(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 582 346**

(51) Int. CI.:

G06K 19/073 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **07.02.2005 E 05717570 (5)**

(97) Fecha y número de publicación de la concesión europea: **20.04.2016 EP 1716520**

(54) Título: **Uso de una firma digital obtenida a partir de por lo menos una característica estructural de un elemento material para proteger informaciones sensibles contra la lectura directa, y procedimiento de lectura de esta información protegida**

(30) Prioridad:

06.02.2004 FR 0401171

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
12.09.2016

(73) Titular/es:

ARJO SOLUTIONS (100.0%)
32 Rue Jacques Ibert
92300 Levallois-Perret, FR

(72) Inventor/es:

BOUTANT, YANN;
LABELLE, DAVID y
SEUX, HERVÉ

(74) Agente/Representante:

CURELL AGUILÁ, Mireia

DESCRIPCIÓN

Uso de una firma digital obtenida a partir de por lo menos una característica estructural de un elemento material para proteger informaciones sensibles contra la lectura directa, y procedimiento de lectura de esta información protegida.

La presente invención se refiere al campo técnico de la protección y de la securización de información. En particular, la invención tiene por objeto el uso de una o varias firmas digitales de un elemento material de estructura compleja, caótica, única y estable, para proteger informaciones sensibles contra la lectura directa, un soporte portador de dicha información protegida y un procedimiento de lectura de esta información protegida.

La llegada de la era digital ha aportado posibilidades nuevas de desarrollo para las organizaciones y los individuos. Si el mundo digital ha permitido el acceso mucho más rápido, fácil y pertinente a la información y a la comunicación en todas sus formas, si ha revolucionado las funciones de almacenamiento y transmisión de la información, se puede considerar también que, intrínsecamente, las plataformas digitales, en general en red, permiten la reproducción, el envío y la captura sin límites de la información, y con frecuencia de manera no controlable.

Por lo tanto, el mundo digital resulta intrínsecamente inadecuado para llevar a cabo funciones de autentificación, de protección/securización de información (confidencialidad), de seguimiento de la información (trazabilidad e integridad), etc.

El documento EP 1 202 225 A2 da a conocer un método para autentificar un documento.

Se han desarrollado componentes tecnológicos completos para paliar estos defectos originales (antivirus, cortafuegos, criptografía, esteganografía, control de acceso, etc.). Las respuestas se basan esencialmente en principios algorítmicos o de programación para aportar estas nuevas dimensiones contra natura al mundo digital.

En este contexto, la presente invención tiene como objetivo proporcionar un procedimiento general novedoso de securización de información sensible, es decir información que se desea proteger, controlar el acceso directo a la misma o verificar su integridad, así como un procedimiento de lectura de la información protegida obtenida, que presenta un alto nivel de seguridad. Este procedimiento presenta la ventaja de, en general, no fundamentar su seguridad en conjeturas matemáticas y/o algorítmicas. La presente invención se refiere a un procedimiento de lectura de información sensible protegida según las características de la reivindicación 1.

Este procedimiento se debe adaptar a la protección de todo tipo de información, especialmente gráfica, digital, estática, dinámica, analógica.

La invención tiene también como objetivo proporcionar un medio nuevo para generar hasta el infinito secuencias totalmente aleatorias.

Este nuevo procedimiento debe aportar respuestas nuevas, complementarias y muy eficaces en aplicaciones tan variadas como:

- la trazabilidad de productos y actividades con un alto nivel de seguridad,
- la gestión documental, incluyendo la indicación de tiempo (datación) y la geolocalización (GPS),
- los documentos de seguridad (fiduciarios, valor monetario, ID, médicos, patentes, etc.),
- la securización de los datos y de los intercambios (comunicaciones),
- las etiquetas incorporadas o no incorporadas,
- los embalajes de cualquier naturaleza (incluyendo inteligentes y RFID),
- la confidencialidad de documentos físicos o información digital,
- el control de acceso (a lugares, máquinas, actividades, dinero e información) y tarjetas multifuncionales,
- el voto electrónico,
- los juegos de azar,
- la lucha contra la falsificación de productos fabricados o de obras intelectuales y artísticas,
- la certificación de origen de documentos en papel o electrónicos (firma electrónica),
- el pago electrónico (incluyendo "e-ticketing" y franqueo postal),
- la protección de clave(s) criptográfica(s) en protocolos clásicos.

La presente invención tiene también por objeto los procedimientos y usos como los descritos en las reivindicaciones.

La siguiente descripción, en referencia a las figuras adjuntas, permite comprender mejor el objeto de la invención.

La figura 1 representa un esquema general que incluye un procedimiento de protección y un procedimiento de lectura de acuerdo con invención.

La figura 2 ilustra unas variantes de obtención de firmas digitales a partir de diferentes elementos materiales.

Las figuras 3 y 4 ilustran un ejemplo de puesta en práctica de los procedimientos de protección y de lectura de la invención y de soporte.

Los procedimientos y usos de la invención utilizan firmas digitales obtenidas a partir de por lo menos una característica estructural de un elemento material, seleccionado por sus características estructurales. En consecuencia, todos los procedimientos y usos de acuerdo con la invención comprenden una etapa de obtención de por lo menos una firma digital a partir de un elemento material, de forma más precisa una etapa de detección de por lo menos una característica estructural del elemento material, con el fin de generar por lo menos una firma digital. El elemento material utilizado presenta una estructura compleja, caótica, única y estable. Según su significado típico, "firma digital" de un elemento material designa una representación, una caracterización numérica que es propia del elemento material. De acuerdo con la invención, se extrae una firma digital de la estructura del elemento material, obteniéndose la misma a partir de por lo menos una característica del elemento material que explica su estructura. De manera ventajosa, la firma digital presenta un carácter aleatorio. Específicamente, las firmas digitales se pueden presentar en forma de una imagen digital de la estructura del elemento material, tal como se ilustra en la figura 2.

La presente invención utiliza el mundo físico, analógico y material que posee, bajo múltiples formas, unos elementos únicos, que en general son el resultado de un procedimiento de creación caótico y/o estocástico. Efectivamente, ciertos elementos materiales contienen características considerablemente caóticas y presentan una extrema complejidad estructural intrínseca, que aporta una riqueza informativa considerable a quien la sabe leer.

En general, los elementos materiales seleccionados para poner en práctica la invención reunirán unas características al mismo tiempo deterministas y aleatorias. Dentro del ámbito de la presente invención, es particularmente ventajoso extraer la parte aleatoria de la mejor manera posible. En general, estos elementos materiales también serán no copiables/no reproducibles.

Además, ciertos elementos materiales tienen una cuasi invariancia estructural en un tiempo determinado, lo cual permite conservarlos y utilizarlos durante este tiempo. La presente invención utiliza elementos materiales cuya estructura es al mismo tiempo compleja, única, caótica y cuasi invariante con el tiempo. Resultan adecuados en particular, en el sentido de invención, los materiales fibrosos, los plásticos, los metales, los cueros, las maderas, los materiales compuestos, el vidrio, los minerales, las estructuras cristalinas, los cuales pueden haber soportado modificaciones o transformaciones. Por ejemplo, se pueden haber imprimido y/o grabado y/o perforado. Como elemento material de acuerdo con la invención también puede servir una combinación de varios materiales. Se prefieren los materiales fibrosos, a base de fibras sintéticas o naturales, y en particular, total o parcialmente de un papel, cartón o no tejido. Así, la invención recurre ventajosamente a materiales manufacturados. También se puede contemplar que el elemento material forme parte de un papel, cartón o no tejido, en el cual se sitúa con un material transparente al modo de detección utilizado para extraer la característica o características estructurales, estable en el tiempo y que garantiza su protección, por ejemplo, un revestimiento de plástico o una resina.

El elemento material utilizado en la presente invención puede ser preexistente, o se puede fabricar, y eventualmente modificar, con el único propósito de ser utilizado en el procedimiento de acuerdo con la invención.

Preferentemente, se utilizará el papel como elemento material que da origen a la(s) firma(s) digital(es) utilizada(s) para garantizar la protección de la información sensible, de acuerdo con la presente invención. Efectivamente, el papel es un material poroso extremadamente complejo constituido esencialmente por fibras celulósicas y cargas minerales. Es anisótropo y heterogéneo. Las fibras se orientan y agrupan en agregados: la floca.

La inestabilidad "natural" del procedimiento material-químico de fabricación, y la variabilidad intrínseca de la materia prima utilizada explican la componente altamente caótica de la estructura del papel. La formación de la estructura de este material se realiza solidificando un flujo de pasta de papel sobre un tamiz (una tela de fabricación). Su factor de formación es apreciable a simple vista por transvisión con iluminación natural: se denomina "épair" (apariencia estructural observada por transvisión). El papel generalmente se produce en banda continua y se conforma típicamente en hojas. Se puede examinar de múltiples maneras y se pueden detectar, por ejemplo, características estructurales que muestran su estado superficial, su porosidad interna, y su organización volumétrica de la red de fibras microscópica o macroscópica (floca) a diferentes escalas.

El papel reúne las propiedades genéricas necesarias para ser utilizado como elemento material generador de firmas digitales aleatorias, a saber, la alta complejidad de su estructura, el aspecto caótico (imprevisible) a escalas diferentes, la unicidad de cada cara de un papel y su cuasi invariancia con el tiempo (envejecimiento muy lento en particular de su estructura, que permite conservar el papel durante décadas, incluso siglos, etc.).

El valor completo de la invención se revela cuando se utiliza un elemento material el cual, entre otras propiedades, posee la de la cuasi invariancia. Es decir, que naturalmente no se modifica o se modifica poco con el tiempo, y que si se miden ciertas características estructurales en un momento determinado, se pueden encontrar estas mismas características, si no intactas, muy similares, en otro momento posterior. Por lo tanto, se puede calificar como estable. Esta estabilidad se puede lograr protegiendo el elemento material contra eventuales agresiones exteriores (rayaduras, perforaciones, deterioros ópticos, etc.). Esta protección se puede lograr insertando el elemento material

de manera definitiva en una envoltura externa, que no impida en absoluto el acceso a las características que interesan del elemento material. También se puede lograr manteniendo el elemento material lejos de toda agresión en una atmósfera acondicionada y/o físicamente protegido, es decir en lugar seguro. El tipo de protección que se aportará al elemento material es función de la aplicación seleccionada (si se recurre frecuentemente o no al elemento material, sensibilidad de la aplicación, etc.).

Las firmas digitales de un elemento material, como se definió anteriormente, se obtienen de la manera siguiente. Se selecciona un elemento físico en los términos de la invención y se extraen una o varias características de su estructura, cuasi invariantes con el paso del tiempo. Ventajosamente, estas características reflejan su estructura caótica, compleja, única y estable. En otras palabras, se extraen una o varias características complejas y caóticas de la estructura única del elemento material. Estas características servirán para generar, después de la digitalización conjuntamente, o no, con otros tratamientos del tipo conformación/acondicionamiento y/o codificación, una firma digital. Esta firma digital, la cual por ella misma refleja la estructura caótica, compleja, única y estable del elemento material seleccionado, se utilizará entonces para garantizar la protección, la securización, de todo tipo de información sensible en forma digital, es decir para evitar la lectura directa. Por lo tanto, en ocasiones será necesario digitalizar, de antemano, la información sensible que se va a proteger, si es que la misma no se encuentra ya en forma digital. Típicamente, por digital se entiende una representación de información o de magnitudes físicas bajo la forma de todo tipo de señales (incluyendo, imágenes reales o complejas, componentes de amplitud y/o de fase) en valores discretos, por ejemplo, en forma de cifras (independientemente de la base: binaria, decimal, hexadecimal, etc.) o en forma de un conjunto cualquiera de símbolos (alfabeto, gramática predefinida, etc.). Los sistemas digitales recurren frecuentemente a los convertidores analógicos-a-digitales y digitales-a-analógicos.

La figura 1 ilustra de manera general, un procedimiento de protección y un procedimiento de lectura de acuerdo con la invención. El procedimiento de protección comprende las siguientes etapas:

1. Se selecciona un elemento físico en los términos de la invención.

2. Se llevan a cabo la adquisición y la conformación/acondicionamiento, incluso la digitalización, de una o varias características del elemento material, gracias a uno o varios sensores con o sin contacto con el elemento material. A estos sensores típicamente les sucede una unidad de tratamiento analógico (por ejemplo, óptico o electrónico) o digital (tarjeta de captura conectada a cualquier plataforma informática o automática).

3. Se generan una o varias firma(s) digital(es) a partir de las características extraídas y las mismas se conforman/acondicionan en la etapa 2. Se puede realizar una codificación (en forma analógica y/o digital) seguida o precedida por una digitalización si las características extraídas en la etapa 2 ya no se encuentran en forma digital, pudiendo variar la naturaleza de estos tratamientos en función del tipo de elemento material seleccionado y de la aplicación para la cual se pone en práctica el procedimiento.

4. La o las firmas digitales se asocian, directamente (por medio de operaciones matemáticas elementales) o indirectamente (por ejemplo, utilizando algoritmos sofisticados de cifrado y/o esteganografía), con información digital sensible, con el fin de garantizar su protección.

Para la protección de información en forma digital, la presente invención pone en práctica un tratamiento digital que utiliza por lo menos una firma digital procedente de un elemento material, lo cual permite hacer que la información sensible original no sea directamente accesible, legible, audible, etc. En otras palabras, se entiende que la información sensible está securizada, requiriendo su lectura o comprensión la realización de un procedimiento posterior de lectura que constituye otro de los aspectos de la invención.

Opcionalmente, la información sensible en su totalidad o de una manera parcial se puede disponer físicamente en el elemento material utilizado en la etapa 1: por ejemplo, se puede imprimir en un documento del cual procede el elemento material.

La información securizada en la etapa 4 se almacena (etapa 6) en un soporte de información (digital, óptico, magnético, electrónico, en papel, específicamente por medio de grabado, impresión, registro, etc.). El almacenamiento puede ser un registro temporal o permanente. El elemento material utilizado en la etapa 1, puede constituir una parte de este soporte. Por otro lado, de acuerdo con la etapa 7, la totalidad o parte de la información protegida en la etapa 4 se pueden transmitir, por medio de una red de telecomunicaciones (de fibra óptica, de ondas de radiocomunicaciones, telefónica, satelital, etc.) o de un transporte en forma física. Al estar protegida la información sensible gracias a la o las firmas digitales extraídas del elemento material, la misma no es accesible posteriormente para quien no posea el elemento material inicial y los algoritmos de codificación para generar las firmas digitales y/o dichas firmas digitales y los algoritmos de realización de las mismas. La información sensible, una vez que se ha protegido, es por lo menos parcialmente ilegible. El procedimiento de lectura se detallará más adelante.

Existen diferentes medios para obtener una firma digital de un elemento material. Las firmas digitales más adecuadas para los procedimientos y usos de la invención, presentan un carácter complejo y aleatorio, que refleja la

estructura del material del cual se extraen. Esta firma se obtiene, ventajosamente, por detección, con la ayuda de uno o varios sensores, de una o varias características estructurales de este elemento cuasi invariantes con el tiempo, que reflejan su estructura compleja, caótica, única y estable, eventualmente seguida por una conformación/un acondicionamiento, una digitalización y una codificación de acuerdo con uno o varios algoritmos de esta o estas características estructurales. Con el término algoritmo se entiende una secuencia determinada de reglas operacionales o de etapas de tratamientos elementales para obtener un resultado a partir de datos o de señales iniciales, tales como algoritmos informáticos (sentido digital del término) (por ejemplo) u operaciones elementales electrónicas u ópticas (sentido analógico del término).

Por otro lado, la adquisición de la característica estructural se puede realizar de forma analógica o digital. Si se realiza la adquisición de forma analógica, o bien se puede digitalizar y a continuación codificar de forma digital para obtener la firma digital, o bien se puede codificar de forma analógica y a continuación digitalizar, para obtener la firma digital. La digitalización se puede llevar a cabo como muy pronto en la etapa 2 de la figura 1, o bien puede ser la última operación realizada en la etapa 3 de la figura 1. Por lo tanto, se pueden utilizar por ejemplo, las siguientes secuencias:

a- Sensor/Unidad de tratamiento digital (tarjeta de captura conectada a plataforma informática)/ Codificador Digital

b- Sensor/Unidad de tratamiento analógico (Acondicionamiento de la señal)/ Convertidor Analógico-a-Digital/Codificador Digital

c- Sensor/Unidad de tratamiento analógico (conformación/acondicionamiento de la señal y Codificación)/ convertidor Analógico-a-Digital

También es posible utilizar, en las etapas 2 y/ó 3, convertidores Analógicos/Digitales y Digitales/Analógicos, con el objeto de llevar a cabo ciertos tratamientos particulares sin desviarse del alcance de la invención, siendo lo importante al final de la etapa 3 obtener firmas digitales.

Por otro lado, ventajosamente, la característica estructural y por lo tanto, la firma digital, reflejan la estructura interna del elemento material, de modo que la característica estructural se mide en un volumen del soporte y en el interior del mismo.

La detección se puede realizar de acuerdo con métodos sin contacto (específicamente ópticos y/o electromagnéticos), en los cuales se utiliza la interacción (reflexión y/o absorción y/o transmisión y/o difusión y/o refracción y/o difracción y/o interferencia) de una onda o radiación electromagnética con el elemento material, y utilizando un sensor óptico/electrónico para realizar la adquisición, incluso la digitalización. El sensor o sensores utilizados se pueden situar entonces en cualquier posición en relación con el elemento material observado, y en relación con la o las fuentes de radiación. Típicamente, las radiaciones utilizadas pueden ser la luz visible y/o infrarroja (IR) y/o ultravioleta (UV) y/o láser o rayos beta y/o gama y/o X. En la selección de la radiación o radiaciones y del sensor o sensores utilizados pueden influir la aplicación del procedimiento, el tipo de elemento material seleccionado, la escala de medición seleccionada, el coste de realización, etc. El sensor o sensores utilizados pueden estar fijos en relación con la fuente y/o el elemento material, o pueden estar en movimiento relativo. También es posible medir la interacción entre la onda y el material de acuerdo con varias orientaciones.

Ventajosamente, los procedimientos y usos de acuerdo con la invención utilizan la firma digital de un elemento material, parte de un papel, cartón, o no tejido, obtenido después de la detección de su interacción con la luz visible, por transvisión, específicamente utilizando un sensor CCD o CMOS.

La detección también se puede realizar de acuerdo con métodos con contacto entre el elemento material y el sensor o sensores de medición. Por ejemplo, como sensor se usa un palpador. Este palpador puede integrar o no, además de la dimensión mecánica (seguimiento de la rugosidad de la superficie), dimensiones electromagnéticas (comportamiento magnético) u otras. En este caso, se requiere un movimiento relativo del palpador y del elemento material.

Otro ejemplo de sensor con contacto consiste en el uso del elemento material como soporte de una onda ultrasónica, por ejemplo, o cualquier otra solicitación aplicada (eléctrica, térmica, química, biológica, etc.). Entonces se registra en diferentes orientaciones el comportamiento/la respuesta del elemento material sometido a esta onda o solicitación.

La extracción de características estructurales del elemento material también se puede realizar a una o varias escalas, desde el nivel microscópico al macroscópico, determinando de este modo la complejidad de la característica estructural medida. La complejidad de la característica determina la correspondiente de la firma digital, seleccionada en el caso de una protección por combinación directa, en función del tamaño de la información sensible a proteger. Si se retoma el ejemplo de un elemento material de tipo papel, se puede examinar su estructura obtenida por transvisión, o la rugosidad de su superficie, y ello al nivel de las fibras (elementos de 100 µm a unos

cuantos mm de longitud y de aproximadamente 10 a 20 µm de ancho), o al nivel de los agregados de fibras (típicamente del orden de 1 a 10 mm).

La superficie de un metal puede ser, ella también, perfectamente lisa a simple vista y resultar muy rugosa, y por lo tanto de interés, como elemento material en el ámbito de esta invención, cuando se observa a escala micrométrica o sub-micrométrica.

La madera es otro ejemplo, ya que se pueden seguir las vetas del material a simple vista, pero la estructura íntima de este material no es accesible más que a partir de una escala de 50 a 100 µm. La figura 2 ilustra firmas digitales que se pueden obtener a partir de estos materiales diferentes, dependiendo de los filtros utilizados.

La detección, en el elemento material, de una característica estructural que refleja su estructura compleja única, se puede realizar examinando el elemento de acuerdo con una línea (1D), de acuerdo con una superficie (2D), o de acuerdo con un volumen (Estereoscopia 3D), de modo que después de la digitalización, la característica estructural se encuentra en la forma de 1D, 2D o 3D. Ventajosamente, la(s) firma(s) digital(es) utilizada(s) refleja(n) la estructura interna del material fibroso y por lo tanto, se obtendrán por observación de las características internas y eventualmente de superficie en un volumen de este último. La detección también se puede realizar de manera independiente del tiempo o "en tiempo real". En este último caso, la característica estructural se muestrea en el tiempo.

Asimismo, se pueden añadir dimensiones a esta fase de detección, observando el elemento material bajo diferentes orientaciones o iluminaciones, en color, con niveles de grises, en forma binaria, etc. La imagen considerada también puede ser una imagen discreta o no discreta, real o compleja (amplitud y fase) en el sentido del tratamiento y del análisis de la imagen.

La o las firmas digitales utilizadas en el procedimiento de la invención se corresponden con dicha característica estructural digitalizada, eventualmente sometida a una codificación (antes o después de la digitalización) de acuerdo con uno o varios algoritmos. También, dicha firma digital se presenta, por ejemplo, en una forma binaria, en la forma de una o varias imágenes en color o en niveles de grises, de una o varias imágenes discretas, reales o complejas (amplitud y fase).

Resulta evidente que el valor completo de la invención se pone de manifiesto al utilizar una o unas firmas digitales que mantienen un carácter complejo y aleatorio característico de la estructura única y estable del material, a pesar del tratamiento aplicado a las características estructurales utilizadas para generar la firma digital.

Para generar una o varias firmas digitales a partir de las características, son también concebibles numerosos métodos y no es razonable pretender citarlos todos. Por lo tanto, las técnicas que se aportan más adelante no constituyen en modo alguno una lista exhaustiva.

Los métodos conocidos de tratamiento y análisis de la señal o de la imagen, de la electrónica o de la óptica están disponibles directamente de forma muy sencilla. Los tratamientos utilizados se basan por lo tanto, en forma digital o analógica, en filtros espaciales y/o de frecuencia (paso-alto, paso-bajo, pasa-banda), y/o la transformada de Fourier, y/o las transformadas denominadas de ondículas, y/o descriptores, y más generalmente, todo tipo de algoritmo que permite analizar, y/o transformar y/o reorganizar y/o clasificar y/o fijar umbrales en los datos sin procesar (incluyendo señales e imágenes) extraídos de la o las características estructurales. Las operaciones de convolución/deconvolución, así como las operaciones lógicas y aritméticas entre imágenes y/o señales pueden ser utilizadas para obtener dichas firmas. A título ilustrativo, la transformada de Fourier de una señal-imagen se podrá utilizar, ya sea por medio de un algoritmo de transformada rápida de Fourier (FFT) si la señal es de naturaleza discreta, ya sea por medio de una lente de Fourier si la señal es de naturaleza óptica.

A la característica o características estructurales extraídas del elemento material también se les pueden aplicar algoritmos más elaborados, tales como los mencionados más arriba de modo que la o las firmas digitales finales se presentan en forma de una señal, una imagen, o cualquier tipo de archivo que se pueda codificar en una forma alfanumérica o digital en base decimal, binaria, octal, hexadecimal u otra.

La fase de protección puede utilizar una o varias firmas digitales procedentes de un mismo elemento material o de varios elementos materiales.

La fase de protección de la información sensible en forma digital, por medio de la o las firmas digitalizadas generadas de esta manera, se puede realizar, como se explicó anteriormente, de manera directa por medio de operaciones matemáticas elementales, o indirecta recurriendo a algoritmos elaborados existentes, por ejemplo de criptografía y/o esteganografía, con o sin compresión previa de datos.

En la vía directa, la protección de la información sensible en forma digital se realiza mediante combinación con por lo menos una firma digital de un elemento material, que convierte en por lo menos parcialmente ilegibles tanto la información sensible en forma digital como la firma digital.

A título de ejemplo, se puede citar la combinación de una firma digital que se presenta en forma binaria (secuencia de "0" y de "1", imagen de la estructura caótica del elemento material), con la información sensible en forma digital codificada, ella también, en forma binaria, realizando una operación lógica (por ejemplo XOR (suma módulo 2)) entre las dos secuencias binarias bit a bit. Las dos secuencias binarias son de manera ideal del mismo tamaño. La firma digital y la información digital a proteger se pueden también combinar sumando, octeto a octeto, las dos cadenas digitales. Nuevamente en este caso, es posible una variedad de combinaciones que se sitúan dentro del alcance de la invención. La combinación se puede realizar, a partir de la forma binaria, hexadecimal, ASCII o alfabética, de la información sensible en forma digital y de la o las firmas digitales del elemento material, aplicando de manera conjunta o no principios de permutación, transposición, sustitución, iteración, enmascarado (operadores lógicos incluyendo XOR, suma, resta, bit a bit (en cadena), o bloque a bloque, etc.) o propiedades matemáticas del álgebra modular (módulo n), de teoría de números.

Una forma más elaborada de combinación utiliza el principio de máscara desechable (“One Time Pad”). La firma digital utilizada es una secuencia perfectamente aleatoria, del mismo tamaño que la información sensible en forma digital (por ejemplo, en número de bits,) y no sirve de máscara más que una sola vez. Por extensión, se puede prever también el uso de una firma digital de tamaño mayor o igual al de la información sensible. Además, cabe indicar que es posible combinar todo tipo de información sensible, independientemente de su tamaño, dada la reserva prácticamente inagotable que constituyen los elementos materiales seleccionables.

La protección de solamente una parte de la información sensible es completamente concebible, basta con seleccionar, en el seno de la información digital, las zonas que van a ser combinadas con la firma digital.

La vía indirecta para securizar la información digital utilizan la o las firmas digitales del elemento material y algoritmos criptográficos (con clave privada y/o con clave pública) y/o esteganográficos. Las firmas digitales juegan el papel de claves criptográficas, esteganográficas, contraseña, frase de pase, archivo de paso, semilla aleatoria, claves de codificación aleatorias, o simplemente se pueden utilizar como "envoltura digital" de una información digital comprimida, cifrada y/o esteganografiada. Se tiene entonces un procedimiento de protección más complejo: la información sensible se puede proteger de acuerdo con métodos conocidos (combinación, algoritmo criptográfico), y a continuación se puede someter al procedimiento de protección de acuerdo con la invención o a la inversa. Cuando la de protección de acuerdo con la invención tiene lugar en la etapa final, se puede considerar que la firma digital juega el papel de envoltura digital.

Si se pueden aprovechar de manera natural las aplicaciones de clave(s) secreta(s) con el procedimiento de la presente invención, entonces, en una versión más elaborada de la invención, se pueden utilizar protocolos existentes de claves asimétricas (pública/privada) utilizando una o varias firmas digitales extraídas del elemento material como claves criptográficas. A modo de ejemplo, del elemento material se pueden extraer dos números primos grandes (una selección intrínsecamente aleatoria aunque fijada en el elemento material y por lo tanto reproducible para el que posee la clave física) que servirán para realizar un procedimiento de tipo RSA (Rivest-Shamir-Adleman), o utilizar por ejemplo, una selección aleatoria extraída del elemento material en cualquier protocolo criptográfico. Así de una manera más general, también se pueden extraer una clave pública y una clave privada a partir de un elemento material relevante en términos de la invención, transmitiéndose por ejemplo la clave pública a un destinatario, permaneciendo la clave privada, por ejemplo, bajo forma física en el elemento material y recurriéndose a ella solo temporalmente cuando sea necesario descodificar un mensaje que fue codificado con la clave pública. También se puede extraer una clave (por ejemplo, privada) de un elemento material pertinente en términos de la invención y utilizar otra clave (por ejemplo, pública) generada por cualquier otro medio. Se pueden prever de forma natural otras adaptaciones de la invención a procedimientos o protocolos criptográficos existentes. En particular, se pueden garantizar fácilmente las funciones de autentificación, certificación, identificación, no repudio, confidencialidad, control de integridad, prueba de conocimiento nulo, firma, intercambio de claves, datación, generación, custodia y gestión de claves, etc. actualmente cubiertas por dichos protocolos existentes.

Ya se utilice la vía directa o indirecta de protección descrita más arriba, las firmas y la información digital se pueden someter aguas arriba, es decir antes de la utilización de la combinación o del algoritmo criptográficos y/o esteganográfico, a un algoritmo de compresión de la información o cualquier otro tratamiento.

La protección por vía directa y la protección por vía indirecta permiten ambas, de ser necesario, proteger nada más que una parte de la información sensible, utilizar varios niveles de acceso a la información sensible original. También parece interesante que la protección utilice varias firmas digitales procedentes de un mismo elemento materiales o de elementos materiales diferentes, permitiendo posteriormente conceder accesos de lectura diferentes a esta información sensible, y específicamente nada más que a ciertas partes solamente de esta información sensible. El uso de varias firmas digitales sucesivamente y/o de una manera secuencial permite una securización de la información digital en múltiples niveles de acceso. Las firmas digitales se generan a continuación en la fase de lectura posterior, en función del nivel de autorización de acceso del operador.

Un dispositivo adecuado para la realización de la protección de información sensible, utilizable en el ámbito de la invención, comprende medios para localizar un elemento material seleccionado y detectar en este último, una o

varias de sus características estructurales, que reflejan en particular su estructura compleja, caótica, única y estable, conectados a una unidad de almacenamiento y de tratamiento, garantizando:

a1) la adquisición, la conformación/el acondicionamiento, la digitalización y eventualmente la codificación de acuerdo con uno o varios algoritmos, de la característica o características estructurales detectadas, para generar una (o unas) firma(s) digital(es), que reflejan ventajosamente el carácter complejo, caótico, único y estable de la estructura del elemento material,

b1) la asociación de la (o las) firma(s) digital(es) generada(s) a informaciones sensibles bajo forma digital para garantizar su protección, generando así informaciones sensibles protegidas.

Para la detección se utilizará preferentemente un sensor óptico. El dispositivo se puede conectar a medios de transmisión a distancia de las informaciones sensibles protegidas (incluso sobre un canal no seguro tal como Internet) y/o de la firma digital y/o de las características estructurales.

Un aspecto importante de la presente invención es que la misma es aplicable, tanto a informaciones de tamaño definido e invariable en el tiempo, como a informaciones “en tiempo real” de tipo señal digital que varían con el tiempo. Si el primer modo de aplicación es fácilmente perceptible, ya que se combina un fragmento delimitado e invariable de informaciones (firma digital) procedente de un elemento material con un fragmento de informaciones digitales a proteger, también delimitado e invariante, el segundo modo de aplicación exige más aclaraciones.

En el caso en el que el procedimiento según la invención se utilice para proteger informaciones sensibles dinámicas, tales como una secuencia sonora y/o de vídeo, es necesario utilizar una firma digital “dinámica”. La firma digital “dinámica” se puede obtener por repetición de una firma digital estática o por detección repetida, con la ayuda de uno o varios sensores, de una o varias características estructurales de un elemento material estático que refleja su estructura compleja única.

Otra de las variantes consiste en obtener una firma digital “dinámica” por detección en continuo, con la ayuda de uno o varios sensores, de una o varias características estructurales de un elemento material en movimiento relativo con respecto al (a los) sensor(es). El elemento material “desfila” por delante del sensor o sensores, de manera sincronizada o no con la señal digital a securizar. El desplazamiento relativo del elemento material y del sensor o sensores también se puede obtener con el movimiento único del sensor o sensores o el movimiento combinado del(de los) sensor(es) y del elemento material, en direcciones y/o con velocidades diferentes. En esta última variante, el elemento material es, por ejemplo, una bobina de papel, cartón o no tejido, en desplazamiento, o papel en curso de fabricación en una máquina de papel. Incluso es concebible combinar instantáneamente la señal digital a proteger con las firmas “dinámicas” obtenidas.

En todo procedimiento de protección/securización de información, es necesario a continuación poder leer las informaciones que se han protegido. El término “leer” debe interpretarse en sentido amplio, incluyendo todo tipo de descodificación, descifrado, etc., que convierta las informaciones sensibles originales, por lo menos parcialmente, en accesibles, comprensibles, legibles.

La presente invención tiene así por objeto un procedimiento de securización de informaciones sensibles, que comprende:

a) una etapa de protección tal como se ha definido anteriormente en la presente, que conduce a informaciones sensibles en forma securizada,

b) una etapa de lectura de las informaciones securizadas obtenidas en la etapa a), que permite recuperar las informaciones sensibles.

En general, entre la etapa de protección y la etapa de lectura, el procedimiento de securización comprende una etapa de registro de las informaciones securizadas en un soporte de datos.

A continuación se describirá la etapa de lectura.

Asimismo, la presente invención tiene también por objeto un procedimiento de lectura de informaciones protegidas en el cual, la lectura de las informaciones protegidas se lleva a cabo en forma digital, por aplicación de un tratamiento digital, que utiliza por lo menos una firma digital obtenida a partir de por lo menos una característica estructural de un elemento material seleccionado entre la totalidad o parte de un material fibroso, de plástico, metálico, de cuero, de madera, compuesto, de vidrio, de mineral, de estructura cristalina.

Todo lo que se ha dicho anteriormente en la parte relativa a la protección de las informaciones sensibles, en particular, lo que se refiere a la elección del elemento material, la obtención de las características estructurales, y las firmas digitales, se aplica a la lectura.

De forma esquemática, la lectura de las informaciones protegidas se efectuará gracias a un tratamiento digital que se corresponde sustancialmente con el tratamiento digital inverso al utilizado para su protección, utilizando una o unas firmas digitales del elemento material que han servido para su protección, como clave(s) de lectura.

Uno de los problemas consiste en mantener y transmitir los elementos de inteligencia necesarios para esta lectura. Estos elementos de inteligencia incluyen, evidentemente, la o las firmas digitales que han servido para la protección de las informaciones sensibles. El mantenimiento se puede realizar a diversos niveles, en primer lugar, es posible registrar, por ejemplo en forma digital, o bien la característica o características estructurales que han servido para generar la (o las) firma(s) digital(es), o bien la (o las) propia(s) firma(s) digital(es). En este caso, se produce una desmaterialización del elemento material el cual ya no es necesario conservar y puede ser destruido. Sin embargo es necesario gestionar perfectamente la seguridad de los datos digitales conservados. En este caso, la(s) firma(s) digital(es) utilizada(s) para la lectura se corresponden exactamente con la(s) utilizada(s) para la protección.

A continuación, también es posible conservar el elemento material que ha servido para generar la firma digital, lo cual implica localizar y proteger el elemento material para su posterior reutilización. En este último caso, en general habrá que tener la capacidad de reproducir todas las etapas realizadas para obtener la firma digital utilizada para la protección. Es decir es, necesario:

- recuperar el elemento material que ha servido para securizar las informaciones sensibles. Este elemento material se habrá podido indexar con estas últimas, por medio de una base de datos, o bien se habrá vinculado a una parte de las informaciones sensibles originales (impresión de un código por ejemplo),

- extraer, adquirir una o varias características estructurales de este elemento material por medio de uno o varios sensores con o sin contacto con el elemento material, seguido(s) en general por una unidad de tratamiento analógico (por ejemplo óptico o electrónico) o digital (tarjeta de captura conectada a cualquier plataforma informática o automática). Se generan así una o varias firma(s) digital(es), eventualmente después de la codificación de las características estructurales, por aplicación de uno o varios algoritmos, cuya naturaleza puede variar en función del tipo de elemento material seleccionado y de la aplicación prevista.

Preferentemente, las etapas realizadas en el procedimiento de lectura utilizan las mismas condiciones de funcionamiento que las correspondientes utilizadas en el procedimiento de protección de las informaciones. La capacidad de recuperar o reproducir perfectamente una o varias firmas digitales dadas a partir de un elemento material es en general indispensable, para realizar correctamente el procedimiento de lectura. El factor de escala, la sensibilidad del sensor (filtrado), el posicionamiento del elemento, etc., son parámetros a tener en cuenta sin duda en la selección de la característica estructural que se va a detectar en el elemento material. No obstante, es posible la consideración de recurrir a claves de control o a códigos correctores de errores, de forma más general técnicas de detección y de corrección de errores, que permitan paliar errores de lectura. También se puede autorizar la recuperación de las informaciones sensibles digitales originales según el resultado exitoso de un test de dependencia estadística entre la o las firmas digitales extraídas en el momento de la lectura y las correspondientes que hayan servido para la securización, por ejemplo almacenadas en una base de datos. En consecuencia, en el caso en el que cuando tiene lugar la lectura las firmas digitales se recuperan a partir del elemento material, estas podrán ser ligeramente diferentes a las utilizadas para la protección y por lo tanto se podrán someter a claves de control, a códigos correctores de errores o a un test de dependencia estadística.

Incluso se pueden utilizar otros medios que permitan recuperar la información digital original, a pesar de una reproducción imperfecta de la firma digital del elemento material en la fase de lectura. Por ejemplo, la introducción de redundancia en las informaciones sensibles originales antes de la fase de protección de las informaciones por el procedimiento objeto de la invención, confiere solidez al procedimiento de lectura.

Cabe indicar, además, que en ciertos casos, es incluso posible utilizar una o unas firmas digitales ligeramente diferentes a las correspondientes que han servido para la protección de los datos originales aunque provenientes del mismo elemento material original, y recuperar, a pesar de todo, por lo menos el significado de las informaciones originales, cuando no sea posible recuperarlas intactas. Por ejemplo, una foto carné ligeramente borrosa o con defectos menores no impide en absoluto reconocer a la persona.

En relación con el transporte de los elementos de inteligencia necesarios para lectura, que incluyen específicamente el elemento material, la característica estructural en forma digital o la firma digital, la invención presenta también una relevancia particular: el elemento generador de la firma digital es de origen físico y puede ser transportado físicamente por un canal totalmente distinto a los canales digitales. Si se llega a un acuerdo sobre otro secreto (algoritmos de generación de firmas digitales, números de firmas digitales útiles en un conjunto más grande, orden de utilización de estas claves, etc.), los elementos de inteligencia digitales se pueden transmitir directamente, incluso pueden ser protegidos ellos mismos por otra variante de la invención, cuando tiene lugar su transmisión.

Antes de la realización del procedimiento de protección, el operador tiene en posesión informaciones sensibles bajo forma digital que van a ser securizadas y un elemento material. Después de su realización, el operador tiene en posesión las informaciones sensibles securizadas y registradas en un soporte de datos, el elemento material y las

informaciones sensibles originales. Estas últimas o bien se pueden almacenar de forma segura para verificar posteriormente la integridad de las informaciones securizadas, por ejemplo, o bien se pueden destruir. Por lo tanto, no queda más que el elemento material y el soporte portador de las informaciones sensibles securizadas. Las informaciones sensibles securizadas no podrán ser leídas más que por el que posea el elemento material y el conocimiento detallado de los medios utilizados para generar la firma digital, y a continuación garantizar la protección de las informaciones. La seguridad del sistema queda garantizada doblemente por la seguridad de mantenimiento del elemento material, y la seguridad del secreto de los detalles del procedimiento. Cuando una información digital se ha securizado a partir del análisis de la textura de un papel, y solamente una zona o zonas bien delimitadas de este papel constituyen el elemento material, entonces la seguridad del procedimiento queda garantizada por la preservación del papel y el conocimiento de las zonas activas de este elemento material. Este ejemplo ilustra la fuerza de este tipo de protección de la información digital, que permite mantener por un lado el elemento material que se ha utilizado (sin tener que revelar por otra parte la naturaleza) y poder, con toda seguridad, transmitir o almacenar la información securizada. Una parte del sistema se mantiene materialmente, y una parte es inmaterial y digital.

Evidentemente, una alternativa mencionada anteriormente consiste en mantener no el elemento material sino su firma digital o las características, por ejemplo en forma digital, que reflejan su estructura compleja caótica, única y estable. Estas últimas se salvaguardan entonces de manera duradera y segura y podrán utilizarse directamente para la lectura, pudiéndose destruir eventualmente el elemento material original. Lo interesante en este caso es obtener la securización basándose en las propiedades estructurales complejas, caóticas y únicas del elemento material, y manteniendo imágenes digitales de las mismas (desmaterialización) para facilitar la realización de la fase de lectura. La seguridad de almacenamiento de las características digitales y/o de las firmas digitales es por lo tanto crítica. De forma claramente obvia las mismas se pueden securizar por medio de todos los medios típicos del tipo criptografía, esteganografía, llave física USB (*Universal Serial Bus*), tarjeta chip u otros.

El procedimiento de lectura según la invención se aplica en las informaciones protegidas en forma digital, a las cuales se somete a un tratamiento digital inverso al utilizado para su protección. Generalmente, se debe reproducir a la inversa el algoritmo, tratamiento o combinación utilizados para la protección, desempeñando entonces la firma utilizada para la protección el papel de clave de lectura, en el sentido amplio del término, de modo que las informaciones sensibles originales vuelven a ser por lo menos parcialmente legibles. A título de ejemplo, se utilizará un algoritmo de reconstrucción, un algoritmo o algoritmos de descifrado inverso a los utilizados para la protección, y la o las firmas digitales servirán de claves de descifrado.

En el caso en el que la fase de lectura utiliza el elemento material para recuperar la firma digital necesaria, se utilizará un dispositivo que comprende medios para localizar un elemento material seleccionado y detectar en este último, una o varias de sus características estructurales, que reflejen en particular su estructura compleja, caótica, única y estable, conectados a una unidad de almacenamiento y de tratamiento garantizando:

a2) la adquisición, la conformación/el acondicionamiento, la digitalización y eventualmente la codificación de acuerdo con uno o varios algoritmos, de la característica o características estructurales detectadas, para generar una (o unas) firma(s) digital(es), que reflejan ventajosamente el carácter complejo, caótico, único y estable de la estructura del elemento material,

b2) la lectura de las informaciones sensibles protegidas mediante la utilización de un tratamiento digital que utiliza la o las firmas digitales generadas en la etapa a2), como clave(s) de lectura, y que se corresponde ventajosamente con el tratamiento digital sustancialmente inverso al utilizado para la asociación de la (o las) firma(s) digital(es) con las informaciones sensibles originales, cuando tiene lugar su protección.

En particular, la unidad de almacenamiento y de tratamiento garantiza:

a2) la digitalización y eventualmente la codificación según uno o varios algoritmos de la o las características estructurales detectadas, para generar una (o unas) firma(s) digital(es),

b2) la lectura de las informaciones sensibles protegidas mediante la utilización de un tratamiento digital que utiliza la o las firmas digitales generadas en la etapa a2), como clave(s) de lectura, y que se corresponde con el tratamiento digital sustancialmente inverso al utilizado para la asociación de la (o las) firma(s) digital(es) con las informaciones sensibles originales, cuando tiene lugar su protección.

Se entiende claramente que el procedimiento de protección y el procedimiento de lectura se pueden realizar con un mismo dispositivo.

La protección según la invención se utiliza, por ejemplo, para proteger informaciones sensibles digitales (telecomunicaciones, música, vídeo, multimedia, etc.), con vistas a su transporte sobre redes poco seguras y/o con vistas a controlar/garantizar su posterior uso. En este tipo de aplicaciones, la desmaterialización del elemento material como clave de securización puede adquirir toda su relevancia. Efectivamente, si se desea llevar a cabo una securización de una señal digital con el fin de transportarla sobre redes poco seguras y/o controlar y/o garantizar su

posterior uso, y además que esta fase de lectura deba producirse geográficamente y/o con un retardo que hacen imposible el transporte del elemento material, se puede imaginar, por ejemplo, la emisión simultánea o ligeramente desfasada de la señal digital securizada y las características estructurales digitalizadas del elemento material y/o las firmas digitales asociadas. La seguridad de la operación se garantiza, por lo tanto, por el aspecto algorítmico a utilizar en el procedimiento de lectura y por la naturaleza intrínsecamente caótica, y por lo tanto imprevisible, del elemento material que se reconoce en sus características estructurales digitalizadas y/o las firmas digitales asociadas. También se pueden imaginar dos tipos distintos de canales de transmisión de la señal digital securizada por un lado, y de las características digitalizadas del elemento material y/o de las firmas digitales asociadas por otro lado.

El soporte de datos en el cual se pueden almacenar las informaciones protegidas constituye también un aspecto importante. Este soporte servirá también normalmente para la transmisión o para el transporte posterior de las informaciones protegidas. El almacenamiento puede tener lugar de manera permanente o temporal. Este soporte es portador de las informaciones protegidas: estas informaciones se pueden imprimir en un soporte físico, por ejemplo en papel, o se pueden registrar en un soporte electrónico, magnético, óptico. Evidentemente, el soporte puede ser portador de otras informaciones. A título de ejemplos ilustrativos, las informaciones digitales protegidas según el procedimiento de la invención se pueden registrar en un disco duro magnético, en banda magnética, en formato óptico, en una memoria holográfica, se pueden grabar en un CD o DVD, en una llave USB, en memoria flash u otros, en forma electrónica en una tarjeta chip, aunque también en una forma impresa o grabada en un material o documento. El soporte físico puede estar constituido por varios materiales, y puede contener la información securizada en diferentes formas. Las informaciones securizadas asimismo se pueden almacenar en forma de una base de datos, fácilmente consultable, ya sea de forma directa, o ya sea mediante una red de telecomunicaciones (por ejemplo Internet).

La información securizada por lo tanto se puede transmitir y recibir por medio de una red de telecomunicaciones o mediante un transporte en forma física.

El soporte puede integrar además medios de transmisión de información o puede integrar uno o múltiples elementos utilizados en una transmisión de información, en particular elementos sensibles a las radio-frecuencias (por ejemplo antenas activas o pasivas) utilizados en una transmisión de información sin contacto y a distancia. Según una variante de realización, el soporte es un documento en papel, un cartón o un no tejido. Puede tratarse en particular de un papel denominado de seguridad (billete de banco, cheque, documento público, billetaje, etc.) que reúna la totalidad o parte de los siguientes elementos de seguridad: elementos incorporados (hilos de seguridad, *planchettes*), filigranas, hologramas, microperforaciones, microimpresiones, diferentes tipos de impresión, reactivos químicos contra la falsificación, etc.

Este soporte se puede presentar bajo la forma de un documento en papel o cartón o no tejido, cuya totalidad o parte se corresponde con el elemento material del cual procede la o las firma(s) digital(es) que haya servido para la protección de las informaciones sensibles, parcial o totalmente protegido por una envoltura transparente externa (por ejemplo por plastificación o revestimiento o extrusión u otros) de otro material que juega un papel protector contra las agresiones exteriores normales de uso aunque también impide la separación del documento y de su envoltura sin destrucción del primero. Asimismo, un tratamiento superficial con una resina transparente puede garantizar la protección.

Así, las informaciones sensibles protegidas se registran en este soporte, por ejemplo por impresión. Según una variante, las informaciones sensibles protegidas aparecerán bajo la forma de un código de barras.

Este soporte también puede presentarse en forma de papel, cartón ondulado o plano, o no tejido, por ejemplo transformado en un sobre, en cartón de embalaje, en una etiqueta, en ropa desechable, etc.

Ciertas formas posibles de soporte de informaciones securizadas que se han enumerado anteriormente en el presente documento, pueden además integrar íntimamente la totalidad o parte del elemento material que haya servido para la protección de las informaciones sensibles y/o la totalidad o parte de las informaciones sensibles originales bajo cualquier forma sea cual sea, impresas o almacenadas en forma digital. Preferentemente, el elemento material estará localizado y protegido.

En las aplicaciones de tarjetas chip y/o de banda magnética, esto resulta particularmente interesante ya que se introduce “la inteligencia” en el soporte y se vinculan de manera biunívoca el elemento material/soporte y las informaciones securizadas. Las informaciones originales por lo tanto no son accesibles más que para el poseedor del elemento material. Este acoplamiento de las informaciones originales y del elemento material permite además una verificación implícita de la autenticidad de la tarjeta. Las informaciones sensibles digitales presentes en claro en el soporte permiten también verificar la integridad de estas informaciones y/o de las informaciones securizadas mediante simple comparación.

Análogamente, el soporte físico puede integrar íntimamente la totalidad o parte del elemento material que haya servido para la utilización de la protección y/o la totalidad o parte de la característica o características estructurales

extraídas del elemento material bajo cualquier forma sea cual sea, y/o la totalidad o parte de la o las firmas digitales del elemento material en cualquier forma sea la que sea. Específicamente, integra por lo menos una firma digital obtenida a partir de una característica cuasi invariante de un elemento material que refleja su estructura compleja única, preferentemente, en forma cifrada.

A título de otros ejemplos de soporte, cuya autenticidad puede ser verificada, se pueden citar:

- una tarjeta en papel en la cual se imprimen, por un lado, las informaciones sensibles originales, y por otro lado, las informaciones sensibles protegidas y una de cuyas partes se corresponde con el elemento material en papel que ha servido para generar la firma electrónica, estando protegido y localizado este elemento por una película plástica,

- un soporte en papel una de cuyas partes se corresponde con el elemento material, atrapado en el seno de un CD en el cual se graban las informaciones protegidas gracias a una firma digital generada con el elemento material de papel.

Consecuentemente, si el procedimiento de lectura autoriza la lectura exitosa de las informaciones sensibles, también valida el carácter auténtico de la o las firmas digitales utilizadas, y/o del elemento material de la cual proceden, y/o del soporte portador de las informaciones sensibles protegidas.

Además, una etapa suplementaria, en el procedimiento de lectura, que compara las informaciones leídas con las informaciones sensibles conocidas del usuario permite validar el carácter auténtico de la o las firmas digitales utilizadas, del elemento material del cual proceden y de las informaciones sensibles. Este aspecto es particularmente ventajoso cuando el soporte sirve para la realización de documentos de identidad, de tarjetas de acceso, etc.

Los procedimientos de protección y de lectura según la invención se pueden integrar evidentemente aguas arriba o aguas abajo de un procedimiento de aplicación más general. En particular, se pondrán utilizar, de manera individual o combinados, con otros procedimientos, para la trazabilidad de productos y servicios, la gestión documental, la fabricación de documentos de seguridad, de documentos públicos, de etiquetas incorporadas o no, la confidencialidad de correo físico o electrónico, la certificación de origen de documentos en papel o electrónicos, el pago electrónico, la firma electrónica, para generar códigos de barras, una carta recomendada con acuse de recibo, seguimiento de correo o de paquetes, sobres, marcas de agua digitales, etc.

Las figuras 3 y 4 ilustran un ejemplo de realización de los procedimientos de protección y lectura según la invención. En este ejemplo, el elemento material considerado es una tarjeta en papel/cartón, incluso una tarjeta de plástico que integra un elemento material de papel/cartón, cuya estructura caótica de material es accesible por transvisión.

La fase de escritura ilustrada en la figura 3 utiliza el procedimiento de protección según la invención, a partir de un conjunto de tarjetas originales vírgenes, que integran, cada una de ellas, un elemento material generador de una firma digital, del tipo que se ha descrito anteriormente en la presente, archivos digitales que contienen dos tipos de información (nivel 1 el cual se imprimirá en una tarjeta y nivel 2 el cual se securizará con el nivel 1 por ejemplo), un PC con tarjeta de captura, una impresora dotada de un módulo de lectura óptica de las características que reflejan la estructura compleja única del elemento material, o en otra configuración un módulo de lectura óptica separado de la impresora. Las informaciones digitales (nivel 1 y nivel 2) que se vincularán a las tarjetas pueden ser parcialmente similares. En el momento del paso de una tarjeta por la impresora o el módulo externo de lectura óptica, se imprime en la misma la información de nivel 1, y se extraen la característica o características estructurales en forma digital del elemento material presente, y se generan las firmas digitales asociadas, que se almacenan temporalmente en el PC, con el fin de obtener una combinación (directa o indirecta) de la información digital (nivel 1 y nivel 2) con dichas firmas. Al final de la fase de escritura, las tarjetas se imprimen con una parte de la información securizada en forma inteligible, y en una base de datos de referencia (con o sin índice de tarjeta/archivo securizado) se almacenan de manera duradera archivos que contienen las informaciones digitales (nivel 1 y nivel 2) cifradas con las firmas digitales extraídas de los elementos materiales sucesivos. Estos archivos cifrados se podrán transmitir mediante un enlace local o una red de telecomunicaciones.

En cuanto a la fase de lectura ilustrada en la figura 4, la misma utiliza el procedimiento de lectura según la invención. El juego de tarjetas originales impresas, obtenidas en la fase de escritura se analiza mediante su paso a través de un lector óptico, una tarjeta de captura y un PC, y las firmas digitales se generan y almacenan de forma temporal en la memoria del PC, con el fin de poder comprobar dichas firmas con los archivos securizados presentes en la base de datos de referencia. Si la tarjeta comprobada permite el acceso a las informaciones digitales de nivel 1 y de nivel 2 contenidas en un archivo cifrado, se dispone entonces de varias informaciones conjuntamente: por un lado que la tarjeta (clave) es auténtica, por otro lado, comparando la información de nivel 1 comprendida en el archivo cifrado y la información de nivel 1 impresa en la tarjeta, que si existe identidad entre ellas entonces el archivo cifrado y/o la información presente en la tarjeta están íntegros, es decir que no han sido modificados desde la creación de la tarjeta.

REIVINDICACIONES

1. Procedimiento de lectura de informaciones sensibles protegidas, caracterizado por que la lectura se realiza sometiendo las informaciones sensibles protegidas en forma digital a un tratamiento digital que utiliza una o unas firmas digitales obtenida(s) a partir de por lo menos una característica estructural de un elemento material seleccionado de entre la totalidad o parte de un material fibroso, de plástico, metálico, de cuero, de madera, compuesto, de vidrio, de mineral o con una estructura cristalina, utilizándose la o las firmas digitales en calidad de clave de lectura.

2. Procedimiento de lectura de informaciones sensibles protegidas según la reivindicación 1, caracterizado por que la protección de las informaciones sensibles ha utilizado las informaciones sensibles en forma digital y por lo menos una firma digital obtenida a partir de por lo menos una característica estructural de un elemento material seleccionado de entre la totalidad o parte de un material fibroso, de plástico, metálico, de cuero, de madera, compuesto, de vidrio, de mineral o con una estructura cristalina, y por que, la lectura se realiza sometiendo las informaciones sensibles protegidas en forma digital a un tratamiento digital inverso al utilizado para su protección y que utiliza una o unas firmas digitales del elemento material regenerada(s) cuando tiene lugar la lectura.

3. Procedimiento de lectura de informaciones sensibles protegidas según la reivindicación 1, caracterizado por que la protección de las informaciones sensibles ha utilizado las informaciones sensibles en forma digital y por lo menos una firma digital obtenida a partir de por lo menos una característica estructural de un elemento material seleccionado de entre la totalidad o parte de un material fibroso, plástico, metálico, de cuero, de madera, compuesto, de vidrio, de mineral o con una estructura cristalina, y por que, la lectura se realiza sometiendo las informaciones sensibles protegidas en forma digital a un tratamiento digital inverso al utilizado para su protección y que utiliza una o unas firmas digitales del elemento material que ha servido para su protección.

4. Procedimiento de lectura de informaciones sensibles protegidas según una de las reivindicaciones 1 a 3, caracterizado por que utiliza por lo menos una firma digital obtenida a partir de por lo menos una característica estructural de un elemento material que refleja su estructura compleja, caótica, única y estable.

5. Procedimiento según una de las reivindicaciones 1 a 4, caracterizado por que la(s) firma(s) digital(es) es(son) aleatorias.

6. Procedimiento según la reivindicación 5, caracterizado por que la(s) firma(s) digital(es) presenta(n) un carácter complejo y aleatorio que refleja la estructura del material de la cual se extraen.

7. Procedimiento según una de las reivindicaciones 1 a 6, caracterizado por que el elemento material se selecciona de entre la totalidad o parte de un papel, cartón o no tejido.

8. Procedimiento según la reivindicación 7, caracterizado por que el elemento material es una parte de un papel, cartón o no tejido, en el que se localiza por medio de un material transparente, estable con el paso del tiempo y que garantiza su protección, por ejemplo, un revestimiento de plástico o una resina.

9. Procedimiento según una de las reivindicaciones 3 a 8, caracterizado por que la o las firmas digitales utilizadas cuando tiene lugar la lectura se corresponden con las utilizadas cuando tiene lugar la protección.

10. Procedimiento según la reivindicación 9, caracterizado por que la o las características estructurales digitales y/o la o las firmas digitales utilizadas cuando tiene lugar la protección se salvaguardan de manera duradera y segura, mientras que el elemento material se destruye, y se utilizan cuando tiene lugar la lectura.

11. Procedimiento según una de las reivindicaciones 3 a 8, caracterizado por que la o las firmas digitales utilizadas cuando tiene lugar la lectura están sometidas a unas claves de control, a códigos correctores de errores o a un test de dependencia estadística.

12. Procedimiento según una de las reivindicaciones 1 a 11, caracterizado por que, si su realización autoriza la lectura exitosa de las informaciones sensibles, valida asimismo el carácter auténtico de la o de las firmas digitales utilizadas, y/o del elemento material del cual proceden.

13. Procedimiento según una de las reivindicaciones 1 a 12, caracterizado por que comprende una etapa suplementaria de comparación de las informaciones leídas, con las informaciones sensibles conocidas del usuario, permitiendo así validar el carácter auténtico de la o de las firmas digitales utilizadas, del elemento material del cual proceden y de las informaciones sensibles.

14. Procedimiento según una de las reivindicaciones 1 a 13, caracterizado por que la firma digital del elemento material se obtiene por detección, con la ayuda de uno o varios sensores, de una o varias características estructurales de este elemento, seguida por una digitalización, eventualmente acompañada de una codificación según uno o varios algoritmos, de esta o estas características estructurales.

15. Procedimiento según la reivindicación 14, caracterizado por que la(s) característica(s) estructural(es) detectada(s) refleja(n) la estructura compleja, caótica, única y estable del elemento material.

16. Procedimiento según la reivindicación 14 o 15, caracterizado por que la detección se realiza gracias a un sensor óptico o electrónico, después de la aplicación sobre el elemento material de una onda o de una radiación electromagnética.

17. Procedimiento según la reivindicación 14 o 15, caracterizado por que la detección se realiza gracias a un sensor con contacto, sirviendo el elemento material como soporte de una onda ultrasónica, o de una solicitación del tipo eléctrico, térmico, químico, biológico, registrándose en diferentes orientaciones el comportamiento/la respuesta del elemento material sometido a esta onda o solicitación.

18. Procedimiento según una de las reivindicaciones 1 a 17, caracterizado por que la firma digital se presenta en una forma binaria o en forma de una imagen real o compleja o varias imágenes con niveles de grises.

19. Procedimiento según una de las reivindicaciones 1 a 18, caracterizado por que utiliza la firma digital de un elemento material, parte de un papel, cartón o no tejido, obtenida después de la detección de su interacción con la luz visible por transvisión, utilizando un sensor CCD o CMOS.

20. Procedimiento según una de las reivindicaciones 1 a 19, caracterizado por que la lectura utiliza uno o unos algoritmos de descifrado, sirviendo la o las firmas digitales de claves de descifrado.

21. Procedimiento según una de las reivindicaciones 2 a 18, caracterizado por que la protección de las informaciones sensibles en forma digital se realiza por medio de un algoritmo esteganográfico, desempeñando la(s) firma(s) digital(es) del elemento material el papel de claves de esteganografía.

22. Procedimiento según una de las reivindicaciones 2 a 18, caracterizado por que la protección de las informaciones sensibles en forma digital se realiza por combinación con por lo menos una firma digital de un elemento material, que convierte en por lo menos parcialmente ilegibles, a la vez las informaciones sensibles en forma digital y la firma digital.

23. Procedimiento según la reivindicación 22, caracterizado por que la combinación se realiza a partir de la forma binaria, hexadecimal, ASCII o alfabética, de las informaciones sensibles en forma digital y de la o las firmas digitales del elemento material, mediante aplicación, de manera conjunta o no, de los principios de permutación, transposición, sustitución, iteración, enmascarado (operadores lógicos incluyendo XOR, suma, resta, bit a bit (en cadena), o bloque a bloque, etc.) o propiedades matemáticas de álgebra modular (módulo n), de teoría de números.

24. Procedimiento según la reivindicación 22, caracterizado por que la combinación se ha realizado por aplicación del principio de máscara desechable.

25. Procedimiento según una de las reivindicaciones 2 a 18, caracterizado por que la protección de las informaciones sensibles en forma digital se ha realizado, utilizando la(s) firma(s) digital(es) como “envoltura digital” de las informaciones digitales sensibles en forma comprimida, cifrada y/o esteganografiada.

26. Procedimiento según una de las reivindicaciones 1 a 25, caracterizado por que la o las características estructurales se digitalizan, y a continuación se muestrean en el tiempo.

27. Procedimiento según una de las reivindicaciones 1 a 25, caracterizado por que las informaciones sensibles son dinámicas, tales como una secuencia sonora y/o de vídeo.

28. Procedimiento según la reivindicación 27, caracterizado por que la protección se realiza por medio de una firma digital dinámica obtenida por repetición de una firma digital estática o por detección repetida, con la ayuda de uno o varios sensores, de una o varias características estructurales de un elemento material estático.

29. Procedimiento según la reivindicación 27, caracterizado por que la protección se realiza por medio de una firma digital dinámica obtenida por detección en continuo, con la ayuda de uno o varios sensores, de una o varias características estructurales de un elemento material en movimiento relativo con respecto al (a los) sensor(es).

30. Procedimiento según la reivindicación 29, caracterizado por que el elemento material es una bobina de papel, cartón o no tejido, en desplazamiento, o papel en curso de fabricación en una máquina de papel.

31. Procedimiento según una de las reivindicaciones 2 a 30, caracterizado por que la protección utiliza varias firmas digitales de un mismo elemento material o de diferentes elementos materiales, y por que la lectura recurre a varias firmas digitales de uno o varios elementos materiales, que autorizan unos niveles de acceso distintos a ciertas partes de las informaciones sensibles.

32. Dispositivo adaptado para la realización del procedimiento de lectura según una de las reivindicaciones 1 a 31, caracterizado por que comprende unos medios para localizar un elemento material seleccionado y detectar en este último, una o varias de sus características estructurales, que reflejan en particular su estructura compleja, caótica, única y estable, conectados a una unidad de almacenamiento y de tratamiento, que garantiza:

a2) la digitalización y eventualmente la codificación, según uno o varios algoritmos de la o de las características estructurales detectadas para generar una (o unas) firma(s) digital(es),

b2) la lectura de las informaciones sensibles protegidas mediante la realización de un tratamiento digital que utiliza la o las firmas digitales generadas en la etapa a2, como clave(s) de lectura, y que corresponde ventajosamente al tratamiento digital sustancialmente inverso al utilizado para la asociación de la (o de las) firma(s) digital(es) con las informaciones sensibles originales, cuando tiene lugar su protección.

33. Dispositivo según la reivindicación 32, caracterizado por que se utiliza un sensor óptico para detectar la o las características estructurales del elemento material.

34. Dispositivo según la reivindicación 32 o 33, caracterizado por que el sensor óptico es un sensor CCD o CMOS que garantiza la detección de la o de las características estructurales por transvisión.

35. Procedimiento de securización de informaciones sensibles que comprende las siguientes etapas:

a) una etapa de protección de la lectura directa de las informaciones sensibles que utiliza una firma digital obtenida a partir de un elemento material, que permite obtener las informaciones sensibles en forma protegida,

b) una etapa de lectura de las informaciones protegidas en la etapa a) de acuerdo con cualquiera de las reivindicaciones 1 a 31, que permite recuperar las informaciones sensibles.

36. Procedimiento de securización según la reivindicación 35, caracterizado por que la etapa a) está seguida por una etapa de registro de las informaciones sensibles en forma protegida en un soporte de datos.

37. Procedimiento de securización según la reivindicación 35 o 36, caracterizado por que la etapa a) de protección de las informaciones sensibles en forma digital se realiza por medio de un algoritmo criptográfico, desempeñando la(s) firma(s) digital(es) del elemento material el papel de clave(s) criptográfica(s) y la etapa b) de lectura es según el procedimiento de la reivindicación 20.

38. Procedimiento de securización según la reivindicación 35 o 36, caracterizado por que la etapa a) de protección de las informaciones sensibles en forma digital se realiza por medio de un algoritmo esteganográfico, desempeñando la(s) firma(s) digital(es) del elemento material el papel de clave(s) esteganográfica(s) y la etapa b) de lectura es según el procedimiento de la reivindicación 21.

39. Procedimiento de securización según la reivindicación 35 o 36, caracterizado por que la protección de las informaciones sensibles en forma digital se realiza por combinación con por lo menos una firma digital de un elemento material, que convierte en por lo menos parcialmente ilegibles, a la vez las informaciones sensibles en forma digital y la firma digital, a partir de su forma binaria, hexadecimal, ASCII o alfabética, mediante la aplicación, conjuntamente o no, de los principios de permutación, transposición, sustitución, iteración, enmascarado (operadores lógicos incluyendo XOR, suma, resta, bit a bit (en cadena), o bloque a bloque, etc.) o propiedades matemáticas del álgebra modular (módulo n), de teoría de los números, y la etapa b) de lectura es según el procedimiento de la reivindicación 23.

40. Procedimiento de securización según la reivindicación 39, caracterizado por que la combinación utilizada en la etapa a) se ha realizado por aplicación del principio de máscara desechable, y la etapa b) de lectura es según el procedimiento de la reivindicación 24.

41. Procedimiento de securización según la reivindicación 35 o 36, caracterizado por que la etapa a) de protección de las informaciones sensibles en forma digital se ha realizado utilizando la(s) firma(s) digital(es) como “envoltura digital” de las informaciones digitales sensibles en forma comprimida, cifrada y/o esteganografiada, y la etapa b) de lectura es según el procedimiento de la reivindicación 25.

42. Procedimiento de securización según una de las reivindicaciones 35 a 41, caracterizado por que la etapa a) utiliza por lo menos una firma digital obtenida a partir de por lo menos una característica estructural de un elemento material que refleja su estructura compleja, caótica, única y estable, y la etapa b) de lectura es según el procedimiento de la reivindicación 4.

43. Procedimiento de securización según una de las reivindicaciones 35 a 42, caracterizado por que el elemento

material de la etapa a) se selecciona de entre la totalidad o parte de un papel, cartón o no tejido, y la etapa b) de lectura es según el procedimiento de la reivindicación 7.

44. Procedimiento de securización según la reivindicación 43, caracterizado por que el elemento material de la etapa a) es una parte de un papel, cartón o no tejido, en el cual se localiza por medio de un material transparente, estable en el tiempo y que garantiza su protección, por ejemplo, un revestimiento plástico o una resina, y la etapa b) de lectura es según el procedimiento de la reivindicación 8.

45. Procedimiento de securización según las reivindicaciones 35 a 44, caracterizado por que la firma digital del elemento material utilizado en la etapa a) se obtiene por detección, con la ayuda de uno o varios sensores, de una o varias características estructurales de este elemento, seguida por una digitalización y eventualmente acompañada de una codificación según uno o varios algoritmos de esta o estas características estructurales, y la etapa b) de lectura es según el procedimiento de la reivindicación 14.

46. Procedimiento de securización según la reivindicación 45, caracterizado por que la(s) característica(s) estructural(es) utilizadas en la etapa a) refleja(n) su estructura compleja, caótica, única y estable, y la etapa b) de lectura es según el procedimiento de la reivindicación 15.

47. Procedimiento de securización según la reivindicación 45 o 46, caracterizado por que la detección se realiza en la etapa a) gracias a un sensor óptico o electrónico, después de la aplicación, en el elemento material de una onda o de una radiación electromagnética, y la etapa b) de lectura es según el procedimiento de la reivindicación 16.

48. Procedimiento de securización según la reivindicación 45 o 46, caracterizado por que la detección se realiza en la etapa a) gracias a un sensor con contacto, sirviendo el elemento material como soporte de una onda ultrasónica, o de una solicitación del tipo eléctrico, térmico, químico, biológico, y siendo el comportamiento/la respuesta del elemento material sometido a esta onda o solicitación registrado en diferentes orientaciones, y la etapa b) de lectura es según el procedimiento de la reivindicación 17.

49. Procedimiento de securización según una de las reivindicaciones 35 a 48, caracterizado por que la firma digital generada en la etapa a) se presenta en una forma binaria o en forma de una imagen o varias imágenes en niveles de grises, y la etapa b) de lectura es según el procedimiento de la reivindicación 18.

50. Procedimiento de securización según una de las reivindicaciones 35 a 49, caracterizado por que utiliza la firma digital generada en la etapa a) de un elemento material, parte de un papel, cartón o no tejido, obtenida después de la detección de su interacción con la luz visible por transvisión, utilizando un sensor CCD o CMOS, y la etapa b) de lectura es según el procedimiento de la reivindicación 19.

51. Procedimiento de securización según una de las reivindicaciones 35 a 50, caracterizado por que la característica o características estructurales utilizadas en la etapa a) se digitalizan, y a continuación se muestrean en el tiempo, y la etapa b) de lectura es según el procedimiento de la reivindicación 26.

52. Procedimiento de securización según una de las reivindicaciones 35 a 51, caracterizado por que las informaciones sensibles son dinámicas, tales como una secuencia sonora y/o de vídeo, y la etapa b) de lectura es según el procedimiento de la reivindicación 27.

53. Procedimiento de securización según la reivindicación 52, caracterizado por que la protección de la etapa a) se realiza por medio de una firma digital dinámica obtenida por repetición de una firma digital estática o por detección repetida, con la ayuda de uno o varios sensores, de una o varias características estructurales de un elemento material estático, de acuerdo con la reivindicación 28.

54. Procedimiento de securización según la reivindicación 53, caracterizado por que la protección de la etapa a) se realiza por medio de una firma digital dinámica obtenida por detección en continuo, con la ayuda de uno o varios sensores, de una o varias características estructurales de un elemento material en movimiento relativo con respecto al (a los) sensor(es), de acuerdo con la reivindicación 29.

55. Procedimiento de securización según la reivindicación 54, caracterizado por que el elemento material es una bobina de papel, cartón o no tejido, en desplazamiento, o papel en curso de fabricación en una máquina de papel, de acuerdo con la reivindicación 30.

56. Procedimiento de securización según una de las reivindicaciones 35 a 55, caracterizado por que la protección de la etapa a) utiliza varias firmas digitales de un mismo elemento material o de diferentes elementos materiales, que permite posteriormente conceder unos accesos de lecturas parciales y/o diferentes a las informaciones sensibles, de acuerdo con la reivindicación 31.

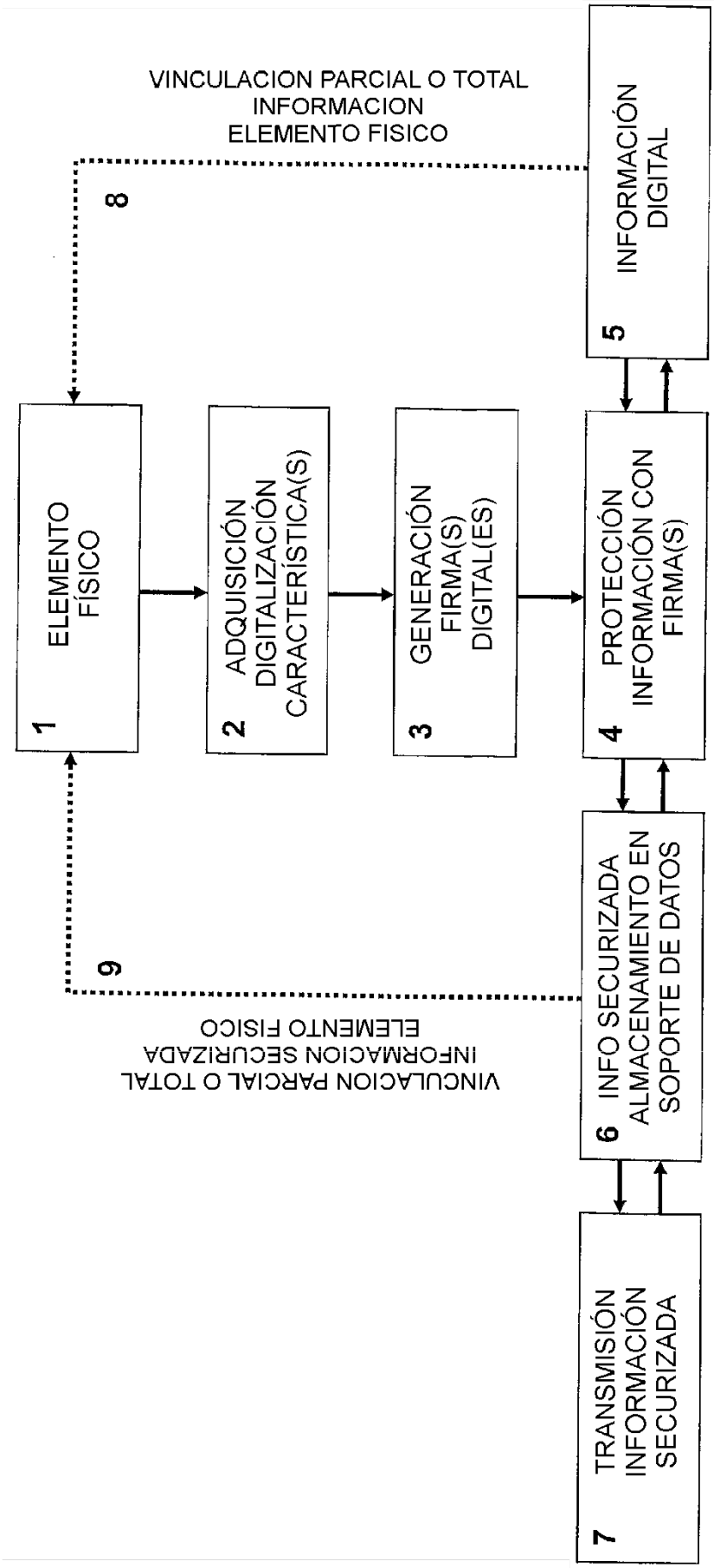
VINCULACION PARCIAL O TOTAL
INFORMACION
ELEMENTO FISICO
8
5 INFORMACIÓN DIGITAL
1 ELEMENTO FÍSICO
2 ADQUISICIÓN DIGITALIZACIÓN CARACTERÍSTICA(S)
3 GENERACIÓN FIRMA(S) DIGITAL(ES)
4 PROTECCIÓN INFORMACIÓN CON FIRMA(S)
9
6 INFO SECURIZADA ALMACENAMIENTO EN SOPORTE DE DATOS
7 TRANSMISIÓN INFORMACIÓN SECURIZADA
VINCULACION PARCIAL O TOTAL
INFORMACION SECURIZADA
ELEMENTO FISICO

FIG. 1

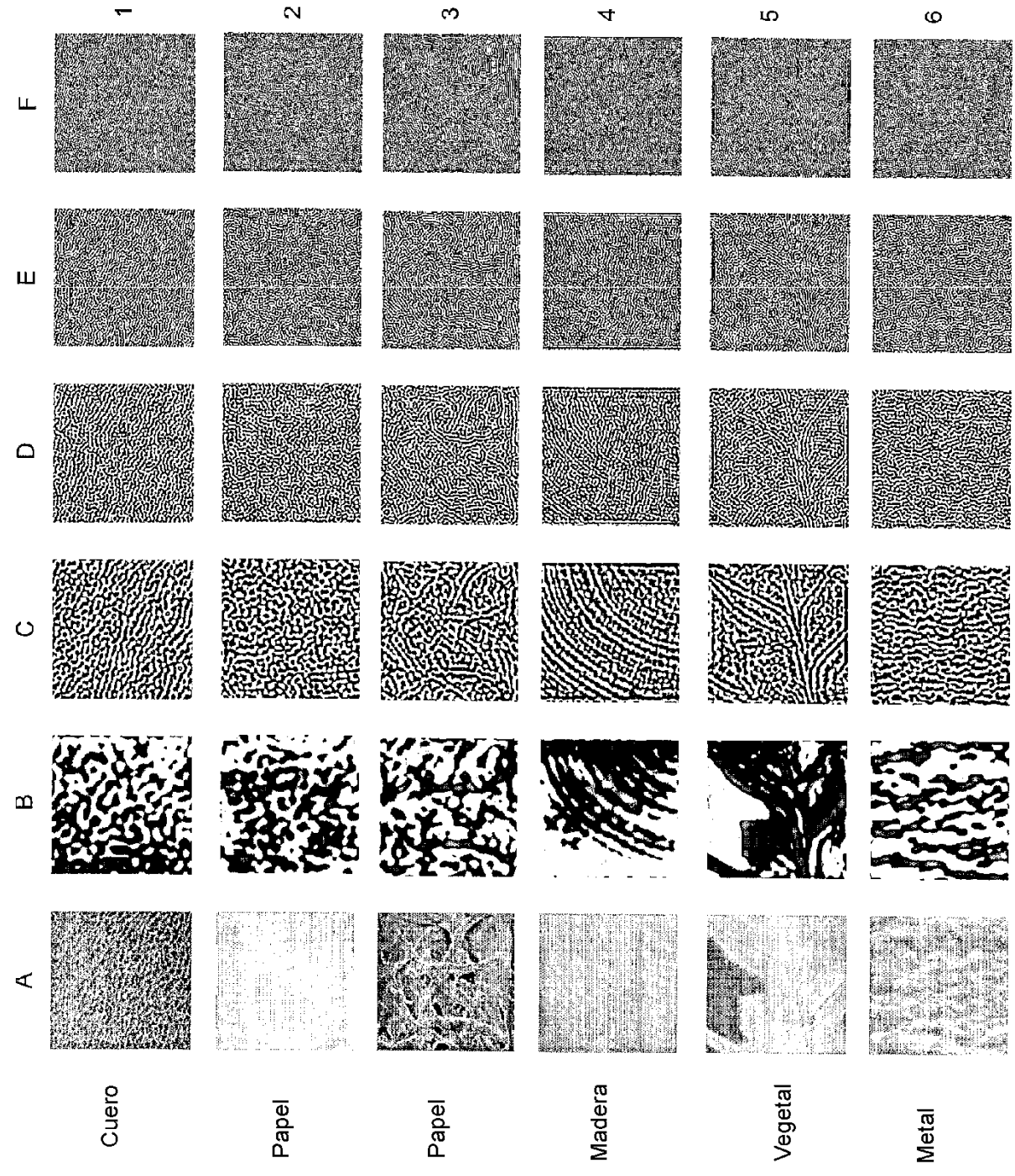

FIG. 2

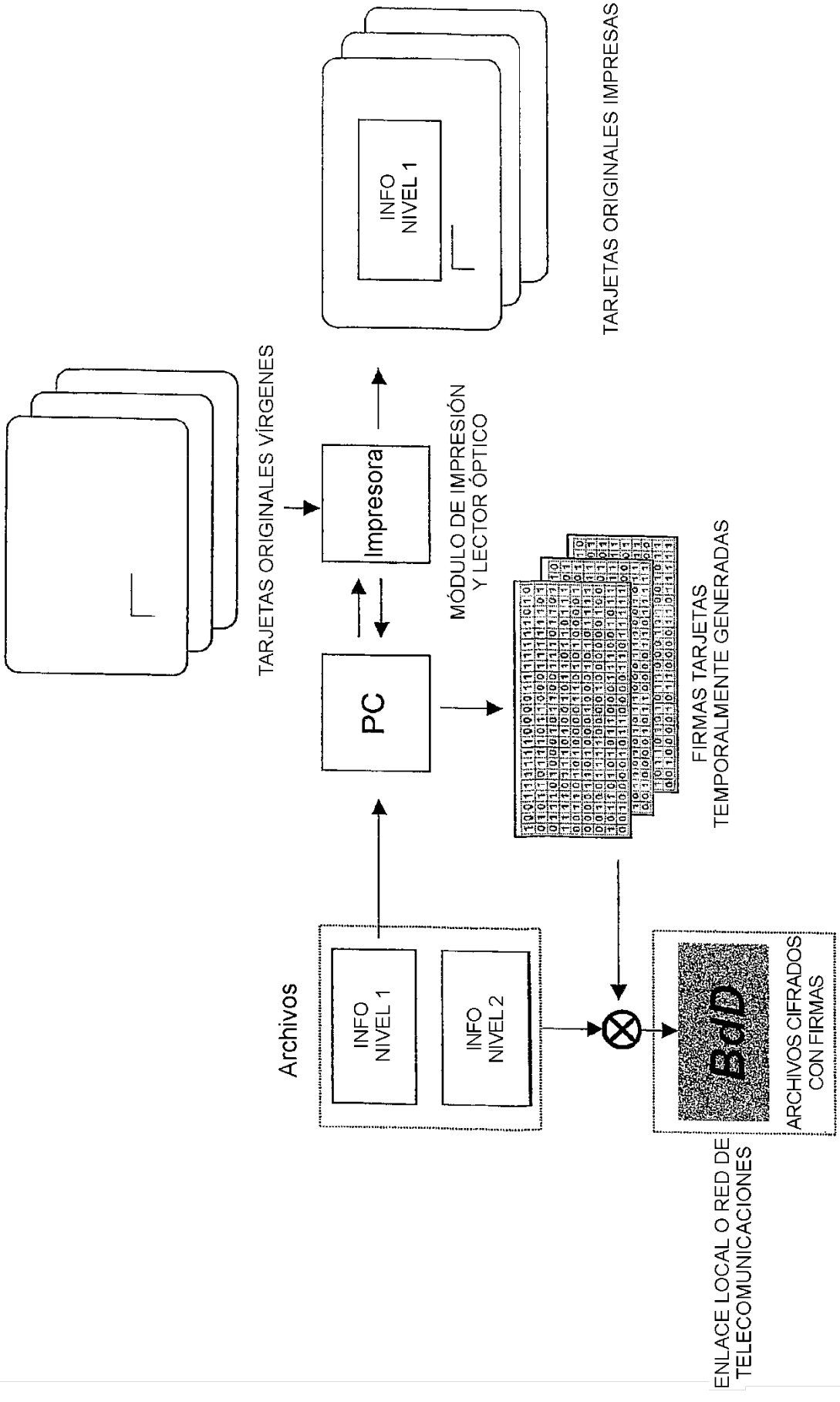
INFO NIVEL 1
TARJETAS ORIGINALES IMPRESAS
TARJETAS ORIGINALES VÍRGENES
Impresora
MÓDULO DE IMPRESIÓN Y LECTOR ÓPTICO
PC
FIRMAS TARJETAS TEMPORALMENTE GENERADAS
Archivos
INFO NIVEL 1
INFO NIVEL 2
BdD
ARCHIVOS CIFRADOS CON FIRMAS
ENLACE LOCAL O RED DE TELECOMUNICACIONES

FIG. 3

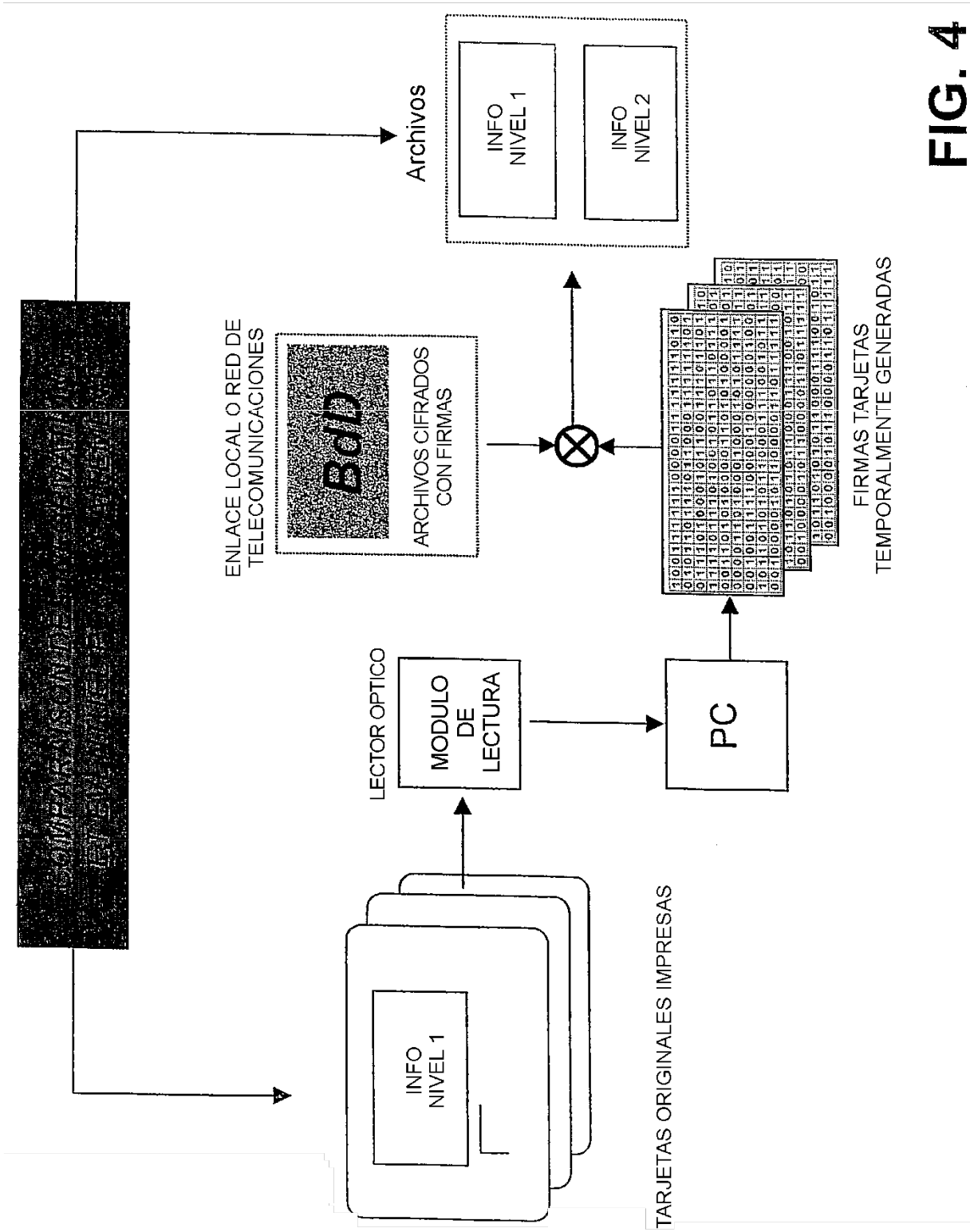
Archivos
INFO NIVEL 1
INFO NIVEL 2
ENLACE LOCAL O RED DE TELECOMUNICACIONES
BdD
ARCHIVOS CIFRADOS CON FIRMAS
FIRMAS TARJETAS TEMPORALMENTE GENERADAS
LECTOR OPTICO
MODULO DE LECTURA
PC
INFO NIVEL 1
TARJETAS ORIGINALES IMPRESAS

FIG. 4