(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 319 347**

(51) Int. Cl.:
H04N 1/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **99114304 .1**
(96) Fecha de presentación : **21.07.1999**
(97) Número de publicación de la solicitud: **0993176**
(97) Fecha de publicación de la solicitud: **12.04.2000**

(54) Título: **Procedimiento para insertar y analizar huellas dactilares electrónicas resistentes a manipulaciones en documentos electrónicos.**

(30) Prioridad: **09.10.1998 DE 198 47 942**

(45) Fecha de publicación de la mención BOPI:
06.05.2009

(45) Fecha de la publicación del folleto de la patente:
06.05.2009

(73) Titular/es: **Deutsche Telekom AG.**
Friedrich-Ebert-Allee 140
53113 Bonn, DE
Daimler-Benz, InterServices (debis) AG.

(72) Inventor/es: **Schwenk, Jörg y**
Ueberberg, Johannes

(74) Agente: **Durán Moya, Luis Alfonso**

DESCRIPCIÓN

Procedimiento para insertar y analizar huellas dactilares electrónicas resistentes a manipulaciones en documentos electrónicos.

La presente invención se refiere a un procedimiento, descrito con detalle en la parte introductoria de la reivindicación 1, tal como da a conocer el documento DE 19816356.8-31.

Debido al rápido crecimiento de Internet y la posibilidad que con ello se ha generado de distribuir documentos electrónicos, existe una creciente demanda de protección contra la difusión ilegal de documentos, a fin de proteger de copias pirata al titular del copyright.

Por ello, grandes empresas, tales como IBM, NEC y Microsoft, pero también sociedades pequeñas, tales como Digimarc (ver 20 Funkschau 17/97; P. 21), así como institutos de investigación tales como la Fraunhofergesellschaft IGD y la GMD Darmstadt, trabajan para incorporar a documentos las llamadas "marcas al agua electrónicas". En los procedimientos diseñados sobre esta base, en los documentos a proteger se incorpora de modo invisible la información que identifica al titular de los derechos de reproducción. La clase de marca al agua electrónica depende del tipo de documento (por ejemplo, Postscript, JPEG, MPEG-1).

Las marcas al agua electrónicas permiten al titular del copyright demostrar su propiedad intelectual en un documento distribuido de modo ilegal. No obstante, las marcas al agua electrónicas no permiten averiguar y demostrar quién es el autor de la distribución ilegal.

Las "huellas dactilares electrónicas" llegan un poco más lejos. Cuando se aplica el principio de asegurar un documento mediante huellas electrónicas, se incorpora al documento de forma invisible, junto con la marca al agua electrónica del titular del copyright, el nombre del cliente que ha adquirido una copia electrónica de ese documento. En caso de que dicho cliente distribuya su copia perjudicando los intereses del titular del copyright, se podrá identificar unívocamente y responsabilizar a dicho cliente, gracias a su huella electrónica que contienen todas las copias ilegales. (Dan Boneh y James Shaw, *Collusion-Secure Fingerprinting for Digital Data.* Proc. CRYPTO "95". LNCS 963, Springer-Verlag, Berlín 1995, 452-465.)

En el libro *Einführung in die endliche Geometrie* (Introducción a la geometría finita), de Albrecht Beutelspacher, Bibliographisches Institut Mannheim; 1. Blockpläne. - 1982-, se define y, con ello, se delimita la geometría finita como "rama relativamente nueva de las matemáticas". Las estructuras geométricas finitas se caracterizan porque se pueden representar en un ordenador sin errores de redondeo (carácter finito), y porque los conjuntos de intersección de dos subestructuras de una estructura geométrica tal tienen un tamaño y forma conocidos. En las circunstancias conocidas de ataques a procedimientos de huellas electrónicas, al final siempre se forman tales conjuntos de intersección. Para evaluar los efectos de dichos ataques es importante poder determinar la dimensión y la estructura de estos conjuntos de intersección.

El principio de la protección de documentos mediante huellas electrónicas adolece hasta ahora de un grave inconveniente debido a que los documentos asignados a cada cliente se diferencian en sus mapas de bits justamente en el lugar en el que está dispuesta la huella electrónica de usuario individual de cada uno de los distintos clientes. En caso de que un cliente entre en posesión del documento de un segundo cliente, o bien si se constituye un grupo de atacantes, éstos podrán, mediante la comparación bit por bit de los dos documentos, detectar los sitios de las diferentes huellas electrónicas y eliminar (borrar) las mismas del documento. Mediante el procedimiento descrito en el documento DE 19816356.8-31, según la figura 1, utilizando estructuras geométricas finitas superpuestas se obstaculiza parcialmente la intención de tales manipulaciones encaminadas a conseguir una copia del documento de la que se han eliminado todas las huellas electrónicas referidas a usuarios, ya que, por ser idéntico, no se detecta un conjunto de intersección S de las huellas electrónicas A, B y C, de modo que se conserva para investigaciones posteriores. No obstante, dichas investigaciones son complejas cuando se trata de grupos de numerosos atacantes, y pueden conducir a resultados ambiguos.

La presente invención tiene por objeto eliminar este inconveniente, hacer posible un mayor número de copias de los documentos, y también permitir un mejor reconocimiento de un grupo numeroso de atacantes.

Los pasos de procedimiento propuestos para conseguir dicho objetivo se describen en la parte de características de la reivindicación 1.

En la parte de características de la reivindicación 2 se describe una posibilidad de perfeccionamiento ventajoso de la invención, para poder investigar aún mejor los intentos de borrado.

A continuación se describe con más detalle la invención, sobre la base de ejemplos de realización. En los dibujos correspondientes,

la figura 1 muestra el conjunto de intersección S, según la patente principal;

la figura 2 muestra un sistema para generar huellas electrónicas en el plano de proyección PG(2,2); y

la figura 3 representa visualmente la invención en un espacio tridimensional.

La invención se fundamenta en el empleo de hiperplanos en espacios de proyección finitos PG(d,q). El parámetro d indica el número máximo de atacantes que el sistema puede procesar. Se cumplen las dos condiciones siguientes:

1. Cada copia del documento está asignada de modo exacto a un cliente.

2. Si se unen k clientes, siendo k < d+1, y borran del documento todas las partes de huellas electrónicas que se pueden detectar mediante una comparación bit por bit, el documento manipulado permite identificar unívocamente a dichos clientes.

Como ejemplo, primero se describe la invención en el plano de proyección PG(2,2). La figura 2 muestra este plano y las distintas huellas electrónicas A, B y C.

En la figura 2 se han dibujado todos los puntos y rectas del plano de proyección PG(2,2). Mediante una función secreta (o función unidireccional), se asigna a cada punto del plano de proyección un sitio del documento. El cliente "a" recibe así un documento en el que están marcados los sitios (por ejemplo, mediante la inversión de bits en el sitio en cuestión), que pertenecen a la huella electrónica A. Para el cliente a quien pertenece la huella electrónica A, serían, por ejemplo, los sitios asignados a los puntos 1, 3, 4, 5 y 6.

Si dos clientes comparan sus huellas electrónicas, encontrarán todos los sitios marcados, salvo el sitio que está en la intersección de las dos huellas. En caso de que, por ejemplo, el cliente con la huella A y el cliente con la huella B comparasen sus huellas electrónicas, podrían encontrar los sitios que se corresponden con los puntos 2, 4, 5 y 7, pero no los sitios 1, 3 y 6.

Todavía es posible una identificación de los clientes cuando se alían un máximo de dos clientes, ya que solamente una pareja concreta de clientes puede dejar de detectar un conjunto dado de puntos de intersección. En el presente ejemplo, los puntos 1,3 y 6 sólo pueden no ser detectados por los clientes a y b, mientras que los clientes b y c no hubieran detectado los puntos 1, 2 y 7, etcétera.

El sistema antes descrito se puede generalizar para más dimensiones d y órdenes q mayores. Para un caso tridimensional, un cubo (véase la figura 3) constituye una buena imagen de la situación: cada huella electrónica consta de los puntos situados sobre caras opuestas del cubo; cada pareja de huellas se cruza exactamente en cuatro rectas, y cada grupo de tres huellas se cruza en exactamente ocho puntos. Esto significa que, sobre la base de las intersecciones de dos (o bien tres) huellas electrónicas, se puede determinar con exactitud cuáles han sido los dos (o bien tres) clientes que han intentado eliminar dichas huellas.

La invención se basa, en general, en la utilización de hiperplanos en un espacio de proyección PG(d,q). Se asignan a cada cliente, como mínimo, dos hiperplanos, pero puede ser un número mayor. Cada hiperplano sólo puede ser asignado una vez a un cliente. Para esta asignación hay diferentes alternativas:

1. Los dos hiperplanos se seleccionan aleatoriamente. Con esta variante puede ocurrir con muy pocas probabilidades que el círculo de sospechosos sea mayor que el círculo de los que actúan ilegalmente.

2. Los dos hiperplanos son "paralelos", o sea, se cortan en un hiperplano H seleccionado.

La variante 2 sirve para evitar el siguiente problema: en un documento se detectan los puntos de intersección de las huellas A y B. Entonces también es posible que dichos puntos se haya generado por la intersección de las huellas A y C, o bien B y C.

No obstante, para dimensiones grandes (a partir de d=3) se puede pasar por alto este problema, ya que es ínfima la probabilidad de que el conjunto de intersección de "d" huellas sea ambiguo y, si se produjese ese caso muy improbable, el algoritmo de descodificación reconocería la ambigüedad. Así pues, no existe el riesgo de que se sospeche de inocentes.

Para la descodificación, o sea, la reconstrucción de los hiperplanos a partir de los puntos de intersección hallados, (o rectas y planos de corte) se buscan conjuntos linealmente dependientes. En caso de que, por ejemplo, en PG(d,q) sólo aparezcan los puntos de intersección 2d de los "d" hiperplanos, se buscan conjuntos parciales de 2d-1 puntos situados en un hiperplano común. Cuando se ha encontrado dicho hiperplano, también queda ya identificada una huella electrónica.

REIVINDICACIONES

1. Procedimiento para la introducción de huellas electrónicas resistentes a manipulaciones y para el análisis de huellas electrónicas en documentos electrónicos, mediante el que se asigna a cada comprador una copia de un documento en el cual hay introducida como marca una huella individual asignada a dicha copia del comprador correspondiente, siendo dicha huella no reconocible por el comprador, de forma que en dicho procedimiento la asignación de los puntos de marcado de la huella electrónica individual, diferente para cada copia, se realiza empleando estructuras geométricas finitas, de manera que la copia de cada comprador se marca en los lugares que se determinan mediante la subestructura geométrica asignada al cliente correspondiente y una función secreta, de forma que los puntos así determinados como huella electrónica para cada comprador dentro de la estructura geométrica se establecen de forma tal que estos puntos se entrecruzan con los puntos de las huellas electrónicas de otros compradores, de forma que se pueden determinar, a partir de los valores de intersección todavía existentes de las huellas electrónicas, cuáles han sido las copias objeto de manipulación y, con ello, quiénes han sido los compradores que han actuado como atacantes, mediante una comparación bit por bit del documento original con una copia de la que se han eliminado partes de huellas electrónicas por manipulación de, como máximo, "d" compradores, estando dicho procedimiento **caracterizado** porque

- se asigna unívocamente a cada lugar de marcado en el documento, mediante la función secreta, un punto del espacio PG de proyección finito con dimensión d y orden q de hiperplanos; porque

- se asignan a cada huella electrónica, como mínimo, dos hiperplanos del espacio PG de proyección finito, con dimensión d y orden q, de los que cada uno está asignado de modo exclusivo a solamente una huella electrónica; y porque

- para cada huella electrónica se marcan exactamente los lugares de marcado que se corresponden con los puntos de los hiperplanos seleccionados.

2. Procedimiento, según la reivindicación 1, **caracterizado** porque

- se reconstruyen objetos geométricos de las huellas electrónicas a partir de los lugares de marcado marcados encontrados en el documento;

- porque se determina en cuáles hiperplanos están contenidos los objetos mediante el análisis de las dependencias lineales entre las huellas electrónicas; y

- porque se determinan sucesivamente, mediante el cálculo de dichos hiperplanos, las huellas electrónicas de los clientes manipuladores.

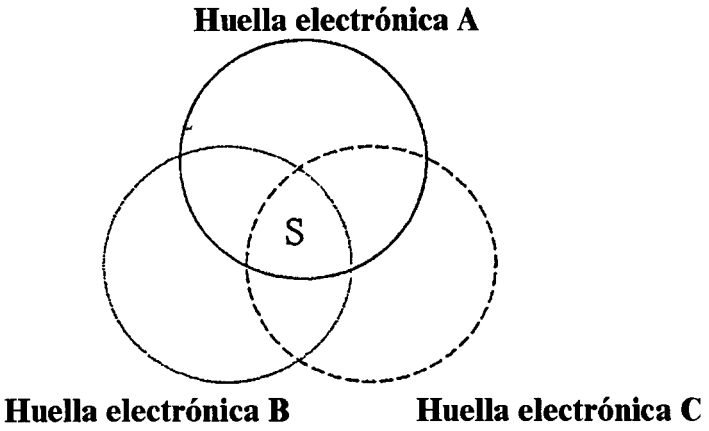
Huella electrónica A
S
Huella electrónica B
Huella electrónica C

Fig. 1

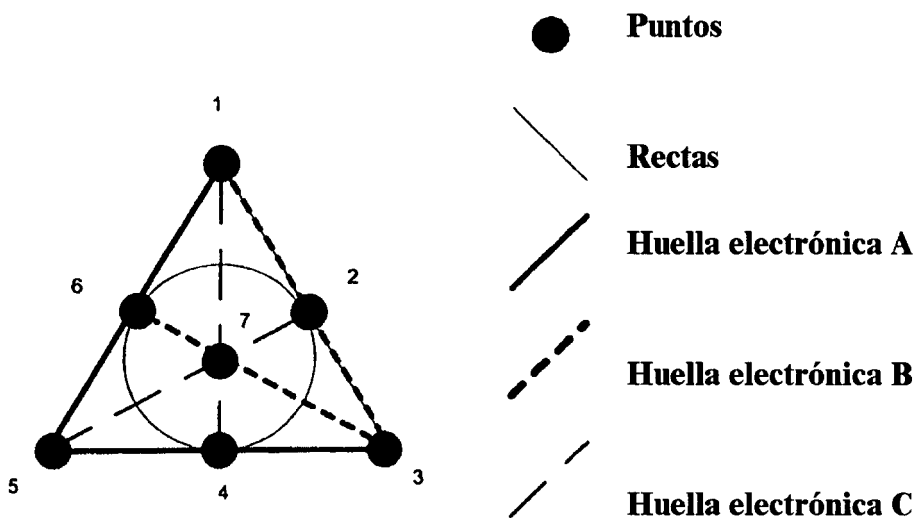
1
2
3
4
5
6
7
Puntos
Rectas
Huella electrónica A
Huella electrónica B
Huella electrónica C

Fig. 2

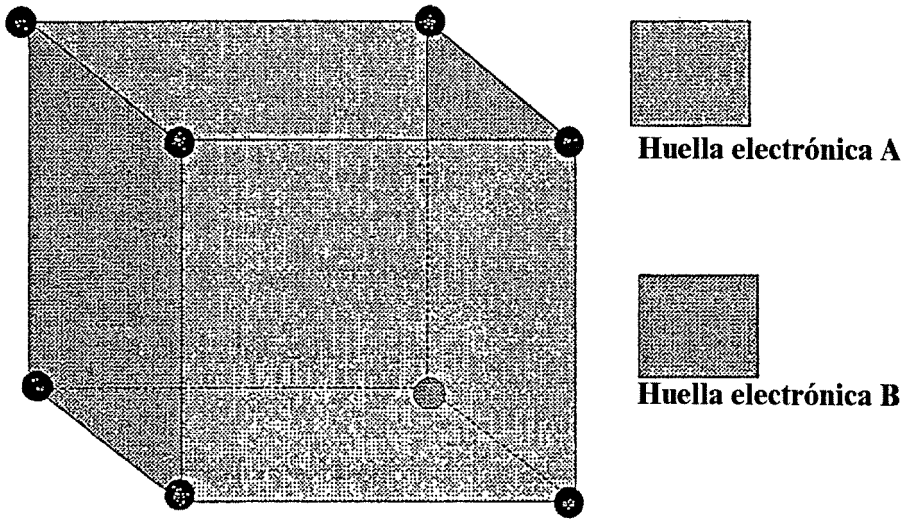

Fig. 3