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

(11) **PI 0207581-4 B1**

(22) Data do Depósito: 25/02/2002

(45) Data de Concessão: 24/05/2016
(RPI 2368)

(54) Título: CRIPTOGRAFAÇÃO DE UM FLUXO DE VÍDEO COMPRIMIDO

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

(30) Prioridade Unionista: 26/02/2001 CH 2001 0344/01

(73) Titular(es): NAGRAVISION SA

(72) Inventor(es): ERIC CHAUBERT

Relatório Descritivo da Patente de Invenção para: **"CRIPTOGRAFAÇÃO DE UM FLUXO DE VÍDEO COMPRIMIDO".**

A presente invenção se refere a um método para criptografar um fluxo de vídeo comprimido, particularmente, permitindo reforçar o nível de segurança e, ao mesmo tempo, não penalizar os recursos durante a descriptografação.

Algoritmos de compressão de vídeo são baseados no fato de que, em geral, as diferenças entre uma imagem e a seguinte são pequenas e que a expressão das diferenças representa uma quantidade de informação muito mais reduzida do que toda a imagem. Tem sido observado que de uma imagem para a outra uma grande quantidade de informação não muda e até é encontrada em um plano ligeiramente diferente.

O princípio é aplicado nos formatos do tipo MPEG-2, MPEG-3 ou *Quick Time*.

De acordo com esses algoritmos, uma primeira imagem, chamada de referência, é transmitida completamente e uma análise das imagens seguintes é realizada a fim de determinar e transmitir as diferenças. De acordo com a norma de MPEG, distinguimos os quadros transmitidos integralmente (*I-Frame*) e os dados diferenciais do tipo MV (vetor de movimento) e do tipo DFD (diferença entre o modelo de MV e a imagem real).

De acordo com as soluções conhecidas, esses dados são, então, criptografados de acordo com um algoritmo adaptado ao nível desejado de segurança.

A fim de manter uma compatibilidade durante a transmissão e o processamento, cada grupo é criptografado por si, isto é, a atribuição dos quadros permanece visível, apenas o conteúdo é criptografado.

Com a evolução dos meios de armazenamento, é comum transmitir os dados criptografados, representando, por exemplo, um filme, para a unidade de um usuário.

Uma vez que o arquivo é armazenado na unidade, um terceiro pode ter todo o tempo necessário para tentar descriptografar os dados.

A fim de evitar esse risco, uma primeira abordagem consiste no aumento do nível de segurança no arquivo, isto é, usar algoritmos poderosos com chaves longas.

Embora essa técnica esteja satisfazendo no nível de segurança, ela apresenta o inconveniente de impor recursos importantes sobre a unidade de descriptografação.

A diversificação de meios de visualização progride em direção ao uso de dados por unidades tendo pequenas capacidades criptográficas. Esse é o caso, por exemplo, dos novos telefones móveis que tem uma tela de visualização. Para esse tipo de unidade, o uso em tempo real de

algoritmos sofisticados não é possível sem degradar o desempenho da unidade.

Desse modo, o uso de blocos de dados criptografados por algoritmos poderosos é incompatível com o uso no destino de todos os tipos de unidades de usuários.

O objetivo da presente aplicação, então, é permitir o uso de algoritmos poderosos com terminais que têm pequenas capacidades criptográficas.

Esse objetivo é alcançado através de um método de criptografação de um fluxo de vídeo comprimido, compreendendo blocos de dados independentes e blocos de dados diferenciais, consistindo na criptografação de acordo com um nível diferente de criptografação dos blocos de dados independentes e dos blocos de dados diferenciais.

Por bloco de dados independente, compreendemos a informação que permite obter o sinal descomprimido, sem referência à informação anterior. Podem ser, por exemplo, quadros completos (*I-Frame*).

Por blocos de dados diferenciais, compreendemos informação que permite obter o sinal descomprimido pela modificação do sinal prévio, aplicando essa informação diferencial.

De fato, essa solução permite concentrar a segurança máxima na informação indispensável para a descompressão das

imagens. De acordo com esse método, um primeiro algoritmo é aplicado nos quadros completos (*I-Frames*) do sinal de vídeo comprimido e um segundo algoritmo é aplicado à informação diferencial do tipo de MV ou do tipo de DFD.

Essa diferença também pode ser feita pelo uso de chaves de um comprimento diferente de acordo com o tipo de dado. Desse modo, os quadros completos serão criptografados por uma chave de 2048 bits, enquanto a informação diferencial será criptografada por uma chave de 128 bits.

De acordo com uma concretização da invenção, a informação diferencial não é criptografada.

Deve ser notado que outras fontes de informação que trabalham no princípio diferencial também podem usar esse método. Esse é o caso, por exemplo, da música comprimida de acordo com o formato MP3.

A presente invenção será melhor compreendida com o auxílio das figuras anexas, tomadas como não limitadoras, nas quais:

A figura 1 ilustra o fluxo comprimido antes da operação de criptografação;

A figura 2 representa o fluxo comprimido na forma criptografada;

A figura 3 representa um fluxo comprimido durante sua transmissão.

Na figura 1, o fluxo comprimido é representado por uma série de quadros do tipo completo (I) e de informação diferencial (P/C). De acordo com esse exemplo, um primeiro quadro completo I 1, é seguido por quadros P/C 1-2, permitindo reconstruir os quadros sucessivos entre o quadro completo I 1 e o quadro I 2.

Da mesma maneira, o quadro completo I 2 é seguido por quadros diferenciais sucessivos P/C 2-3, permitindo alcançar o quadro completo I 3.

Esse fluxo é, então, criptografado, seletivamente, de acordo com o tipo de quadro, tal como ilustrado na figura 2. Nessa figura, foi usada uma primeira chave k1 de um comprimento de 2048 bits para criptografar os quadros completos I 1, I 2 e I 3. Uma segunda chave k2, por exemplo, de 128 bits, foi usada para a criptografação dos quadros diferenciais P/C 1-2 e P/C 2-3.

O comprimento das chaves k1 e k2 é dado aqui como uma indicação e poderia ser de qualquer outro comprimento.

De acordo com a invenção, a diferença de qualidade da criptografação pode ser feita no nível das chaves ou no nível do algoritmo usado. Desse modo, a criptografação de acordo com k1 representa, por exemplo, um algoritmo do tipo IDEA e a criptografação de acordo com k2 representa um algoritmo do tipo DES.

Durante a difusão desse fluxo, os quadros completos são enviados inicialmente como ilustrado pela figura 3.

Essa particularidade permite que a unidade de recebimento comece, imediatamente, a descriptografação dos quadros que precisam de um longo processamento. Uma vez que esses quadros tenham sido descriptografados, o processamento dos quadros diferenciais pode ser feito em tempo real devido à rápida execução do tipo de algoritmo escolhido para esses quadros.

De acordo com uma concretização da invenção, o nível da criptografação para os quadros completos é diferente, dependendo de se é um primeiro quadro, tal como o quadro I 1 ou os quadros seguintes (I 2 e I 3). De fato, para se beneficiar do sinal descriptografado e descomprimido, temos que processar, imediatamente, o primeiro quadro e, a seguir, os quadros de diferenças. Isso é porque o primeiro quadro de uma série é criptografado com um algoritmo de descriptografação mais rápida do que os quadros completos seguintes.

Esse algoritmo pode ser o mesmo que o dos quadros diferenciais ou outro algoritmo.

REIVINDICAÇÕES

1. Método de criptografação de um fluxo de vídeo comprimido, compreendendo blocos de dados independentes (I) e os blocos de dados diferenciais (P/C), **caracterizado pelo** fato de consistir na criptografação de acordo com um primeiro nível de criptografação dos blocos de dados independentes (I) e a um segundo nível de criptografação dos blocos de dados diferenciais (P/B), cada bloco a ser processado de forma independente.

2. Método de criptografação de um fluxo de vídeo comprimido, de acordo com a reivindicação 1, **caracterizado pelo** fato de que os blocos de dados independentes (I) são criptografados por um algoritmo de alto nível, enquanto que os blocos de dados diferenciais (P/C) são criptografados por um algoritmo de descriptografação rápida.

3. Método, de acordo com a reivindicação 1, **caracterizado pelo** fato de que os blocos de dados independentes (I) são criptografados por uma ou diversas chaves longas, enquanto que os blocos de dados diferenciais (P/C) são criptografados por uma ou diversas chaves curtas.

4. Método, de acordo com qualquer uma das reivindicações 1 a 3, **caracterizado por**, durante a transmissão do sinal comprimido, os blocos de dados independentes (I) são agrupados por série, o método que consiste em criptografar

o primeiro bloco desta série de acordo com um nível diferente de criptografação daquele dos blocos independentes seguintes.

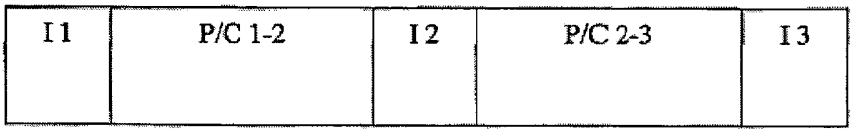

Fig 1.

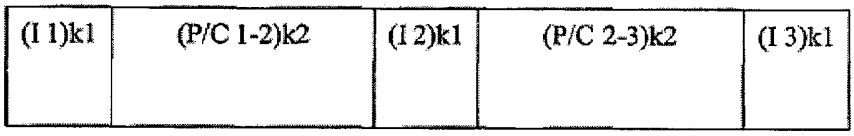

Fig 2.

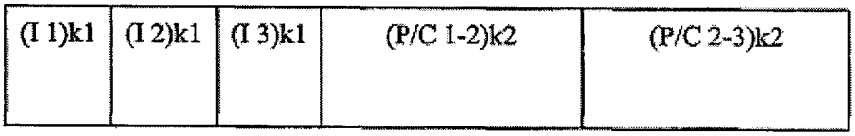

Fig 3.

Resumo da Patente de Invenção para: **"CRIPTOGRAFAÇÃO DE UM FLUXO DE VÍDEO COMPRIMIDO"**.

O objetivo da presente invenção é permitir o recebimento de um fluxo de dados comprimidos pelo uso de algoritmos poderosos em terminais tendo pequenas capacidades criptográficas.

Esse objetivo é alcançado por um método de criptografação de um fluxo de vídeo comprimido compreendendo blocos de dados independentes e blocos de dados diferenciais, consistindo na criptografação de acordo com um nível diferente de criptografação dos blocos de dados independentes e dos blocos de dados diferenciais.