(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 238 168**

(21) Número de solicitud: 200302924

(51) Int. Cl.[7]: **G06T 1/00**
H04N 1/44
H04N 7/16
H04L 9/22

(12) SOLICITUD DE PATENTE A1

(22) Fecha de presentación: **10.12.2003**

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

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

(71) Solicitante/s:
Consejo Superior de Investigaciones Científicas
Serrano, 117
28006 Madrid, ES
Universidad de Salamanca

(72) Inventor/es: **Hernández Encinas, Luis;**
Álvarez Marañón, Gonzalo y
Martín del Rey, Ángel

(74) Agente: **No consta**

(54) Título: **Procedimiento y dispositivo para dividir de forma secreta, compartir y recuperar imágenes.**

(57) Resumen:
Procedimiento y dispositivo para dividir de forma secreta, compartir y recuperar imágenes.
Se presenta un procedimiento y dispositivo que permite: 1. Dividir de forma secreta una imagen digitalizada, definida por cualquier número de colores, en partes o sombras, de modo que sean repartidas de forma segura entre un grupo de participantes, 2. Compartir las sombras de la imagen secreta, sin que cada uno de los participantes pueda acceder al secreto de forma individual, y 3. Recuperar la imagen original, a partir de la utilización de un número de sombras fijado de antemano, de modo que no sea posible obtener ninguna información de la imagen secreta original uniendo la información procedente de menos sombras de las prefijadas. 4. El procedimiento está basado en un esquema gráfico umbral, criptográficamente seguro, que utiliza un autómata celular bidimensional.

ES 2 238 168 A1

DESCRIPCIÓN

Procedimiento y dispositivo para dividir de forma secreta, compartir y recuperar imágenes.

Objeto de la invención

Se presenta un procedimiento y dispositivo que permite:

(1) Dividir de forma secreta una imagen digitalizada, definida por cualquier número de colores, en partes o sombras, de modo que sean repartidas de forma segura entre un grupo de participantes,

(2) Compartir las sombras de la imagen secreta, sin que cada uno de los participantes pueda acceder al secreto de forma individual, y

(3) Recuperar la imagen original, a partir de la utilización de un número de sombras fijado de antemano, de modo que no sea posible obtener ninguna información de la imagen secreta original uniendo la información procedente de menos sombras de las prefijadas.

El procedimiento está basado en un esquema gráfico umbral, criptográficamente seguro, que utiliza un autómata celular bidimensional.

Sectores de la técnica en los que tiene aplicación

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

Estado de la técnica

Un *esquema para la división de secretos* es un método que permite dividir un secreto entre un conjunto de n participantes de modo que sólo determinados conjuntos de usuarios cualificados pueden recuperar el secreto original. La idea básica de estos esquemas consiste en permitir que un Director (o Tercera parte de confianza), en el que confían todos los participantes, divida el secreto a compartir en tantas piezas (denominadas *sombras*) como participantes. Dichas sombras son distribuidas entre los n participantes en el protocolo, de modo que para recuperar el secreto original se deben unir k sombras, $1 \leq k \leq n$, y de tal manera que la unión de $k - 1$ sombras, o menos, no permite obtener información alguna del secreto original.

Los esquemas para la división de secretos fueron introducidos independientemente por Shamir ([Sha79]) y Blakley ([Bla79]). Su motivación original era la de salvaguardar de la pérdida o del robo las claves utilizadas en los procedimientos criptográficos. Posteriormente, estos esquemas han sido ampliamente utilizados en otros protocolos criptográficos (ver, por ejemplo, [MOV97]) y en otras actividades, como en el control de accesos, en la apertura de cajas fuertes o de seguridad, e incluso en el lanzamiento de misiles.

El ejemplo básico de un esquema para la división de secretos (tanto el basado en el de Shamir como en el de Blakley) es *el esquema umbral* k-de-n o (k, n), donde k y n son números enteros tales que $1 \leq \mathrm{k} \leq n$. En estos esquemas existen n participantes y un director. El director calcula de forma secreta n sombras, S_i, $0 \leq \mathrm{i} \leq n - 1$, a partir de un secreto inicial, S, y distribuye de forma segura cada una de las sombras a cada uno de los n participantes, P_o, ..., $P_{\mathrm{n}-1}$, de modo que:

1. Cualesquiera k, o más, participantes que utilicen sus sombras pueden recuperar fácilmente el secreto original, S,

2. Cualquier grupo de $k - 1$ participantes, o menos, no obtendrá ninguna información acerca del secreto.

En general, el secreto que se divide y comparte en los esquemas presentados anteriormente son datos de texto o mensajes. Sin embargo, también es posible dividir y compartir imágenes. El primer esquema para dividir imágenes se debió a Naor y Shamir ([NS95]) y se denomina *Criptografía visual*. Esta Criptografia se fundamenta en los esquemas visuales umbrales k-de-n ([Sti92]); es decir, la imagen original se divide en n sombras, cada una de las cuales se fotocopia a una transparencia y se distribuye de forma segura a cada uno de los participantes. Para recuperar la imagen secreta original no es preciso llevar a cabo ningún protocolo criptográfico, basta con superponer cualesquiera k transparencias, pero no menos (una descripción de estos protocolos puede verse en [HM99] y [HMM00]).

Originalmente, estos esquemas visuales sólo podían ser aplicados a imágenes en blanco y negro; aunque en los últimos años se han desarrollado nuevos esquemas que permiten utilizar imágenes en tonos de gris ([LT03], [TL02],

[VT97]) y en color ([CTC99], [Hou03], [RP96]). Sin embargo, en los esquemas visuales para imágenes en color o tonos de gris ya se deben llevar a cabo determinados cómputos con las imágenes y no basta con superponer las transparencias de cada una de ellas. Por otra parte, para todos estos esquemas, cada pixel es cifrado por medio de varios píxeles para cada una de las *n* sombras (el número de píxeles necesarios para cifrar cada uno de los píxeles originales se conoce como *expansión del píxel*). Este hecho hace que el tamaño de cada una de las sombras sea mayor que el de la imagen original, lo cual es un inconveniente. De hecho, si el factor de expansión del pixel es el mínimo posible (caso de las imágenes en blanco y negro), es decir, es 2, entonces cada una de las sombras tiene el doble número de píxeles en horizontal y el doble número en vertical, que la imagen original. En otras palabras, cada sombra es el doble de larga y el doble de ancha que la imagen original.

Otra desventaja que presentan estos esquemas, cualquiera que sea el número de colores de imagen secreta a dividir y compartir, es la gran pérdida de contraste que se produce a la hora de recuperar la imagen original; es decir, nunca se recupera la imagen primitiva. En todos los casos se hace uso de la capacidad visual humana que permite apreciar y reconocer los rasgos generales de una imagen que tiene poca resolución y una gran pérdida de contraste.

Otros algoritmos para dividir y compartir imágenes que no hacen uso de la criptografia visual se describen en [CH98] y [TCCO2].

Por otra parte, el diseño de protocolos criptográficos mediante autómatas celulares no es novedoso, aunque sí lo es en el uso de los esquemas para compartir secretos, como el que se realiza en esta invención. Así, los autómatas celulares se han propuesto para su uso tanto en sistemas de cifrados en flujo ([DHH03], [Wol86]) como en bloque ([Gut93]), en criptosistemas de clave pública ([Gua87]) y en criptosistemas gráficos de clave secreta ([HMO2], [HMH02]).

En esta invención se presenta un nuevo esquema umbral para dividir de forma secreta, compartir y recuperar una imagen secreta. La imagen puede ser en blanco y negro, en tonos de gris o en color. La invención se basa en un tipo de sistemas dinámicos discretos conocidos como *autómatas celulares*, que pueden ser utilizados para dividir una imagen secreta en sombras de modo que (1) cada sombra tiene el mismo tamaño que la imagen original y (2) la imagen recuperada es exactamente la misma que la original, sin que haya pérdida de resolución ni de contraste alguno. Estas dos propiedades son las que hacen que esta invención sea completamente novedosa.

Referencias

[A1o03] R. **Alonso-Sanz**, *Reversible cellular automata with memory: two-dimensional patterns from a single seed*, *Phys*. D **175** (2003), 1-30.

[B1a79] G.R. **Blakley**, *Safeguarding cryptographic keys*, AFIPS Conference Proceedings **48** (1979), 313-317.

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

[CTC99] C.C. **Chang**, C.S. **Tsai** and T.S. **Chen**, *A technique for sharing a secret color image*, *Proc. Ninth National Conf. on Information Security, Taichung*, 1999, 63-72.

[CH98] C. **Chang** and R. **Hwang**, *Sharing secret images using shadow codebooks*, *Inform. Sci*. **111** (1998), 335-345.

[DHH03] R. **Díaz Len**, A. **Hernández Encinas**, L. **Hernández Encinas**, S. **Hoya White**, A. **Martín del Rey**, G. **Rodríguez Sánchez** and I. **Visus Ruíz**, *Wolfram cellular automata and their cryptographic use as pseudorandom bit generators, Internat*. *J. Pure Appl. Math*. **4** (2003), 87-103.

[Gua87] P. **Guan**, *Cellular automaton public-key cryptosystem, Complex Systems* **1** (1987), 51-57.

[Gut93] H. A. **Gutowitz**, *Cryptography with dynamical systems, in Cellular Automata and Cooperative Systems*, *Proc. of the NATO Advanced Study Institute*, Dordrech, 1993, 237-274.

[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.

[HM99] L. **Hernández Encinas** y J. **Minguet Melián**, *Criptografía visual, Novática* **138** (1999), 63-68.

[HMM00] L. **Hernández Encinas**, F. **Montoya Vitini** y J. **Muñoz Masqué**, *Esquemas criptográficos visuales*, SIC **38** (2000), VI-X.

[HMM98] L. **Hernández Encinas**, F. **Montoya Vitini**, J. **Muñoz Masqué** and A. **Peinado Domínguez**, *Maximal*

periods of orbits of the BBS generator, *Proc. 1998 Int. Conf. on Inform. Secur. & Cryptol.*, 71-80, Seúl, 1998.

[Hou03] Y. **Hou**, *Visual cryptography for color images*, *Pattern Recognition* **36** (2003), 1619-1629.

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

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

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

[RP96] V. **Rijmen** and B. **Preneel**, *Efficient colour visual encryption or 'Shared colours of Benetton'*, Rump Session of Eurocrypt'96, available in htpp://www.iacr.org/ conferenc es/ec 96/rump/preneel.ps

[Sha79] A. **Shamir**, *How to share a secret*, *Commun. ACM* **22** (1979), 612-613.

[Sti92] D.R. **Stinson**, *An explication of secret sharing schemes, Des. Codes Cryptogr*. **2** (1992), 357-390.

[TL02] C. **Thien** and J.C. **Lin**, *Secret image sharing, Computer & Graphics* **26** (2002), 765-770.

[TM90] T. **Toffoli** and N. **Margolus**, *Invertible cellular automata: A review, Phys. D* **45** (1990), 229-253.

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

[VT97] E.R. **Verheul** and H.C.A. van **Tilborg**, *Construction and properties of k out of n visual secret sharing schemes, Des. Codes Cryptogr*. **11** (1997), 179-196.

[Wo186] S. **Wolfram**, *Random sequence generation by cellular automata*, *Adv. Appl. Math*. 7 (1986), 123-169.

Explicación de la invención

Breve descripción de la invención

A partir del protocolo genérico de los esquemas umbrales que se han mencionado en la sección sobre el Estado de la Técnica (ver Figura 1), se presenta aquí el protocolo general del esquema gráfico umbral para dividir en secreto, compartir y recuperar imágenes, definidas por cualquier número de colores, que se propone en esta invención. Este esquema gráfico umbral sigue la misma estructura general de los esquemas umbrales anteriores, y se diferencia de los mismos en que utiliza un proceso novedoso para la división secreta de la imagen y para su posterior recuperación.

El secreto del que se parte para ser dividido, compartido y recuperado, es una imagen digitalizada, que está almacenada en un fichero. El protocolo de esta invención es llevado a cabo por un director (o tercera parte de confianza) en el que confían todos los participantes, y comienza con el establecimiento del tipo de esquema umbral *k*-de-*n* que va a llevar a cabo; es decir, la determinación del número de participantes en el protocolo (*n*) y del número mínimo de sombras (*k*) que se requieren para recuperar la imagen secreta.

A continuación se procede a la lectura digital de la imagen que se desea dividir de manera secreta. De este modo se conocen sus características esenciales: tamaño (número de píxeles en cada fila y en cada columna) y número de colores. Una vez conocidos todos estos datos, el procedimiento es ejecutado por el director, quien genera de forma aleatoria tanto *k* - 1 números como *k* - 1 imágenes del mismo tamaño y del mismo tipo que la original (en blanco y negro, en tonos de gris o en color). A continuación la imagen secreta es manipulada, utilizando las *k* - 1 imágenes aleatorias generadas, mediante un procedimiento basado en un *autómata celular bidimensional híbrido con memoria y reversible*, por el que se elaboran, de forma consecutiva y ordenada, las n sombras necesarias. Una vez obtenidas las sombras, el director destruye las *k* - 1 imágenes aleatorias utilizadas; distribuye las sombras, de forma ordenada y secreta, a cada uno de los participantes, y da a conocer a todos los participantes los *k* - 1 números generados. De esta forma todos los participantes comparten partes de una imagen secreta, y del mismo tamaño que ésta, pero no tienen acceso a la imagen de forma individual.

La recuperación de la imagen secreta original se lleva a cabo compartiendo la información que proporcionan, al menos, *k* sombras consecutivas de las *n* existentes. Este proceso se lleva a cabo sin necesidad de la colaboración del director y en el mismo se utiliza el *autómata celular bidimensional híbrido con memoria inverso* al utilizado en la fase de la división.

Descripción detallada de la invención

A partir del esquema general para la división de secretos, señalado anteriormente (ver Figura 1), se presenta a

continuación una descripción detallada de cómo llevar a cabo el esquema gráfico umbral *k*-de-*n* para la división secreta y posterior recuperación de imágenes, que es el objeto de la presente invención.

En primer lugar se presentarán, de forma resumida, las herramientas matemáticas que se utilizan en el esquema gráfico umbral propuesto en esta invención y a continuación se procederá a describir las tres fases del proceso que se sigue para llevar a cabo el protocolo de esta invención:

1. Inicialización del esquema gráfico umbral *k*-de-*n*,
2. División de la imagen secreta en *n* sombras y
3. Recuperación de la imagen original a partir de *k* sombras consecutivas de las *n* existentes.

1. *Herramientas matemáticas*

En el esquema gráfico umbral *k*-de-*n* para dividir de forma secreta, compartir y recuperar de forma cualificada imágenes definidas por píxeles y con cualquier número de colores, se utilizan dos herramientas matemáticas: un autómata celular bidimensional híbrido con memoria y reversible, y un generador de bits pseudoaleatorio, criptográficamente seguro.

La primera de las herramientas matemáticas es una clase de sistema dinámico discreto, denominado *Autómata Celular* (AC), que constituye el fundamento del esquema gráfico umbral; mientras que la segunda, el generador de bits, sólo se precisa para generar, de forma aleatoria y segura, las *k* - 1 matrices que utilizará el director en la fase de la división secreta de la imagen.

Un autómata celular bidimensional (*I, S, V, f*) es un sistema dinámico discreto formado por un espacio celular (matriz), *I*, de *r* x *s* objetos idénticos, llamados células, y representadas como <*i, J*>, con $0 \leq i \leq r - 1$, $0 \leq j \leq s - 1$. El estado de la célula <*i, j*> en el instante de tiempo *t* se representa por $a_{ij}^{(t)}$ y es un elemento del *conjunto de estados, S*. La evolución del autómata celular en pasos discretos del tiempo viene determinado por su *función de transición local*:

$$f : S^v \; S,$$

que permite determinar el estado de cada célula en el instante $t + 1$ en función de los estados de *v* células en el instante *t*, incluyendo la propia célula, y que constituye su *vecindad, V*.

Si en la evolución de una célula dada se utilizan diferentes funciones de transición local en lugar de una sola, el AC se dice *híbrido*. En el caso en que en tal evolución intervengan los estados de las células vecinas en los tiempos *t* - 1, *t* - 2, etc., se dice que el AC tiene *memoria* ([Alo03]). Un AC se dice *reversible* ([TM90]) si existe otro AC, llamado su *inverso*, que determina su evolución inversa. La evolución de un AC a lo largo del tiempo se representa por $\{C^{(t)}\}_{0 \leq t \leq 1}$, siendo $C^{(0)}$ la configuración inicial.

Si el esquema gráfico umbral a desarrollar es un esquema *k*-de-*n*, en la invención se utilizará un autómata celular bidimensional híbrido con memoria y reversible (ACMR), definido por las siguientes características:

a) El espacio celular, *I*, es una imagen genérica del mismo tamaño, $r \times s$, que la imagen considerada en el esquema gráfico umbral.

b) El conjunto de estados, *S*, es el conjunto de los números enteros módulo un entero, *c*: $S = Z_c$, siendo $c = 2^b$ el número máximo de colores de la imagen secreta que se utilice en cada uno de los protocolos. Es decir, si la imagen es en blanco y negro entonces $b = 1$ y $c = 2$; si la imagen sólo contiene tonos de gris, se tiene $b = 8$; esto es, $c = 2^8 = 256$ tonos de gris; y si la imagen es en color, entonces $b = 24$ y, en consecuencia, el máximo número de colores será $c = 2^{24} = 16.777.216$.

Dado que el espacio celular de los autómatas celulares que se utilizarán es finito, se considerarán condiciones de contorno periódicas:

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

c) La vecindad de la célula <*i, j*> en el instante *t*, $V_{ij}^{(t)}$, es la *vecindad de Moore*, en la que se consideran $v = 9$ vecinos, y que puede representarse como sigue:

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

d) La evolución del ACMR, para que sea reversible, vendrá expresada mediante una función de transición, *f*, de la siguiente forma:

$$f \equiv a_{ij}^{(t+1)} = f^{(1)}(V_{ij}^{(t)}) + f^{(2)}(V_{ij}^{(t-1)}) + \ldots + f^{(k-1)}(V_{ij}^{(t-k+2)}) + f^{(k)}(V_{ij}^{(t-k+1)}) \bmod c,$$

donde la última función de transición local, $f^{(k)}$, es la identidad:

$$f^{(k)}(V_{ij}^{(t-k+1)}) = a_{ij}^{(t-k+1)}.$$

y las $f^{(h)}$, $1 \leq h \leq k - 1$, son $k - 1$ funciones de transición locales de la forma:

$$f^{(h)}(V_{ij}^{(t-h)}) = \lambda_{-1,-1}\, a_{i-1,j-1}^{(t-h)} + \lambda_{-1,0}\, a_{i-1,j}^{(t-h)} + \lambda_{-1,1}\, a_{i-1,j+1}^{(t-h)} + \lambda_{0,-1}\, a_{i,j-1}^{(t-h)} + \lambda_{0,0}\, a_{i,j}^{(t-h)} + \lambda_{0,1}\, a_{i,j+1}^{(t-h)} + \lambda_{1,-1}\, a_{i+1,j-1}^{(t-h)} + \lambda_{1,0}\, a_{i+1,j}^{(t-h)} + \lambda_{1,1}\, a_{i+1,j+1}^{(t-h)},$$

y que pueden ser representadas como f_{w_i}, siendo w_i un entero decimal, $0 \leq w\_i \leq 511$:

$$w\_i = \lambda_{-1,-1}\, 2^8 + \lambda_{-1,0}\, 2^7 + \lambda_{-1,1}\, 2^6 + \lambda_{0,-1}\, 2^5 + \lambda_{0,0}\, 2^4 + \lambda_{0,1}\, 2^3 + \lambda_{1,-1}\, 2^2 + \lambda_{1,0}\, 2^1 + \lambda_{1,1}\, 2^0.$$

La segunda herramienta matemática que se utilizará es un *generador de bits pseudoaleatorio* (GBPA), consistente en un algoritmo determinístico que, al recibir como entrada una secuencia de bits realmente aleatoria de longitud pequeña *l*, proporciona como salida una secuencia de bits de longitud mucho más grande $g >> l$, y que parece ser aleatoria. La entrada al algoritmo de longitud *l* se conoce como semilla, mientras que la salida que proporciona el algoritmo se denomina *secuencia de bits pseudoaleatoria* ([MOV97]). Es conveniente que el GBPA tenga buenas propiedades aleatorias con el fin de evitar posibles ataques a la seguridad del esquema, por el análisis estadístico de las secuencias utilizadas en el esquema. Por tanto, es necesario que el generador sea *criptográficamente seguro* (GBPACS); es decir, que su seguridad se base en la dificultad de resolver un problema matemático. Esta seguridad significa que no debe existir ningún algoritmo eficiente 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.

2. Fase 1

Inicialización del esquema gráfico umbral k-de-n

El primer paso para llevar a cabo el esquema gráfico umbral que se propone en esta invención consiste en decidir los parámetros del esquema (ver Figura 2); esto es, determinar los valores de *n* (participantes) y de *k* (sombras). A continuación se debe tratar la imagen para su manipulación en el esquema gráfico umbral, para lo que se procede a la lectura del fichero de la imagen, *I*, obteniéndose los siguientes datos: número máximo de colores de la imagen, $c = 2^b$, con $b = 2, 8, 24$; número de filas: *r*; número de columnas: *s*; y color de cada uno de los *r* x *s* píxeles de la imagen: P_{ij}, donde $1 \leq i \leq r$, $1 \leq j \leq s$. La imagen deberá ser considerada como una matriz con coeficientes en Z_c, de la siguiente manera:

a) Si *I* es una imagen en blanco y negro, entonces *M* es una matriz *r* x *s* cuyo coeficiente (*i, j*) es 1 (resp. 0) si el pixel p_{ij}, es negro (resp. blanco); es decir, los coeficientes de *M* están en Z_2 (c = 2, y por tanto, b = 1).

b) Si *I* es una imagen con niveles de gris, entonces el código RGB de cada pixel p_{ij} es la terna (*R, G, B*), con $R = G = B$ y $0 \leq R, G, B \leq 255$. Por tanto, cada pixel se puede representar mediante un número $0 \leq R \leq 255$. Así pues, *M* es una matriz *r* x *s* con coeficientes en Z_c, $c = 2^8 = 256$.

c) Finalmente, si *I* es una imagen en color, cada pixel está dado por 24 bits, ocho para cada color básico: rojo (*R*), verde (*G*) y azul (*B*). Por tanto, *M* es una matriz *r* x *s* con coeficientes en Z_c, $c = 2^{24} = 16.777.216$.

Una vez que la imagen está codificada mediante una matriz, el director procede con la primera de las fases del esquema gráfico umbral de la siguiente forma:

1) Genera un conjunto $\{w\_1, w\_2, ..., w\_k\text{-}1\}$ de $k - 1$ números enteros aleatorios, de modo que $0 \leq w\_h \leq 511$, con $1 \leq h \leq k - 1$. Estos números representan los números de las reglas de transición para el ACMR a utilizar, y deben ser distribuidos entre los n participantes (o publicados) si se desea que el papel del director se limite a elaborar las sombras y no sea necesaria su colaboración para el proceso de recuperación de la imagen original secreta.

2) Construye el ACMR cuya función de transición es:

$$f \equiv a_{ij}^{(t+1)} = f_{w\_1}(V_{ij}^{(t)}) + f_{w\_2}(V_{ij}^{(t-1)}) + \ldots + f_{w\_k-1}(V_{ij}^{(t-k+2)}) + a_{ij}^{(t-k+1)} \bmod c,$$

con f_{w_h}:$(Z_c)^9$ Z_c.

3) Considera la matriz correspondiente a la imagen secreta a compartir como la configuración inicial del ACMR; es decir, $M = C^{(0)}$. Además, genera k - 1 configuraciones aleatorias: $C^{(1)}$,..., $C^{(k-1)}$, para poder iniciar la evolución del ACMR, por medio de un GBPACS, con el objetivo de evitar un ataque al esquema por la suposición de los valores de estas k - 1 matrices. Las k - 1 configuraciones generadas deben ser destruidas después de calcular las sombras.

3. Fase 2

División de la imagen secreta en n sombras

Para llevar a cabo la división de la imagen secreta en sombras, el director utiliza el ACMR generado en la fase anterior y lleva a cabo los siguientes pasos (ver Figura 3):

1) Elige un entero umbral m, con $k \leq m$, con el fin de evitar posibles solapamientos entre las condiciones iniciales y las sombras. Debe tenerse en cuenta que el número de iteraciones del ACMR crece con m, por lo que este número no debe ser mucho mayor que k.

2) Calcula, a partir de las k primeras configuraciones, $C^{(0)}$,..., $C^{(k-1)}$, la evolución de orden $m + n$ - 1 del ACMR iterando la función de transición f:

$$\{C^{(0)}, C^{(1)}, ..., C^{(k-1)}, C^{(k)}, ..., C^{(m)}, ..., C^{(m+n-1)}\}.$$

3) Las sombras a ser distribuidas entre los n participantes, P_0, ..., P_{n-1}, son las últimas n configuraciones calculadas:

$$S_0 = C^{(m)}, S_1 = C^{(m+1)}, ...S_{n-1} = C^{(m+n-1)}.$$

Además, cada participante recibe o conoce el conjunto de números aleatorios generado por el director en el paso 1) de la fase de inicialización. De este modo, cada uno de ellos puede construir la función inversa de la función de transición del ACMR, con el objeto de recuperar la imagen original, sin necesidad de depender de la colaboración del director.

4. Fase 3

Recuperación de la imagen original a partir de k sombras consecutivas de las n existentes

Para recuperar la imagen secreta original son necesarias cualesquiera k (de las n) sombras consecutivas, pero no menos. Los pasos siguientes definen esta fase (ver Figura 4).

a) Para recuperar la imagen secreta, $C^{(0)}$; es decir, la configuración inicial del ACMR, se requieren k sombras consecutivas de la forma:

$$S_h = C^{(m+h)}, S_{h+1} = C^{(m+h+1)}, \ldots, S_{h+k-1} = C^{(m+h+k-1)}, \quad 0 \leq h \leq n - k.$$

b) Se considera la función de transición inversa del ACMR utilizado en la fase de división, g, que viene dada por

$$g \equiv a_{ij}^{(t+1)} = -f_{w\_k-1}(V_{ij}^{(t)}) - f_{w\_k-2}(V_{ij}^{(t-1)}) - \ldots - f_{w\_1}(V_{ij}^{(t-k+2)}) + a_{ij}^{(t-k+1)} \bmod c.$$

c) Tomando $T^{(h)}$ como la configuración h-ésima del ACMR inverso; es decir,

$$T^{(0)} = C^{(m+h+k-1)}, T^{(1)} = C^{(m+h+k-2)}, \ldots, T^{(k-1)} = C^{(m+h)},$$

e iterando $m + h + k - 1$ veces la función de transición g, se obtiene la configuración original; es decir, la imagen secreta.

Debe tenerse en cuenta que la imagen recuperada es exactamente la misma que la imagen original debido a que el ACMR utilizado es reversible. Esta propiedad del esquema propuesto en esta invención no se verifica en ningún otro esquema gráfico propuesto hasta la fecha. Además, como cada participante conoce la función de transición, no hace falta la colaboración del director para recuperar la imagen secreta.

El precio que hay que pagar por el hecho de recuperar exactamente la imagen secreta original es el de llevar a cabo los cálculos de la fase de recuperación, cuando en la criptografía visual, para imágenes en blanco y negro (no para las de tonos de gris o en color), bastaba con superponer las transparencias correspondientes.

Descripción de las figuras

Figura 1

Protocolo general de un esquema umbral k-de-n

En esta figura se presenta el protocolo general que se sigue en un esquema umbral *k-de-n*, en el que determinado secreto es dividido en *n* sombras y hacen falta *k* de ellas, al menos, para recuperar el secreto original.

Figura 2

Protocolo de la fase 1: Inicialización del esquema gráfico umbral k-de-n

El protocolo que se sigue en la primera fase del esquema gráfico umbral desarrollado en esta invención es el que se presenta en la Figura 2. En él se inicializan los datos que van a ser empleados posteriormente; es decir, se determinan los parámetros del esquema, las propiedades de la imagen secreta y se generan los números y matrices necesarios.

Figura 3

Protocolo de la fase 2: División de la imagen secreta en n sombras

En la Figura 3 se resume el protocolo de la fase de división del esquema propuesto. En esta fase se lleva a cabo la división secreta de la imagen en sombras mediante la determinación de la evolución del autómata celular empleado.

Figura 4

Protocolo de la fase 3: Recuperación de la imagen original a partir de k sombras consecutivas de las n existentes

La tercera fase del esquema gráfico se presenta en esta figura. Es este caso se procede a la recuperación de la imagen secreta original sin más que calcular la evolución del autómata celular inverso al utilizado en la fase de división.

Figura 5

Ejemplo de esquema 4-de-4 para una imagen en blanco y negro

Un caso particular de cómo dividir una imagen en blanco y negro, por ejemplo el diseño de un circuito, se presenta en esta figura. La imagen tiene 269 x 213 píxeles y los parámetros del esquema gráfico son: $n = k = m = 4$, es decir, se han considerado cuatro participantes y hacen falta las cuatro sombras para recuperar el circuito original. La imagen original esta representada por (a) y la imagen recuperada por (f); mientras que las imágenes (b), (c), (d) y (e) son las sombras generadas por el esquema. Puede observarse que las imágenes (a) y (f) son idénticas, mientras que a partir de cualquiera de las sombras no se obtiene ninguna información sobre la imagen original.

Figura 6

Ejemplo de esquema 3-de-10 para una imagen en tonos de gris

Como ejemplo de imagen en tonos de gris se ha elegido la radiografía de una muñeca (imagen (a) de la Figura 6). Esta radiografía tiene 249 tonos de gris y su tamaño es de 181 x 157 píxeles. El esquema gráfico umbral considerado es un esquema 3-de-10 con un umbral $m = 20$; es decir, para recuperar la radiografía son necesarias 3 sombras consecutivas de las 10 que se han elaborado. Las sombras aparecen marcadas de la (b) a la (k), mientras que la imagen recuperada a partir de las sombras (i), (j) y (k) está señalada como (1).

Figura 7

Ejemplo de esquema 3-de-6 para una imagen en color

En esta figura se muestra una imagen parcial de Júpiter con sus lunas, de 24852 colores (imagen (a) de la Figura 7) y el resultado de haberle aplicado el esquema gráfico umbral 3-de-6 desarrollado en esta invención, con un umbral $m = 4$. La imagen recuperada es la (h) y las sombras obtenidas se han denotado de la (b) a la (g).

Exposición detallada de un modo de realización de la invención

A continuación se describe una posible implementación de cómo llevar a cabo el proceso para dividir de forma secreta, compartir y recuperar una imagen cualquiera, denotada por *I*, siguiendo las fases indicadas en la sección relativa a la Descripción detallada de la invención.

Dado que el esquema propuesto permite utilizar imágenes en blanco y negro, en tonos de gris y en color, se considerarán como imágenes secretas las que se muestran como imágenes (a) en las Figuras 5, 6 y 7, respectivamente. Para cada tipo de imagen se va a considerar un esquema gráfico umbral diferente, con el fin de mostrar la versatilidad del esquema que se propone en esta invención.

Por otra parte, como es necesario utilizar un generador de bits para el paso 3) de la fase de inicialización cuando se generan las k – 1 matrices a emplear en la evolución del autómata celular, para esta exposición detallada se ha optado por emplear uno de los GBPACS más utilizados: el generador BBS ([BBS86]). Este generador se define considerando el bit de paridad (bit menos significativo) de cada uno de los números obtenidos en la siguiente iteración:

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

siendo x_0 la semilla, $n = p \cdot q$, con p y q dos números primos grandes, cada uno de ellos congruentes con 3 módulo 4, y verificando las condiciones señaladas en [HMMP98], donde ha sido caracterizado. Su seguridad se basa en la presunta intratabilidad computacional de resolver el problema de la factorización entera.

Fase de inicialización

Ejemplo 1

(Imagen en blanco y negro)

La imagen en blanco y negro que representa el diseño de un circuito (imagen (a) de la Figura 5) tiene 269 x 213 = 57297 píxeles. Para este caso se han considerado los siguientes valores: $n = k = 4$; es decir, se ha supuesto la existencia de cuatro participantes y la necesidad de que todos ellos se pongan de acuerdo para recuperar el circuito original.

En el paso 1) de la fase de inicialización se deben generar k - 1 = 3 números aleatorios para determinar las funciones de transición. Estos números son 232, 29 y 225. Así pues, las funciones de transición señaladas en el paso 2) de esta fase y utilizadas por el director para este ejemplo son:

$$f_{232}(V_{ij}^{(t)}) = a_{i-1,j}^{(t)} + a_{i-1,j+1}^{(t)} + a_{i,j-1}^{(t)} + a_{i,j+1}^{(t)},$$

$$f_{29}(V_{ij}^{(t)}) = a_{i,j}^{(t)} + a_{i,j+1}^{(t)} + a_{i+1,j-1}^{(t)} + a_{i+1,j+1}^{(t)},$$

$$f_{225}(V_{ij}^{(t)}) = a_{i-1,j-1}^{(t)} + a_{i-1,j}^{(t)} + a_{i-1,j+1}^{(t)} + a_{i+1,j+1}^{(t)}.$$

En el paso 3) es preciso generar k - 1 = 3 matrices aleatorias, del mismo tamaño que la imagen original, para comenzar la evolución del autómata celular. Como se ha indicado, estas 3 matrices, $C^{(1)}$, $C^{(2)}$ y $C^{(3)}$, se han obtenido mediante el generador BBS (se omiten sus expresiones debido a su larga extensión).

Ejemplo 2

(Imagen en tonos de gris)

Para el caso de imagen en tonos de gris se ha tomado la radiografía de una muñeca (imagen (a) de la Figura 6), que tiene 249 tonos de gris. El tamaño de la misma es de 181 x 157 = 47656 pixeles y se ha considerado un esquema gráfico umbral con $n = 10$ participantes y $k = 3$. Así pues, para recuperar la radiografía original es preciso reunir 3 sombras consecutivas de las 10 elaboradas. Por simplicidad, los k - 1 = 2 números aleatorios necesarios para las funciones de transición son los dos primeros del ejemplo anterior, es decir, las funciones a considerar son f_{232} y f_{29}. Las k - 1 = 2 matrices aleatorias necesarias para este esquema, $C^{(1)}$ y $C^{(2)}$, se han generado de forma similar a como se ha hecho para el ejemplo anterior.

Ejemplo 3

(Imagen en color)

La imagen en color que se ha empleado para el tercer ejemplo son cortes de fotos de las superficies de Júpiter y sus lunas. Esta imagen tiene 24852 colores (imagen (a) de la Figura 7) y el esquema gráfico umbral realizado es un esquema 3-de-6. También por simplicidad, las funciones de transición empleadas son las mismas que las del Ejemplo 2. En este caso, al igual que en el anterior, se han generado dos matrices, $C^{(1)}$ y $C^{(2)}$ para proceder a la evolución del autómata celular.

Fase de división

Según el protocolo ya mencionado, en el primer paso de esta fase se deben elegir los umbrales m de modo que no haya solapamientos entre las primeras configuraciones del autómata y las sombras a calcular. Finalmente se procede a determinar la evolución del ACMR y a repartir las sombras de forma segura.

Ejemplo 1

(Imagen en blanco y negro)

En este ejemplo se ha elegido un valor de $m = 4$, de modo que la evolución completa del ACMR proporciona las siguientes configuraciones:

$$I = C^{(0)}, C^{(1)}, C^{(2)}, C^{(3)}, S_0 = C^{(4)}, S_1 = C^{(5)}, S_2 = C^{(6)}, S_3 = C^{(7)}.$$

Las imágenes (b), (c), (d) y (e) de la Figura 5 son las sombras obtenidas mediante el esquema utilizado para este ejemplo. Puede observarse que todas ellas son del mismo tamaño que la imagen original y que no se deriva ninguna información del circuito original a partir de cualquiera de ellas.

Ejemplo 2

(Imagen en tonos de gris)

El umbral considerado en este ejemplo ha sido elevado, $m = 20$, con el fin de estimar tiempos de computación para valores diferentes. La evolución del autómata para determinar las 10 sombras necesarias ha sido la siguiente:

$$I = C^{(0)}, C^{(1)}, C^{(2)}, \ldots, C^{(19)}, S_0 = C^{(20)}, S_1 = C^{(21)}, \ldots, S_9 = C^{(29)}.$$

Las sombras pertenecientes a los 10 participantes se muestran como las imágenes (b), (c), (d), (e), (f), (g), (h), (i), (j) y (k) de la Figura 6.

Ejemplo 3

(Imagen en color)

Para este último ejemplo, el umbral elegido ha sido $m = 4$, de modo que la evolución obtenida en este caso es la siguiente:

$$I = C^{(0)}, C^{(1)}, C^{(2)}, C^{(3)}, S_0 = C^{(4)}, S_1 = C^{(5)}, \ldots, S_5 = C^{(9)}.$$

Las 6 sombras correspondientes a la imagen original por el esquema considerado son las imágenes (b), (c), (d), (e), (f) y (g) de la Figura 7.

Fase de recuperación

A la hora de recuperar la imagen secreta original, dado que todos los participantes conocen la función de transición empleada y el número de orden de la sombra que poseen, es necesario que se unan k consecutivos de ellos para llevar a cabo la fase de recuperación.

Ejemplo 1

(Imagen en blanco y negro)

La imagen recuperada es la imagen (f) de la Figura 5. Dicha imagen se ha obtenido después de 4 iteraciones del autómata inverso al empleado en la fase de división. Se puede apreciar que dicha imagen es exactamente del mismo tamaño y con la misma resolución que la que la imagen (a) de la misma figura.

Ejemplo 2

(Imagen en tonos de gris)

En este ejemplo se han utilizado las sombras S_7, S_8 y S_9 para recuperar, después de 27 iteraciones (el máximo número en este ejemplo), la imagen (1) de la Figura 6, que es la misma que la imagen secreta. El mismo resultado se habría obtenido de utilizar cualesquiera otras 3 sombras consecutivas.

Ejemplo 3

(Imagen en color)

La imagen secreta se ha obtenido después de utilizar las sombras S_2, S_3 y S_4. La imagen recuperada se muestra como imagen (h) en la Figura 7. Se puede observar que esta imagen es exactamente la misma que la imagen secreta original y que no presenta ninguna pérdida de resolución.

Funcionamiento e implementación

El protocolo propuesto para dividir de forma secreta, compartir y recuperar imágenes se ha implementado de forma práctica mediante varios programas utilizando el lenguaje C++ de Visual Studio .Net 6.0, bajo el sistema operativo Windows XP Profesional, Versión 2002, Service Pack 1; en un ordenador Pentium III a 996 Mhz con dos microprocesadores y 512 Mbytes de memoria RAM.

Con estas implementaciones, que no están completamente depuradas, el tiempo de computación necesario para generar las sombras y recuperar el secreto a partir de las mismas depende, como es lógico, de varios factores:

1. Del tamaño de la imagen original, dado que el proceso se lleva a cabo para cada uno de los píxeles de la imagen.

2. Del número participantes del protocolo, n, debido a que cuanto mayor sea este número, más sombras se deben elaborar.

3. Del valor de k, al tener que generarse k - 1 matrices del mismo tamaño que la imagen original y, en menor medida, k - 1 números aleatorios. Nótese que el tiempo dedicado a este paso podría acortarse si el director tuviera precomputados y almacenados de forma segura, un gran número de bits.

4. Del umbral elegido, m, con $k \leq m$, dado que las n sombras comienzan a elaborarse a partir de dicho valor.

Obsérvese que el número de colores de la imagen no tiene influencia significativa en el tiempo de computación puesto que las operaciones que deben ejecutarse son, en los tres tipos de imágenes, esencialmente las mismas, debido a la codificación que se lleva a cabo a la hora de expresar una imagen como una matriz de números.

Con relación al proceso de división secreta, una vez que la imagen original ha sido leída, el tiempo requerido para generar los k - 1 números aleatorios y las k - 1 matrices del mismo tamaño que la imagen secreta, para cada uno de los ejemplos desarrollados anteriormente, se señala a continuación. También se indica en cada ejemplo, el tiempo preciso para recuperar la imagen, teniendo en cuenta que para este proceso, se deben leer y tener almacenadas en memoria todas las sombras a utilizar.

Ejemplo 1

(Imagen en blanco y negro)

Para los valores $n = k = m = 4$, las 4 sombras se han obtenido en 1 segundo; mientras que para la lectura de las cuatro sombras y la consiguiente obtención de la imagen secreta se han requerido 3.8 segundos.

Ejemplo 2

(Imagen en tonos de gris)

Para los parámetros considerados en este ejemplo, $n = 10$, $k = 3$ y $m = 20$, el tiempo para generar las 10 sombras

ha sido de 2.4 segundos. Para la recuperación de la imagen secreta original a partir de las sombras S_7, S_8 y S_9 se han necesitado 2.7 segundos. Sin embargo, este tiempo se habría reducido a 2.3 segundos si las sombras empleadas hubieran sido S_0, S_1 y S_2.

Ejemplo 3

(Imagen en color)

El tiempo requerido para obtener las 3 sombras, a partir de los valores $n = 6$, $k = 3$, y $m = 4$, ha sido de 1.2 segundos; mientras que el tiempo requerido pare recuperar la imagen original a partir de las sombras ha sido de 2.5 segundos.

Los tiempos de computación de la fase recuperación si se utilizan las últimas sombras generadas; es decir, las que corresponden a los valores $m + n - 1$, $m + n - 2$,..., son mayores que los de la fase de división de la imagen, debido a que deben leerse y almacenarse en memoria todas las sombras que vayan a ser utilizadas; mientras que el número de iteraciones del ACMR es similar al empleado a la hora de generar las sombras. Sin embargo, es posible que el tiempo de recuperación de la imagen original sea menor que el utilizado por el director para elaborar las sombras si, por ejemplo, las sombras que se emplean son las más cercanas al valor umbral m.

Por otra parte, el tiempo real de ejecución del protocolo; es decir, la determinación de la evolución del ACMR, sin tener en cuenta el tiempo necesario para la lectura y almacenamiento en memoria de los datos parciales, es similar en ambos casos, dado que las operaciones son, básicamente, las mismas.

Nótese que el procedimiento es muy rápido, dado que para el tamaño de las imágenes utilizadas (236 x 184 píxeles, de media) sólo se requieren 1.5 segundos, de media, para la elaboración de las sombras y 3 segundos para la recuperación de la imagen secreta. Por otra parte, debe tenerse en cuenta que los tiempos presentados anteriormente podrían ser mejorados si se depuran los programas utilizados o si el procedimiento completo se implementara en hardware.

Aplicaciones de la invención

Las aplicaciones de esta invención son todas aquellas en las que se requiera proteger imágenes con vistas a evitar su pérdida o robo, o cuando se desea llevar a cabo un protocolo que, por sus especiales características, necesite del consentimiento de varias partes para recuperar la imagen dividida. Así pues, entre las principales aplicaciones de esta invención destacan las siguientes:

- División segura de cualquier imagen mediante sombras para evitar su pérdida y poder recuperarla, incluso con la desaparición de algunas de sus sombras.
- División de una imagen en partes para impedir que la imagen original sea robada.
- Protección de una imagen secreta de modo que sea necesaria la colaboración de varios participantes para poder recuperarla.

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

- Informática
- Militar
- Industrial
- Artística
- Cartográfica
- Médica

REIVINDICACIONES

1. Procedimiento para dividir de forma secreta, compartir y recuperar imágenes que incluye los siguientes pasos:

a) Selección de la imagen secreta a dividir o de las partes (sombras) en que fue dividida la misma para recuperarla,

b) Elección del esquema gráfico umbral *k*-de-*n* a utilizar,

c) Elección de un autómata celular bidimensional híbrido con memoria y reversible (ACMR), $A = (1, S, V, f)$, y de su inverso $A^{-1} = (1, S, V, g)$,

d) Elección de un generador de bits pseudoaleatorio criptográficamente seguro,

e) Aplicación reiterada de la función de la transición del autómata celular correspondiente a cada uno de los píxeles de la imagen secreta o de cada sombra de sombras de la imagen para llevar a cabo su recuperación,

caracterizado porque el espacio celular del ACMR, *I*, es una imagen genérica del mismo tamaño que la que se vaya a utilizar en el esquema gráfico umbral; porque el conjunto de estados, $S = Z_c$, está formado por los posibles colores, *c*, que pueden llegar a definir la imagen ($c = 2$ para imágenes en blanco y negro, $c = 2^8 = 256$ para imágenes en tonos de gris y $c = 2^{24} = 16.777.216$ para imágenes en color); porque la vecindad, *V*, considerada es la vecindad de Moore y porque las funciones de transición, *f* y *g*, que determinan la evolución de los autómatas celulares dependen de $k - 1$ números (entre 0 y 511) generados al azar por el director del esquema, cuya expresión binaria es de la forma:

$$\lambda_{-1,-1}\, 2^8 + \lambda_{-1,0}\, 2^7 + \lambda_{-1,1}\, 2^6 + \lambda_{0,-1}\, 2^5 + \lambda_{0,0}\, 2^4 + \lambda_{0,1}\, 2^3 + \lambda_{1,-1}\, 2^2 + \lambda_{1,0}\, 2^1 + \lambda_{1,1}\, 2^0,$$

siendo $\lambda_{i,j} \in \{0,1\}$. Las funciones de transición son:

$$f \equiv a_{ij}^{(t+1)} = f^{(1)}(V_{ij}^{(t)}) + f^{(2)}(V_{ij}^{(t-1)}) + \ldots + f^{(k-1)}(V_{ij}^{(t-k+2)}) + a_{ij}^{(t-k+1)} \bmod c,$$

$$g \equiv a_{ij}^{(t+1)} = -f^{(k-1)}(V_{ij}^{(t)}) - f^{(k-2)}(V_{ij}^{(t-1)}) - \ldots - f^{(1)}(V_{ij}^{(t-k+2)}) + a_{ij}^{(t-k+1)} \bmod c,$$

donde las $f^{(h)} : (Z_c)^9 \to Z_c$, $1 \le h \le k - 1$, son $k - 1$ funciones de transición locales de la forma:

$$f^{(h)}(V_{ij}^{(t-h)}) = \lambda_{-1,-1}\, a_{i-1,j-1}^{(t-h)} + \lambda_{-1,0}\, a_{i-1,j}^{(t-h)} + \lambda_{-1,1}\, a_{i-1,j+1}^{(t-h)} + \lambda_{0,-1}\, a_{i,j-1}^{(t-h)}$$
$$+ \lambda_{0,0}\, a_{i,j}^{(t-h)} + \lambda_{0,1}\, a_{i,j+1}^{(t-h)} + \lambda_{1,-1}\, a_{i+1,j-1}^{(t-h)} + \lambda_{1,0}\, a_{i+1,j}^{(t-h)} + \lambda_{1,1}\, a_{i+1,j+1}^{(t-h)}.$$

2. Procedimiento para dividir de forma secreta imágenes según la reivindicación 1, **caracterizado** porque el director del esquema gráfico umbral sigue los siguientes pasos:

a) Considera la imagen, *I*, de *r* filas y *s* columnas, como una matriz, *M*, con coeficientes en Z_c, utilizando la codificación estándar RGB de sus píxeles p_{ij}, $1 \le i \le r, 1 \le j \le s$.

b) Utiliza la matriz de la imagen, $M = C^{(0)}$, como la configuración inicial del autómata celular *A*.

c) Emplea el generador de bits pseudoaleatorio criptográficamente seguro para generar una secuencia de k - 1 matrices del mismo tamaño que la imagen considerada, $C^{(1)}$, ..., $C^{(k-1)}$, para poder iniciar la evolución del ACMR.

d) Selecciona un entero umbral *m*, con $k \le m$, con el fin de evitar solapamientos entre las condiciones iniciales y las sombras.

e) Calcula, a partir de las *k* primeras configuraciones, $C^{(0)}$,..., $C^{(k-1)}$ la evolución de orden $m + n$ - 1 del ACMR, sin más que iterar convenientemente la función de transición f del autómata celular:

$$\{C^{(0)}C^{(1)}, ..., C^{(k-1)}, C^{(k)}, C^{(m)}, ..., C^{(m+n-1)}\}$$

f) Distribuye de forma secreta a cada participante, P_0,..., P_{n-1}, en el esquema gráfico la sombra que le corresponde:

$$S_0 = C^{(m)}, S_1 = C^{(m+1)}, ..., S_{n-1} = C^{(m+n-1)}.$$

g) Da a conocer a todos los participantes los *k* - 1 números aleatorios que generó para elaborar la función de transición *f*.

3. Procedimiento para recuperar imágenes según la reivindicación 1, **caracterizado** porque *k* - 1, o menos, participantes no pueden obtener ninguna información de dicha imagen secreta y porque cualesquiera *k* participantes consecutivos pueden recuperar la imagen secreta original, sin necesidad de la colaboración del director, llevando a cabo los siguientes pasos:

a) Se reúnen *k* participantes y comparten sus *k* sombras consecutivas:

$$S_h = C^{(m+h)}, S_{h+1} = C^{(m+h+1)}, \ldots, S_{h+k-1} = C^{(m+h+k-1)}, \quad 0 \le h \le n - k.$$

b) Calculan la imagen secreta original $C^{(0)}$, iterando $m + h + k$ - 1 veces la función de transición *g*, a partir de las *k* configuraciones que comparten

$$T^{(0)} = C^{(m+h+k-1)}, T^{(1)} = C^{(m+h+k\cdot 2)}, \ldots, T^{(k-1)} = C^{(m+h)}.$$

4. Dispositivo para dividir de forma secreta, compartir y recuperar imágenes constituido por un sistema electrónico que implementa en hardware o software un algoritmo para la ejecución de los procedimientos según las reivindicaciones 1-3.

5. Dispositivo de almacenamiento de datos utilizable para dividir de forma secreta, compartir y recuperar imágenes, **caracterizado** porque implementa un algoritmo para la ejecución del procedimiento según las reivindicaciones 1-3.

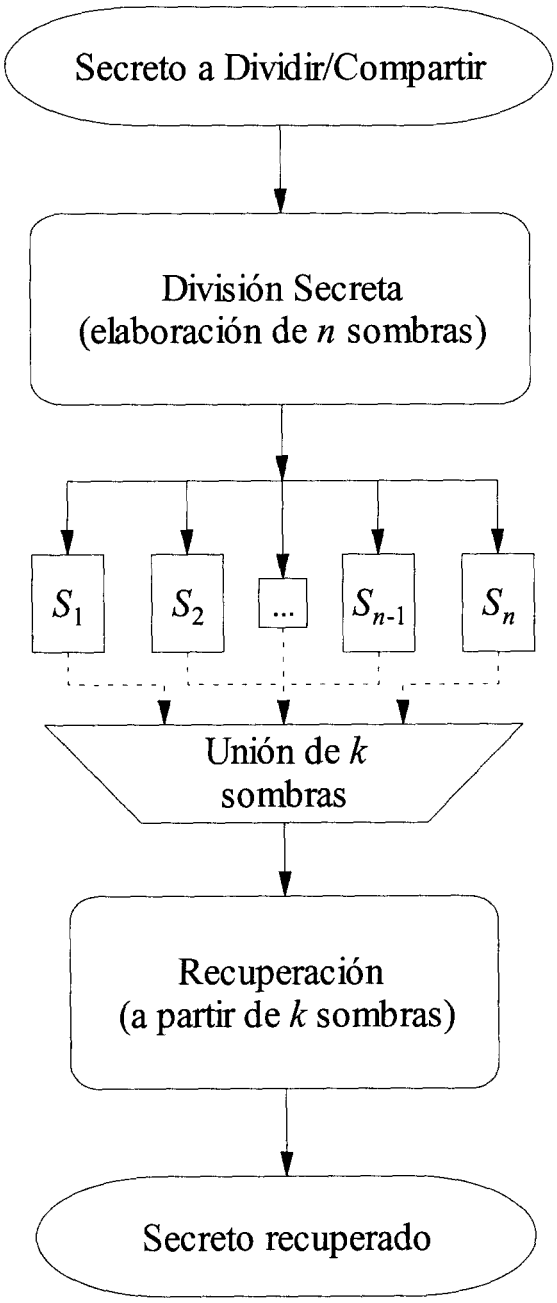

Secreto a Dividir/Compartir
División Secreta
(elaboración de n sombras)
S1
S2
...
Sn-1
Sn
Unión de k
sombras
Recuperación
(a partir de k sombras)
Secreto recuperado

Figura 1

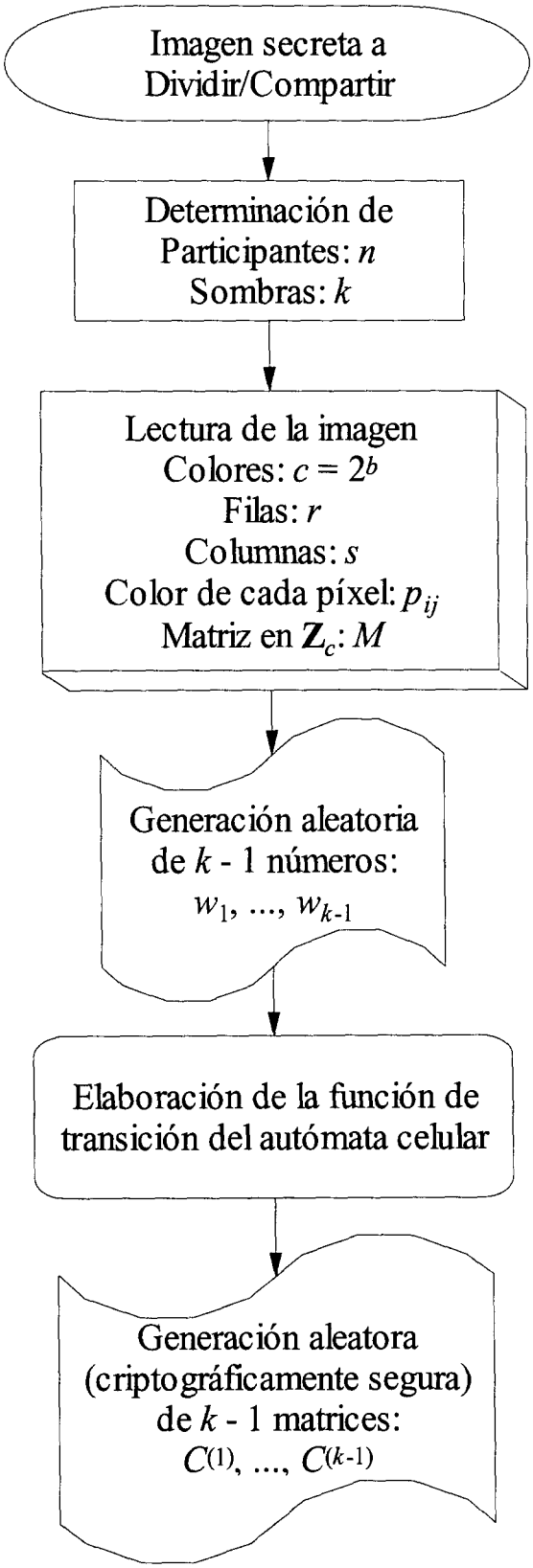


Imagen secreta a Dividir/Compartir
Determinación de Participantes: n Sombras: k
Lectura de la imagen Colores: $c = 2^b$ Filas: r Columnas: s Color de cada píxel: p_{ij} Matriz en $\mathbf{Z}_c$: M
Generación aleatoria de k - 1 números: $w_1, ..., w_{k-1}$
Elaboración de la función de transición del autómata celular
Generación aleatora (criptográficamente segura) de k - 1 matrices: $C^{(1)}, ..., C^{(k-1)}$

Figura 2

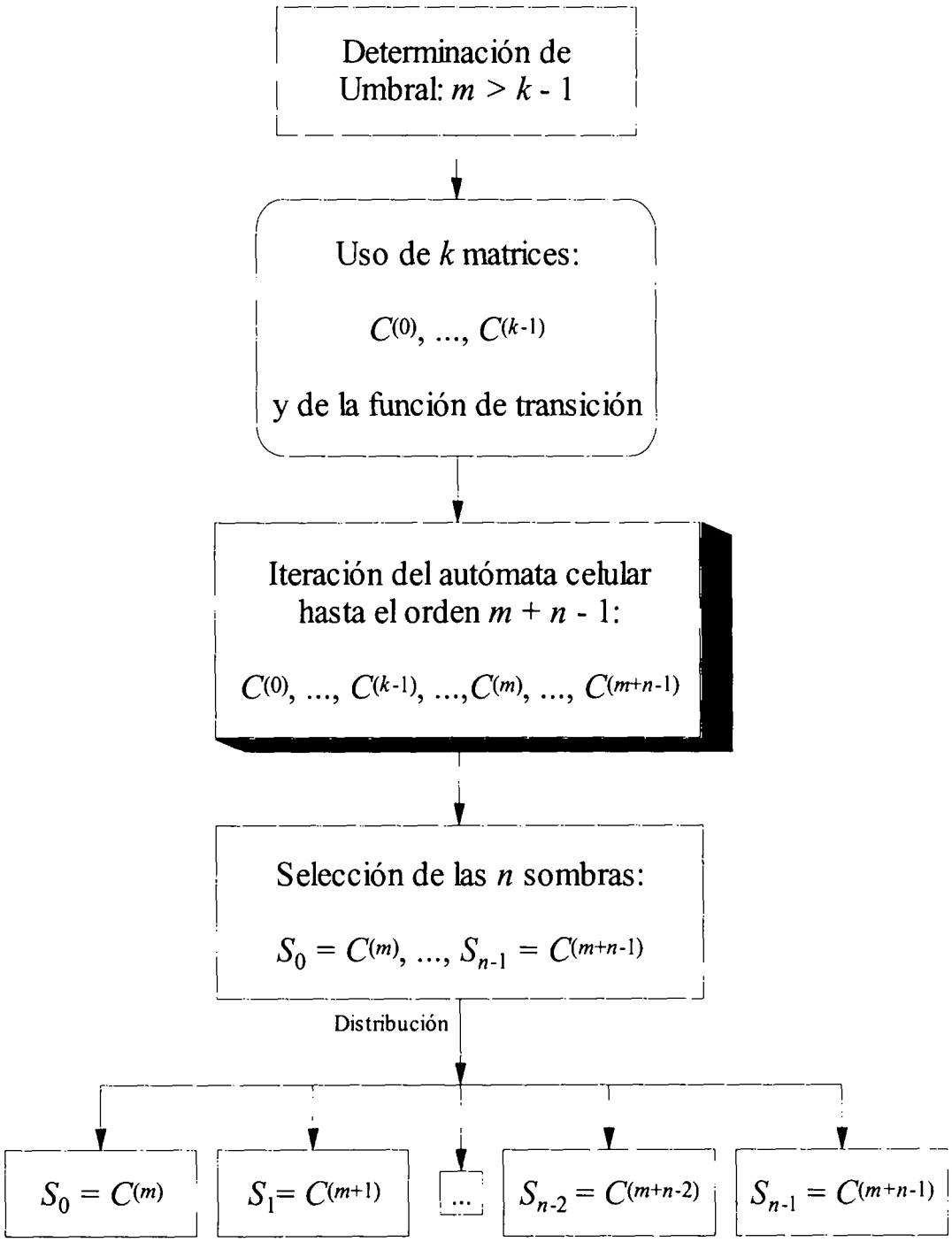

Determinación de Umbral: $m > k - 1$
Uso de k matrices:
$C^{(0)}, \ldots, C^{(k-1)}$
y de la función de transición
Iteración del autómata celular hasta el orden $m + n - 1$:
$C^{(0)}, \ldots, C^{(k-1)}, \ldots, C^{(m)}, \ldots, C^{(m+n-1)}$
Selección de las n sombras:
$S_0 = C^{(m)}, \ldots, S_{n-1} = C^{(m+n-1)}$
Distribución
$S_0 = C^{(m)}$
$S_1 = C^{(m+1)}$
...
$S_{n-2} = C^{(m+n-2)}$
$S_{n-1} = C^{(m+n-1)}$

Figura 3

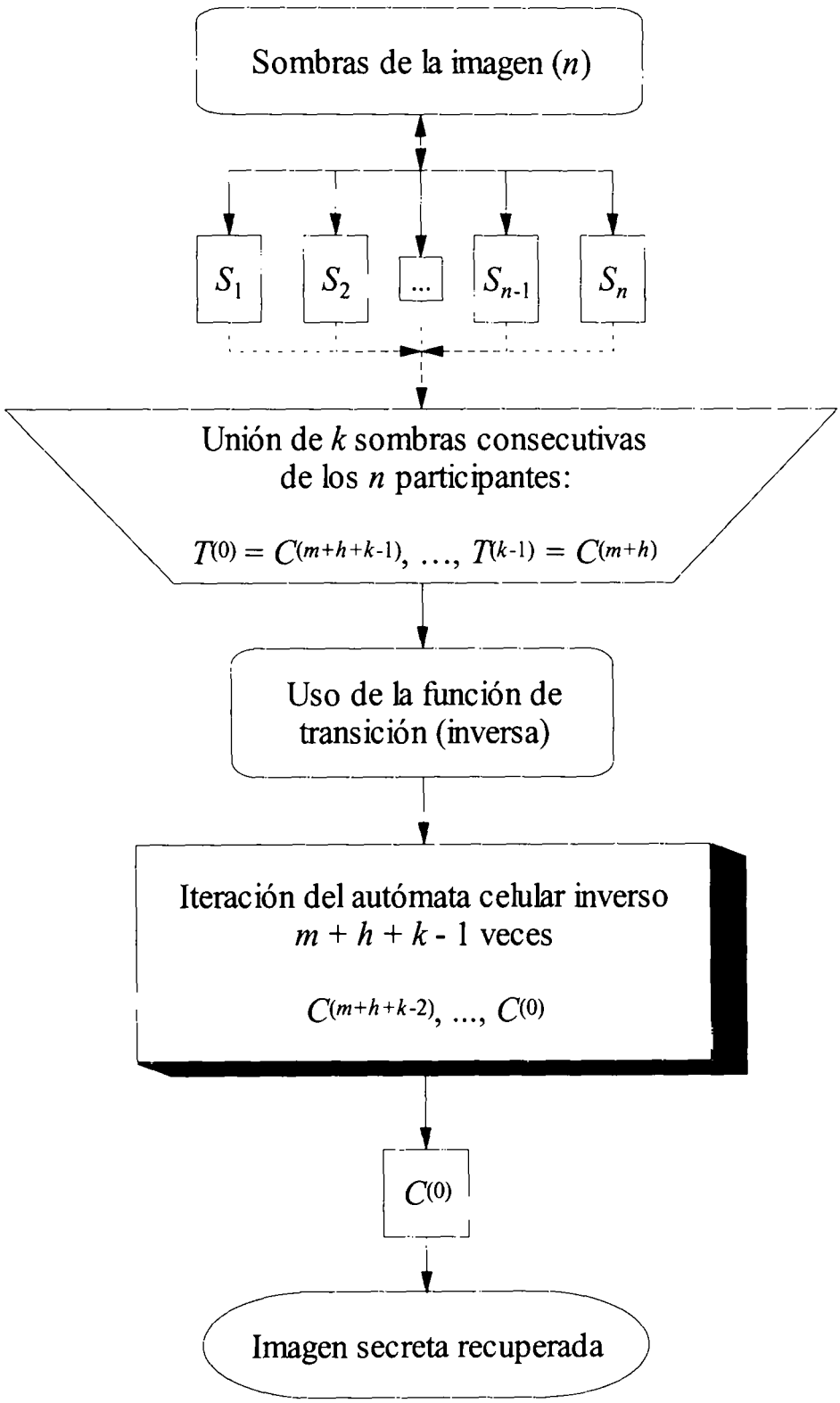

Sombras de la imagen (n)
S1
S2
...
Sn-1
Sn
Unión de k sombras consecutivas de los n participantes:
T(0) = C(m+h+k-1), ..., T(k-1) = C(m+h)
Uso de la función de transición (inversa)
Iteración del autómata celular inverso m + h + k - 1 veces
C(m+h+k-2), ..., C(0)
C(0)
Imagen secreta recuperada

Figura 4

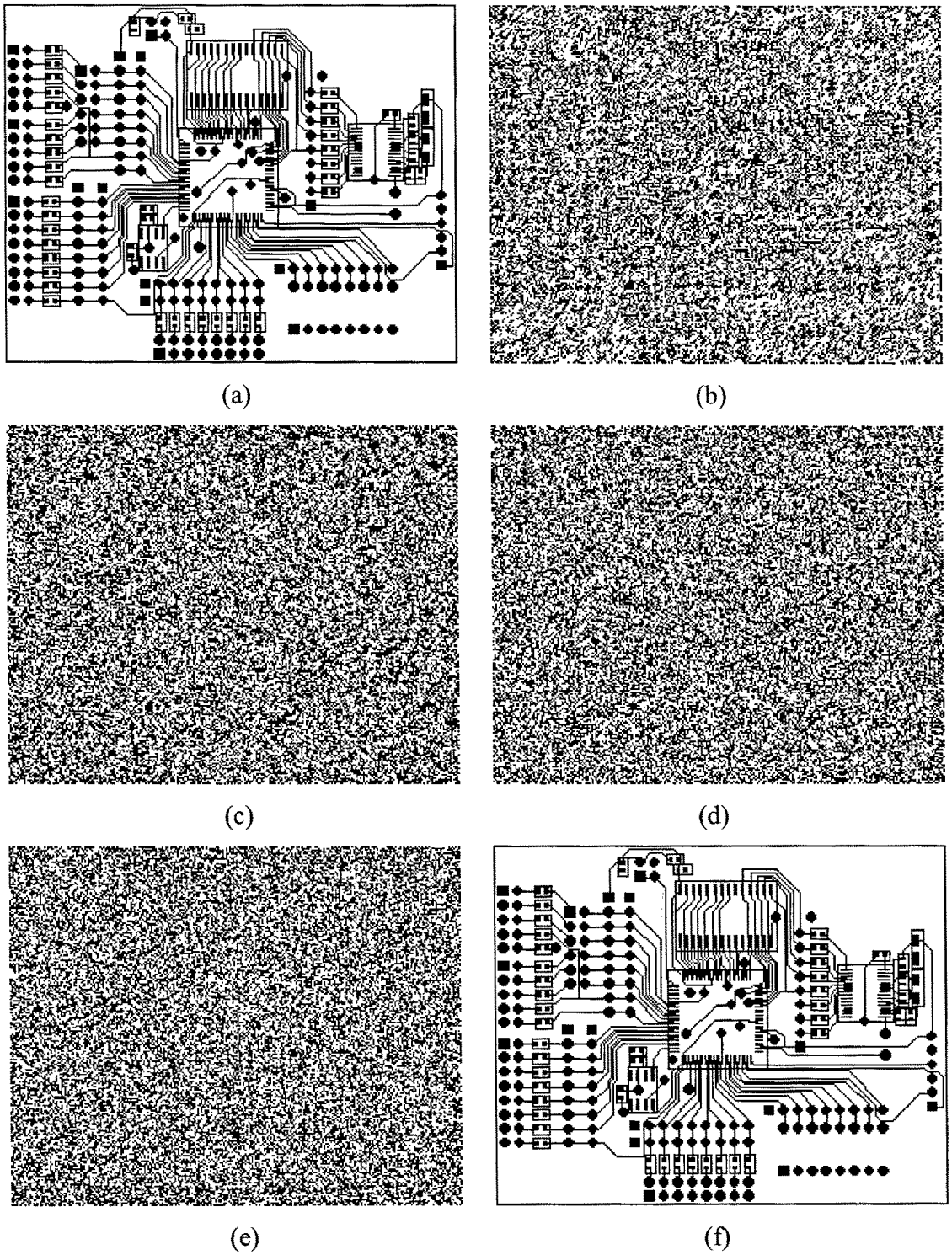


Figura 5

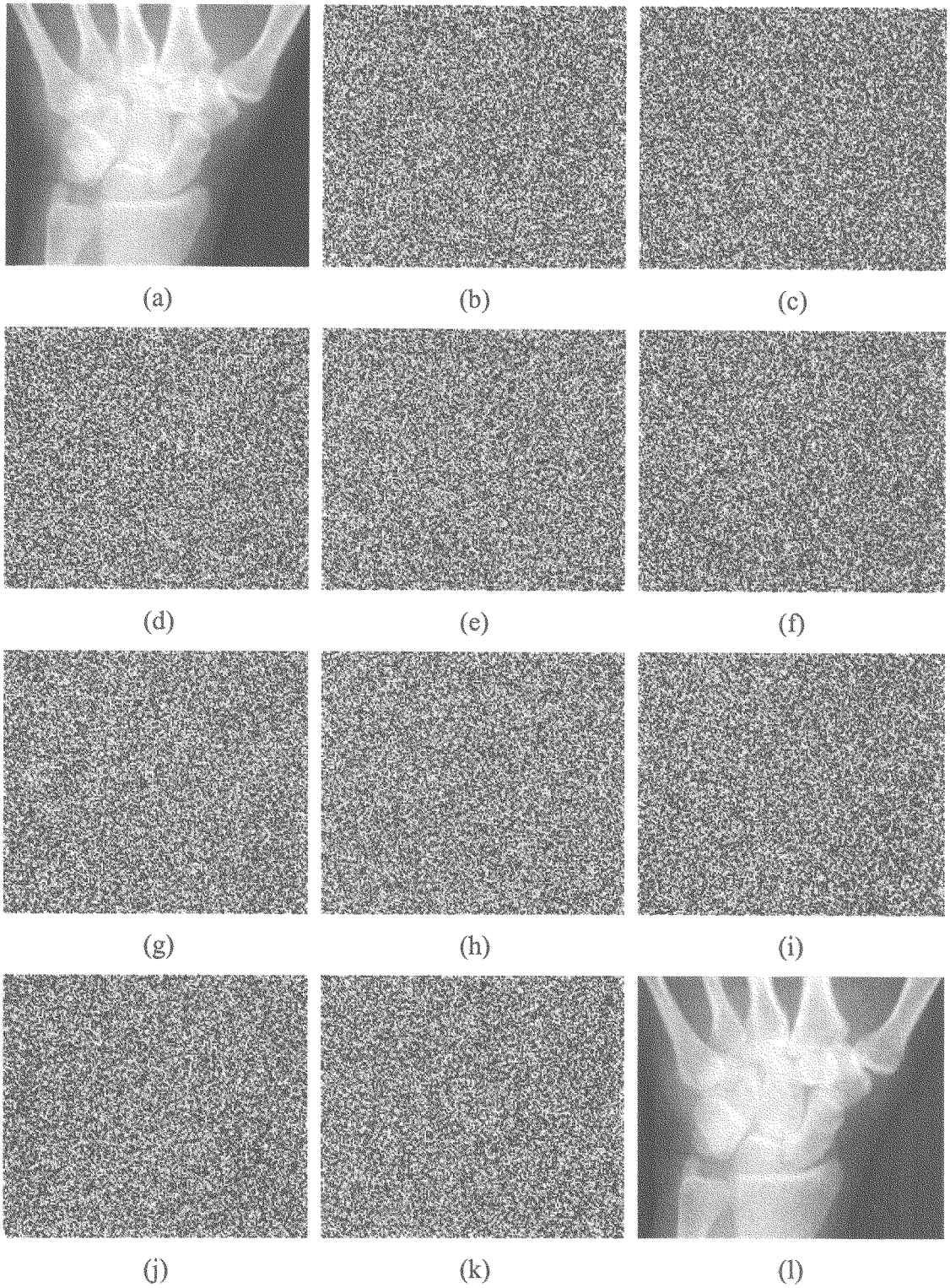
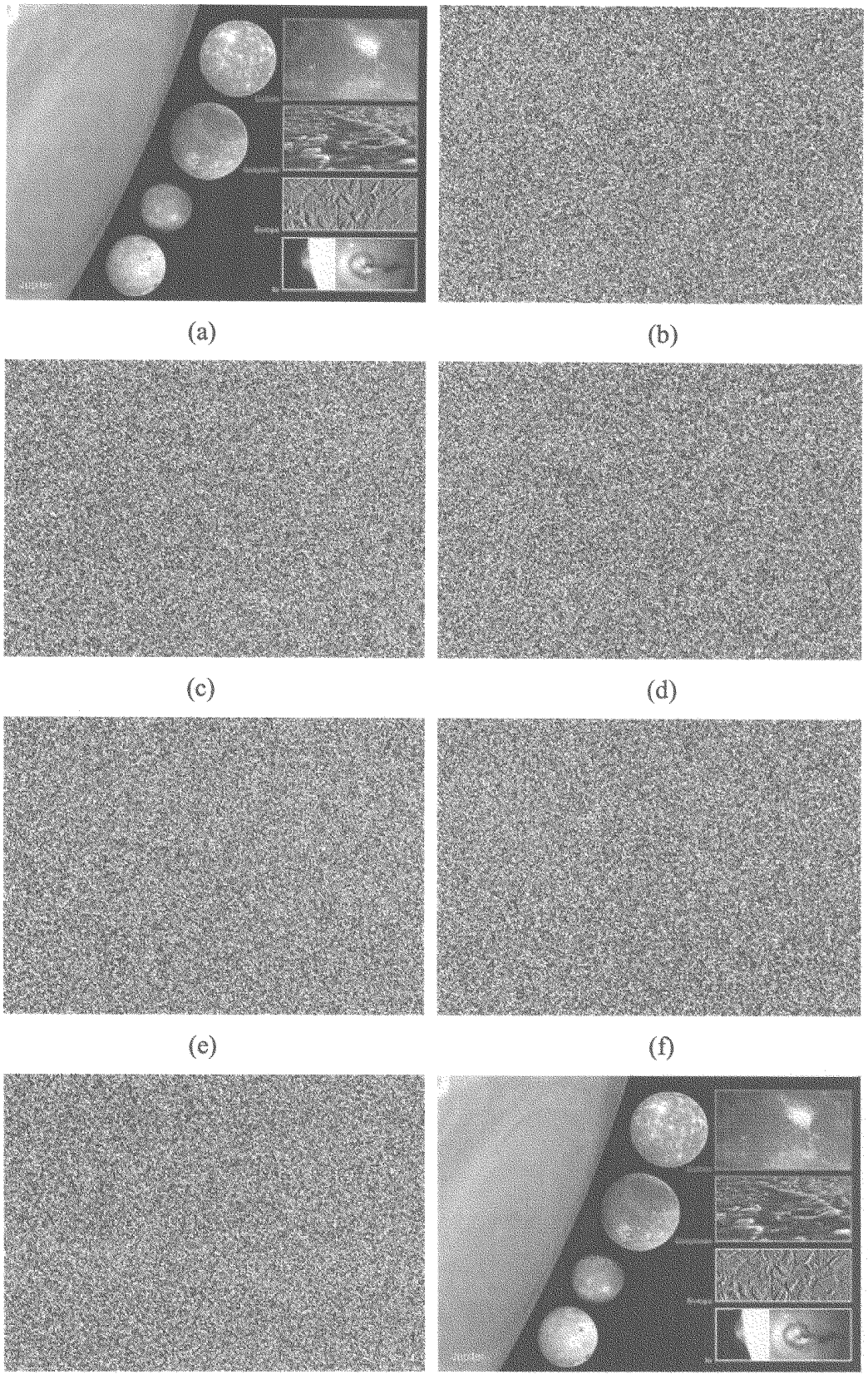


Figura 6



(a) (b)

(c) (d)

(e) (f)

(g) (h)

Figura 7

OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) ES 2 238 168

(21) Nº de solicitud: 200302924

(22) Fecha de presentación de la solicitud: **10.12.2003**

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TÉCNICA

(51) **Int. Cl.[7]:** G06T 1/00, H04N 1/44, 7/16, H04L 9/22

DOCUMENTOS RELEVANTES

Categoría	Documentos citados	Reivindicaciones afectadas
A	WO 0180169 A1 (DIGIMARC CORP [US]) 25.10.2001	1
A	US 2002012445 A1 (PERRY BURT W [US]) 31.01.2002	1
A	US 2002009208 A1 (ALATTAR ADNAN et al.) 24.01.2002	1

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