(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 238 151**

(21) Número de solicitud: 200301902

(51) Int. Cl.:
H04L 9/22 (2006.01)
H04L 9/18 (2006.01)
H04L 29/06 (2006.01)
G09C 1/00 (2006.01)
H04N 1/44 (2006.01)
H04N 7/167 (2006.01)

(12) PATENTE DE INVENCIÓN B1

(22) Fecha de presentación: **06.08.2003**

(43) Fecha de publicación de la solicitud: **16.08.2005**

Fecha de la concesión: **04.10.2006**

Fecha de modificación de las reivindicaciones: **23.12.2004**

(45) Fecha de anuncio de la concesión: **01.11.2006**

(45) Fecha de publicación del folleto de la patente: **01.11.2006**

(73) Titular/es:
Consejo Superior de Investigaciones Científicas
Serrano, 117
28006 Madrid, ES

(72) Inventor/es: **Hernández Encinas, Luis y**
Álvarez Marañón, Gonzalo

(74) Agente: **No consta**

(54) Título: **Procedimiento y dispositivo de encriptación de imágenes mediante un criptosistema gráfico simétrico.**

(57) Resumen:
Procedimiento y dispositivo de encriptación de imágenes mediante un criptosistema gráfico simétrico.
Se presenta un procedimiento y dispositivo para encriptar imágenes digitalizadas, con cualquier número de colores, basado en un generador pseudoaleatorio de bits, criptográficamente seguro, y en un autómata celular bidimensional. El criptosistema es seguro contra todos los ataques conocidos. Este procedimiento y dispositivo es de aplicación en todo aquellos procesos en los que se requiera proteger imágenes, ya sea para su transmisión o su almacenamiento, como por ejemplo en los sectores informática, militar, industrial, artística, cartografía y médica.

ES 2 238 151 B1

DESCRIPCIÓN

Procedimiento y dispositivo de encriptación de imágenes mediante un criptosistema gráfico simétrico.

Sectores de la técnica en los que tiene aplicación

- Criptografía
- Tratamiento de imágenes
- Tecnologías de las comunicaciones
- Seguridad informática

Estado de la técnica

Hoy en día existen varios métodos y algoritmos que permiten llevar a cabo, de modo seguro, el intercambio de información en redes de ordenadores. Entre tales métodos destacan los sistemas criptográficos simétricos o secretos, que se caracterizan por el hecho de que tanto el proceso de cifrado como el de descifrado de la información son similares y ambos se llevan a cabo mediante determinados algoritmos que dependen de una clave que es únicamente conocida por el emisor y por el receptor de la información. De forma más precisa (ver Figura 1), el proceso que se sigue tanto para el cifrado como para el descifrado de datos consiste en llevar a cabo una transformación inicial, sin valor criptográfico, de los datos originales de modo que sean utilizables por el algoritmo que se vaya a emplear en el módulo iterativo. A continuación se procede a iterar el algoritmo de cifrado/descifrado, que es alimentado por la clave del usuario que cifra o descifra los datos. El resultado de este proceso vuelve a sufrir una transformación final (que es la inversa a la inicial) de modo que su resultado son los datos cifrados (si los originales estaban en claro) o descifrados (si los de partida estaban ya cifrados). Los criptosistemas de clave secreta más utilizados en la actualidad son DES ([FIPS77]), IDEA ([LMM91]), RC5 ([Riv95]) y Rijndael ([Rij02]). La fortaleza de estos criptosistemas simétricos ante posibles ataques para romper su confidencialidad se basa en mantener secreta la clave utilizada y en la intratabilidad computacional de resolver el problema matemático en el que se fundamenta.

En la literatura especializada existen diferentes propuestas para el tratamiento de imágenes desde un punto de vista criptográfico. La primera de ellas se conoce como criptografia visual ([NS95]) y hace uso de los esquemas visuales umbrales t de n. En este procedimiento criptográfico, un director elabora de forma secreta n sombras de la imagen, que fotocopia a transparencias, y proporciona, también de forma secreta, una sombra a cada uno de los n participantes. Para recuperar la imagen original se deben superponer al menos t transparencias de las n existentes, siendo imposible obtener información alguna sobre la imagen inicial con menos de t transparencias. Sin embargo, este procedimiento presenta algunos problemas, entre los que destaca la pérdida de contraste de la imagen recuperada con respecto a la original. Hasta hace poco tiempo, la criptografia visual sólo era capaz de manipular imágenes en blanco y negro ([Sti01]) y en tonos de gris ([BDN00], [LT03]). Sin embargo, recientemente se ha presentado una propuesta para el tratamiento visual de imágenes en color ([H03]). Este hecho pone de manifiesto la importancia de los protocolos criptográficos para la manipulación de imágenes. No obstante, sigue persistiendo el problema -ya sea para imágenes en blanco y negro, en tonos de grises y en colores-, de que la imagen que se recupera, después de llevar a cabo el protocolo de la criptografia visual, pierde mucha resolución con relación a la imagen original.

Otra propuesta utiliza sistemas dinámicos continuos ([Fri97] y [Fri98]), lo que conlleva dificultades a la hora de implementar los protocolos en los que se basa. Estos problemas son de índole práctica, debido a la diferencia entre la aritmética caótica de los sistemas dinámicos propuestos, que es continua por su propia definición, y la aritmética discreta que se utiliza en los ordenadores. Este hecho hace que las implementaciones prácticas pierdan la esencia caótica de los sistemas en los que se fundamentan.

Existen también propuestas para el tratamiento criptográfico de imágenes en las que se utilizan, de forma iterada, diferentes métodos de compresión de las mismas ([BA92], [CHCO1], [CL94], [K93] y [Sch9l]). Sin embargo, en todas estas propuestas se presenta, de nuevo, el problema de que las imágenes recuperadas no coinciden con las originales por una pérdida de definición en los pixeles que la componen. Este hecho contradice la propia esencia del concepto de criptografia, por el que lo descifrado debe coincidir con aquello que se cifró. Es cierto que con el tratamiento de imágenes, se puede “apreciar” cuál era la imagen original, sobre todo si la primera era ampliamente conocida, pero esta pérdida de resolución impide el cifrado de imágenes que requieren una gran definición, como pueden ser mapas, diseños, etc.

Cabe señalar otra propuesta que no tiene los inconvenientes que se han señalado anteriormente ([HMH02] y [HMV02]). Sin embargo, este protocolo tiene dos inconvenientes. El primero de ellos es que no se puede utilizar de forma práctica nada más que para imágenes con hasta 256 colores o 256 tonos de gris, debido a la gran cantidad de cálculos y de memoria que requieren. El segundo inconveniente de esta propuesta está en que no es segura, es decir, es posible llevar a cabo un ataque al texto claro elegido que permita obtener la clave utilizada para cifrar una imagen. Para tener éxito con este ataque, si se dispone de la máquina de cifrado, basta con cifrar imágenes homogéneas de forma iterada y analizar cómo evoluciona el criptosistema, de modo que se pueda recuperar la clave original.

Finalmente, en [HMO2] se presenta una nueva propuesta para el cifrado de imágenes digitalizadas, que utiliza autómatas celulares, y que en este caso pueden estar definidas por cualquier número de colores. Esta propuesta también presenta la ventaja de recuperar la imagen original, sin pérdida de contraste, pero no es segura pues puede ser rota mediante el ataque al texto claro elegido.

Además de los protocolos anteriores, existen algunas aplicaciones de la criptografía con imágenes que hacen interesante un criptosistema como el que aquí se presenta, de modo que pueda ser utilizado con dichos fines. Tales aplicaciones permiten la autenticación e identificación visual ([NP97]), la identificación de documentos y firmas digitales de fotografías ([BME99] y [OR98]), los esquemas para desarrollar métodos para la protección intelectual de imágenes definidas por tonos de gris ([0002]), y los esquemas para compartir secretos ([TL02] y [T0002]).

Así pues, queda abierto el problema de diseñar un criptosistema seguro y eficiente que permita encriptar imágenes utilizando cualquier número de colores y cuyo criptograma resultante vuelva a ser una imagen con las mismas dimensiones que la original. Este problema es el que se resuelve en la presente invención. Es decir, en esta solicitud se presenta la invención de un criptosistema que permite encriptar y descriptar de forma segura y eficiente una imagen digitalizada definida por cualquier número de colores, es decir, con hasta 2^{24} = 16.777.216 colores.

Referencias

[BME99] B. **Bellamy**, J.S. **Mason** and M. **Ellis**, *Photograph signatures for the protection of identification documents, Proc. of Crypto & Coding'99*, LNCS **1746** (1999), 119-128.

[BBS86] L. **Blum**, M. **Blum** and M. **Shub**, *A simple unpredictable pseudo-random mumber generator, SIAM J. Comput*. **15** (1986), 364-383.

[BA92] N. **Bourbakis** and C. **Alexopoulos**, *Picture data encryption using SCAN patterns, Pattern Recogn*. **25** (1992), 567-581.

[BDN00] C. **Blundo**, A. De **Santis** and M. **Naor**, *Visual cryptography for grey level images, Inform. Proc. Lett.* **75** (2000), 255-259.

[CC02] C.C. **Chang** and J.C. **Chuang**, *An image intellectual property protection scheme for gray-level images using visual secret sharing strategy, Pattern Recogn. Lett*. **23** (2002), 931-941.

[CHCO1] Ch. **Chang**, M. **Hwang** and T. **Chen**, *A new encryption algorithm for images cryptosystems, J. Syst. Software* **58** (2001), 83-91.

[CL94] H.K. **Chang** and J.L. **Liou**, *An image encryption scheme based on quadtree compression scheme, Proc. of Int. Comput. Symp*., 230-237, Taiwan, 1994.

[FIPS77] Federal Information Standard Publication, *Data Encryption Standard*, FIPS 46, U.S. Department of Commerce/National Bureau of Standards, National Technical Information Service, Springfield, VI, 1977.

[Fri97] J. **Fridrich**, *Secure image ciphering based on chaos*, Final Technical Report, Rome Laboratories, NY, February 1997.

[Fri98] J. **Fridrich**, *Symmetric ciphers based on two-dimensional chaotic maps, Internat. J. Bifur. Chaos* **8** (1998), 1259-1284.

[HMO2] L. **Hernández Encinas** y A. **Martín del Rey**, *Método y aparato para el cifrado de imágenes digitalizadas*, Oficina Española de Patentes y Marcas, Solicitud de Patente de Invención Número 200201500.

[HMH02] L. **Hernández Encinas**, A. **Martín del Rey** and A. **Hernández Encinas**, *Encryption of images with 2-dimensional cellular automata*, Proc. of The 6th Multiconference on Systemics, Cybernetics and Informatics, Vol. I: Information Systems Development I, 471-476, Orlando, 2002.

[HMV02] L. **Hernández Encinas**, A. **Martín del Rey** e I. **Visus Ruiz**, *Cifrado de imágenes en tonos de gris mediante autómatas celulares, Actas de la VII Reunión Española de Criptología y Seguridad de la Información, Tomo I*, 379-389, Oviedo, 2002.

[HMMP98] L. **Hernández Encinas**, F. **Montoya Vitini**, J. **Muñoz Masqué** and A. **Peinado Domínguez**, *Maximal periods of orbits of the BBS generator, Proc. 1998 Int. Cont.. on Inform. Secur. & Cryptol*., 71-80, Seúl, 1998.

[H03] Y.C. **Hou**, *Visual cryptography for color images, Pattern Recogn* **36** (2003), 1619-1629.

[K93] C. J. **Kuo**, *Novel image encryption technique ans its application in progressive transmission, J. Electron. Imaging* **2** (1993), 345-351.

[LMM91] X. **Lai**, J. L. **Massey** and S. **Murphy**, *Markov ciphers and differential cryptanalysis, Proc. of Eurocrypt'91*, LNCS **547** (1991), 17-38.

[LT03] C.C. **Lin** and W.H. **Tsai**, *Visual cryptography for gray-level images by dithering techniques, Pattern Recogn. Lett*. **24** (2003), 349-358.

[LIP] FreeLIP, disponible en ftp://sable.ox.ac.uk/pub/math/.

[MOV97] A. **Menezes**, P. van **Oorschot** and S. **Vanstone**, *Handbook of applied cryptography*, CRC Press, Boca Raton, FL, 1997.

[NP97] M. **Naor** and B. **Pinkas**, *Visual authentication and identification, Proc. of Crypto'97*, LNCS **1294** (1997), 322-336.

[NS95] M. **Naor** and A. **Shamir**, *Visual cryptography, Proc. of Eurocrypt'94*, LNCS **950** (1995), 1-12.

[OR98] L. **O'Gorman** and I. **Rabinovich**, *Secure identification documents via pattern recognition and public-key cryptography*, IEEE *Trans. Pattern Anal. Mach. Intell*. **20**, 10 (1998), 1097-1102.

[PW85] N.H. **Packard** and S. **Wolfram**, *Two-dimensional cellular automata, J. Statist. Phys*. **38** (1985), 901-946.

[Rij02] Rijndael, disponible en http://csrc.nist.gov/encryption/aes/rijndael/

[Riv95] R.L. **Rivest**, *The RC5 encryption algorithm, Proc. of The Fast Software Encryption*, LNCS **1008** (1995), 86-96.

[RSA78] R.L. **Rivest**, A. **Shamir** and L. **Adleman**, *A method for obtaining digital signatures and public-key cryptosystem*, Commun. ACM **21** (1978), 120-126.

[Sch9l] C. **Schwartz**, *A new graphical method for encryption of computer data, Cryptologia* **15** (1991), 43-46.

[Sti01] D.R. **Stinson**, *Cryptography. Theory and Practice, 2nd. edition*, CRC Press, Boca Raton, FL, 2001.

[TL032] C.C: **Thien** and J.C. **Lin**, *Secret image sharing, Computer & Graphics* **26** (2002), 765-770.

[TCC02] C.S. **Tsai**, C.C. **Chang**, and T.S. **Chen**, *Sharing multiple secrets in digital images, J. Syst. Software* **64** (2002), 163-170.

[VV85] U.V. **Vazirani** and V.V. **Vazirani**, *Efficient and secure pseudo-random number generation, Proc. of Crypto'84*, LNCS **196** (1985), 193-202.

Explicación de la invención

Breve descripción de la invención

A partir del esquema general de los criptosistemas de clave simétrica que se mencionó en la sección sobre el Estado de la Técnica (ver Figura 1), se presenta aquí el esquema general del criptosistema gráfico simétrico que se propone en esta invención. Este esquema sigue la misma estructura general del anterior, pero presenta algunas modificaciones particulares, que lo hacen único para el tratamiento de imágenes definidas por cualquier número de colores (ver Figura 2).

Partiendo de los datos de una imagen digitalizada, almacenada en un fichero, se procede a una primera transformación de los datos, mediante la Transformación Inicial, cuya tarea consiste en adecuar los datos que definen la imagen para que pueda ser manipulada por el Módulo Iterativo. Una vez conocidos los datos fundamentales de la imagen, los valores correspondientes al número de filas y de columnas son enviados al Generador de bits pseudoaleatorio que, junto con la clave suministrada por el usuario, procede a generar una secuencia de bits pseudoaleatoria de longitud suficiente como para ser utilizada en el Módulo Iterativo.

El Módulo Iterativo recibe los siguientes datos:

1. Número de filas de la imagen (conocido a partir de la imagen),
2. Número de columnas de la imagen (conocido a partir de la imagen),
3. Valor de cada uno de los pixeles (conocido a partir de la imagen),
4. Secuencia de bits pseudoaleatoria (secreta y derivada de la clave),

y procede al encriptado o descriptado de los pixeles de la imagen. Estos procesos están basados en operaciones matemáticas que modifican los pixeles de la imagen de partida, dando lugar a la imagen cifrada, si la original era la imagen en claro a encriptar; o a la imagen en claro, si la que se emplea en el algoritmo es la imagen cifrada. Los procesos de cifrado y descifrado son similares, aunque no exactamente iguales, y utilizan la misma clave de usuario.

Una vez que los pixeles de la imagen han sido modificados por el Módulo Iterativo, son transformados mediante la Transformación Final, que los devuelve para que puedan ser almacenados en un fichero y puedan ser tratados como una imagen.

Descripción detallada de la invención

A partir del esquema general del proceso de cifrado/descifrado de imágenes que se describe en la presente invención (ver Figura 2), se presenta a continuación una descripción detallada de cómo llevar a cabo ambos procesos.

Para ello, en primer lugar se presentarán las herramientas matemáticas que se emplean en el criptosistema gráfico simétrico propuesto, a continuación se comentará el protocolo que se sigue para obtener la clave secreta que se empleará tanto a la hora de cifrar como de descifrar una imagen y finalmente se procederá a describir el proceso de cifrado, para luego presentar el de descifrado.

1. *Herramientas matemáticas*

En el presente criptosistema gráfico de clave simétrica para el cifrado y descifrado de imágenes definidas por pixeles y con cualquier número de colores, se utilizan dos herramientas matemáticas básicas: un generador de bits pseudoaleatorio, criptográficamente seguro, y un autómata celular bidimensional reversible. La primera de ellas permite obtener una secuencia de bits pseudoaleatorios, derivados de la clave secreta del usuario, y la segunda utiliza la secuencia de bits secreta generada por la primera para llevar a cabo tanto el proceso de encriptado como de descriptado.

Un *generador de bits pseudoaleatorio* (GBPA) es un algoritmo determinístico que proporciona como salida una secuencia de bits de longitud muy grande g >> l que parece ser aleatoria, al proporcionarle como entrada una secuencia de bits realmente aleatoria de longitud mucho menor l. La entrada al algoritmo se conoce como *semilla*, mientras que la salida que proporciona se denomina *secuencia de bits pseudoaleatoria* ([MOV97]). Por tanto, es muy deseable que el generador de bits que se utilice tenga buenas propiedades de pseudoaleatoriedad con el fin de evitar posibles ataques por análisis estadístico de las secuencias que genera. Así pues, es necesario que el generador sea *criptográficamente seguro* (GBPACS) es decir, que su seguridad esté basada, por ejemplo, en la dificultad de resolver un problema matemático. En este sentido, la seguridad significa que no existe ningún algoritmo de tiempo polinómico que pueda distinguir una secuencia del generador pseudoaleatorio de una secuencia realmente aleatoria de la misma longitud, con una probabilidad significativamente mayor que 1/2. Entre los GBPACS más utilizados se encuentran el generador RSA ([RSA78]) y el generador BBS ([BBS86]), para los que su seguridad se basa en la presunta intratabilidad de resolver el problema de la factorización entera.

La otra herramienta que se utilizará será un *autómata bidimensional reversible* ([PW85]). Se define un autómata celular (AC) como la cuaterna A = (L, S, V, f), siendo L el *espacio celular* formado por una matriz 2-dimensional, de tamaño $r \times s$, de objetos idénticos llamados *células*, <i, j>, con $0 \leq i \leq r - 1$, $0 \leq j \leq s - 1$. S es el *conjunto de estados*, es decir, el conjunto finito de todos los posibles valores que pueden tomar las células. El *conjunto de índices* $V \subset Z_2$ es un conjunto finito ordenado de modo que para cada célula, <i,j>, su *vecindad*, $V_{<ij>}$ es el siguiente conjunto:

$$V_{<ij>} = \{< i + \alpha, j + \beta >, \forall(\alpha,\beta) \in V\} \subset L.$$

Además, la *función de transición local f*: $S^n \rightarrow S$ es la función que determina la evolución del AC a lo largo del tiempo. Dado que los AC que se utilizarán son finitos, para que estén bien definidos, se considerarán condiciones de contorno periódicas, es decir, el espacio celular se entenderá como un toro en dos dimensiones:

$$a_{ij}^{(t)} = a_{kl}^{(t)} \Leftrightarrow i \equiv k \,(\mathrm{mod}(r - 1)) \text{ y } j \equiv l \,(\mathrm{mod}(s - 1)),$$

donde $a_{ij}^{(t)} \in S$ representa el estado de la célula <i, j> en el instante t, y a mod b es la operación que consiste en tomar el resto de la división entera de a entre b. Un AC se dice *reversible* (ACR) si existe otro AC, llamado su *inverso*, que determina su evolución inversa.

2. *Lectura de datos y clave secreta*

El tratamiento criptográfico de una imagen comienza con la Transformación Inicial que, a partir de la lectura del fichero de la imagen, I, proporciona los siguientes datos: número de colores, c, con $2 \leq c \leq 2^{24}$; número de filas: r; número de columnas: s; y la expresión binaria de cada uno de los $r \times s$ pixeles de la imagen:

$$P_{ij} = (p_{ij}^{1}, p_{ij}^{2}, ..., p_{ij}^{24}), 1 \leq i \leq r, 1 \leq j \leq s.$$

con $p_{ij}^{n} \in Z_2$. Además, si el píxel P_{ij} ocupa la posición m contando a partir de la parte superior izquierda de la imagen, se tiene que $m = (i - 1)\, s + j$, con $1 \leq m \leq r \times s$.

La clave del criptosistema gráfico desarrollado en esta invención es la clave del GBPACS utilizado, que permitirá obtener una secuencia de bits pseudoaleatoria secreta. Por tanto, la seguridad del criptosistema está garantizada por la seguridad del GBPA. Nótese que para romper el criptosistema propuesto se deberá determinar la clave del generador. Como generadores a utilizar se recomiendan el generador BBS o el RSA, si bien, puede utilizarse cualquier otro que sea criptográficamente seguro. Si se utiliza como clave K, la secuencia de bits pseudoaleatoria se denotará por $B = (B_1, B_2,..., B_{r\times s})$, siendo esta secuencia de longitud $r \times s \times 24$, donde $B_m = (b_{m1}, b_{m2}, ..., bm_{24})$, y $b_{mn} \in Z_2$

3. *Proceso de cifrado*

El protocolo para el cifrado de una imagen, que es el Módulo Iterativo (véase Figura 2), utiliza un ACR A = (L, S, V, f), definido de la siguiente manera:

(i) El espacio celular, L, es una matriz rectangular del mismo tamaño que la imagen, de modo que L puede considerarse como un conjunto de $r \times s$ píxeles.

(ii) El conjunto de estados es $S = Z_2 \times {}^{...(24...} \times Z_2$, con $|S| = 2^{24}$; por lo que cada color se puede identificar con un elemento de S. Si $x_m \in S$, es $x_m = (u_m{}^{1}, ..., u_m{}^{24})$ siendo $u_m{}^{n} \in Z_2$, $1 \leq n \leq 24$.

(iii) El conjunto de índices, V, se selecciona de forma pública de modo que |V|=24.

(iv) Para determinar el pixel encriptado de P_{ij}, Q_{ij}, $1 \leq i \leq r$, $1 \leq j \leq s$, se tienen en cuenta los 24 píxeles de la vecindad de P_{ij}, $V_{<ij>}$:P_{ij1}, P_{ij2},...,P_{ij24}, y se aplica la función de transición f: $S^{24} \rightarrow S$ como sigue:

$$P_{ij} \rightarrow Q_{ij}$$

$$f(P_{ij1}, P_{ij2}, \ldots, P_{ij24}) =$$

$$B_m \oplus (\pi_1(P_{ij1}), \pi_2(P_{ij2}), \ldots, \pi_{24}(P_{ij24})) =$$

$$(b_{m1}, b_{m2}, \ldots, b_{m24}) \oplus (p_{ij1}{}^{1}, p_{ij2}{}^{2}, \ldots, p_{ij24}{}^{24}) =$$

$$(b_{m1} \oplus p_{ij1}{}^{1}, b_{m2} \oplus p_{ij2}{}^{2}, \ldots, b_{m24} \oplus p_{ij24}{}^{24}) =$$

$$(q_{ij}{}^{1}, q_{ij}{}^{2}, \ldots, q_{ij}{}^{24}) = Q_{ij},$$

es decir, $q_{ij}{}^{n} = b_{mn} \oplus p_{ijn}{}^{n}$; siendo m la posición del píxel P_{ij}, B_m es la *m*-ésima componente de la secuencia de bits B,π_n: $S \rightarrow Z_2{}^{(n)}$ es la proyección sobre la *n*-ésima componente y $\oplus$ es la operación XOR.

La imagen cifrada, C, resulta de una única aplicación de la función de transición a cada uno de los pixeles de la imagen en claro I. De esta manera, la imagen cifrada estará también definida por $r \times s$ píxeles, pero ahora contendrá d colores, $2 \leq d \leq 2^{24}$.

Como se puede apreciar por la construcción del criptosistema, su factor de expansión (el cociente entre los tamaños de la imagen cifrada y de la imagen en claro) es 1. Por otra parte, no es necesario iterar el ACR más de una vez, dado que la seguridad del criptosistema no se incrementa por tal hecho.

Terminado el proceso de encriptado, la Transformación Final recibe del Módulo Iterativo el número de colores de la imagen, d; el número de filas, r; el de columnas, s; y los valores binarios de cada uno de los píxeles, Q_{ij}, de la imagen encriptada C. A partir de estos datos, se procede a la transformación de los datos que permite almacenarlos en un fichero de imagen.

4. *Proceso de descifrado*

El proceso de descriptado es similar al de cifrado y sólo difiere en el Módulo Iterativo, es decir, las Transformaciones Inicial y Final son las mismas. El receptor de la imagen cifrada utiliza el AC inverso de A = (L, S, V, f), es decir, A^{-1}=(L, S, W, g). En este caso, L y S son los mismos para A^{-1} que para A. El conjunto de índices de A^{-1}, es el mismo conjunto de índices que el de A, pero tomados en orden inverso, esto es, W= -V.

Para descriptar un píxel Q_{kl}, con $1 \leq k \leq r$, $1 \leq l \leq s$, se tienen en cuenta los 24 píxeles de la vecindad de Q_{kl}, $W_{<k,l>}$: Q_{ij1}, Q_{ij2}, ..., Q_{ij24}, y se aplica la función de transición g: $S^{24} \rightarrow S$ como sigue:

$$Q_{kl} \rightarrow R_{kl}$$

$$g\,(Q_{ij1}, Q_{ij2}, \ldots, Q_{ij24}) =$$

$$B'_t \oplus (\pi_1(Q_{ij1}), \pi_2(Q_{ij2}), \ldots, \pi_{24}(Q_{ij24})) =$$

$$(b'_{t1}, b'_{t2}, \ldots, b'_{t24}) \oplus (q_{kl1}{}^{1}, q_{kl2}{}^{2}, \ldots, q_{kl24}{}^{24}) =$$

$$(b'_{t1} \oplus q_{kl1}{}^{1}, b'_{t2} \oplus q_{kl2}{}^{2}, \ldots, b'_{t24} \oplus q_{kl24}{}^{24}) =$$

$$(b'_{t1} \oplus b_{m1} \oplus p_{kl}{}^{1}, b'_{t2} \oplus b_{m2} \oplus p_{kl}{}^{2}, \ldots, b'_{t24} \oplus b_{m24} \oplus p_{kl}{}^{24}) =$$

$$(p_{kl}{}^{1}, p_{kl}{}^{2}, \ldots, p_{kl}{}^{24}) = P_{kl},$$

con $b'_{tn} \oplus g_{kln}{}^{n} = p_{kl}{}^{n}$; t la posición de Q_{kl}, π_n: $S \rightarrow Z_2{}^{(n)}$ es la proyección sobre la *n*-ésima componente y el símbolo $\oplus$ representa la operación XOR.

Así pues, para recuperar el *t*-ésimo píxel, P_{kl}, se tiene que aplicar la función de transición g a su correspondiente píxel encriptado, Q_{kl}. La imagen en claro, I, se recupera aplicando una vez la función de transición a cada píxel de C. Según este proceso, la imagen recuperada es exactamente la misma que la original (píxel por píxel), es decir, no hay ninguna pérdida de resolución.

En resumen, un objeto de la presente invención lo constituye un procedimiento de encriptación y descriptación mediante un criptosistema gráfico simétrico basado en:

a) Un generador de bits pseudoaleatorio criptográficamente seguro,

b) Un autómata celular bidimensional reversible,

que encripta y descripta imágenes digitalizadas, definidas por cualquier número de colores.

Un objeto particular de la presente invención lo constituye un procedimiento de encriptación y descriptación mediante un criptosistema gráfico simétrico en el que el generador de bits pseudoaleatorio criptográficamente seguro, a partir de la clave secreta compartida por dos usuarios y que es utilizada como semilla del generador, genera una secuencia de bits pseudoaleatoria. Una realización concreta de dicho procedimiento es aquel en el que procedimiento de encriptación se basa en un autómata celular bidimensional reversible definido por una cuaterna (L, S, V, f), donde L es una imagen genérica del mismo tamaño que la que se vaya a utilizar en el proceso de cifrado; S es el conjunto formado por los 2^{24} = 16.777.216 posibles colores que pueden llegar a definir la imagen; V es la vecindad de cada píxel y f es la regla de transición que determina la evolución del autómata celular, tal como se ha comentado anteriormente.

Otra realización concreta de dicho procedimiento es aquel en el que procedimiento de descriptación mediante un criptosistema gráfico simétrico según las reivindicaciones 1 y 2, caracterizado por un autómata celular bidimensional reversible definido por una cuaterna (L, S, W, g), donde L es una imagen genérica del mismo tamaño que la que se vaya a utilizar en el proceso de descifrado; S es el conjunto formado por los 2^{24} = 16.777.216 posibles colores que pueden llegar a definir la imagen; W es la vecindad de cada píxel y g es la regla de transición que determina la evolución del autómata celular, tal como se ha comentado anteriormente.

Otro objeto de la presente invención lo constituye un dispositivo para encriptar y descriptar imágenes mediante un criptosistema gráfico simétrico constituido por un sistema electrónico que implementa en hardware o software un algoritmo para la ejecución del procedimiento anteriormente mencionado.

Otro objeto de la presente invención lo constituye un dispositivo de almacenamiento de datos utilizable para encriptar y descriptar imágenes mediante un criptosistema gráfico simétrico, caracterizado porque implementa un algoritmo para la ejecución del procedimiento anteriormente mencionado.

Finalmente, otro objeto de la presente invención lo constituye el uso del procedimiento y dispositivo mencionados anteriormente en todos aquellos procesos en los que se requiera proteger imágenes, ya sea para su transmisión o su almacenamiento. Téngase en cuenta que un usuario puede utilizar una clave secreta tanto para encriptar una imagen y transmitirla a un destinatario con el que comparte su clave, como para almacenarla de forma segura en su propio disco duro, con una clave que sólo él conozca. Así pues, entre las principales aplicaciones de esta invención destacan las siguientes:

- Almacenamiento seguro de cualquier imagen mediante su imagen encriptada en el formato de la imagen original.

- Transmisión de todo tipo de imágenes que hayan sido previamente encriptadas, de modo que la información que contengan no sea accesible, salvo para quienes estén autorizados.

Estas aplicaciones son de gran utilidad en campos relacionados con las siguientes actividades:

- Informática
- Militar
- Industrial
- Artística
- Cartografía
- Médica

Descripción de las figuras

Figura 1

Esquema general de un criptosistema de clave simétrica

En esta figura se presenta el esquema general para el cifrado y descifrado de datos mediante un criptosistema de clave simétrica o secreta. En primer lugar se suministran los datos, que son sometidos a una Transformación Inicial, sin carácter criptográfico, de modo que puedan ser manipulados por el Módulo Iterativo, que es donde realmente se lleva a cabo el proceso de cifrado/descifrado, mediante una clave de usuario que sólo él conoce. Después de este proceso, los datos resultantes son enviados a la Transformación Final, que reordena los datos en la forma inversa a como se procedió con la Transformación Inicial. Como resultado se obtienen los datos encriptados, si los originales estaban en claro; o los descriptados, si los de partida estaban ya cifrados.

Figura 2

Esquema general del proceso de cifrado/descifrado propuesto

El esquema general del protocolo que se presenta en esta invención se muestra en esta figura. Se puede apreciar que, en general, su estructura responde al esquema de los criptosistemas de clave simétrica (ver Figura 1). No obstante, hay algunas diferencias a destacar. Entre otras, que la clave de usuario es utilizada por un generador de bits pseudoaleatorio, criptográficamente seguro, para extender la clave original a una clave mucho más larga y que es utilizada para el cifrado/descifrado de la imagen. Por otra parte, se señalan los datos que son suministrados por cada módulo para el protocolo propuesto.

Figura 3

Generación de la secuencia de bits a partir de la clave secreta

En esta figura se muestra el procedimiento que se sigue para generar la secuencia de bits pseudoaleatoria a partir de la clave secreta del usuario y que será suministrada al Módulo Iterativo para el llevar a cabo el cifrado/descifrado de la imagen. Este procedimiento es el mismo tanto para el protocolo de encriptación como de descriptación. En particular en la figura se presenta el protocolo a seguir en el caso particular en que se considere el generador BBS, pero cualquier otro GBPACS seguirá un procedimiento muy similar.

Figura 4

Protocolo propuesto para el cifrado de una imagen

La Figura 4 desarrolla el proceso que se lleva a cabo en el Módulo Iterativo para el cifrado de una imagen. Dicho proceso necesita conocer el número de filas, columnas, el valor en bits de cada pixel y la secuencia de bits pseudoaleatoria generada a partir de la clave. A partir de estos datos, y del conocimiento público del módulo BBS y de la vecindad, se lleva a cabo el proceso de cifrar cada uno de los pixeles de la imagen.

Figura 5

Protocolo propuesto para el descifrado de una imagen

En esta figura se presenta el protocolo que se propone para el descifrado de una imagen. Dicho proceso es muy similar al de cifrado. Sólo varía el orden en que son considerados los vecinos de cada píxel y en la forma de elegir los bits de la secuencia pseudoaleatoria.

Figura 6

Ejemplo de imagen en claro

La Figura 6 presenta un ejemplo de imagen en claro para ser encriptada. La imagen corresponde a un "Autorretrato" de Tamara de Lempicka y contiene 602 filas, 800 columnas, es decir, 481600 píxeles; y c = 85803 colores.

Figura 7

Ejemplo de imagen cifrada

En la Figura 7 se incluye el resultado de encriptar la imagen mostrada en la Figura 6 mediante la clave que se incluye en la sección dedicada a la Exposición detallada de un modo de realización de la invención. Debido a las propiedades del criptosistema que se presenta, la imagen encriptada tiene el mismo tamaño que la original, es decir, 602 filas y 800 columnas; o lo que es igual, 481600 píxeles. El número de colores es, como cabria esperar, mucho mayor: 474799.

Exposición detallada de un ejemplo de realización de la invención

Descripción

A continuación se describe una posible implementación de cómo llevar a cabo el proceso de cifrado y de descifrado de un imagen cualquiera, siguiendo las pautas marcadas en la sección relativa a la Descripción detallada de la invención.

Se encriptará la imagen que se muestra en la Figura 6, definida por r = 602 filas, s = 800 columnas, es decir, por un total de 481600 píxeles; y por c = 85803 colores.

Claves

La elección de las claves depende del generador pseudoaleatorio de bits elegido. En este caso, hemos considerado el GBPACS conocido como BBS, dado que ha sido caracterizado en [HMMP98] y se conocen, por tanto, para qué parámetros del mismo se obtienen longitudes de órbitas máximas.

Para obtener las claves de este generador se deben considerar dos números primos grandes, p y q, cada uno de ellos congruentes con 3 módulo 4 y verificando las condiciones señaladas en [HMMP98]. A continuación se determina el valor del módulo BBS: $n = p \times q$, que se hace público, mientras que se mantienen en secreto los valores de p y q. La publicación del valor de n no merma la seguridad del criptosistema puesto que la misma se basa en la dificultad de calcular los valores de p y q, es decir, de factorizar n. El siguiente paso es el de determinar el valor de la clave secreta que compartirán los dos usuarios que se intercambiarán la imagen cifrada. Dicha clave es la semilla del generador BBS, K, que también debe verificar determinadas condiciones (ver [HMMP98]). A partir de los valores anteriores se itera la función $x^2 \pmod n$ para obtener la secuencia de números que darán lugar a los bits. De forma más precisa, el proceso a seguir para generar la secuencia de bits es el siguiente (ver Figura 3): se considera $x_0 = K$ y se itera la expresión dada por

$$x_i = (x_{i-1})^2 (\mathrm{mod}\ n), i > 0,$$

de modo que a partir de los valores enteros x_i se obtienen los bits de la secuencia. En la propuesta original del generador ([BBS86]) sólo se consideraba el bit menos significativo (el bit de paridad) de x_i; sin embargo, se ha demostrado ([VV85]) que si se toman los $\lfloor \log_2 (\log_2 n) \rfloor$ bits menos significativos de x_i, el generador BBS sigue siendo seguro, supuesto que el problema de la factorización de números es un problema intratable computacionalmente. Considerando esta nueva versión del BBS, su eficiencia se ve incrementada notablemente.

En el ejemplo que nos ocupa, se considerará una clave que bien podría ser utilizada en la práctica puesto que su longitud es de 1024 bits (valor recomendado para implementaciones prácticas), y que viene dada por los siguientes valores:

p = 21356 60840 00904 44908 14294 61912 33044 48726 67056 27770 91639 84681 78856 45992 32341 56958 35057 42091 15098 30798 10115 93632 49071 27705 00854 09456 56744 86832 77097 70615 03863,

q = 19102 22295 03150 73922 29063 28699 65980 67095 94325 63598 98052 32092 35809 52388 60543 17244 68454 91521 66614 46956 28835 97718 10065 68101 69525 42919 27519 18819 59100 55918 43279,

n = p × q = 40795 86951 21099 38917 54804 02638 77833 57710 21051 85001 83480 19522 46842 87856 97634 85052 14129 09959 66022 75789 15738 85235 98425 52977 83390 32214 40675 81164 15742 55828 31687 54047 58970 02501 96771 58151 62865 69703 77460 32565 62268 04385 39180 72558 40139 07770 04502 97538 17997 97372 88123 63690 00159 61886 13363 80260 01716 07863 16076 66545 94908 6777.

Una vez que se da a conocer el módulo BBS, n, los dos usuarios que van a utilizar el criptosistema que se propone en esta invención, se ponen de acuerdo en la clave secreta que van a utilizar, K, que en este caso será la semilla del generador BBS. Nótese que como la clave pública del generador no tiene por qué modificarse (salvo cuando las normas de seguridad así lo aconsejen), la clave secreta debe ser diferente para cada imagen, o al menos, para cada pareja de usuarios. Dicha semilla podría ser la siguiente:

K = 24036 88089 14855 42194 08780 82014 68160 80201 24435 74791 86003 70808 69817 02168 06034 74249 97038 26708 94839 69522 81767 89191 94832 26050 76074 09495 06651 79114 81213 15981 23484 51879 02828 49820 38094 47857 03683 77627 64872 17160 52538 54161 84144 97589 01730 51799 78262 51461 25123 11304 71889 41449 99949 34474 26583 39113 30749 85764 42420 85026 68074 3088.

A partir de los datos anteriores, se debe generar una secuencia de al menos

$$602 \times 800 \times 24 = 11558400 \text{ bits},$$

para garantizar que se podrán encriptar todos los pixeles de la imagen original. Se debe tener en cuenta que no es necesario iterar 11558400 veces el algoritmo BBS según la modificación señalada anteriormente. En este caso, dado que $\lfloor \log_2 (\log_2 n) \rfloor = 10$, el número de iteraciones será 10 veces menor.

Cifrado

Según el protocolo de cifrado mencionado anteriormente, se debe elegir de forma pública una vecindad para el ACR. En este ejemplo, se considerará el cuadrado de tamaño 5 × 5 alrededor de la célula <i,j>, exceptuando la propia célula, por lo que se tendrá:

$$V = \{(-2, -2), ..., (-2, 2), ..., (0, -1), (0, 1), ..., (2, -2), ...(2, 2)\},$$

y la vecindad, $V_{<ij>}$, puede representarse como sigue:

<*i*–2, *j*–2>	< *i*–2, *j*–1>	< *i*–2, *j*>	<*i*–2, *j*+1>	<*i*–2, *j*+2>
<*i*–1, *j*–2>	<*i*–1, *j*–1>	< *i*–1, *j*>	<*i*–1, *j*+1>	<*i*–1, *j*+2>
<*i*, *j*–2>	<*i*, *j*–1>	**<*i*, *j*>**	<*i*, *j*+1>	<*i*, *j*+2>
<*i*+1, *j*–2>	<*i*+1, *j*–1>	<*i*+1, *j*>	<*i*+1, *j*+1>	<*i*+1, *j*+2>
<*i*+2, *j*–2>	<*i*+2, *j*–1>	<*i*+2, *j*>	<*i*+2, *j*+1>	<*i*+2, *j*+2>

El conjunto anterior puede representarse mediante dos variables h y w, de modo que $V_{<ij>} = \{(i + h, j + w)\}$, siendo:

$$h = \lfloor (n - 1)/5 \rfloor - 2, w = (n - 1)(\text{mod } 5) - 2, 1 \leq n \leq 12,$$

$$h = \lfloor n/5 \rfloor - 2, w = n(\text{mod } 5) - 2, 13 \leq n \leq 24,$$

donde ⌊ a ⌋ es el mayor entero que es menor que a.

Según esta elección de la vecindad, para determinar el píxel encriptado de P_{ij}, Q_{ij}, $1 \leq i \leq r$, $1 \leq j \leq s$, se consideran los 24 píxeles de la vecindad de P_{ij}, $V_{<ij>}$: $P_{i-2,j-2}$, ..., $P_{i-2,j+2}$, ..., $P_{i,j-1}$, $P_{i,j+1}$, ..., $P_{i+2,j+2}$, y se aplica la función de transición f: $S^{24} \rightarrow S$ como sigue:

$$P_{ij} \rightarrow Q_{ij}$$

$$f(P_{i-2,j-2}, P_{i-2,j-1}, \ldots, P_{i+2,j+2}) =$$

$$B_m \oplus (\pi_1(P_{i-2,j-2}), \pi_2(P_{i-2,j-1}), \ldots, \pi_{24}(P_{i+2,j+2})) =$$

$$(b_{m1}, b_{m2}, \ldots, b_{m24}) \oplus (p_{i-2,j-2}{}^1, p_{i-2,j-1}{}^2, \ldots, p_{i+2,j+2}{}^{24}) =$$

$$(b_{m1} \oplus p_{i-2,j-2}{}^1, b_{m2} \oplus p_{i-2,j-1}{}^2, \ldots, b_{m24} \oplus p_{i+2,j+2}{}^{24}) =$$

$$(q_{ij}{}^1, q_{ij}{}^2, \ldots, q_{ij}{}^{24}) = Q_{ij},$$

es decir, $q_{ij}{}^n = b_{mn} \oplus p_{i+h,j+w}{}^n$; siendo m = (i – 1) s + j la posición del píxel P_{ij}, B_m la *m*-ésima componente de la secuencia de bits B, π_n: $S \rightarrow Z_2{}^{(n)}$ es la proyección sobre la *n*-ésima componente y $\oplus$ la operación XOR.

Descifrado

Una vez que se ha elegido de forma pública la vecindad V anterior, para el ACR inverso se tiene que:

$$W = \{(2, 2), ..., (2, -2), ..., (0, 1), (0, -1), ..., (-2, 2), ..., (-2, -2)\}.$$

También en este caso, la vecindad de la célula <k, l>, $W_{<k,l>}$, se puede codificar por las mismas dos variables h y w: $W_{<k,l>} = \{(k–h, 1–w)\}$. Así pues, la función de transición g: $S^{24} \rightarrow S$, a utilizar para descriptar un píxel es como sigue:

$$Q_{kl} \rightarrow R_{kl}$$

$$g(Q_{k+2,l+2}, Q_{k+2,l+1}, \ldots Q_{k-2,l-2}) =$$

$$B'_t \oplus (\pi_1(Q_{k+2,l+2}), \pi_2(Q_{k+2,l+1}), \ldots, \pi_{24}(Q_{k-2,l-2})) =$$

$$(b'_{t1}, b'_{t2}, \ldots, b'_{t24}) \oplus (q_{k+2,l+2}{}^1, q_{k+2,l+1}{}^2, \ldots, q_{k-2,l-2}{}^{24}) =$$

$$(b'_{t1} \oplus q_{k+2,l+2}{}^1, b'_{t2} \oplus q_{k+2,l+1}{}^2, \ldots, b'_{t24} \oplus q_{k-2,l-2}{}^{24}) =$$

$$(b'_{t1} \oplus b_{m1} \oplus p_{kl}{}^1, b'_{t2} \oplus b_{m2} \oplus p_{kl}{}^2, \ldots, b'_{t24} \oplus b_{m24} \oplus p_{kl}{}^{24}) =$$

$$(p_{kl}{}^1, p_{kl}{}^2, \ldots, p_{kl}{}^{24}) = P_{kl},$$

con $b'_{tn} \oplus q_{k-h,l-w}{}^n = p_{kl}{}^n$; t = (k – h – 1) s + 1– w la posición de $Q_{k-h,l-w}$,y por tanto se tiene que $b'_{t,n} = b_{(k-1-h)s+l-w,n}$, π_n: $S \rightarrow Z_2{}^{(n)}$ es la proyección sobre la *n*-ésima componente y el símbolo $\rightarrow$ representa la operación XOR.

Funcionamiento e implementación

El esquema propuesto para el encriptado y descriptado de imágenes se ha implementado de forma práctica mediante varios programas utilizando el lenguaje C++ en un ordenador Pentium III a 1000 Mhz con dos microprocesadores y 512 Mbytes de memoria RAM. En particular y dado que las claves no pueden ser determinadas ni manipuladas con las librerías estándar de C++ debido a su tamaño, para la generación de las claves y las secuencias de bits pseudoaleatorios se ha utilizado la librería FreeLIP (Large Integer Package) desarrollada por A.K. Lenstra y en la actualidad mantenida por P. Leyland (ver [LIP]). Por otra parte, el protocolo de cifrado/descifrado se ha implementado en C++ de Visual Studio .Net 6.0.

Con estas implementaciones, que no están completamente depuradas, el tiempo de computación necesario para generar la clave privada del generador BBS (primos p y q), la clave pública de 1024 bits (n) y la clave secreta (K) ha sido de 45 segundos; mientras que para la generación de la secuencia de bits pseudoaleatoria de 12 millones de bits el tiempo necesario ha sido de 75 segundos. Con relación a los procesos de cifrado y descifrado, el tiempo requerido para leer la imagen original que se muestra en la Figura 6, almacenarla en memoria y encriptarla, utilizando la secuencia

generada anteriormente, ha sido de 9 segundos. El mismo proceso anterior (lectura, almacenamiento y ejecución) llevado a cabo para la imagen encriptada (ver Figura 7) ha requerido 10 segundos.

Como se puede apreciar, el mayor tiempo de computación se lo lleva el proceso de generación de las claves, lo cual era previsible. Nótese además, que el procedimiento de cifrado/descifrado es muy rápido, dado que para el tamaño de las imágenes utilizadas (602 x 800 pixeles) sólo se requieren unos 10 segundos de ejecución. Por otra parte, los tiempos presentados anteriormente podrían ser mejorados si se depuran los programas utilizados o si se implementan en hardware.

REIVINDICACIONES

1. Procedimiento de encriptación y descriptación mediante un criptosistema gráfico simétrico **caracterizado** porque utiliza

a) Un generador de bits pseudoaleatorio criptográficamente seguro,

b) Un autómata celular bidimensional reversible,

que encripta y descripta imágenes digitalizadas, definidas por cualquier número de colores.

2. Procedimiento de encriptación y descriptación mediante un criptosistema gráfico simétrico según la reivindicación 1, **caracterizado** porque el generador de bits pseudoaleatorio criptográficamente seguro, a partir de la clave secreta compartida por dos usuarios y que es utilizada como semilla del generador, genera una secuencia de bits pseudoaleatoria.

3. Procedimiento de encriptación mediante un criptosistema gráfico simétrico según las reivindicaciones 1 y 2, **caracterizado** por un autómata celular bidimensional reversible definido por una cuaterna (L, S, V, f), donde L es una imagen genérica del mismo tamaño que la que se vaya a utilizar en el proceso de cifrado; S es el conjunto formado por los 2^{24} = 16.777.216 posibles colores que pueden llegar a definir la imagen; Ves la vecindad de cada pixel y f es la regla de transición que determina la evolución del autómata celular.

4. Procedimiento de descriptación mediante un criptosistema gráfico simétrico según las reivindicaciones 1 y 2, **caracterizado** por un autómata celular bidimensional reversible definido por una cuaterna (L, S, W, g), donde L es una imagen genérica del mismo tamaño que la que se vaya a utilizar en el proceso de descifrado; S es el conjunto formado por los 2^{24} = 16.777.216 posibles colores que pueden llegar a definir la imagen; W es la vecindad de cada pixel y g es la regla de transición que determina la evolución del autómata celular.

5. Dispositivo para encriptar, almacenar datos y descriptar imágenes **caracterizado** porque está constituido por un sistema electrónico que implementa en hardware o software un algoritmo para la ejecución de un procedimiento según las reivindicaciones 1 a la 4.

6. Uso del procedimiento según las reivindicaciones 1 a la 4 y del dispositivo según la reivindicación 5 para la protección del almacenaje y transmisión de imágenes.

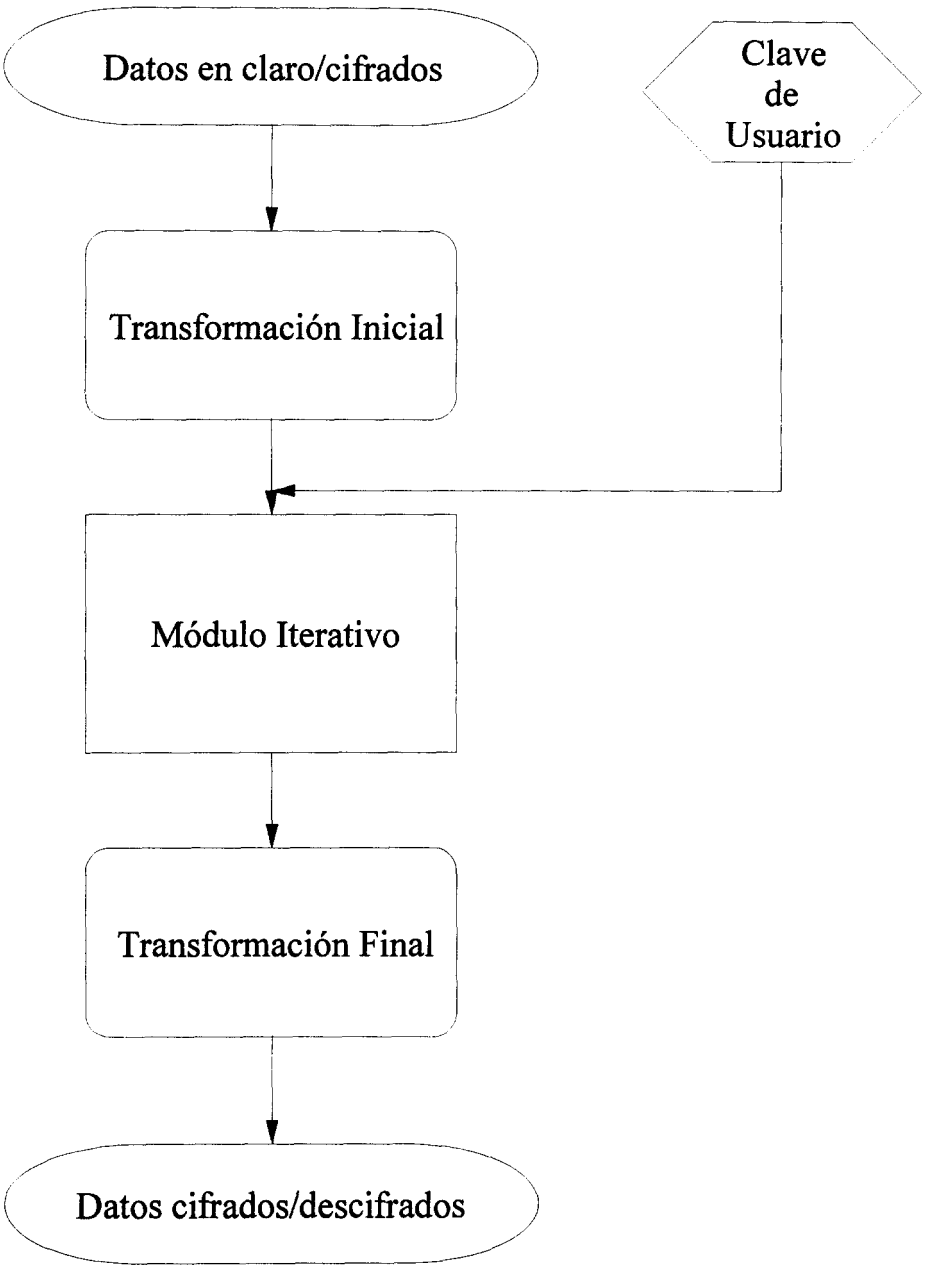
Datos en claro/cifrados
Clave de Usuario
Transformación Inicial
Módulo Iterativo
Transformación Final
Datos cifrados/descifrados

Figura 1

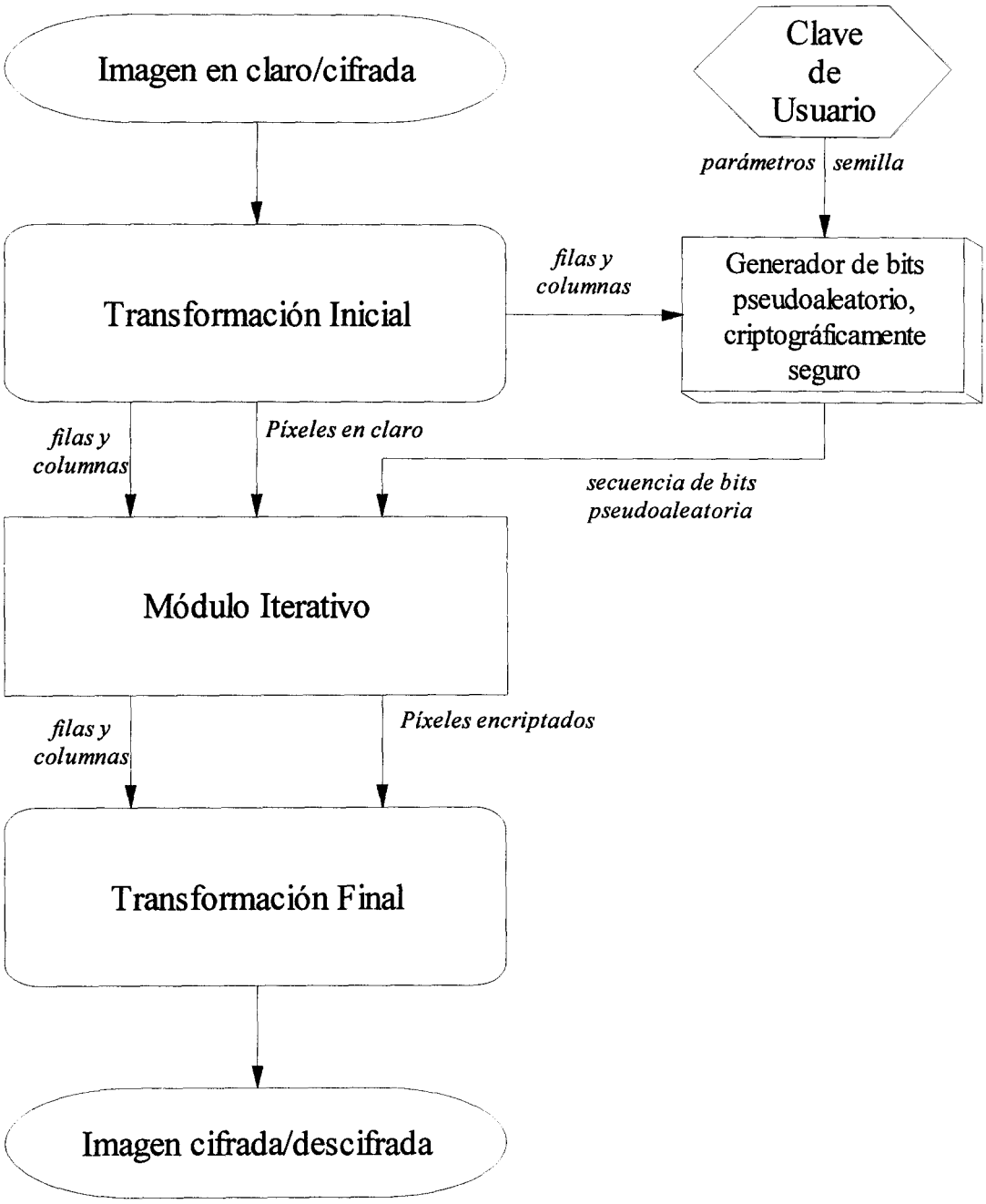
Imagen en claro/cifrada
Clave de Usuario
parámetros
semilla
Transformación Inicial
filas y columnas
Generador de bits pseudoaleatorio, criptográficamente seguro
filas y columnas
Píxeles en claro
secuencia de bits pseudoaleatoria
Módulo Iterativo
filas y columnas
Píxeles encriptados
Transformación Final
Imagen cifrada/descifrada

Figura 2

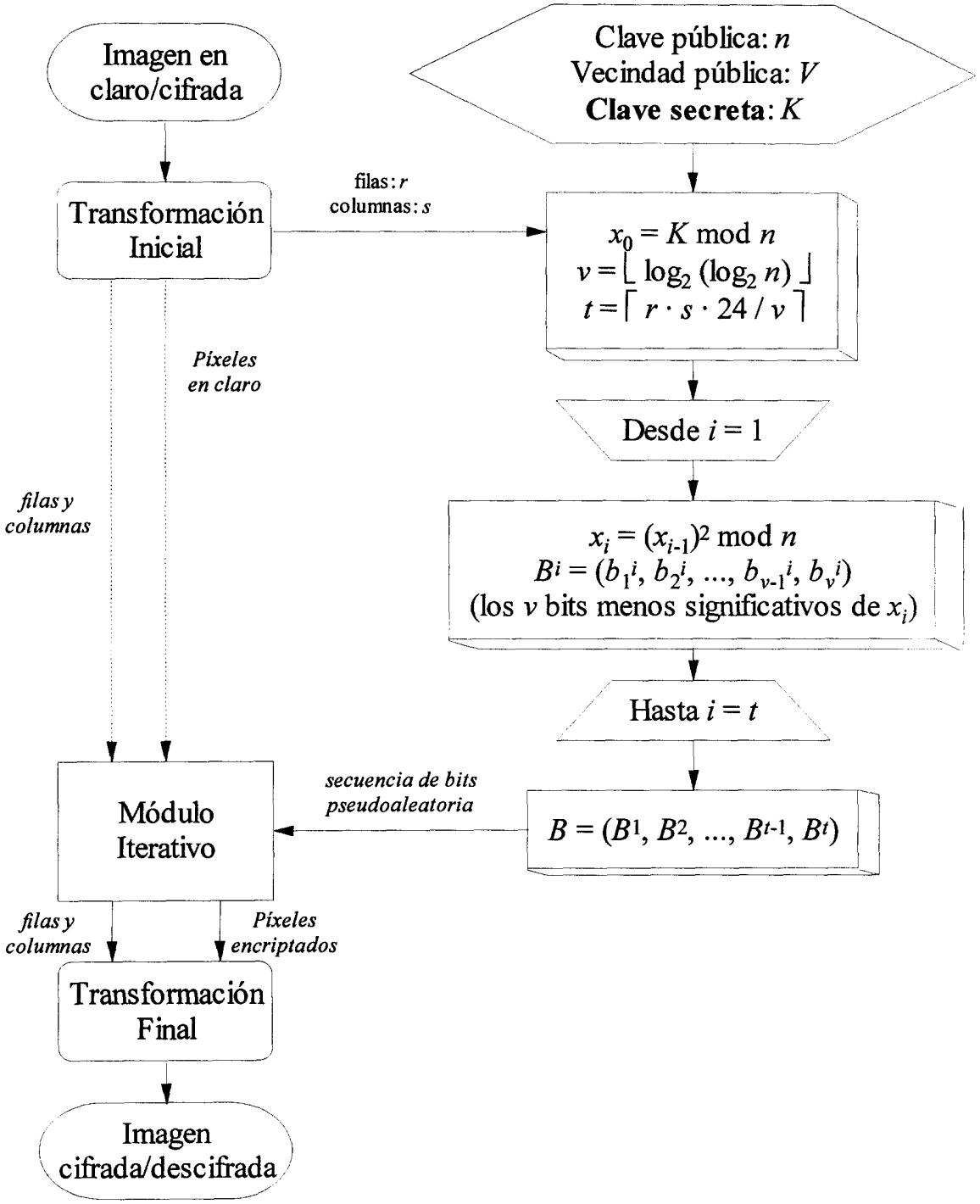
Imagen en claro/cifrada
Clave pública: n
Vecindad pública: V
Clave secreta: K
Transformación Inicial
filas: r
columnas: s
$x_0 = K \bmod n$
$v = \lfloor \log_2 (\log_2 n) \rfloor$
$t = \lceil r \cdot s \cdot 24 / v \rceil$
Píxeles en claro
Desde $i = 1$
filas y columnas
$x_i = (x_{i-1})^2 \bmod n$
$B^i = (b_1^i, b_2^i, ..., b_{v-1}^i, b_v^i)$
(los v bits menos significativos de x_i)
Hasta $i = t$
Módulo Iterativo
secuencia de bits pseudoaleatoria
$B = (B^1, B^2, ..., B^{t-1}, B^t)$
filas y columnas
Píxeles encriptados
Transformación Final
Imagen cifrada/descifrada

Figura 3

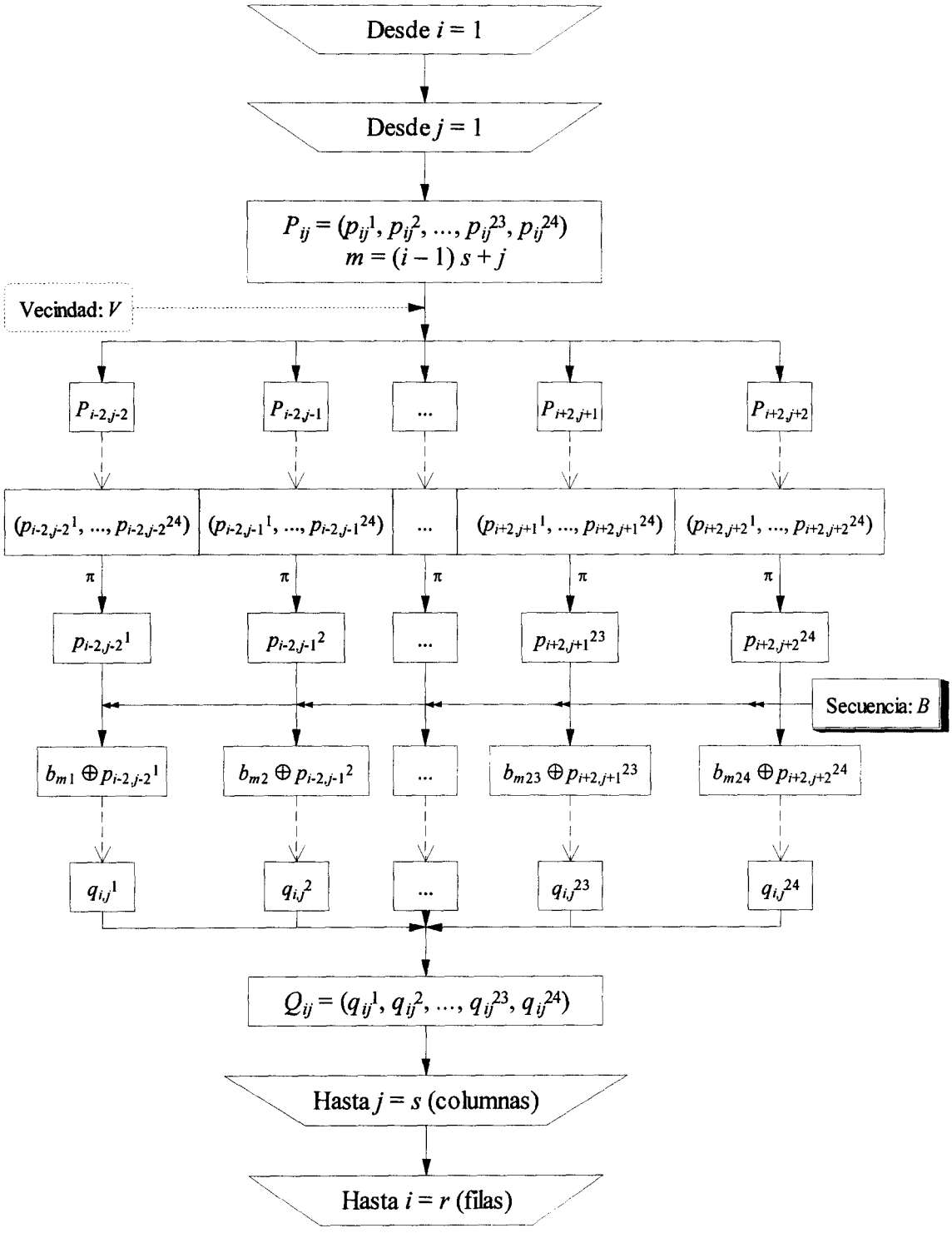
Desde $i = 1$
Desde $j = 1$
$P_{ij} = (p_{ij}^1, p_{ij}^2, \ldots, p_{ij}^{23}, p_{ij}^{24})$
$m = (i-1)\,s + j$
Vecindad: V
$P_{i-2,j-2}$
$P_{i-2,j-1}$
...
$P_{i+2,j+1}$
$P_{i+2,j+2}$
$(p_{i-2,j-2}^1, \ldots, p_{i-2,j-2}^{24})$
$(p_{i-2,j-1}^1, \ldots, p_{i-2,j-1}^{24})$
...
$(p_{i+2,j+1}^1, \ldots, p_{i+2,j+1}^{24})$
$(p_{i+2,j+2}^1, \ldots, p_{i+2,j+2}^{24})$
π
$p_{i-2,j-2}^1$
$p_{i-2,j-1}^2$
...
$p_{i+2,j+1}^{23}$
$p_{i+2,j+2}^{24}$
Secuencia: B
$b_{m1} \oplus p_{i-2,j-2}^1$
$b_{m2} \oplus p_{i-2,j-1}^2$
...
$b_{m23} \oplus p_{i+2,j+1}^{23}$
$b_{m24} \oplus p_{i+2,j+2}^{24}$
$q_{i,j}^1$
$q_{i,j}^2$
...
$q_{i,j}^{23}$
$q_{i,j}^{24}$
$Q_{ij} = (q_{ij}^1, q_{ij}^2, \ldots, q_{ij}^{23}, q_{ij}^{24})$
Hasta $j = s$ (columnas)
Hasta $i = r$ (filas)

Figura 4

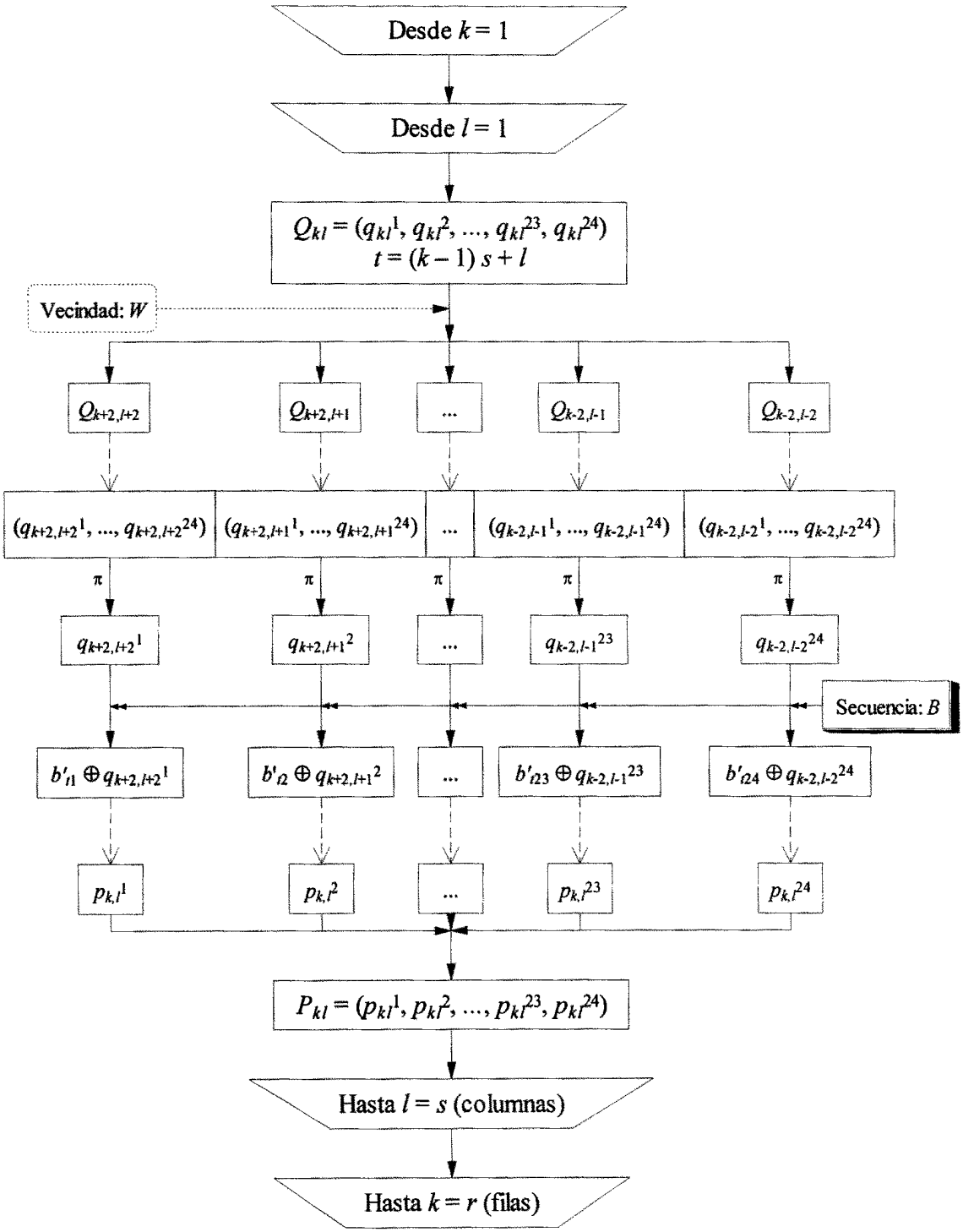
Desde $k = 1$
Desde $l = 1$
$Q_{kl} = (q_{kl}^1, q_{kl}^2, \ldots, q_{kl}^{23}, q_{kl}^{24})$
$t = (k-1)\,s + l$
Vecindad: W
$Q_{k+2,l+2}$
$Q_{k+2,l+1}$
...
$Q_{k-2,l-1}$
$Q_{k-2,l-2}$
$(q_{k+2,l+2}^1, \ldots, q_{k+2,l+2}^{24})$
$(q_{k+2,l+1}^1, \ldots, q_{k+2,l+1}^{24})$
...
$(q_{k-2,l-1}^1, \ldots, q_{k-2,l-1}^{24})$
$(q_{k-2,l-2}^1, \ldots, q_{k-2,l-2}^{24})$
π
$q_{k+2,l+2}^1$
$q_{k+2,l+1}^2$
...
$q_{k-2,l-1}^{23}$
$q_{k-2,l-2}^{24}$
Secuencia: B
$b'_{t1} \oplus q_{k+2,l+2}^1$
$b'_{t2} \oplus q_{k+2,l+1}^2$
...
$b'_{t23} \oplus q_{k-2,l-1}^{23}$
$b'_{t24} \oplus q_{k-2,l-2}^{24}$
$p_{k,l}^1$
$p_{k,l}^2$
...
$p_{k,l}^{23}$
$p_{k,l}^{24}$
$P_{kl} = (p_{kl}^1, p_{kl}^2, \ldots, p_{kl}^{23}, p_{kl}^{24})$
Hasta $l = s$ (columnas)
Hasta $k = r$ (filas)

Figura 5

Figura 6

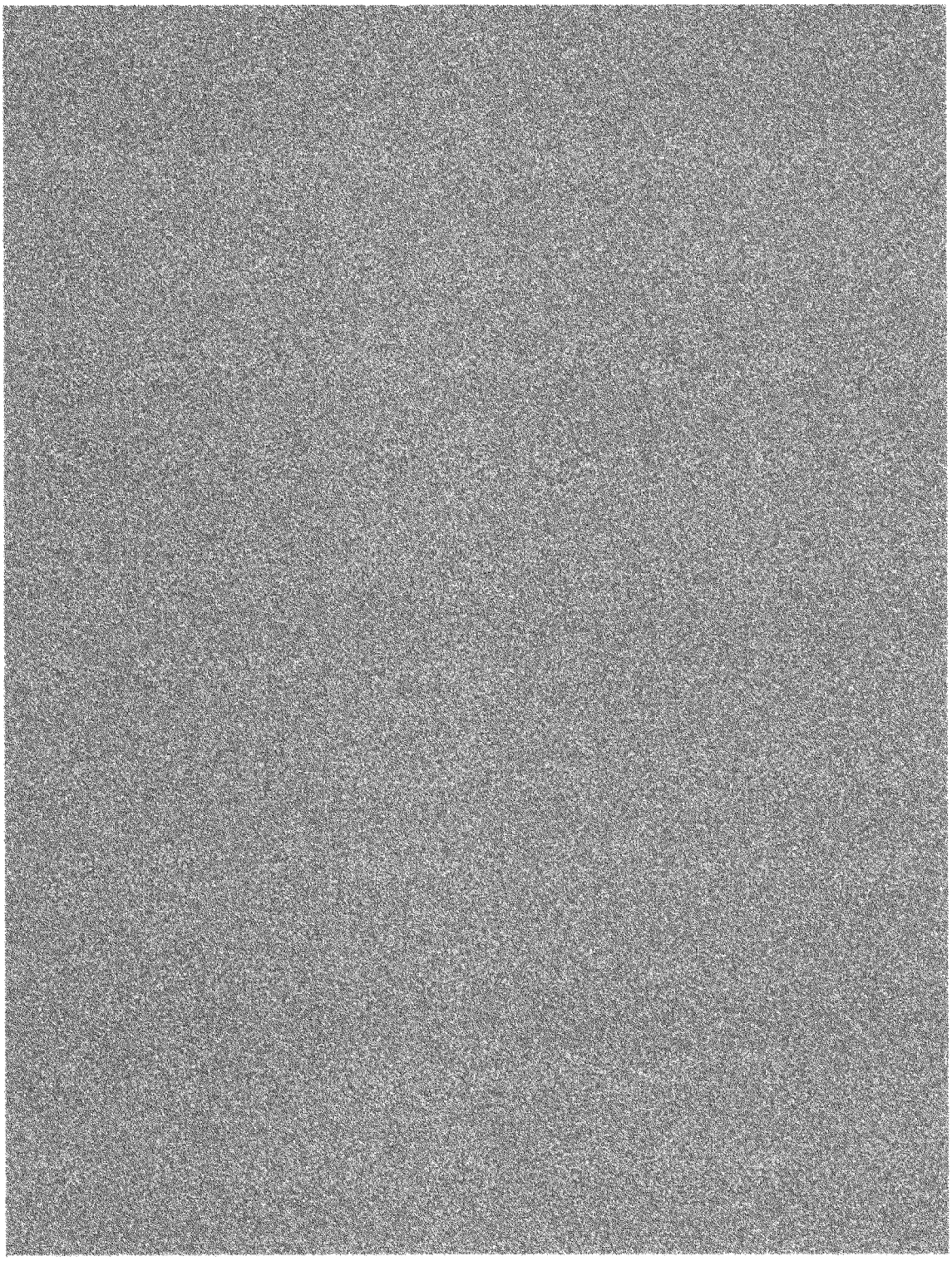

Figura 7

OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) ES 2 238 151

(21) Nº de solicitud: 200301902

(22) Fecha de presentación de la solicitud: **06.08.2003**

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TÉCNICA

(51) **Int. Cl.[7]:** H04L 9/22, 9/18, G09C 1/00, H04N 1/44, 7/167, H04L 29/06

DOCUMENTOS RELEVANTES

Categoría	Documentos citados	Reivindicaciones afectadas
X	EP 0872976 A1 (UNITED TECHNOLOGIES AUTOMOTIVE) 21.10.1998, columna 3, líneas 13-58; columna 4, líneas 1-58; columna 5, líneas 1-31,51-58; columna 6, líneas 1-6; columna 7, líneas 27-42; columna 8, líneas 5-54; columna 9, líneas 49-58; columna 11, líneas 56-58; columna 12, líneas 1,2; columna 13, líneas 13-58; reivindicaciones; figuras.	1,2
X	WO 0247272 A1 (CRYPTICO AS et al.) 13.02.2002, página 1, líneas 1-13,36-44; página 2, líneas 1-8; página 5, líneas 31-45; página 6, líneas 1-45; página 7, líneas 1-45; página 8, líneas 1-45; página 9, líneas 1-45; página 10, líneas 1-45; página 11, líneas 1-45; página 12, líneas 1-45; página 13, líneas 1-45; página 14, líneas 1-45; página 15, líneas 1-45; página 16, líneas 1-45; página 17, líneas 1-45; página 18, líneas 1-45; página 19, líneas 1-45; página 20, líneas 1-45; página 21, líneas 1-45; página 22, líneas 1-45; página 23, líneas 1-45; página 24, líneas 1-45; página 25, líneas 1-45; página 26, líneas 1-45; página 27, líneas 1-45; página 28, líneas 1-45; página 29, líneas 1-45; página 30, líneas 1-45; página 31, líneas 1-45; página 32, líneas 1-45; página 33, líneas 1-45; página 34, líneas 1-45; página 35, líneas 1-45; página 36, líneas 1-9; página 37, líneas 15-22; reivindicaciones; figuras.	1,2
X	US 5363448 A1 (KOOPMAN et al.) 08.11.1994, columna 2, líneas 45-68; columna 3, líneas 1-68; columna 4, líneas 1-43,61-68; columna 5, líneas 1-6; columna 6, líneas 19-34,55-68; columna 7, líneas 1-17; columna 8, líneas 18-30; columna 21, líneas 31-39; reivindicaciones; figuras.	1,2

Categoría de los documentos citados

X: de particular relevancia
Y: de particular relevancia combinado con otro/s de la misma categoría
A: refleja el estado de la técnica
O: referido a divulgación no escrita
P: publicado entre la fecha de prioridad y la de presentación de la solicitud
E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	Examinador	Página
15.07.2005	Mª C. González Vasserot	1/1