

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 968 914**

51 Int. Cl.:

H04L 9/40 (2012.01)
H04W 4/12 (2009.01)
H04W 12/06 (2011.01)
H04W 12/08 (2011.01)
H04L 51/212 (2012.01)
H04L 51/222 (2012.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

- 86 Fecha de presentación y número de la solicitud internacional: **14.03.2018** **PCT/FR2018/050616**
87 Fecha y número de publicación internacional: **20.09.2018** **WO18167431**
96 Fecha de presentación y número de la solicitud europea: **14.03.2018** **E 18714315 (1)**
97 Fecha y número de publicación de la concesión europea: **22.11.2023** **EP 3596900**

54 Título: **Procedimiento de mensajería digital que asocia un mensaje a un sujeto material**

30 Prioridad:

14.03.2017 FR 1752087
03.11.2017 FR 1760343

45 Fecha de publicación y mención en BOPI de la traducción de la patente:
14.05.2024

73 Titular/es:

KERQUEST (100.0%)
96, rue des Etaies
73310 Chindrieux, FR

72 Inventor/es:

BOUTANT, YANN;
ROSSET, GAEL y
HAZEBROUCK, AURÉLIEN

74 Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

ES 2 968 914 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Procedimiento de mensajería digital que asocia un mensaje a un sujeto material

- 5 La presente invención pertenece al campo técnico de la mensajería digital, cualquiera que sea el contenido transmitido (cifrado o no) o el esquema de remitente(s)/destinatario(s) elegido (anónimo(s), 1:1 o 1:N o incluso N:1), y para mensajes con disponibilidad limitada o no limitada en el tiempo (efímeros o perennes). Por mensajería digital, se entiende un sistema técnico (ordenador, aplicación, red, ...) que permite el enrutamiento de un mensaje y su contenido digital desde un remitente a un destinatario.
- 10 Los sistemas de mensajería digital actuales permiten a un remitente enviar contenido digital a uno o más destinatarios. Este contenido pasa en formato digital del remitente al(a los) destinatario(s) y permanece en formato digital. En ocasiones, el contenido puede tener una vida útil limitada, es decir, estar asociado a un sistema de borrado integrado o externo. El contenido también puede cifrarse, lo que generalmente requiere el intercambio previo de claves de cifrado entre el remitente y el destinatario. Incluso el contenido cifrado se envía sin condiciones particulares del remitente al destinatario, quien puede acceder al contenido una vez que ha pasado de un servidor a otro y ha llegado a su destino de copia de seguridad o visualización. Todos los sistemas actuales se basan en un identificador único para definir un remitente o un destinatario. De este modo, el destinatario o al menos el propietario del identificador de destino siempre recupera el contenido procedente de un remitente. Se han llevado a cabo iniciativas en el campo para perfeccionar las condiciones de entrega de un mensaje, por ejemplo, siempre que se encuentre en una determinada ubicación geográfica (generalmente definida por triangulación por GPS, wi-fi, radio o acústica u otra) o cerca de otro usuario perteneciente a un grupo de usuarios; estas aplicaciones se denominan mensajería en función de la posición, en inglés "location-based messaging".
- 20 De este modo, los sistemas propuestos no permiten el intercambio de contenido digital entre un remitente y un destinatario estrictamente condicionado a la implementación de uno o más sujetos materiales. Los procedimientos existentes no permiten adjuntar contenido digital a un sujeto material.
- 30 L'état de la technique est par exemple connu de par les documents EP 2 573 986 A1 et US 2016/248784 A1. El documento EP 2 573 986 A1 divulga sistemas y métodos que aumentan la seguridad de la transmisión de mensajes electrónicos. El documento US 2016/248784 A1 trata de la autenticación de un usuario basándose en una imagen de un objeto en posesión del usuario.
- 35 La invención pretende, por tanto, subsanar esta carencia proponiendo condicionar la entrega de un mensaje a la condición de que el destinatario haya estado en un momento u otro en relación con un sujeto material o una imagen del mismo. Esta forma de hacer las cosas permite mejorar simplemente la confidencialidad de los mensajes sin recurrir necesariamente a la criptografía. Adicionalmente, se sabe en psicología que el ser humano siempre ha utilizado su particular relación con los objetos materiales para recordar momentos particulares, para comunicar o ritualizar ciertos eventos o compartir emociones. El término "souvenir", que caracteriza el objeto que traemos de nuestros viajes o que ofrecemos a nuestros seres queridos, o que está vinculado a un monumento, da testimonio de esta complicidad entre la memoria personal o colectiva y los sujetos materiales que nos rodean. Se trata, por tanto, de un procedimiento de mensajería seguro y que además, dependiendo de los sujetos materiales elegidos, aporta una dimensión adicional de evocación.
- 40 De este modo, la presente invención tiene como objetivo en primer lugar transmitir contenido desde uno o más remitentes a uno o más destinatarios condicionando su entrega a al menos una doble autenticación, a saber, por una parte, la autenticación del destinatario y por otra parte, la autenticación de un sujeto material que sirve como clave para la entrega del mensaje y que ha sido utilizado para su preparación. Se trata, pues, de un procedimiento de mensajería digital asociado a este sujeto material.
- 50 Es una forma figurada de poner "Post-it[™]" digitales en cualquier tipo de objeto material (físico) y crear una experiencia muy interesante para el(los) destinatario(s) e incluso para el(los) remitente(s). Esta virtualización del contenido adjunto también tiene la ventaja de evitar la contaminación visual real o virtual, porque se puede configurar y está entre dos mundos.
- 55 La invención está definida por la reivindicación 1. En las reivindicaciones dependientes están definidos unos modos de realización preferidos.
- 60 Por lo tanto, la invención tiene la ventaja de garantizar que el o los destinatarios han estado en posesión o en presencia del sujeto material antes de la entrega del mensaje y, por tanto, de asegurar de forma simple el intercambio.
- En el sentido de la invención, la noción de transmisión de mensajes designa de manera equivalente transmisión en modo "push" o recuperación en modo "pull". Asimismo, en el sentido de la invención, la expresión "determinación de un autenticador unitario" es sinónima de la expresión "extracción de un autenticador unitario".
- 65 Cabe señalar que cada autenticador puede estar compuesto, en particular, por la imagen correspondiente, sin que

este sea necesariamente el caso.

Por mensaje se entiende un conjunto digital que comprende al menos un contenido, así como información de un remitente y un destinatario o incluso metadatos de otra naturaleza (marca de tiempo, geolocalización, ...).

5 En el sentido de la invención, el término "sistema servidor" debe entenderse como un sistema informático que comprende uno o más servidores no necesariamente situados en el mismo lugar y que está adaptado para implementar la invención. De este modo, dentro del marco de este sistema de servidor, la máquina que garantiza la transmisión de mensajes no es necesariamente la que garantiza las operaciones de autenticación, ni la que opera el
10 guardado de los datos, entendiéndose que el sistema servidor también puede incluir una única máquina que realice todas las operaciones asignadas en el marco de la invención. En el caso de un sistema servidor con arquitectura distribuida, los servidores implementados se denominan comúnmente "nodos".

15 En el sentido de la invención, por "referencia de calibración" se entiende una imagen de referencia que puede ser de cualquier naturaleza, tal como por ejemplo: una imagen de un sujeto de referencia de la misma familia, tipo o categoría como que los sujetos materiales implementados, una imagen de puntos notables cerca de la región de autenticación, una imagen de un patrón o signo presentes en o cerca de cada región de autenticación, sin que esta lista sea limitativa.

20 Según una característica de la invención, el procedimiento de transmisión de un mensaje comprende una etapa de grabación de al menos un identificador de un destinatario asociado a al menos un autenticador unitario de un sujeto material.

25 Según una característica de la invención, se lleva a cabo la determinación, en cada imagen de región de autenticación de un sujeto material, de puntos singulares y de descriptores de una región singular asociada con cada punto singular, estando asociados los descriptores con cada punto singular correspondiente, y determinación a partir de dicha imagen de un autenticador unitario de dicho sujeto material.

30 Por otro lado, según la invención, las diferentes etapas no se realizan necesariamente en el orden secuencial de su enumeración.

De este modo por ejemplo y según una variante de implementación, en una fase de grabación del mensaje se llevan a cabo al menos las siguientes etapas:

- 35 - grabación del contenido del mensaje electrónico a transmitir en el sistema servidor, estando asociado el contenido con el mensaje a transmitir,
- grabación en el sistema servidor de al menos un identificador de al menos un destinatario del mensaje, estando cada identificador asociado con el mensaje a transmitir,
- grabación en el sistema servidor de al menos un identificador de al menos un remitente del mensaje, estando cada identificador asociado con el mensaje a transmitir,
- 40 - implementación de al menos un sujeto material que tiene al menos una región de autenticación que presenta una microestructura con un aumento de observación dado,
- adquisición por un dispositivo accesible por el remitente de al menos una primera imagen de una región de autenticación,
- determinación a partir de la primera imagen de al menos un primer autenticador unitario de un sujeto material,
- 45 - grabación de un autenticador unitario del sujeto material en el sistema servidor en asociación con el mensaje a transmitir.

En una fase de recuperación del mensaje por parte de cada destinatario, se llevan a cabo al menos las siguientes etapas:

- 50 - adquisición por un dispositivo accesible por el destinatario de al menos una segunda imagen de una región de autenticación de un sujeto material,
- determinación en la segunda imagen de puntos singulares y descriptores de una región singular asociada a cada punto singular, estando asociados los descriptores con cada punto singular correspondiente,
- 55 - extracción a partir de la segunda imagen de un segundo autenticador unitario candidato del sujeto material,
- implementación de una alineación por medio de los puntos singulares y sus descriptores asociados y a continuación comparación de las primera y segunda imágenes y/o sus respectivos autenticadores unitarios,
- implementación de una fase de autenticación del identificador del destinatario por una parte y del autenticador unitario candidato del sujeto material con los asociados al mensaje a entregar y almacenar en el sistema servidor,
- 60 - en caso de similitud suficiente entre las primera y segunda imágenes o sus respectivos autenticadores unitarios y de concordancia entre el identificador del destinatario grabado en el sistema servidor y el identificador del destinatario candidato, transmisión al destinatario del mensaje asociado a su identificador y al sujeto material generador.

65 La etapa de determinación de puntos singulares y descriptores en la primera imagen puede tener lugar entonces ya sea en la fase de grabación o en la fase de recuperación o incluso fuera de estas fases.

En el sentido de la invención, la microtextura de la región de autenticación es intrínseca y aleatoria en el sentido de que resulta de la naturaleza misma de la región de autenticación del sujeto material. En una forma de implementación preferida de la invención, cada sujeto material utilizado pertenece a las familias de sujetos que comprenden al menos una región de autenticación que comprende una estructura intrínseca esencialmente aleatoria no fácilmente reproducible, es decir cuya reproducción es difícil o incluso imposible porque resulta en particular de un proceso no predecible en la escala de observación. Una región de autenticación de este tipo con una estructura de medio continuo intrínseca esencialmente aleatoria no fácilmente reproducible corresponde a las funciones físicas no clonales en inglés "Physical Unclonable Functions" (PUF) tal como se definen en particular en la publicación en inglés Encyclopedia of Cryptography and Security edición 01/2011 páginas 929 a 934 en el artículo de Jorge Guajardo. De manera preferente, la región de autenticación de un sujeto material de acuerdo con la invención corresponde a una función física no clonal intrínseca designada en inglés por "Intrinsic PUFs" en el artículo mencionado anteriormente. Los inventores aprovechan el hecho de que la naturaleza aleatoria de la microestructura de la región de autenticación es inherente o intrínseca a la naturaleza misma del sujeto porque, como resultado de su modo de elaboración, de desarrollo o de crecimiento de modo que no sea necesario añadir a la región de autenticación una estructura particular, en particular una impresión, o incluso un grabado.

Sin embargo, si la microestructura propiamente dicha de un sujeto material puede usarse para determinar un autenticador unitario, también se puede utilizar, pero también, por ejemplo, las marcas dejadas por la interacción de un grabado, de una impresión, de una embutición, un estampado con el sujeto material en su aspecto aleatorio (por ejemplo: papel con impresión por chorro de tinta, la forma de las gotas depositadas sobre el papel puede ser suficiente).

Según una característica de la invención, en la fase de grabación del mensaje, al menos un identificador de cada destinatario se graba en el sistema servidor en el mensaje a transmitir y en la fase de recuperación, se utiliza un identificador del destinatario junto con el autenticador del sujeto material candidato y el mensaje sólo se transmite al destinatario en caso de autenticación positiva de este último por parte del sistema servidor o de cualquier otro dispositivo. En el sentido de la invención, un identificador es un dato o un conjunto de datos que permite identificar a un destinatario o a un remitente ofreciendo al mismo tiempo un grado relativamente alto de certeza de que la identidad de este último no ha sido usurpada. De este modo, un identificador puede ser, por ejemplo, un dato biométrico o la combinación de un nombre de usuario y una contraseña conocidos sólo por la persona titular del identificador.

El autenticador unitario puede ser la o las propias imágenes adquiridas, una imagen extraída o derivada de ellas, o cualquier conjunto de datos digitales deducidos de la o las imágenes adquiridas y que caractericen a esta última o estas últimas. Por ejemplo, descriptores invariantes locales de características locales calculados a partir de la o de las imágenes adquiridas que contienen la información espacial estructural o microestructural de la región de autenticación.

Según otra característica de la invención, antes de la fase de recuperación del mensaje, a cada destinatario se le transmite información relativa al sujeto material, cuya imagen de la zona de autenticación debe utilizarse para la recuperación del mensaje. En el sentido de la invención, la información relativa al sujeto material puede ser información de ubicación, posición, o incluso información tal como instrucciones que permitan al destinatario saber qué debe hacer para encontrarse en presencia del sujeto material.

Según una variante de esta característica, la información relativa al sujeto material comprende al menos una información de geolocalización del sujeto material.

Según otra característica de la invención, antes de la fase de recuperación del mensaje, el sujeto material es entregado a cada destinatario.

Según otra característica de la invención, se notifica al destinatario mediante un dispositivo la disponibilidad de un mensaje para su atención, o por cualquier otro medio. Un dispositivo de este tipo puede entonces recibir, en modo denominado "push", un mensaje informándole de la disponibilidad de un mensaje a recuperar o verificar periódicamente, en el modo denominado "pull" la posible disponibilidad de un mensaje a recuperar. La notificación también puede ser una visualización contextual como parte de una visualización en realidad aumentada.

Según otra característica más de la invención, en la fase de recuperación del mensaje, el mensaje es visualizado por cada destinatario en asociación con una imagen del sujeto material y/o su entorno. Entonces es posible utilizar técnicas de realidad aumentada de todo tipo para este fin.

Según una característica de la invención, en la fase de grabación, la determinación de un autenticador unitario de un sujeto material se efectúa por medio de un algoritmo dado y porque durante la fase de recuperación se implementa un dispositivo de comunicación móvil que comprende medios de adquisición de imágenes y medios de cálculo y que está adaptado para implementar el mismo algoritmo para determinar el segundo autenticador unitario, el autenticador unitario candidato de un sujeto material.

Según una característica de la invención, en la fase de grabación, el autenticador unitario de un sujeto material es una

imagen de autenticación y durante la fase de recuperación se implementa un dispositivo de comunicación móvil que comprende medios de adquisición de imágenes y medios de cálculo y que está adaptado para implementar un algoritmo dado para la alineación o incluso la comparación de la imagen de autenticación y la imagen de verificación.

5 Según una característica de la invención, en la fase de grabación, el autenticador unitario de un sujeto material es una imagen de autenticación y durante la fase de recuperación se implementa un dispositivo de comunicación móvil que comprende medios de adquisición de imágenes y medios de cálculo y que está adaptado para transmitir a un sistema servidor la imagen de verificación, de manera segura o no, sin realizar localmente los cálculos de alineación o comparación.

10 Según una característica de la invención, las fases de alineación, de determinación de un autenticador unitario y de comparación se efectúan en parte en un dispositivo de comunicación móvil que comprende medios de adquisición de imágenes y medios de cálculo y en parte en al menos un sistema servidor.

15 Por supuesto, las diversas características y variantes de la invención pueden asociarse entre sí según diversas combinaciones en la medida en la que no sean exclusivas entre sí.

Parece que la invención propone en particular un sistema de mensajería que permite a un remitente (designado por un identificador) enviar un contenido digital a uno o más destinatarios (designados por uno o más identificadores), estando asociado el contenido con al menos un sujeto material (cada uno designado por al menos un autenticador unitario). En la figura 1 se muestra un diagrama de bloques de un ejemplo de dicho sistema de mensajería.

20 De este modo, para enviar un mensaje, el remitente implementa la creación de al menos un autenticador unitario del sujeto material, discriminante y característico intrínseco de un sujeto material, que sirve como ancla para el contenido a transmitir. Para poder acceder al contenido del mensaje, el destinatario debe proporcionar al servidor su identificador como para cualquier sistema de mensajería actual, pero también un autenticador unitario del mismo sujeto material utilizado en el momento de la creación del mensaje por parte del remitente. Un autenticador unitario del sujeto material puede ser una o más imágenes de la región de autenticación del sujeto material o cualquier métrica extraída de dichas imágenes y que caracteriza parcialmente la microestructura del sujeto material. En el sentido de la invención, el contenido del mensaje puede ser de cualquier naturaleza, como por ejemplo datos y/o una aplicación o incluso un enlace de inicio de transferencia, un enlace de hipertexto sin que esta lista sea exhaustiva ni limitativa.

25 En el sentido de la invención, se entiende por imagen, en primer lugar una imagen óptica cuya cadena de adquisición comprende una parte óptica y que resulta de la solicitud de al menos una región de un sujeto material (llamada región de autenticación) por radiación luminosa, preferentemente pero no necesariamente visible para el sistema visual humano. La iluminación del sujeto material se puede adaptar al comportamiento óptico de la región de autenticación en reflexión y/o en transmisión. También se puede utilizar iluminación ambiental cuando sea adecuado. El término imagen también debe entenderse en sentido amplio y no limitado al significado exclusivo de una imagen óptica que resulta, en particular, de la solicitud de una región de autenticación mediante radiación luminosa. De este modo, las imágenes de autenticación y verificación pueden obtenerse mediante cualquier tipo de solicitud de la región de autenticación en asociación con una cadena de adquisición adecuada (transición de analógico a digital), entendiéndose que se implementa el mismo tipo o naturaleza de solicitud para la adquisición de imágenes de autenticación y de verificación. Entre los tipos de solicitudes o posibles modos de adquisición se pueden citar en particular: ultrasonidos, rayos X, tomografía por rayos X o láser, radiografía X, resonancia magnética, sin que esta lista sea limitativa o exhaustiva.

30 Según un ejemplo de implementación de la invención, un remitente selecciona, en una fase de grabación, un contenido digital, un destinatario y al menos un sujeto material. Por medio de un dispositivo electrónico conectado a una red informática, este remitente iniciará la implementación de las siguientes etapas:

50 - determinación del identificador del remitente, determinación del identificador del destinatario y determinación de un autenticador unitario del sujeto material como mínimo;
- constitución del mensaje asociado: el conjunto de los datos digitales citados anteriormente (identificador del remitente, identificador del destinatario, contenido digital y autenticador unitario del sujeto material) se reúnen para constituir un mensaje asociado, conjunto de datos digitales indexados multiunitariamente y listo para ser manipulado en cualquier infraestructura de telecomunicaciones existente y según todo tipo de protocolos conocidos o adaptados (protocolos de correo electrónico, protocolos de mensajería instantánea, protocolos de mensajería (WAP, SMS, MMS,...), ...).

60 El mensaje asociado es soportado, a continuación, por la infraestructura de telecomunicaciones seleccionada y se guardará al menos en un contenedor digital (sistema de servidor local o remoto) para que pueda implementarse (entregarse) posteriormente.

65 A continuación, el sistema servidor o cualquier otro dispositivo notifica directa o indirectamente al destinatario de la disponibilidad del mensaje asociado y recibe una indicación del sujeto material (y/o la región de autenticación del sujeto material) que se ha asociado inicialmente con el mensaje para que pueda acercarse al sujeto material e

implementar la parte de recuperación del procedimiento, objeto de la presente invención.

A continuación se realiza una etapa de determinación de un identificador de destinatario y una fase de determinación de un autenticador unitario candidato del sujeto material (autenticador unitario de verificación). Para estar autorizado a acceder al contenido del mensaje asociado, deberá utilizarse el mismo sujeto material que el implementado durante la generación del mensaje, o incluso sustancialmente la misma región de autenticación del mismo sujeto material que la implementada inicialmente por el remitente. Esta fase de determinación de un autenticador unitario candidato comprende las siguientes etapas: adquisición de al menos una imagen de verificación (imagen adquirida a partir de una región de autenticación del sujeto material candidato) / realización de una alineación relativa o absoluta de las imágenes de autenticación y de verificación y determinación de un autenticador unitario del sujeto material candidato / en el caso de que la alineación no sea posible, concluir con el fallo prematuro de la autenticación de imágenes de sujetos materiales.

A continuación se realiza de manera local (en el dispositivo del destinatario o cerca de él) o remota (en al menos un sistema servidor), o parcialmente local y parcialmente remota, una fase de autenticación. Esta operación se lleva a cabo mediante uno o más dispositivos electrónicos equipados con al menos un procesador y una memoria, incluso medios de telecomunicaciones, que permiten realizar las secuencias de cálculos digitales y comparaciones entre el identificador guardado del destinatario y el identificador candidato del destinatario, por una parte, y, por otra parte, los autenticadores unitarios del sujeto material candidato y el sujeto material guardado durante la fase de grabación del mensaje. Esta etapa requerirá interacción con al menos un sistema de servidor.

En caso de invalidación de la fase de autenticación (NO), el procedimiento finaliza con una notificación del fallo de entrega al menos al destinatario y puede, si es necesario, proponer al destinatario que reanude la fase de recuperación desde el principio.

En caso de validación de la fase de autenticación (SÍ), la siguiente etapa es la entrega del mensaje asociado con la posibilidad de que el destinatario acceda al contenido digital según lo desee el remitente.

En el sentido de la invención y según la implementación más simple, los identificadores de remitente y destinatario se componen respectivamente de nombres de usuario y contraseñas preexistentes, el autenticador unitario del sujeto material se reduce, por su parte, a una imagen adquirida por medio de un dispositivo electrónico comunicante equipado con al menos un sensor (posiblemente de una fuente de solicitud propia) que contiene al menos características físicas intrínsecas del sujeto material

En el sentido de la invención, el remitente puede ser cualquier entidad (persona, autómatas, robot u objeto comunicante) designada como emisor del contenido de un mensaje. Puede ser anónimo sin que esto sea necesario.

En el sentido de la invención, el destinatario puede ser cualquier entidad (persona, autómatas, robot u objeto comunicante) designada como receptor del contenido de un mensaje. El destinatario puede ser único, múltiple y restringido, es decir, reservado para un grupo predefinido, o no restringido, es decir, accesibles a todos teniendo un acceso controlado por la necesidad de implementar el sujeto material o la posibilidad de volver a calcular el autenticador unitario del sujeto material auténtico. Un autenticador unitario del sujeto material puede ser una imagen de la zona de autenticación del sujeto material o cualquier métrica extraída de dicha imagen y que caracterice parcialmente la microestructura del sujeto material.

En el sentido de la invención, el sujeto material es preferentemente independiente del remitente y del destinatario. La invención se basa en parte en las propiedades de unicidad, de no reproducibilidad y de imprevisibilidad del sujeto material. Según la invención, el sujeto material no es un animal vivo y preferentemente está inerte o muerto en lugar de vivo, es decir, el sujeto material no es capaz de cambiar espontáneamente como parte de un proceso de crecimiento o regeneración de un organismo vivo. La invención utiliza o implementa la microestructura o estructura del sujeto material, traducido a microtextura o textura en cualquier imagen adquirida de dicho sujeto material. El sujeto material puede ser un objeto físico (material, producto,...) o una escena natural (paisaje,...) cuya naturaleza y complejidad sean compatibles con las características necesarias para la implementación de la invención.

En el sentido de la invención, se debe entender por región de autenticación, una parte de un sujeto material cuya imagen extraída contiene información espacial, sobre la estructura o microestructura del sujeto material (por ejemplo, faltas de homogeneidad presentes de forma natural). En el marco de la invención con un aumento de observación dado, el término textura o microtextura se refiere a lo que es visible u observable en una imagen, mientras que el término estructura o microestructura se refiere al sujeto material en sí. De este modo, con un aumento de observación dado, una textura o microtextura corresponde a una imagen de la estructura o microestructura de la región de autenticación de un sujeto material.

Una región de autenticación es, por tanto, un espacio físico sobre o en el sujeto material que ha permitido generar durante la fase de grabación un autenticador unitario a partir del sujeto material y que debe ser reutilizado al menos durante la fase de recuperación para permitir la recuperación de un mensaje. Una región de autenticación no necesitó estar marcada físicamente en el sentido de la invención. Se puede grabar la posición de la región de autenticación en

el sujeto material a autenticar. Una grabación de este tipo permite, aunque no sea absolutamente necesario, facilitar la fase de verificación. Un sujeto material utilizado en la implementación del procedimiento objeto de la presente invención sin la más mínima marca no puede ser conocido ni detectado por nadie que no sea el remitente o el destinatario del mensaje asociado. Por ejemplo, se pueden utilizar para guiar al destinatario durante la fase de recuperación, datos telemétricos, de ubicación (GPS u otros), giroscópicos (acelerómetro(s) integrado(s) en un terminal móvil, por ejemplo), para que esté en condiciones lo más parecidas posible a las utilizadas por el remitente inicialmente.

Por supuesto, también se puede implementar un sujeto material en el cual se habrá identificado o incluso marcado una zona de lectura utilizada. De este modo, según otra característica más de la invención, la posición de la región de autenticación en el sujeto a autenticar está identificada en el sujeto a autenticar. Esta identificación puede ser explícita porque hay una o más marcas que indican la región de autenticación o implícita porque la región de autenticación está situada en o cerca de una región característica del sujeto, por ejemplo cerca de un patrón decorativo.

Al menos una imagen de autenticación (primera imagen adquirida a partir de una región de autenticación de un sujeto material) se implementa durante la constitución del mensaje por el o los remitentes y al menos una imagen de verificación (segunda imagen adquirida de una región de autenticación de un sujeto material candidato) debe ser implementada por el o los destinatarios para permitir el acceso al contenido del mensaje en el único caso en el que el sujeto material candidato sea un sujeto material que haya sido utilizado durante la creación del mensaje asociado. La creación del mensaje también puede tener lugar durante la llamada fase de grabación o la llamada fase de autenticación. De manera preferente, la imagen de autenticación del sujeto material y/o el sujeto material está en posesión o presencia del remitente, quien también puede ser descrito como el autor o creador antes de que el destinatario esté en posesión o presencia del sujeto material. Dicho de otro modo, el sujeto material es conocido por el remitente antes de ser conocido por el destinatario. De este modo, según una forma de implementación de la invención, el remitente prepara el mensaje asociado al sujeto material que ha elegido sin tener conocimiento previo del destinatario, dicho de otro modo, sin identificación previa del destinatario.

La invención al efectuar un análisis de similitud entre una primera imagen, que se llama imagen de autenticación, y una segunda imagen, que se llama imagen de verificación o imagen candidata, presenta la ventaja de permitir la entrega del contenido del mensaje al destinatario, mientras que las condiciones para tomar una imagen del sujeto material para la imagen de verificación o segunda imagen nunca son idénticas a las cumplidas durante la producción por el remitente de la primera imagen o imagen de autenticación. De hecho, entre las adquisiciones de las primera y segunda imágenes, el sujeto material puede haber sido ligeramente degradado, las condiciones de iluminación u otra sollicitación no son las mismas, el sensor utilizado es, por regla general, diferente (por ejemplo, óptica y resolución) y las posiciones relativas del sensor, de la fuente de sollicitación y del sujeto material también son diferentes.

Para responder a las dificultades provocadas por las diferencias en las condiciones de adquisición de las primera y segunda imágenes, la invención propone en una implementación preferida realizar una alineación de las dos imágenes o una alineación de una de las imágenes con respecto a la otra. Por alineación, se entiende a la puesta en correspondencia de imágenes (mono o multifuentes), es decir la identificación de diferentes atributos sujetos a una determinada relación. Esta puesta en correspondencia se basa generalmente en la búsqueda de una posible transformación geométrica que permita el paso de una imagen a otra, directa o relativamente a al menos una imagen de referencia. Para hacer esto, los principales métodos conocidos son la búsqueda de primitivas geométricas comunes (emparejadas) entre las dos imágenes para el cálculo de la transformación o incluso la búsqueda de similitud (correlación u otra) entre características locales de intensidad entre las dos imágenes para el cálculo de la transformación. La transformación buscada en el sentido de la invención puede ser lineal (denominada transformación rígida, por ejemplo homografía) pero también no lineal (transformación deformable). De este modo, es posible aplicar el procedimiento objeto de la presente invención a sujetos materiales sólido pero también a sujetos materiales elásticos, total o parcialmente, incluso que presentan características híbridas.

En el sentido de la invención, la alineación de las imágenes de verificación (segunda imagen) y de autenticación (primera imagen) debe entenderse de imagen(es) a imagen(es), de parte(s) de imagen(es) a parte(s) de imagen(es), o incluso de un conjunto de puntos singulares y sus caracterizaciones locales hacia otro conjunto de puntos singulares y sus caracterizaciones locales, de pares (puntos singulares, descriptores locales) a pares (puntos singulares, descriptores locales), o cualquier información derivada que permita una puesta en correspondencia y, llegado el caso, un cálculo de transformación geométrica. En el ejemplo anterior, los pares mencionados se consideran autenticadores unitarios del sujeto material.

La alineación realizada es un requisito previo para la comparación propiamente dicha de las imágenes o de los autenticadores unitarios asociados a dichas imágenes. Para hacer esto, son posibles numerosas métricas sin distorsionar la presente invención. Se citará el cálculo de firmas extraídas de las primera y segunda imágenes según el mismo algoritmo y el cálculo consecutivo de una distancia entre estas métricas y el uso de un umbral de aceptación, o incluso la comparación directa de puntos singulares en correspondencia en la primera. imagen y la segunda imagen con un umbral de aceptación en cuanto al número de emparejamientos de puntos singulares, por ejemplo. Estos puntos singulares pueden ser ventajosamente invariantes o cuasi-invariantes a transformaciones lineales o afines (rotaciones, homotecias, traslaciones y factores de escala).

De la misma manera una distancia, la inversa de una distancia o divergencia apropiada se puede utilizar como indicador de similitud, y también se puede aplicar para el emparejamiento de puntos de interés característicos detectados y cuantificados por medio de descriptores locales entre mosaicos de imágenes, por ejemplo, de filtros de Law o patrones binarios locales (LBP) o gradientes de niveles de señal (por ejemplo del tipo SURF, SIFT, KAZE, ORB, BRISK,...). Para estos últimos tratamientos en particular puede ser relevante pasar por una etapa de filtrado previa para borrar las diferencias en la iluminación local y/o una ecualización de histograma y revelar, de este modo, el interés en la microestructura/microtextura de la imagen en el sentido de la invención.

En el marco de la invención, métodos computacionales que utilizan redes neuronales artificiales, que implícitamente alinean, calculan pesos de similitud, extraen características y/o clasifican, también pueden utilizarse. De este modo, en un modo de implementación de la invención una alineación densa, es decir que se basa en un gran número de puntos o zonas de correspondencia, permite el reconocimiento y, de este modo, también la autenticación del sujeto material.

Un autenticador unitario de un sujeto material puede ser información digital deducida de propiedades de unicidad, imprevisibilidad o incluso no reproducibilidad de dicho sujeto material y que garantiza que cualquier generación de un autenticador unitario candidato del mismo sujeto material se situará a una distancia inferior a un cierto umbral mientras que cualquier generación de un autenticador unitario de otro sujeto material se situará a una distancia superior a este mismo umbral, siendo este umbral seleccionado para reducir al máximo el riesgo de colisiones (aceptación de un falso por un verdadero y rechazo de un verdadero por un falso). A continuación se implementa, por ejemplo, una comparación estadística con indicador de similitud y umbral de aceptación.

Un autenticador unitario de un sujeto material puede ser un conjunto (multidimensional) cuyo límite se determina de tal manera que cualquier autenticador unitario candidato proveniente del mismo sujeto material (misma región de autenticación) sea un elemento de este conjunto en el sentido de criterio de pertenencia, y que cualquier autenticador unitario candidato proveniente de otro sujeto material no es un elemento de este conjunto, reduciendo al máximo el riesgo de colisiones (aceptación de un falso por un verdadero y rechazo de un verdadero por un falso). El universo de autenticadores unitarios constituido de este modo puede ser configurable a priori o modificable a posteriori.

En el marco de la invención, se tiene en cuenta que cualquier sujeto material es susceptible de estar sujeto a modificaciones voluntarias o involuntarias a lo largo del tiempo y que cualquier captura y adquisición de una imagen del sujeto material también induce variabilidad. De manera ventajosa, el procedimiento según la invención es resistente a las alteraciones parciales del sujeto a autenticar y robusto frente a las variaciones en las condiciones de adquisición de las imágenes de autenticación y de verificación. El procedimiento objeto de la presente invención es resistente a alteraciones materiales del sujeto o modificaciones de las condiciones de adquisición de baja amplitud, estando esta noción de baja amplitud condicionada por la elección del índice de similitud y el umbral de aceptación o incluso del criterio de pertenencia y el límite. Sin embargo, el procedimiento según la invención no se puede implementar en caso de modificaciones o alteraciones excesivamente significativas en la escala de la región de autenticación o condiciones de captura demasiado diferentes para las primera y segunda imágenes.

La propia elección del sujeto material es un elemento determinante de la solidez de todo el procedimiento. Puede ser interesante en determinadas aplicaciones utilizar sujetos materiales que se degradan/evolucionan más o menos rápidamente en el tiempo para limitar naturalmente el período de disponibilidad de los mensajes a la vida útil o de recuperación de un autenticador unitario del sujeto material correcto en el sentido de la invención. Incluso se puede pensar en caracterizar el índice de degradación del sujeto material para estimar su antigüedad como elemento de datación o determinación de la "antigüedad" del mensaje.

Cabe señalar que la invención proporciona una cierta fiabilidad y seguridad de los mensajes y de su distribución gracias a su asociación con sujetos materiales, incluso si no está destinado específicamente a ser un procedimiento seguro de transmisión de mensajes. Para reforzar la seguridad del procedimiento según la invención, es posible implementar cualquier mecanismo de seguridad de datos y materiales/dispositivos electrónicos, por ejemplo cifrado de datos, firmas electrónicas, token de seguridad. Asimismo, la seguridad puede garantizarse mediante un sistema de registro distribuido y seguro, de tipo "blockchain", de todas las transacciones de mensajería realizadas desde la primera implementación o puesta en marcha de un sistema de mensajería según la invención. El elemento seguro en el contexto de un mecanismo de este tipo podría ser entonces el mensaje intercambiado o el o los sujetos materiales implementados o su imagen o incluso la combinación del mensaje y del o de los sujetos materiales asociados.

Por otro lado, es posible que el contenido del mensaje implementado en el presente procedimiento por un remitente pueda continuar evolucionando en su fase de almacenamiento y esto hasta su entrega al destinatario. De este modo, el remitente puede decidir sobre la información precisa y definitiva que constituye el contenido del mensaje asociado, pero también puede elegir reglas de evolución e información de partida (contenido inicial) que evolucionará hasta al menos su entrega. Por ejemplo, el contenido de todo o parte de tipo flujo RSS actualizado durante el guardado (el guardado en el servidor de datos es dinámico en este caso); o incluso es perfectamente posible un contenido total o parcialmente dependiente del día de entrega (día que el remitente desconoce en el momento de anclar su mensaje).

En una variante del procedimiento según la invención, se ofrece al destinatario la posibilidad de volver a publicar un mensaje total o parcialmente diferente del mensaje asociado y enviarlo de vuelta al remitente inicial.

5 Asimismo, la notificación al(a los) destinatario(s) se puede realizar especificando un número de identificación único del mensaje (por ejemplo, construido a partir de un valor aleatorio acoplado a un valor incremental) que sirve como índice de retorno y que permite un control 1:1 más rápido, durante la(s) fase(s) de recuperación y de autenticación.

10 Según una variante de implementación, un remitente puede enviar a un destinatario una indicación sobre el sujeto material a través de cualquier canal, incluso, aunque sea menos relevante, a través del sistema servidor (cifrado o no al mismo tiempo que la notificación). Un modo de comunicación de la indicación respecto al sujeto material puede ser por ejemplo por SMS o MMS o por teléfono, cuando el mensaje asociado se transmite por correo electrónico, por ejemplo.

15 La invención se puede implementar con dispositivos electrónicos adecuados que comprendan al menos un sensor (cámara, sensor CCD, CMOS, ultrasonido,...), una memoria y un procesador, o incluso, llegado el caso, una fuente de sollicitación (luminosa u otra). Entre los dispositivos electrónicos adecuados para una implementación de la invención se pueden citar: ordenador, tableta, teléfono inteligente, máscara de realidad aumentada, gafas de realidad aumentada.

20 Cabe señalar que es posible elegir como sujeto material un producto manufacturado (industrial o artesanal), una obra de arte, un elemento o una escena natural. En el caso de una caja de perfume por ejemplo, y en el momento de la compra en tienda se puede implementar el procedimiento como remitente y enviar a un destinatario dicha caja de perfume. El destinatario cuando se le entrega está, por lo tanto, en posesión del sujeto material, el acercamiento, por lo tanto, se ha realizado, ha sido notificado por cualquier medio por el remitente que tiene un mensaje para su atención
25 (posiblemente con un número de identificación de mensaje único) y a continuación puede implementar el procedimiento y recibir el contenido digital deseado por el remitente.

También es posible elegir un entorno urbano como sujeto material, una piedra de un monumento famoso (la catedral de Notre-Dame de París, el Coliseo de Roma, ...) e implementar el procedimiento objeto de la invención.

30 Entre las posibles aplicaciones de la invención, es posible citar interacciones e intercambios entre un fabricante/distribuidor de productos y los consumidores, búsquedas del tesoro cuyas pistas y/o instrucciones se transmiten mediante el sistema de mensajería según la invención. Otra posible aplicación es la grabación de productos a efectos de garantía o el acceso a o la entrega de instrucciones de uso.

35 Por supuesto, se pueden considerar otras variantes del procedimiento u otras implementaciones de la invención en el contexto de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Procedimiento de transmisión de un mensaje electrónico por parte de un remitente a un destinatario que comprende las siguientes etapas:

- 5 - inicialmente, elección por parte del remitente de un sujeto material, independiente del remitente y del destinatario, que tiene una región de autenticación que presenta una microestructura con un aumento de observación dado, a continuación adquisición o implementación por parte del emisor de una primera imagen de la región de autenticación,
- 10 - grabación por parte del remitente del mensaje electrónico a transmitir en un sistema servidor,
- determinación a partir de la primera imagen de un primer autenticador unitario del sujeto material y grabación en el sistema servidor del primer autenticador unitario, estando asociado el primer autenticador unitario con el mensaje a transmitir,
- 15 - grabación en el sistema servidor un identificador del destinatario del mensaje, estando asociado el identificador con el mensaje a transmitir,
- notificación al destinatario de la existencia del mensaje,
- transmisión al destinatario de información relativa al sujeto material cuya imagen de la región de autenticación deberá ser utilizada por el destinatario para la recuperación del mensaje,
- 20 - adquisición por parte del destinatario de una segunda imagen de la región de autenticación del sujeto material, adquiriéndose la segunda imagen con una calidad sustancialmente equivalente a la de la primera imagen de modo que la primera y la segunda imagen contengan un nivel sustancialmente equivalente de información relativa a la región de autenticación,
- determinación a partir de la segunda imagen de un segundo autenticador unitario del sujeto material,
- 25 - transmisión al sistema servidor de un identificador del destinatario que ha realizado la adquisición de la segunda imagen con origen en el segundo autenticador unitario, estando asociado el identificador de dicho destinatario con el segundo autenticador unitario,
- comparación de los autenticadores unitarios,
- en caso de similitud entre los primer y segundo autenticadores unitarios y de coincidencia entre el identificador del destinatario grabado en el servidor y el identificador del destinatario transmitido, transmisión al destinatario del mensaje, estando asociado el mensaje con el identificador del destinatario grabado en el servidor y el primer autenticador unitario.
- 30

2. Procedimiento según la reivindicación 1, **caracterizado por que** un autenticador unitario del sujeto material es una imagen de su región de autenticación.

- 35 3. Procedimiento según una de las reivindicaciones anteriores, **caracterizado por que** comprende una etapa de grabación de al menos un identificador del destinatario asociado con al menos un autenticador unitario del sujeto material.

- 40 4. Procedimiento según una de las reivindicaciones 1 o 3, **caracterizado por que** comprende la determinación, en cada imagen de región de autenticación del sujeto material, de puntos singulares y de descriptores de una región singular asociada con cada punto singular, estando asociados los descriptores con cada punto singular correspondiente, y determinación a partir de dicha imagen de un autenticador unitario de dicho sujeto material.

- 45 5. Procedimiento según una de las reivindicaciones anteriores, **caracterizado por que** la información relativa al sujeto material comprende al menos una información seleccionada entre:

- una información de geolocalización del sujeto material
- una indicación de la región de autenticación del sujeto material.

- 50 6. Procedimiento según una de las reivindicaciones anteriores, **caracterizado por que** en la fase de recuperación, el mensaje es visualizado por el destinatario en asociación con una imagen del sujeto material y/o su entorno.

- 55 7. Procedimiento según una de las reivindicaciones anteriores, **caracterizado por que** la determinación de un autenticador unitario del sujeto material se efectúa por medio de un algoritmo dado y **por que** se implementa un dispositivo de comunicación móvil que comprende medios de adquisición de imágenes y medios de cálculo y que está adaptado para implementar el mismo algoritmo dado para la determinación del segundo autenticador unitario.

- 60 8. Procedimiento según una de las reivindicaciones anteriores, **caracterizado por que** se implementa un dispositivo de comunicación móvil que comprende medios de adquisición de imágenes y medios de cálculo y que está adaptado para transmitir al sistema servidor la segunda imagen, de manera segura o no, sin realizar localmente los cálculos de comparación.

- 65 9. Procedimiento según una de las reivindicaciones 1 a 7, **caracterizado por que** las fases de determinación de los autenticadores unitarios y comparación se efectúan en parte en un dispositivo de comunicación móvil que comprende medios de adquisición de imágenes y medios de cálculo y en parte en el sistema servidor.

- 5 10. Procedimiento según una de las reivindicaciones anteriores, **caracterizado por que** el sujeto material pertenece a las familias de sujetos que comprenden al menos una región de autenticación que comprende una estructura intrínseca esencialmente aleatoria no fácilmente reproducible, cuya reproducción es difícil o incluso imposible **por que** resulta en particular de un proceso no predecible en la escala de observación.
- 10 11. Procedimiento según una de las reivindicaciones anteriores, **caracterizado por que** para la determinación de autenticadores unitarios, se lleva a cabo una etapa de alineación sobre las primera y segunda imágenes, ya sea una con respecto a otra, o con respecto a una misma referencia de alineación.
- 10 12. Procedimiento según la reivindicación anterior, **caracterizado por que** la alineación implementada es un alineación densa que se basa en un gran número de puntos o zonas de correspondencia, y que permite el reconocimiento y la autenticación del sujeto material.
- 15 13. Procedimiento según una de las reivindicaciones anteriores, **caracterizado por que** se implementa un sistema de registro distribuido y seguro, de tipo "blockchain", en el que está grabado al menos uno de los siguientes elementos:
- 20 - el mensaje transmitido,
- el sujeto material implementado,
- una imagen del sujeto material implementado.
14. Procedimiento según una de las reivindicaciones anteriores, **caracterizado por que** el mensaje evoluciona hasta su entrega a su destinatario.
- 25 15. Procedimiento según una de las reivindicaciones anteriores, **caracterizado por que** se implementa una red neuronal artificial para las etapas de determinación y/o comparación de los autenticadores unitarios.

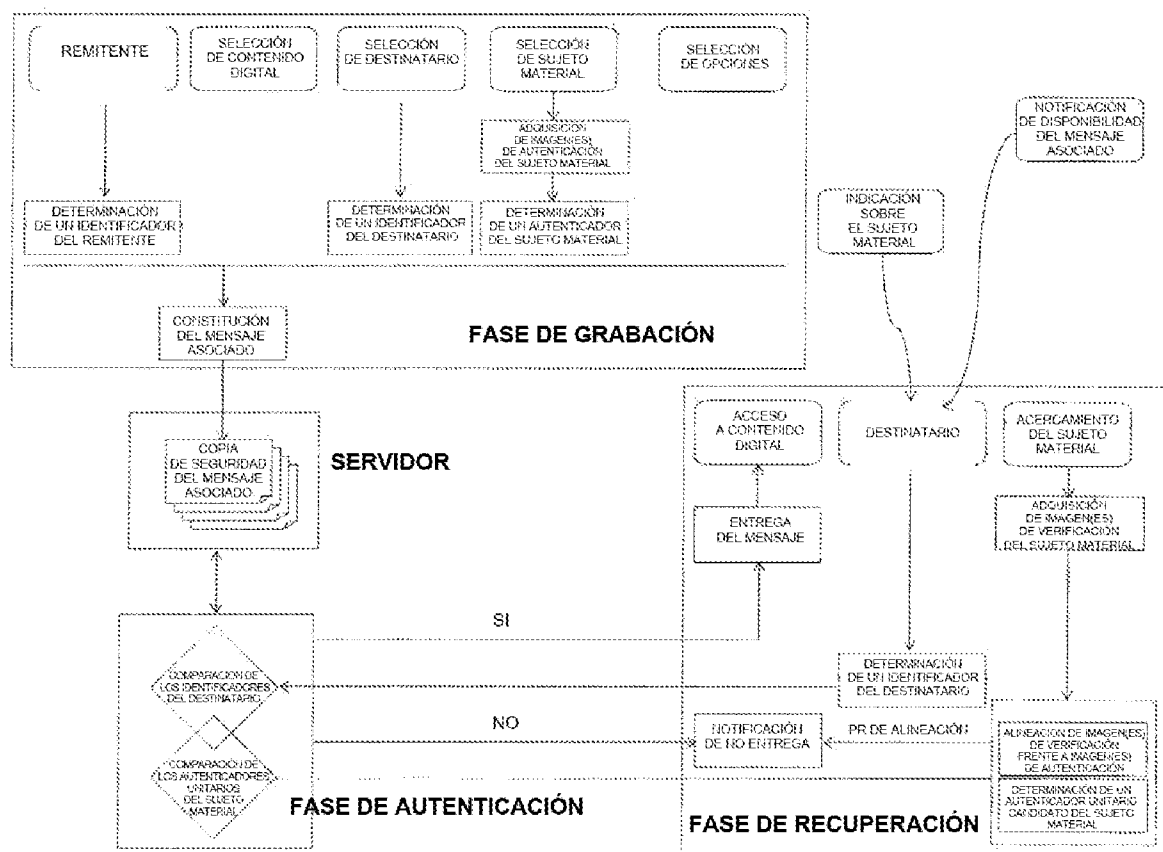


Fig. 1