MEMÓRIA DESCRITIVA

DA

PATENTE DE INVENÇÃO

Nº 96 818

NOME: KUDELSKI S.A. Fabrique d'Enregistreurs Nagra, suíça, industrial e comercial, com sede em 22, route de Genève, CH-1033 Cheseaux--sur-Lausanne, Suíça.

EPÍGRAFE: "PROCESSO PARA CIFRAR E DECIFRAR UM SINAL DE VÍDEO"

INVENTORES: André Kudelski.

Reivindicação do direito de prioridade ao abrigo do artigo 4º da Convenção da União de Paris de 20 de Março de 1883.

Suíça, em 21 de Fevereiro de 1990, sob o nº. 00 563/90-7.

Descrição referente à patente de invenção de KUDELSKI S.A. Fabrique d'Enregistreurs Nagra, suiça, industrial e comercial, com sede em 22, route de Genève, CH - 1033 CHESEAUX-SUR-LAUSANNE, Suiça, para:

"PROCESSO PARA CIFRAR E DECIFRAR UM SINAL DE VIDEO"

A presente invenção refere-se a um processo para cifrar e decifrar um sinal de vídeo, que consiste em, num local de emissão (ou de transmissão), cifrar sequências do sinal de vídeo de acordo com uma função de cifração pré-determinada, que pode ser diferente para cada sequência, emitir cada sequência do sinal de vídeo assim cifrado e depois, no local da recepção, decifrar a sequência do sinal de vídeo emitido.

A presente invenção pode ser aplicada essencialmente aos sistemas de televisão pagos ("pay-TV") nos quais é essencial cifrar a emissão de vídeo e decifrar ou descodificar o programa em casa do assinante que possua um descodificador apropriado e que tem direito a ver o programa emitido.

São bem conhecidos alguns processos de cifração e, por conseguinte, de decifração, pretendendo-se nesses processos tornar a imagem e/ou o som incompreensíveis ou tornar a visão e/ou a audição pouco confortáveis.

Um processo de cifração que consiste em permutar um número constante e determinado de linhas de imagem de vídeo de acordo com uma função de permutação pré-determinada é bem

conhecido. Neste caso, a decifração consiste em realizar a função inversa da usada na altura da emissão para permutar este número determinado de linhas de imagem. Como não é técnicamente fácil permutar assim um grande número de linhas de imagem, o limite é agora de cerca de 32 linhas permutadas na imagem.

Este processo de cifração bem conhecido, por vezes designado por processo de inversão de blocos, tem um inconveniente que consiste em exigir, no lado da recepção, uma memória de grande capacidade visto ser necessário precisamente depois de emitir para o aparelho de TV uma sequência de 32 linhas,e ter mais algumas linhas seguintes memorizadas para poder emitir imediatamente a imagem seguinte. Este processo é relativamente simples de realizar, no local da emissão, mas há problemas de precisão, fiabilidade e custos no local da recepção devido ao grande número de descodificadores. Por outro lado, este processo não é suficientemente fiável contra certa pirataria visual. De facto, é possível recuperar a ordem da permutação, mesmo que esta ordem varie frequentemente durante a fase de emissão.

Pode ver-se que, no exemplo atrás referido, a função de decifração é quase a mesma que a função de cifração, visto ambas as funções serem da mesma natureza, sendo uma a inversa da outra. Além disso, esta função é simples para os piratas porque não está ligada com outros parâmetros ou informações.

A presente invenção tem por objecto evitar os inconvenientes citados.

Para isso, o processo segundo a presente invenção é caracterizado por, no local da transmissão, se cifrar uma primeira sequência de vídeo de acordo com uma primeira função de cifração e uma outra sequência de vídeo de acordo com uma outra função de cifração e, no local da recepção, memorizar a outra sequência do sinal de vídeo cifrada de acordo com a outra função de cifração em vez da primeira sequência do sinal de vídeo cifrada de acordo com a primeira função de cifração, substituindo-a e, no ins-

tante desta substituição, a outra sequência do sinal de vídeo é memorizada de maneira cifrada de acordo com a função de cifração actual, que é igual a uma combinação determinada da primeira função de cifração e da outra função de cifração.

Segundo uma forma de realização da presente invenção, cada uma das funções de cifração consiste em emitir um grupo de linhas da imagem de vídeo por uma ordem diferente da ordem normal, que corresponde à imagem inintelígível, proporcionando no local da recepção uma memória de armazenamento que compreende um múmero determinado de linhas de memória, sendo cada uma das linhas de memória susceptível de armazenar uma linha de imagem recebida, provocando o armazenamento de uma linha de imagem recebida a emissão da referida linha armazenada anteriormente na sua linha de memória para o televisor, indicando-se para cada linha de imagem emitida o endereço da linha de memória na qual esta linha de imagem emitida deve ser armazenada, e determinando o instante de emissão desta linha de imagem de modo tal que ela substitui na memória uma linha de imagem anterior no instante em que esta linha de imagem anterior deve ser enviada para o televisor pela ordem normal das linhas de imagem para gerar a imagem inteligível (ou imagem clara).

De acordo com uma forma de realização da presente invenção, no local da emissão, o processo de cifração consiste em: atribuir a cada linha de imagem de pelo menos uma imagem produzida de maneira inteligível, antes da sua cifração, o endereço pseudoaleatório da linha de memória da memória de armazenamento na qual esta linha de imagem será armazenada no local da recepção e determinar o instante da emissão (ou a ordem de emissão) desta linha de imagem para fazer com que, no local da recepção, esta linha de imagem emita para o televisor a linha de imagem armazenada anteriormente no mesmo endereço, devido a que o seu armazenamento na linha de memória correspondente ao seu endereço corresponde precisamente ao instante correcto (ou à ordem de passagem correcta) para recuperar a imagem inteligí-

vel.

De acordo com uma forma de realização da presente invenção, no local de emissão, o processo de cifração compreende ainda: manter permanentemente uma tabela de correspondência entre o número de cada linha de imagem de pelo menos uma imagem da emissão produzida de maneira inteligível, antes da sua cifração, e o seu endereço de memorização na memória de armazenamento no local da recepção, eliminar eventualmente desta tabela as referidas linhas de imagem quando elas são finalmente emitidas para o televisor, dispor um número de pilhas igual ao número de linhas de memória da memória de armazenamento usada no local da recepção, correspondendo uma linha a uma pilha, empilhar sucessivamente em cada pilha o número de cada linha de imagem que será endereçada para a linha de memória correspondente a essa pilha durante a recepção de uma ou várias imagens, fazendo isso a começar pela última linha da ou das imagens e fazendo o empilhamento assim até à primeira linha da primeira imagem, depois, quando estiverem constituidas todas as pilhas deste modo para a ou as imagens, efectuar o desempilhamento de cada pilha, a começar no fundo da pilha, e determinando, para cada linha de imagem assim extraida de uma pilha pelo referido desempilhamento, o seu instante de emissão (ou a sua ordem de emissão), sendo este instante de emissão correspondente ao instante em que a linha de imagem na mesma pilha precisamente por cima da linha de imagem que se acabou de desempilhar deve ser emitida para o televisor para gerar a imagem inteligível.

A presente invenção será compreendida mais completamente com referência a descrição seguinte de uma forma de realização e aos desenhos anexos, cujas figuras representam:

A fig. 1, o modo de armazenamento numa memória tampão do descodificador segundo a presente invenção; e

A fig. 2, um meio para a realização do processo

segundo a presente invenção.

Uma linha de uma imagem digital inclui convencionalmente um grande número, por exemplo 256 ou 512, de amostras digitais, mas apenas oito amostras (a,b,c,d,e,f,g,h) estão representadas nos desenhos, para simplificar.

Com referência à fig. 1, está ilustrado um modo de endereçamento e armazenamento das linhas de imagem cifrada recebidas no descodificador do assinante. Pode ver-se uma memória de armazenamento (8), convencionalmente denominada memória tampão, que inclui 32 linhas de memória, podendo cada linha armazenar as informações digitais de uma linha de imagem completa.

De acordo com o processo da presente invenção, uma linha emitida (Z) substitui na memória tampão (8) uma linha anterior (X) na linha n da mesma memória tampão (8). O armazenamento da linha de imagem (Z) na linha n da memória tampão (8) faz com que a imagem anterior (X) seja enviada para o televisor. Eventualmente depois de um recondicionamento ou cancelamento em rotação. Por conseguinte, a ordem da emissão da linha de imagem depende do endereço n de cada uma dessas linhas, visto que cada linha(Z) será emitida apenas quando substituir uma linha (X) anterior na memória tampão, apenas no instante em que a linha anterior será enviada para o televisor.

Pode ver-se que a ordem de emissão das linhas não é permutada simplesmente e arbitrariamente, mas sim resulta de uma combinação com o endereço de cada linha de imagem na memória tampão que está no local da recepção. Assim, a função de cifração por permutação das linhas é relativa e não absoluta.

De acordo com uma forma de realização da presente invenção, e com referência à fig. 2, no local da emissão o processo de cifração consiste em:

a) manter permanentemente uma tabela de correspondência entre, por um lado, o número L de cada linha de imagem de pelo menos uma imagem produzida de maneira inteligível, antes da sua cifração e, por outro lado, o seu endereço de memorização B na memória tampão (8) no local de recepção;

b) eliminar desta tabela as linhas de imagem quando elas são finalmente emitidas para o televisor, para poder constituir a tabela seguinte;

c) proporcionar um número B de pilhas (P) igual ao número B de linhas de memória de armazenamento (ou memória tampão) usada no lado da recepção e dar uma referência a cada pilha, que é idêntica à da linha de memória que lhe corresponde;

d) empilhar sucessivamente em cada pilha P o número de cada linha de imagem que será endereçada para esta pilha durante a fase de recepção da ou das imagens (309,308,307,306, 305, ...), empilhando assim até à primeira linha da primeira imagem — numa imagem de vídeo, as linhas activas são convencionalmente designadas por índices de 23 a 309;

e) depois, quando estiverem constituidas todas as pilhas para a ou as imagens, efectuar o desempilhamento de cada pilha (de P1 a P32), começando pelo fundo da pilha (para a primeira pilha P1, 308, depois 306, etc. são as primeiras a extrair) e determinar, para cada linha de imagem assim extraida de uma pilha, no referido desempilhamento (por exemplo para a linha 308), o instante de emissão, sendo esse instante o que corresponde ao instante em que a linha de imagem da mesma pilha imediatamente por cima da que está a ser desempilhada (neste exemplo a linha 306) deve ser enviada para o televisor para formar a imagem inteligível;

f) depois podem dispor-se as linhas de imagem da ou das imagens numa memória de maior dimensão, de acordo com os instantes em que cada uma deve ser emitida e, quando todas as

linhas da ou das imagens, estiverem dispostas desta maneira, basta emitir as linhas de imagem de acordo com a sua disposição nesta memória.

REIVINDICAÇÕES

- 1ª -

Processo para cifrar e decifrar um sinal de vídeo que consiste em, no local de emissão, cifrar as sequências de sinais de vídeo de acordo com uma determinada função de cifração, que pode ser diferente para cada sequência, emitir cada uma das sequências do sinal de vídeo assim cifradas e depois, no local da recepção, decifrar as sequências do sinal de vídeo emitidas, caracterizado por, no local de emissão, se cifrar uma primeira sequência do sinal de vídeo de acordo com uma primeira função de cifração e cifrar uma outra sequência do sinal de vídeo de acordo com uma outra função de cifração e, no local da recepção armazenar a outra sequência do sinal de vídeo cifrada de acordo com a outra função de cifração no lugar da primeira sequência do sinal de vídeo cifrada de acordo com a função de cifração, substituindo-a, e, na altura desta substituição, armazenar a outra sequência do sinal de vídeo de uma maneira cifrada de acordo com uma função de cifração actual que é igual a uma combinação determinada da primeira função de cifração e da outra função de cifração.

- 2ª -

Processo de acordo com a reivindicação 1, caracterizado por cada uma das funções de cifração compreender sucessivamente a emissão de um grupo de linhas da imagem de vídeo de

acordo com uma ordem diferente da ordem normal correspondente à imagem inteligível, dispondo-se no local da recepção de uma memória de armazenamento que compreende um número determinado de linhas de memória, sendo cada uma das linhas de memória capaz de armazenar uma linha de imagem recebida, fazendo o armazenamento de uma linha de imagem recebida com que a linha armazenada anteriormente na referida linha de memória seja emitida para um aparelho de televisão, por cada linha de imagem emitida, determinando o endereço da linha de memória na qual a referida linha de memória deve ser armazenada o tempo de emissão da referida linha de imagem de modo que ela substitua uma linha de imagem anterior na memória no instante em que a referida linha de imagem anterior deve ser emitida para o referido aparelho de televisão pela ordem normal das linhas de imagem, para gerar a imagem inteligível.

- 3ª -

Processo de acordo com qualquer das reivindicações anteriores, caracterizado por, no local de emissão, o referido processo de cifração compreender as fases de:

- atribuir a cada linha de imagem (23 a 309) de uma imagem produzida de maneira inteligível, antes da sua cifração, o endereço pseudo-aleatório (B) da linha de memória da memória de armazenamento (8) na qual a referida linha de imagem será armazenada no local de recepção; e

- determinar o tempo de emissão (ou a ordem de emissão) da referida linha de imagem para fazer com que, no local de recepção, a referida linha de imagem emita para o aparelho de televisão a linha de imagem armazenada anterior no mesmo endereço, devido ao seu armazenamento da linha de memória para que está endereçada, sendo a emissão para o aparelho de televisão feita no tempo exacto (ou pela ordem exacta) para recuperar a imagem inteligível.

- 4ª -

Processo de acordo com qualquer das reivindicações anteriores, caracterizado por, no local de emissão, o referido processo de cifração compreender ainda as fases de:

- manter permanentemente uma tabela de correspondência (9) entre, por um lado, o número (23 a 309) de cada linha de imagem de pelo menos uma imagem de emissão produzida de maneira inteligível antes da sua cifração e, por outro lado, o seu endereço de memória (B) na memória de armazenamento (8) no lado da recepção;

- dispor de um certo número de pilhas (P1 a P32) igual ao número de linhas de memória da memória de armazenamento (8) usada no lado da recepção;

- empilhar sucessivamente em cada pilha o número de cada linha de imagem que será endereçada para a referida pilha durante a fase de recepção da referida imagem, fazendo isso a começar na última linha (309) da imagem e empilhando assim até à primeira linha (23) da referida imagem; depois

- quando todas as pilhas (P1 a P32) estiverem assim constituidas para a imagem, efectuar o desempilhamento de cada pilha começando no fundo da pilha ((208) para P1) e determinando, para cada linha de imagem assim extraida de uma pilha pelo referido desempilhamento, o seu tempo de emissão (ou a sua ordem de emissão), sendo esse tempo de emissão o tempo correspondente ao tempo em que a linha de imagem na mesma pilha precisamente por cima da que acabou de ser desempilhada deve ser emitida para o referido aparelho de televisão para gerar a imagem inteligível.

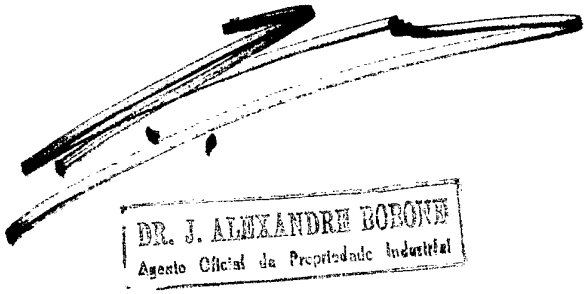
Foi inventor André Kudelski, suiço, residênte em Chemin de la Crésentine, CH-1023 Crissier, Suiça.

A requerente declara que o primeiro pedido desta patente foi apresentado na Suiça, em 21 de Fevereiro de 1990,

sob o No. 00 563/90-7.

Lisboa, 20 FEV. 1991

O AGENTE OFICIAL



R E S U M O

"PROCESSO PARA CIFRAR E DECIFRAR UM SINAL DE VIDEO"

A invenção refere-se a um processo para cifrar e decifrar um sinal de vídeo que consiste em:

- atribuir a cada linha de imagem (23 a 309) de uma imagem produzida de maneira inteligível, antes da sua cifração, o endereço pseudo-aleatório (B) da linha de memória, da memória de armazenamento (8) onde será armazenada, no local da recepção, a referida linha de imagem; e

- determinar o tempo de emissão (ou a ordem de emissão) da referida linha de imagem para fazer com que, no local de recepção, a referida linha de imagem, devido ao seu armazenamento na linha de memória para que está endereçada, emita para o aparelho de televisão a imagem anteriormente armazenada no mesmo endereço, sendo a emissão para o aparelho de televisão feita no tempo exacto (ou pela ordem de passagem exacta) para recuperar a imagem inteligível.

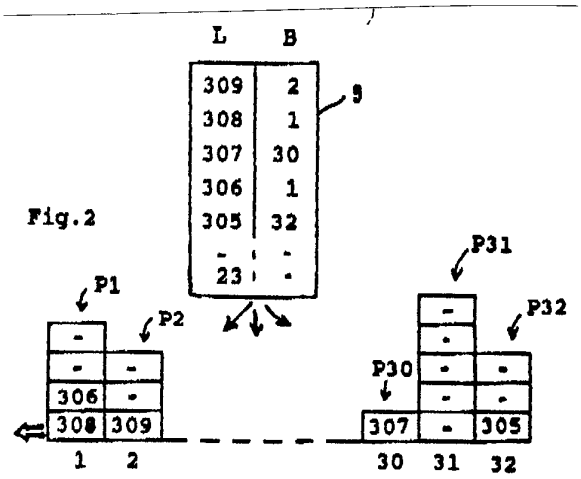


Fig.2

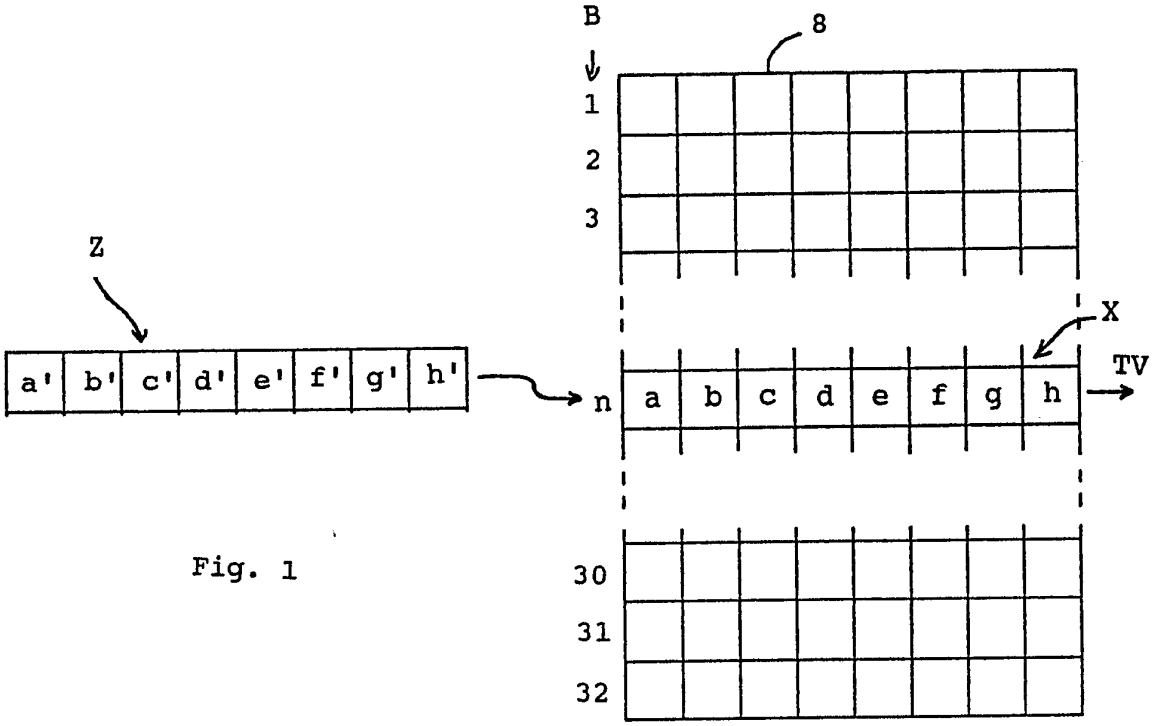

B
8
1
2
3
Z
a' b' c' d' e' f' g' h'
n
a b c d e f g h
X
TV
30
31
32

Fig. 1

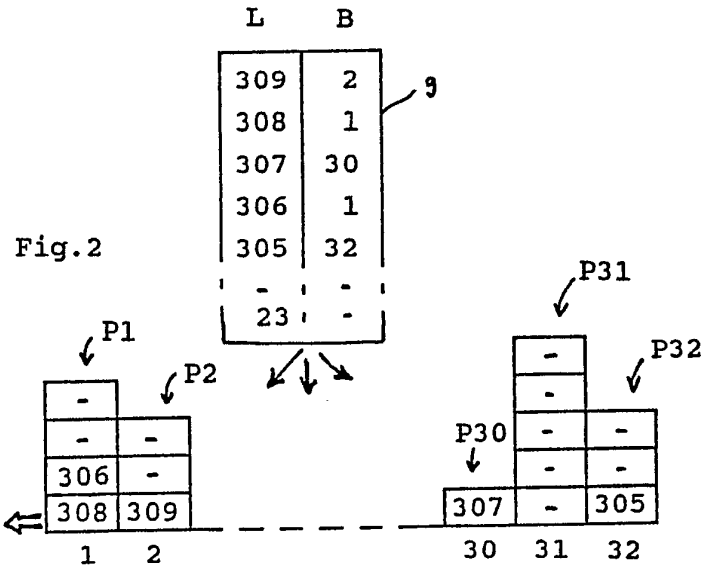

L
B
309 2
308 1
307 30
306 1
305 32
- -
23 -
9
P1
P2
P30
P31
P32
306
308 309
307 305
1 2
30 31 32

Fig.2