de que, antes de enviar a chave de um fluxo complementar correspondendo a um nível de qualidade, compreende a etapa de receber (S2) uma solicitação de um receptor para a dita recepção de nível de qualidade do fluxo.

4. Método, de acordo com qualquer reivindicação anterior, **CARACTERIZADO** pelo fato de que, em uma combinação de dois tipos de escalabilidade, uma primeira escalabilidade e uma segunda escalabilidade, a etapa de obter a chave do fluxo complementar de um nível de qualidade mais baixo para um dado primeiro nível de escalabilidade compreende a etapa de:

- Dividir a chave de um nível em uma parte esquerda e uma parte direita;

- Aplicar a função unidirecional à parte direita da chave; e

- Concatenar a parte esquerda da chave com a parte direita obtida para obter a chave do nível de qualidade mais baixo.

5. Método, de acordo com qualquer reivindicação anterior, **CARACTERIZADO** pelo fato de que, em uma combinação de dois tipos de escalabilidade, uma primeira escalabilida-

de e uma segunda escalabilidade, a etapa de obter a chave do fluxo complementar de um nível de qualidade mais baixo para um dado segundo nível de escalabilidade compreende a etapa de:

- Dividir a chave de um nível em uma parte esquerda e uma parte direita;
- Aplicar a função unidirecional à parte esquerda da chave; e

Concatenar a parte direita obtida com a parte esquerda da chave para obter a chave do nível de qualidade mais baixo.

6. Método, de acordo com qualquer reivindicação anterior, **CARACTERIZADO** pelo fato de que uma função unidirecional diferente é utilizada para cada tipo de escalabilidade.

7. Método para calcular chaves de descriptografia pretendido para descriptografar um quadro de aperfeiçoamento escalável codificado, o dito quadro de aperfeiçoamento compreendendo uma pluralidade de fluxos complementares ordenados em termos de nível de qualidade, cada fluxo complementar correspondendo a uma combinação de mais de um tipo de escalabilidade, onde um fluxo complementar de um nível de qualidade mais baixo corresponde a uma qualidade mais baixa em cada tipo de escalabilidade, o dito método sendo **CARACTERIZADO** pelo fato de que compreende no nível do receptor (5.2) as etapas de:

- Receber (S3) a chave ($K_{m,t}$) do fluxo complementar correspondendo a um nível de qualidade exigido ($S_{m,t}$); e
- Gerar (S4), a partir da chave recebida, as chaves subsequentes somente dos fluxos complementares correspondendo aos níveis de qualidade mais baixos ao aplicar sucessivamente uma função unidirecional (h) à chave recebida, onde a saída da função unidirecional é diferente para cada tipo de escalabilidade.

8. Método, de acordo com a reivindicação anterior, **CARACTERIZADO** pelo fato de que, antes da etapa de receber (S3) a chave do fluxo complementar, compreende a etapa de indicar (S2) a dita recepção de nível de qualidade exigido do fluxo.

9. Dispositivo para criptografar um quadro de aperfeiçoamento escalável codificado (3.2) compreendendo uma pluralidade de fluxos complementares ordenados em termos de nível de qualidade, cada fluxo complementar correspondendo a uma combinação de mais de um tipo de escalabilidade, onde um fluxo complementar de um nível de qualidade mais baixo corresponde a uma qualidade mais baixa em cada tipo de escalabilidade, o dito dispositivo sendo **CARACTERIZADO** pelo fato de que compreende dispositivo de criptografia para gerar uma chave aleatória ($K_{M,T}$) correspondendo à chave do fluxo complementar do nível de qualidade mais alto ($S_{m,t}$), para gerar as chaves dos fluxos complementares dos níveis de qualidade mais baixos ao aplicar sucessivamente uma função unidirecional (h) à chave aleatória ($K_{M,T}$), onde a saída de função unidirecional é diferente para cada tipo de escalabilidade.

10. Dispositivo para descriptografar um quadro de aperfeiçoamento escalável codificado compreendendo uma pluralidade de fluxos complementares ordenados em termos de nível de qualidade, cada fluxo complementar correspondendo a uma combinação de mais de um tipo de escalabilidade, onde um fluxo complementar de um nível de qualidade mais baixo corresponde a uma qualidade mais baixa em cada tipo de escalabilidade, o dito dispositivo **CARACTERIZADO** pelo fato de que compreende dispositivo de descriptografia para gerar, a partir de uma chave recebida ($K_{m,t}$), as chaves subsequentes somente dos fluxos complementares correspondendo aos níveis de qualidade mais baixos ao aplicar sucessivamente uma função unidirecional (h) à chave aleatória, onde a saída de função nidirecional é diferente de cada tipo de escalabilidade.

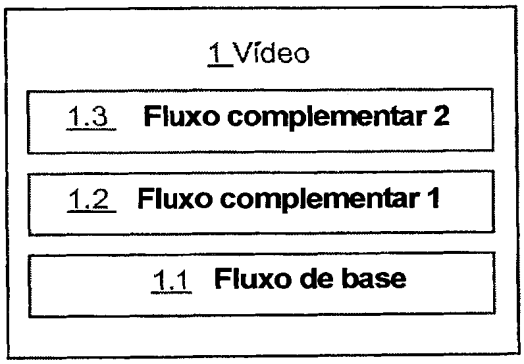

1 Vídeo
1.3 Fluxo complementar 2
1.2 Fluxo complementar 1
1.1 Fluxo de base

FIG. 1

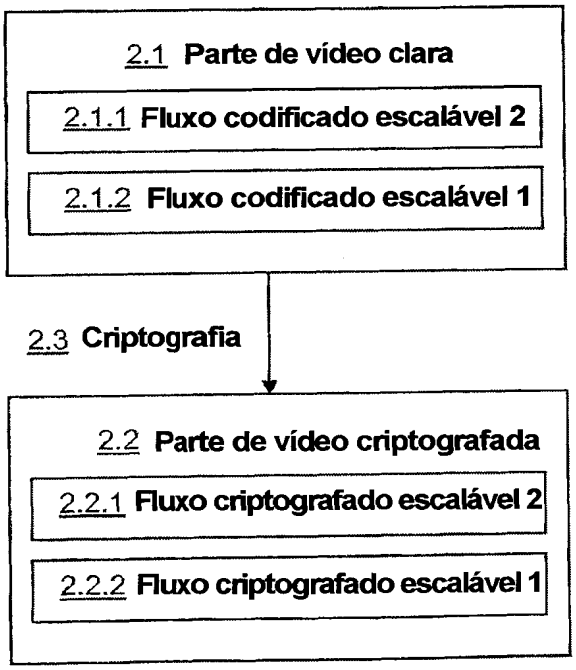

2.1 Parte de vídeo clara
2.1.1 Fluxo codificado escalável 2
2.1.2 Fluxo codificado escalável 1
2.3 Criptografia
2.2 Parte de vídeo criptografada
2.2.1 Fluxo criptografado escalável 2
2.2.2 Fluxo criptografado escalável 1

FIG. 2

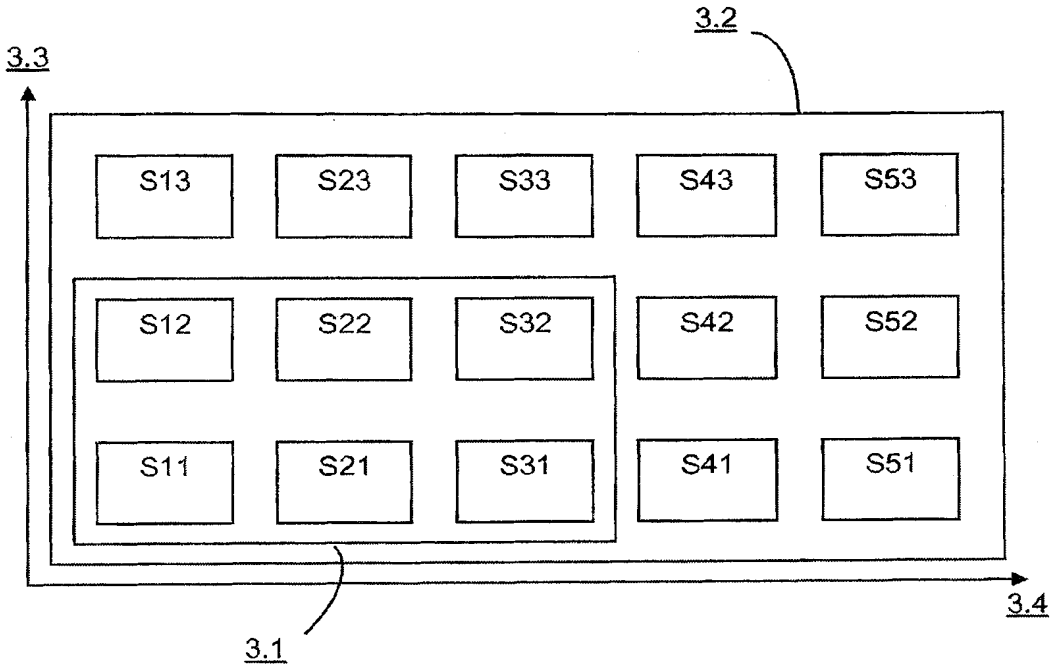

3.2
3.3
S13
S23
S33
S43
S53
S12
S22
S32
S42
S52
S11
S21
S31
S41
S51
3.4
3.1

FIG. 3

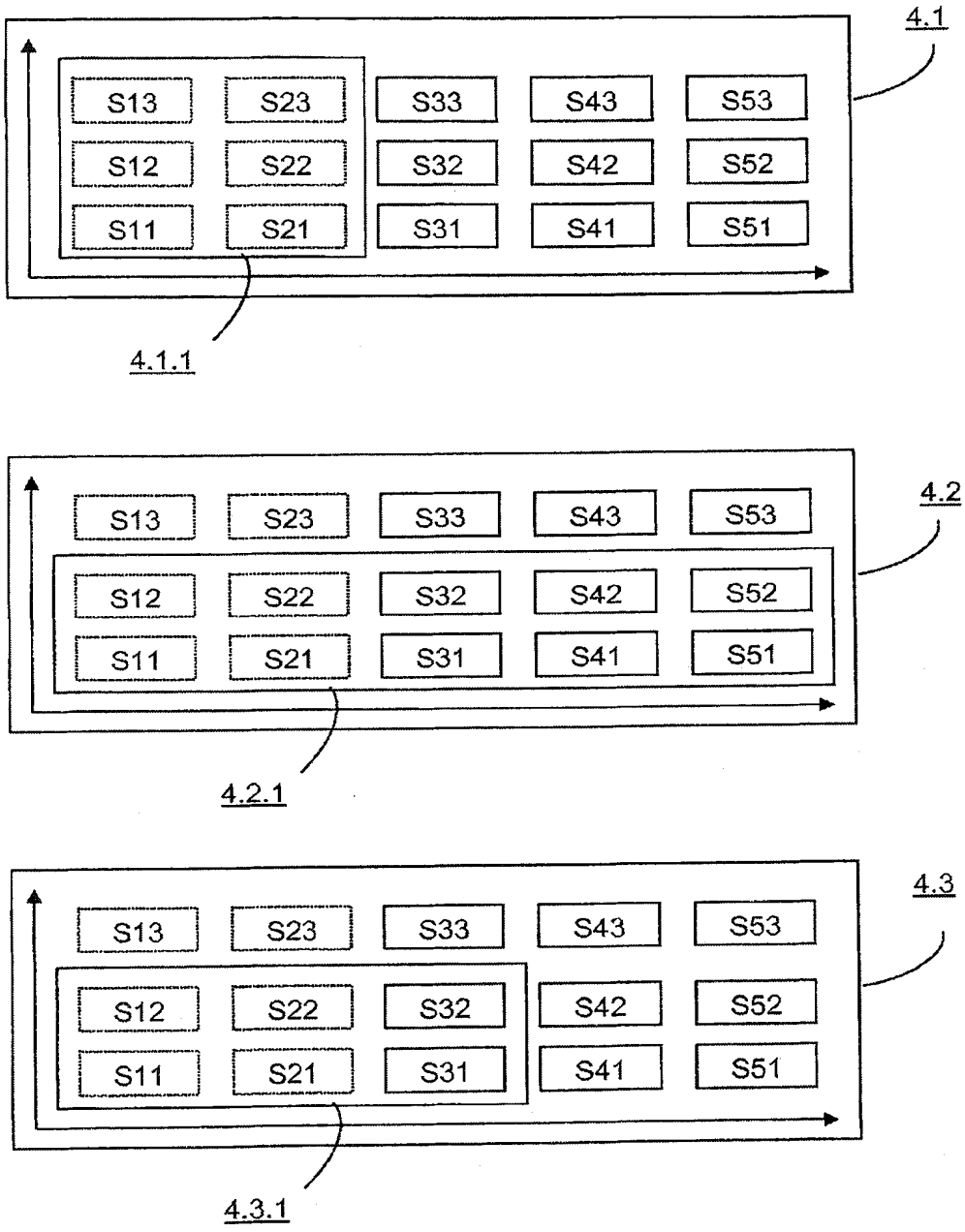

4.1
S13
S23
S33
S43
S53
S12
S22
S32
S42
S52
S11
S21
S31
S41
S51
4.1.1
4.2
S13
S23
S33
S43
S53
S12
S22
S32
S42
S52
S11
S21
S31
S41
S51
4.2.1
4.3
S13
S23
S33
S43
S53
S12
S22
S32
S42
S52
S11
S21
S31
S41
S51
4.3.1

FIG. 4

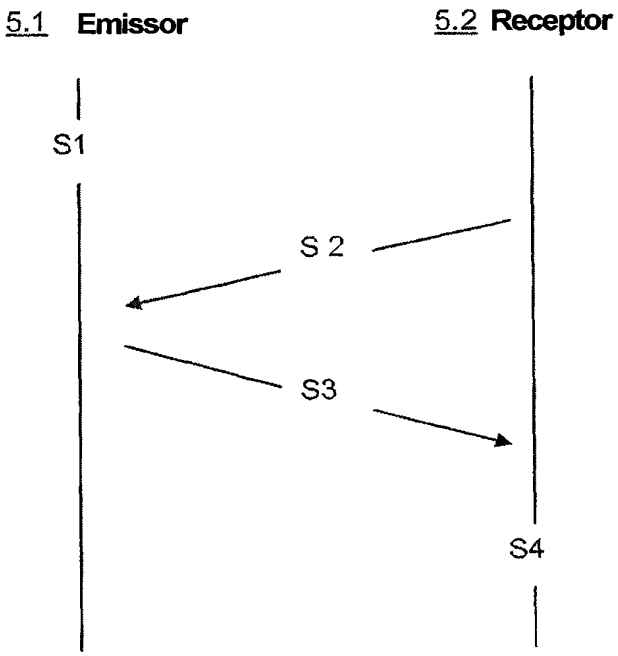


FIG. 5

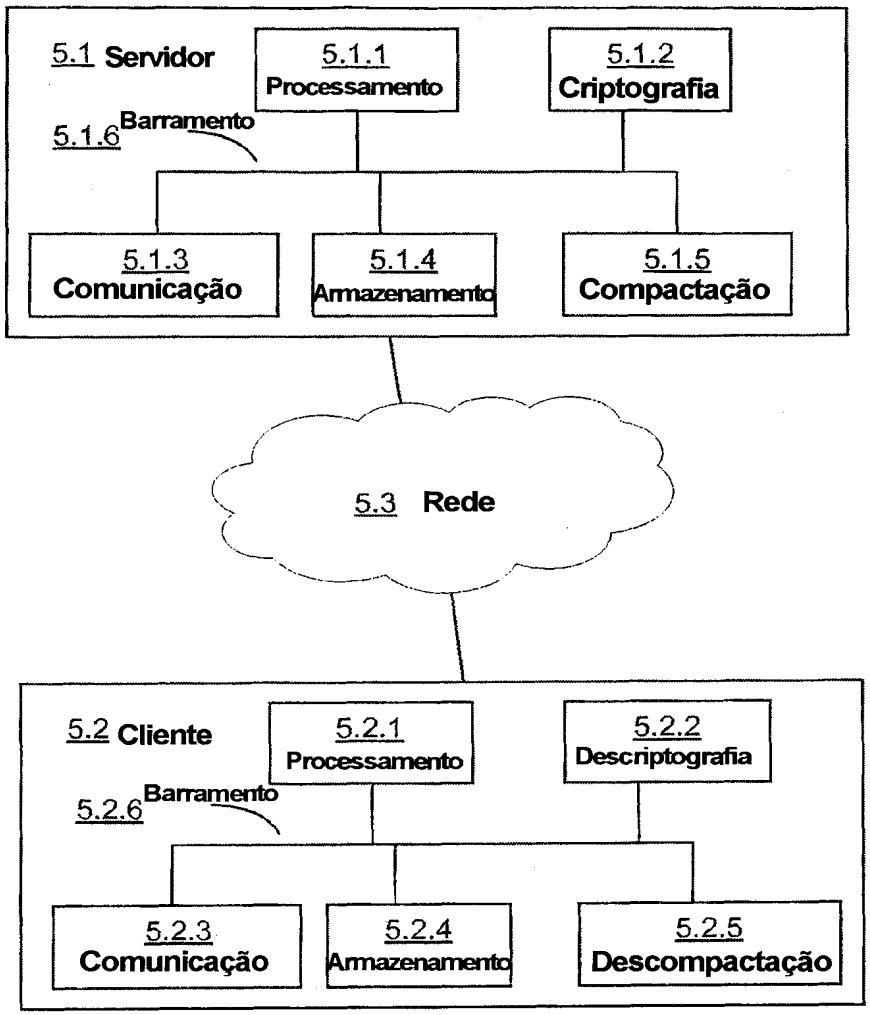

5.1 Servidor
5.1.1 Processamento
5.1.2 Criptografia
5.1.6 Barramento
5.1.3 Comunicação
5.1.4 Armazenamento
5.1.5 Compactação
5.3 Rede
5.2 Cliente
5.2.1 Processamento
5.2.2 Descriptografia
5.2.6 Barramento
5.2.3 Comunicação
5.2.4 Armazenamento
5.2.5 Descompactação

FIG. 6

RESUMO

"MÉTODO E DISPOSITIVO PARA GERENCIAR UMA TRANSMISSÃO DE CHAVES"

A presente invenção diz respeito a um método e a um dispositivo para criptografar um quadro de aperfeiçoamento escalável codificado (3.2) enviado por um emissor (5.1) para um receptor (5.2), o quadro de aperfeiçoamento compreendendo uma pluralidade de fluxos complementares ordenados em termos de nível de qualidade, cada fluxo complementar correspondendo a uma combinação de mais de um tipo de escalabilidade, onde um fluxo complementar de um nível de qualidade mais baixo corresponde a uma qualidade mais baixa em cada tipo de escalabilidade, compreendendo no nível do emissor as etapas de gerar uma chave (S1) por fluxo complementar para criptografar o dito fluxo complementar de uma tal maneira que todos os tipos de escalabilidade podem ser usados simultaneamente ou de forma individual, as ditas chaves sendo geradas de uma tal maneira que somente as chaves dos fluxos complementares de níveis de qualidade mais baixos do que o nível de qualidade de um fluxo complementar podem ser obtidas a partir da chave do dito fluxo complementar, e enviar (S3) a chave de um fluxo complementar correspondendo a um nível de qualidade exigido para o receptor, a chave permitindo a um receptor gerar somente as chaves dos fluxos complementares dos níveis de qualidade mais baixos. A presente invenção também diz respeito a um método e a um dispositivo para descriptografar um quadro de aperfeiçoamento escalável codificado recebido.