(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 992 093**

(51) Int. Cl.:

G06Q 20/34 (2012.01)
G07F 7/08 (2006.01)
G07F 7/12 (2006.01)
G06F 21/62 (2013.01)
G06F 21/84 (2013.01)
H04L 9/00 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **07.08.2019 PCT/FR2019/051912**

(87) Fecha y número de publicación internacional: **18.06.2020 WO20120849**

(96) Fecha de presentación y número de la solicitud europea: **07.08.2019 E 19759671 (1)**

(97) Fecha y número de publicación de la concesión europea: **24.07.2024 EP 3895108**

(54) Título: **Dispositivo y procedimiento para asegurar los datos de seguridad de una tarjeta de pago bancario**

(30) Prioridad:

11.12.2018 FR 1872665

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
09.12.2024

(73) Titular/es:

CCS12 (100.0%)
6, allée Turcat Méry
13008 Marseille, FR

(72) Inventor/es:

ABISDID, CHARLI y
ABISDID, MARLÈNE

(74) Agente/Representante:

URÍZAR VILLATE, Ignacio

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

Dispositivo y procedimiento para asegurar los datos de seguridad de una tarjeta de pago bancario

Campo técnico.

La invención se refiere a un dispositivo y un procedimiento para la protección de los datos de seguridad de una tarjeta de pago bancario.

La presente invención se refiere al campo de la protección de los datos que generalmente están inscritos en una de las caras de una tarjeta de pago bancario con el fin de asegurar las operaciones de pago.

Técnica anterior.

Los datos de seguridad asociados a una cuenta bancaria se colocan en una tarjeta de pago, tales como el número de la tarjeta, el nombre del cliente y su fecha de vencimiento, que generalmente aparecen en relieve en el anverso (o cara frontal) de dicha tarjeta. El código de seguridad o criptograma visual se coloca en el reverso (o cara posterior) de la tarjeta. El usuario debe proporcionar habitualmente estos datos de seguridad al realizar una transacción en línea o por teléfono.

Este método de pago está hoy en día muy extendido. Sin embargo, a pesar de los esfuerzos de los bancos, los comerciantes en línea y otras empresas especializadas en la seguridad de tarjetas bancarias, el fraude por piratería en línea o telefónica, o simplemente por el robo físico de la tarjeta y del teléfono, se ha incrementado considerablemente. En menor medida, también ocurre la piratería visual de los datos de seguridad, por ejemplo, durante un pago directo a un comerciante. Esto puede suceder durante el pago de una compra en una tienda donde el vendedor copia los datos de seguridad sin que el titular de la tarjeta lo sepa. El pirata puede luego realizar transacciones a distancia para su propio beneficio utilizando estos datos de seguridad, en detrimento del propietario de la tarjeta, o vender estos datos a un tercero.

Se han desarrollado algunos dispositivos para intentar mejorar la seguridad de los datos de las tarjetas bancarias.

Los documentos de patentes FR3051581 o US 2014/0279555 proponen, por ejemplo, soluciones donde el criptograma ya no es un dato estático impreso en la tarjeta, sino un dato dinámico generado por la tarjeta en el momento de la confirmación de una transacción bancaria. Sin embargo, este tipo de tarjeta es particularmente complejo de fabricar y costoso. Además, en caso de robo de la tarjeta, el criptograma, aunque se genere de manera dinámica, será visible para el ladrón en el momento de la confirmación de una transacción bancaria fraudulenta. El criptograma cambiante protege los datos almacenados por los comerciantes en línea. En caso de piratería, esta solución es, por tanto, relevante únicamente para casos de phishing, consistentes en el robo de los datos almacenados en los comerciantes en línea por parte de un hacker.

El documento de patente FR3051060 divulga un procedimiento de protección del criptograma. Se imprimen varios criptogramas en la tarjeta, emitidos y reconocidos por el banco. Estos criptogramas deben ser utilizados en un orden predefinido. Una marca que se puede mover manualmente en relación con los criptogramas permite al propietario de la tarjeta, según un protocolo personal, memorizar la posición del criptograma que deberá utilizar para la siguiente transacción. Si bien esta solución puede ser interesante en ciertos aspectos, presenta inconvenientes. De hecho, en caso de robo de la tarjeta, el ladrón conocerá todos los criptogramas. Dado que su número es limitado, basta con "probar" sucesivamente varios criptogramas para validar una transacción bancaria fraudulenta.

El documento US 2010/243741 divulga un procedimiento de protección conforme al preámbulo de la reivindicación principal. Los datos ocultos se inscriben en un soporte distinto de la tarjeta. Al combinar este soporte con la tarjeta, el usuario puede recuperar todos los datos de seguridad. El documento US5326964 divulga un procedimiento similar. Este tipo de procedimiento es relativamente limitado en términos de seguridad.

Un objetivo de la invención es remediar los inconvenientes del estado de la técnica. Otro objetivo de la invención es proponer una solución que permita mejorar la protección de los datos de seguridad de una tarjeta de pago y hacerla inutilizable en caso de robo.

Resumen de la invención.

La solución propuesta por la invención es un procedimiento para asegurar los datos de seguridad de una tarjeta de pago bancario asociada a una cuenta bancaria, cuyos datos de seguridad son estáticos e incluyen el número

de dicha tarjeta, los datos de identificación del titular de dicha tarjeta, la fecha de expiración de dicha tarjeta y un criptograma, siendo el número de la tarjeta bancaria y el criptograma una serie de varios dígitos y/o letras.

Este procedimiento comprende los pasos de:

- Inscribir parcialmente los datos de seguridad de manera inteligible en dicha tarjeta de forma que ciertos datos de seguridad están ocultos, siendo los datos ocultos formados por varios dígitos y/o letras del número de dicha tarjeta y/o al menos un dato de identificación del titular y/o al menos un elemento de la fecha de expiración y/o al menos un dígito y/o letra del criptograma,

- Transmitir, únicamente al titular de la tarjeta, un medio de divulgación de los datos ocultos. El procedimiento además comprende los siguientes pasos:

- Ocultar los datos ocultos, visibles en la tarjeta, entre varios datos,

- Disponer los datos en una cuadrícula,

- Inscribir de manera visible la cuadrícula en una cara de la tarjeta, El medio de divulgación de los datos ocultos incluye un revelador de los datos ocultos, siendo este revelador una imagen virtual en realidad aumentada generada por una aplicación informática instalada en un terminal móvil del titular de la tarjeta, siendo dicha imagen del revelador mostrada en una pantalla del terminal móvil y superpuesta a una imagen real de la cuadrícula, también mostrada en dicha pantalla, siendo la imagen real de la tarjeta capturada por el dispositivo de adquisición óptica del terminal móvil, y los datos ocultos están pregrabados en la memoria del terminal móvil.

Los datos de seguridad ahora solo están parcialmente inscritos de manera inteligible en la tarjeta de pago bancario. Por lo tanto, si la tarjeta es robada, el ladrón nunca podrá usarla ya que no podrá conocer todos los datos de seguridad. Solo el titular de la tarjeta conoce estos datos. La invención pretende así crear una barrera de seguridad, especialmente antes de cualquier transacción en línea. De hecho, para realizar una compra en línea, es necesario proporcionar ciertos datos de seguridad que solo el titular de la tarjeta podrá proporcionar. En caso de robo de la tarjeta, la disposición de los datos en la cuadrícula hace que el número de combinaciones a "probar" para validar una transacción bancaria fraudulenta sea mucho mayor que en las soluciones conocidas en el estado de la técnica (aproximadamente 10,000 veces más numerosas). Por lo tanto, la invención asegura considerablemente las tarjetas de pago, haciéndolas inutilizables cuando son recuperadas de manera fraudulenta por personas malintencionadas.

Otras características ventajosas de la invención se enumeran a continuación. Cada una de estas características puede considerarse por sí sola o en combinación con las características destacadas definidas anteriormente, y pueden ser objeto, si procede, de una o más solicitudes de patentes divisionales:

- Según una realización, el procedimiento incluye un paso para generar la imagen en realidad aumentada del revelador en forma de una imagen de una cubierta cuya forma es complementaria a la imagen real de la cuadrícula y que contiene una serie de ventanas que solo permiten ver la imagen real de los datos ocultos cuando la imagen de dicha cubierta se superpone a la imagen de la cuadrícula.

- Según una realización, la imagen en realidad aumentada del revelador se genera en forma de una imagen que resalta la imagen real de los datos ocultos cuando dicha imagen en realidad aumentada se superpone a la imagen de la cuadrícula.

- Ventajosamente, el número de la tarjeta está compuesto por cuatro series de cuatro dígitos, comprendiendo el procedimiento un paso para ocultar la segunda y/o la tercera serie.

- El procedimiento puede incluir un paso para disponer de manera aleatoria o lógica los datos ocultos en la cuadrícula.

Otro aspecto de la invención se refiere a un dispositivo para asegurar los datos de seguridad de una tarjeta de pago bancario asociada a una cuenta bancaria, cuyos datos de seguridad son estáticos e incluyen el número de dicha tarjeta, los datos de identificación del titular de dicha tarjeta, la fecha de expiración de dicha tarjeta y un criptograma, siendo el número de la tarjeta bancaria y el criptograma una serie de varios dígitos y/o letras.

El dispositivo también incluye las siguientes características:

- Los datos de seguridad solo se inscriben parcialmente de manera inteligible en la tarjeta, de manera que algunos datos de seguridad están ocultos, estando estos datos ocultos formados por varios dígitos y/o letras del número de dicha tarjeta y/o al menos un dato de identificación del titular y/o al menos un elemento de la fecha de expiración y/o al menos un dígito y/o letra del criptograma.

- El dispositivo incluye un medio de divulgación de los datos ocultos.

- Los datos ocultos son visibles en la tarjeta y están ocultos entre varios datos dispuestos en una cuadrícula, estando dicha cuadrícula inscrita de manera visible en una cara de la tarjeta.

- El medio de divulgación del dispositivo incluye un revelador de los datos ocultos, siendo este revelador una imagen virtual en realidad aumentada generada por una aplicación informática instalada en un terminal móvil del titular de la tarjeta, siendo dicha imagen del revelador mostrada en una pantalla del terminal móvil y superpuesta a una imagen real de la cuadrícula también mostrada en dicha pantalla, siendo la imagen real de la tarjeta capturada por el dispositivo de adquisición óptica del terminal móvil y los datos ocultos pregrabados en la memoria del terminal móvil.

Según una realización, la imagen en realidad aumentada del revelador se presenta en forma de una imagen de una cubierta cuya forma es complementaria a la imagen real de la cuadrícula y que contiene una serie de ventanas que solo permiten ver la imagen real de los datos ocultos cuando la imagen de dicha cubierta se superpone a la imagen de la cuadrícula. Según una realización, la imagen en realidad aumentada del revelador se presenta en forma de una imagen que resalta la imagen real de los datos ocultos cuando dicha imagen en realidad aumentada se superpone a la imagen de la cuadrícula. Según una realización, la cuadrícula tiene varias casillas, cada una de las cuales contiene un número comprendido entre 0 y 9, estando representado cada número una o más veces en dicha cuadrícula.

Descripción breve de las figuras.

Otros beneficios y características de la invención serán más evidentes al leer la descripción de una realización preferida que sigue, con referencia a los dibujos adjuntos, que se proporcionan como ejemplos indicativos y no limitativos, y en los que:

Fig. 1a es una vista del anverso (cara frontal) de una tarjeta conforme a la invención, según una realización no cubierta por las reivindicaciones,

Fig. 1b es una vista del reverso (cara posterior) de la tarjeta de la figura 1a,

Fig. 2a es una vista del anverso de una tarjeta conforme a la invención, según otra realización no cubierta por las reivindicaciones,

Fig. 2b es una vista del reverso de la tarjeta de la figura 2a,

Fig. 3a es una vista del anverso de una tarjeta conforme a la invención, según otra realización no cubierta por las reivindicaciones,

Fig. 3b es una vista del reverso de la tarjeta de la figura 3a,

Fig. 4a es una vista del anverso de una tarjeta conforme a la invención, según otra realización no cubierta por las reivindicaciones,

Fig. 4b es una vista del reverso de la tarjeta de la figura 4a,

Fig. 5a es una vista del anverso de una tarjeta conforme a la invención, según otra realización cubierta por las reivindicaciones,

Fig. 5b esquematiza una cubierta utilizada para descubrir los datos ocultos en la tarjeta de la figura 5a,

Fig. 5c muestra la tarjeta de la figura 5a combinada con la cubierta de la figura 5b,

Fig. 5d esquematiza otro tipo de revelador utilizado para descubrir los datos ocultos en la tarjeta de la figura 5a,

Fig. 5e muestra la tarjeta de la figura 5a combinada con el revelador de la figura 5d,

Fig. 6a es una vista frontal de un terminal móvil utilizado para implementar el procedimiento según otra realización cubierta por las reivindicaciones,

Fig. 6b esquematiza una imagen real de una tarjeta de pago bancario mostrada en una pantalla del terminal móvil de la figura 6ª, [Fig. 6c] esquematiza una imagen virtual de un revelador mostrada en la pantalla del terminal móvil de la figura 6b, cuya imagen virtual está superpuesta a la imagen real de la cuadrícula también mostrada en dicha pantalla,

Fig. 6d esquematiza otra imagen virtual de un revelador mostrada en la pantalla del terminal móvil de la figura 6b, cuya imagen virtual está superpuesta a la imagen real de la cuadrícula también mostrada en dicha pantalla.

Descripción de las realizaciones.

Las figuras adjuntas representan una tarjeta de pago 1 o tarjeta bancaria (CB). La tarjeta 1 está asociada a la cuenta bancaria de su titular. Se presenta de manera convencional en forma de una tarjeta de plástico que mide aproximadamente 86 mm x 54 mm. Está equipada en el anverso con un chip electrónico 2 con contactos a ras, y en el reverso, eventualmente con una banda magnética 3. El chip 2 y/o la banda 3 permiten realizar pagos en comercios físicos que disponen de un terminal de pago electrónico o en comercios en línea. También permite la retirada de efectivo en cajeros automáticos (ATM).

La tarjeta 1 está asociada a datos de seguridad. Estos datos de seguridad son estáticos, en el sentido de que son fijos y no cambian con el tiempo. Como es conocido, los datos de seguridad incluyen el número 4 de la tarjeta 1, los datos de identificación 5 del titular de la tarjeta, la fecha de expiración 6 de la tarjeta, y un criptograma 7. El número 4, los datos de identificación 5 y la fecha de expiración 6 generalmente se inscriben en el anverso de la tarjeta 1, mientras que el criptograma 7 se inscribe en el reverso de dicha tarjeta. El número 4 se compone de varias series de dígitos, por ejemplo, 4 series de 4 dígitos, lo que suma un total de 16 dígitos. El número 4 también puede consistir en varios dígitos no organizados en serie, un código alfanumérico (una combinación de dígitos y letras), o una serie de letras. Los datos de identificación 5 generalmente incluyen el nombre y apellido del titular de la tarjeta o el nombre de una empresa titular de la cuenta bancaria asociada a la tarjeta 1. La fecha 6 consta de dos elementos, típicamente el mes de vencimiento de dos dígitos (por ejemplo, 02 para febrero) y el año de vencimiento de dos dígitos (por ejemplo, 25 para 2025). Evidentemente, el mes y/o el año podrían consistir en más o menos dígitos y estar asociados a letras. El criptograma 7 consta de varios dígitos, típicamente 3 dígitos (por ejemplo, 432), pero puede consistir en más dígitos (por ejemplo, 4) o menos dígitos (por ejemplo, 2). El criptograma 7 también puede consistir en dígitos y/o letras.

En las figuras 1a y 1b, los datos de seguridad se protegen al inscribir parcialmente el número 4 en la tarjeta 1. Al menos una serie de dígitos está oculta de tal forma que nunca es visible en la tarjeta 1. Preferentemente, se oculta la segunda y/o la tercera serie, dado que la primera serie puede ser común a varias tarjetas de pago y la cuarta serie generalmente aparece en los recibos. También se pueden ocultar todas las series. Los dígitos (y/o letras) ocultos pueden ser reemplazados por cruces (XXXX), puntos, guiones, etc. La segunda y tercera serie pueden ocultarse simultáneamente. También se puede considerar ocultar un dígito en cada serie, de modo que ninguna de las series esté completamente inscrita en la tarjeta 1.

En las figuras 2a y 2b, los datos de seguridad se protegen al inscribir parcialmente el identificador 5 del titular en la tarjeta 1. El nombre del titular (DUPONT) está oculto de tal manera que solo el nombre de pila (ERIC) es visible en la tarjeta 1. También se puede ocultar el nombre de pila para que nunca sea visible, siendo inscrito solo el apellido. Incluso se pueden ocultar el nombre y el apellido del titular. Los datos ocultos pueden ser reemplazados por cruces (XX.XX), puntos, guiones, etc. Es ventajoso poder identificar al titular de la tarjeta 1, incluso cuando el nombre y/o el apellido del titular estén ocultos. Para ello, el número de la tarjeta de identidad o el pasaporte del titular pueden inscribirse en la tarjeta 1. Un comerciante que quiera asegurarse de que la tarjeta 1 pertenece a su titular podrá entonces pedirle su tarjeta de identidad o pasaporte.

En las figuras 3a y 3b, los datos de seguridad se protegen al inscribir parcialmente la fecha de vencimiento 6 en la tarjeta 1. El año está oculto de tal manera que nunca es visible. Solo se inscribe el mes. También se puede ocultar el mes para que nunca sea visible, inscribiéndose solo el año. Incluso se pueden ocultar tanto el mes como el año de vencimiento. Los datos ocultos pueden ser reemplazados por cruces (X.XXX), puntos, guiones, etc.

En las figuras 4a y 4b, los datos de seguridad se protegen al inscribir parcialmente el criptograma 7 en la tarjeta 1. Al menos un dígito (y/o letra), preferentemente 2 dígitos (y/o letras) y, preferentemente, todos los dígitos (y/o letras) del criptograma están ocultos. Los dígitos (y/o letras) ocultos pueden ser reemplazados por cruces (XX.XX), puntos, guiones, etc.

Las realizaciones descritas anteriormente pueden combinarse, en el sentido de que se pueden ocultar simultáneamente varios elementos de los datos de seguridad. Por ejemplo, se puede ocultar todo o parte del número 4 y todo o parte del criptograma 7. También se puede ocultar todo o parte del número 4 y todo o parte de la fecha de vencimiento 6. Todas las combinaciones posibles están cubiertas por la presente invención.

En lo que sigue de la descripción, los elementos ocultos de los datos de seguridad se denominan "datos ocultos". Los datos de seguridad de la tarjeta 1 pueden almacenarse en el chip 2 y/o en la banda magnética 3. Para evitar cualquier piratería, se prevé preferentemente eliminar los datos ocultos del chip 2 y/o de la banda magnética 3.

Solo se comunica al titular de la tarjeta un medio para divulgar estos datos ocultos. Este medio de divulgación puede consistir en un documento enviado por correo al titular de la tarjeta 1, en el que se imprimen los datos ocultos. Para asegurar la comunicación de los datos ocultos, este documento puede ser un documento sellado, enviado en un sobre distinto, o adjunto al envío de la tarjeta 1. Podría tratarse del mismo documento en el que se imprime el código PIN de la tarjeta 1 (generalmente un código de 4 dígitos) que permite retirar dinero de los cajeros automáticos y pagar a los comerciantes. El titular podrá entonces memorizar o almacenar estos datos ocultos, que solo serán conocidos por él.

Para retirar dinero de los cajeros automáticos y pagar a los comerciantes, el titular utilizará de manera habitual el código PIN de la tarjeta 1. Para compras en línea, simplemente deberá completar los datos de seguridad requeridos con los datos ocultos. Así, si el titular pierde su tarjeta 1, el ladrón no podrá utilizarla para realizar compras fraudulentas en línea o por teléfono, ya que nunca conocerá los datos ocultos. El nivel de seguridad proporcionado por la invención es tal que puede reemplazar la autenticación por SMS-OTP, que generalmente se utiliza para asegurar los pagos en línea. El procedimiento de autenticación por SMS-OTP está muy extendido y consiste en enviar un SMS (Short Message Service) al teléfono móvil del titular, que incluye un código de un solo uso (OTP o "One Time Password"). Este código de un solo uso debe ingresarse además de los datos de seguridad para validar una transacción en línea.

Las figuras 5a, 5b y 5c ilustran una realización de la invención cubierta por las reivindicaciones. En la figura 5a, los datos ocultos corresponden a la segunda serie de dígitos del número 4. Los dígitos ocultos son visibles pero están escondidos entre varios dígitos organizados en una cuadrícula 40. La cuadrícula 40 está preferentemente impresa o inscrita de manera visible en el anverso de la tarjeta 1, a la altura del número 4 para facilitar su uso.

Sin embargo, también podría estar impresa en el reverso.

En la figura 5a, la cuadrícula 40 contiene 25 casillas, cada una con un número entre 0 y 9. La cuadrícula 40 puede tener un número superior de casillas, por ejemplo, 100 casillas, cada una de las cuales contiene un número entre 0 y 9, representando cada número 10 veces. La cuadrícula 40 también puede tener un número inferior de casillas, por ejemplo, 10 casillas, cada una con un número entre 0 y 9, estando representado cada número una sola vez. Los números pueden estar dispuestos de manera aleatoria en la cuadrícula 40, o, por el contrario, organizados de manera lógica. La cuadrícula 40 está preferentemente formada por líneas y columnas. El número de líneas está comprendido entre 0 y 10 y el número de columnas también está comprendido entre 0 y 10. La cuadrícula 40 también puede estar formada por uno o varios círculos concéntricos cuadriculados, en los que se colocan los números. Por supuesto, si los datos ocultos del número 4 contienen letras, estas letras pueden ser integradas en la cuadrícula 40.

En referencia a la figura 5b, se proporciona al titular un revelador que permite desvelar los datos ocultos, es decir, los dígitos faltantes del número 4, en la cuadrícula 40. Según una configuración dada como ejemplo, pero no cubierta por las reivindicaciones, este revelador se presenta en forma de una cubierta 41 material que tiene una forma complementaria a la cuadrícula 40 y que contiene una serie de ventanas 410 transparentes o perforadas. A excepción de las ventanas 410, el resto de la cubierta es opaco. La cubierta 41 puede ser enviada en un documento sellado, en un sobre aparte, o adjunta al envío de la tarjeta 1.

En referencia a la figura 5c, cuando la cubierta 41 se coloca sobre la cuadrícula 40, o en otras palabras, coopera con dicha cuadrícula, las ventanas 410 revelan los dígitos ocultos del número 4. La asociación entre la cubierta y la cuadrícula es similar a la técnica de criptografía de la rejilla de Cardano. En el ejemplo ilustrado, la serie 4321 es revelada, correspondiendo esta serie a los datos inicialmente ocultos. El titular podrá entonces memorizar o registrar estos datos ocultos, los cuales solo él conocerá. Si no recuerda los datos ocultos, el titular también podrá reutilizar la cubierta 41 para volver a hacerlos aparecer.

En la variante de realización de la figura 5d, también proporcionada a modo de ejemplo y no cubierta por las reivindicaciones, el revelador se presenta en forma de un soporte 41' transparente que tiene una forma complementaria a la cuadrícula 40. Este soporte transparente 41' está fabricado, por ejemplo, de plástico. Contiene elementos gráficos 41O' organizados y configurados para resaltar los datos ocultos cuando dicho soporte se superpone a la cuadrícula 40. En la figura 5d, estos elementos gráficos 410' se presentan en forma de puntos colocados sobre la superficie del soporte 41'. En referencia a la figura 5e, cuando el soporte 41' se coloca sobre la cuadrícula 40, los puntos están posicionados en las casillas de dicha cuadrícula en las que se encuentran los datos ocultos del número 4. Los elementos gráficos 41O' permiten, por tanto, revelar únicamente los datos ocultos. Los elementos gráficos 41O' no necesariamente se presentan en forma de puntos, sino que pueden adoptar otra forma, por ejemplo, una serie de círculos que rodean los dígitos 4-3-2-1 de la serie oculta cuando el soporte 41' coopera con la cuadrícula 41. El soporte 41' puede estar provisto de una marca que indique el lado que debe colocarse contra la cuadrícula 40. Asimismo, en la figura 5d, el soporte 41' incluye opcionalmente una cuadrícula similar a la cuadrícula 40 para facilitar la colocación correcta del soporte sobre dicha cuadrícula, haciendo coincidir ambas cuadrículas.

Las figuras 6a, 6b, 6c y 6d ilustran otra realización de la invención cubierta por las reivindicaciones. Los datos ocultos corresponden a la segunda serie de dígitos del número 4. Los dígitos ocultos son visibles, pero están escondidos entre varios dígitos organizados en una cuadrícula 40, como en la realización de las figuras 5a a 5c.

La implementación del procedimiento según esta realización requiere el uso de un terminal móvil 9 (figura 6a), preferiblemente en forma de un teléfono móvil o smartphone, como el iPhone®, Samsung Galaxy®, o cualquier otro terminal electrónico que funcione con un sistema operativo del tipo Windows, Mac, iOS, Android, etc. El terminal móvil 9 es el que pertenece al titular (usuario) de la tarjeta 1.

El terminal móvil 9 incluye, de manera clásica, uno o varios procesadores o microprocesadores 90, una o varias memorias 91, una interfaz gráfica 92 y un medio de adquisición óptica 93, todos ellos conectados entre sí a través de un bus común. Una o varias aplicaciones informáticas —o programas informáticos— están almacenadas en la(s) memoria(s) 91, y cuyas instrucciones (o códigos), cuando son ejecutadas por el(los) procesador(es) 90, permiten llevar a cabo las funcionalidades descritas anteriormente en la descripción.

Los datos de seguridad de la tarjeta 1, y al menos los datos ocultos, se almacenan preferentemente en la memoria 90. Si el usuario posee varias tarjetas bancarias, los datos de seguridad de cada una de ellas, y al menos sus datos ocultos, están prealmacenados en la memoria 90. Cabe señalar que la memoria 91 puede ser una memoria nativa del terminal 9, o una memoria remota, por ejemplo, integrada en un servidor informático físicamente distante de dicho terminal.

La interfaz gráfica 92 ofrece al usuario la posibilidad de introducir, seleccionar y/o ingresar datos o instrucciones, así como mostrar imágenes capturadas por el medio de adquisición óptica 93. Se presenta, por ejemplo, en forma de una pantalla táctil, o una pantalla conectada a un teclado, entre otros.

El medio de adquisición óptica 93 se presenta ventajosamente como un lector óptico, del tipo cámara y/o cámara fotográfica integrada en el terminal móvil 9. Este medio de adquisición óptica 93 está asociado a una aplicación informática de lectura.

El usuario puede verse obligado a instalar una aplicación informática en su terminal móvil 9 para implementar total o parcialmente la invención desde dicho terminal, especialmente para la visualización de imágenes en realidad aumentada. Esta aplicación informática puede estar preinstalada en el terminal 9. Sin embargo, el usuario tiene la posibilidad de buscar esta aplicación informática en tiendas en línea como Google Play®, iTunes®, o en un sitio web dedicado, y luego descargarla en su terminal 9.

Por motivos de claridad, debe entenderse que, en el sentido de la invención, "el terminal 9 hace algo" significa "la aplicación informática ejecutada por el procesador o microprocesador 90 del terminal 9 hace algo". De la misma manera, "la aplicación informática hace algo" significa "la aplicación informática ejecutada por el procesador o microprocesador 90 del terminal 9 hace algo".

Con referencia a la figura 6b, el usuario abre su aplicación de lectura desde su terminal móvil 9 y captura toda o parte de la imagen de la tarjeta 1 con el medio de adquisición óptica 93. La imagen real de la tarjeta 1 se muestra entonces en la interfaz gráfica 92 del terminal 9.

El terminal 9, mediante una aplicación de reconocimiento visual como Google Lens®, reconoce que el objeto fotografiado es una tarjeta bancaria y que esta tarjeta incluye la cuadrícula 40. Basado en el reconocimiento óptico de caracteres de tipo OCR (acrónimo en inglés de "Optical Character Recognition"), el terminal 9 analizará la imagen de la cuadrícula 40 y, más particularmente, los números dispuestos en ella. El terminal 9 buscará en la memoria 91 los datos ocultos (por ejemplo, la serie 4321) y buscará estos datos en la imagen de la cuadrícula 40 (por ejemplo, cada uno de los números 4-3-2-1). El terminal 9 generará entonces una imagen en realidad aumentada del revelador y mostrará esta imagen virtual en la pantalla 92, superponiéndola a la imagen real de la cuadrícula 40.

En la figura 6c, la imagen en realidad aumentada del revelador se presenta en forma de una imagen de una cubierta 941 cuya forma es complementaria a la imagen real de la cuadrícula 40. La imagen de la cubierta 941 incluye aquí una serie de ventanas que solo muestran la imagen real de los datos ocultos cuando la imagen de dicha cubierta se superpone a la imagen de la cuadrícula. En el ejemplo de la figura 6c, la serie 4321 es revelada por la imagen virtual de la cubierta 941, siendo esta serie la que corresponde a los datos inicialmente ocultos.

En la figura 6d, la imagen en realidad aumentada del revelador se presenta en forma de una imagen 941 que resalta la imagen real de los datos ocultos cuando dicha imagen en realidad aumentada se superpone a la imagen de la cuadrícula 40. Esta imagen virtual aquí es una serie de círculos que rodean la imagen de los dígitos 4-3-2-1 de la serie oculta. Sin embargo, estos números también pueden resaltarse de otras formas, por

ejemplo, mediante el uso de resaltado, ampliación o desenfoque de los otros números escritos en la cuadrícula 40, etc.

En cualquier caso, la imagen virtual generada puede incluir los datos ocultos que se muestran en una zona gráfica dedicada 942.

El sistema de cuadrícula y cubierta descrito en referencia a las figuras 5a, 5b, 5c, 6b, 6c y 6d se aplica de manera similar a los datos de identificación 5 (nombre y/o apellido del titular, en cuyo caso la cuadrícula 40 contiene una serie de letras), la fecha de vencimiento 6 y/o el criptograma 7 y/o el número de la tarjeta de identidad o pasaporte del titular, en el caso de que los datos ocultos formen parte de estos elementos.

La disposición de los diferentes elementos y/o medios y/o pasos de la invención, en las realizaciones descritas anteriormente, no debe entenderse como una disposición obligatoria en todas las implementaciones. En particular, una o más características presentadas en una realización pueden combinarse con una o más características presentadas solo en otra realización.

.

REIVINDICACIONES

1.Procedimiento para la protección de los datos de seguridad de una tarjeta de pago bancario (1) asociada a una cuenta bancaria, cuyos datos de seguridad son estáticos e incluyen el número (4) de dicha tarjeta, datos de identificación (5) del titular de la tarjeta, la fecha de expiración (6) de dicha tarjeta, y un criptograma (7), cuyo número de tarjeta bancaria y criptograma están compuestos por varios dígitos y/o letras, comprendiendo dicho procedimiento las siguientes etapas:

- inscribir parcialmente los datos de seguridad de manera inteligible en dicha tarjeta, de modo que se oculten algunos datos de seguridad, y los datos ocultos estén formados por varios dígitos y/o letras del número (4) de dicha tarjeta y/o al menos un dato de identificación (5) del titular y/o al menos un elemento de la fecha de expiración (6) y/o al menos un dígito y/o letra del criptograma (7),

- transmitir únicamente al titular de la tarjeta (1) un medio de divulgación (41) de los datos ocultos, caracterizado porque dicho procedimiento incluye las siguientes etapas:

- ocultar los datos ocultos, visibles en la tarjeta, entre varios datos,

- organizar los datos en una cuadrícula (40),

- inscribir de manera visible la cuadrícula (40) en una cara de la tarjeta (1),

- el medio de divulgación (41) de los datos ocultos incluye un revelador de los datos ocultos, el cual se presenta en forma virtual como una imagen en realidad aumentada generada por una aplicación informática instalada en un terminal móvil (90) del titular de la tarjeta (1), cuya imagen del revelador se muestra en una pantalla de dicho terminal superpuesta a una imagen real de la cuadrícula (40) que también se muestra en dicha pantalla, la imagen real de la tarjeta se captura mediante el medio de adquisición óptica del terminal móvil (90), y los datos ocultos están pregrabados en la memoria del terminal móvil (90).

2. Procedimiento según la reivindicación 1, que consiste en generar la imagen en realidad aumentada del revelador en forma de una imagen de un cache (41') cuya forma es complementaria a la imagen real de la cuadrícula (40) y que tiene una serie de ventanas (410') que solo permiten visualizar la imagen real de los datos ocultos cuando la imagen de dicho cache se superpone a la imagen de dicha cuadrícula.

3. Procedimiento según la reivindicación 1, que consiste en generar la imagen en realidad aumentada del revelador en forma de una imagen que resalta la imagen real de los datos ocultos cuando dicha imagen en realidad aumentada se superpone a la imagen de la cuadrícula (40).

4. Procedimiento según cualquiera de las reivindicaciones anteriores, en el que el número (4) de la tarjeta está compuesto por cuatro series de cuatro dígitos, y el procedimiento incluye una etapa en la que se oculta la segunda y/o la tercera serie.

5. Procedimiento según cualquiera de las reivindicaciones 1 a 4, que incluye una etapa de organizar de manera aleatoria los datos ocultos en la cuadrícula (40).

6. Procedimiento según cualquiera de las reivindicaciones 1 a 4, que incluye una etapa de organizar de manera lógica los datos ocultos en la cuadrícula (40).

7. Dispositivo de protección de los datos de seguridad de una tarjeta de pago bancario (1) asociada a una cuenta bancaria, cuyos datos de seguridad son estáticos e incluyen el número (4) de dicha tarjeta, los datos de identificación (5) del titular de la tarjeta, la fecha de expiración (6) de dicha tarjeta, y un criptograma (7), cuyo número de tarjeta bancaria y criptograma están compuestos por varios dígitos y/o letras, y en el que:

- solo están inscritos parcialmente de manera inteligible en la tarjeta (1) de modo que se ocultan algunos datos de seguridad, y los datos ocultos están formados por varios dígitos y/o letras del número (4) de dicha tarjeta y/o al menos un dato de identificación (5) del titular y/o al menos un elemento de la fecha de expiración (6) y/o al menos un dígito y/o letra del criptograma (7),

- el dispositivo incluye un medio de divulgación (41) de los datos ocultos, caracterizado porque:

- los datos ocultos son visibles en la tarjeta y están ocultos entre varios datos organizados en una cuadrícula (40), que está inscrita de manera visible en una cara de la tarjeta (1),

- el medio de divulgación (41) del dispositivo incluye un revelador de los datos ocultos, el cual se presenta en forma virtual como una imagen en realidad aumentada generada por una aplicación informática instalada en un terminal móvil (9) del titular de la tarjeta (1), cuya imagen del revelador se muestra en una pantalla de dicho

terminal superpuesta a una imagen real de la cuadrícula (40) que también se muestra en dicha pantalla, la imagen real de la tarjeta se captura mediante el medio de adquisición óptica (93) del terminal móvil (90), y los datos ocultos están pregrabados en la memoria (91) del terminal móvil (90).

8. Dispositivo según la reivindicación 7, en el que la imagen en realidad aumentada del revelador se presenta en forma de una imagen de un cache (41') cuya forma es complementaria a la imagen real de la cuadrícula (40) y que tiene una serie de ventanas (410') que solo permiten visualizar la imagen real de los datos ocultos cuando la imagen de dicho cache se superpone a la imagen de dicha cuadrícula.

9. Dispositivo según la reivindicación 7, en el que la imagen en realidad aumentada del revelador se presenta en forma de una imagen que resalta la imagen real de los datos ocultos cuando dicha imagen en realidad aumentada se superpone a la imagen de la cuadrícula (40).

10. Dispositivo según cualquiera de las reivindicaciones 7 a 9, en el que la cuadrícula (40) tiene varias casillas, cada una conteniendo un dígito comprendido entre 0 y 9.

11. Dispositivo según la reivindicación 10, en el que cada dígito está representado varias veces en la cuadrícula (40).

12. Dispositivo según la reivindicación 10, en el que cada dígito está representado una sola vez en la cuadrícula (40).

13. Dispositivo según cualquiera de las reivindicaciones 7 a 9, en el que los datos ocultos corresponden a un número de tarjeta de identidad o pasaporte del titular de la tarjeta (1), inscrito en dicha tarjeta.

Fig. 1a

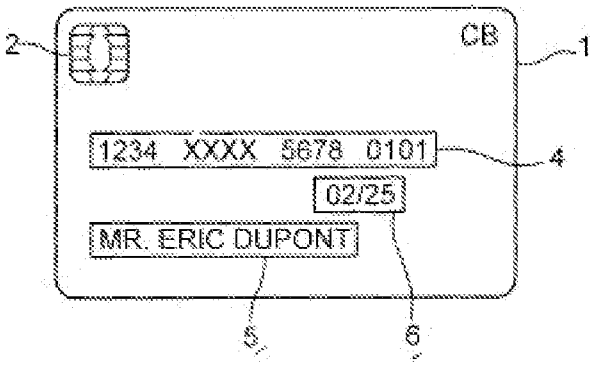


Fig. 1b

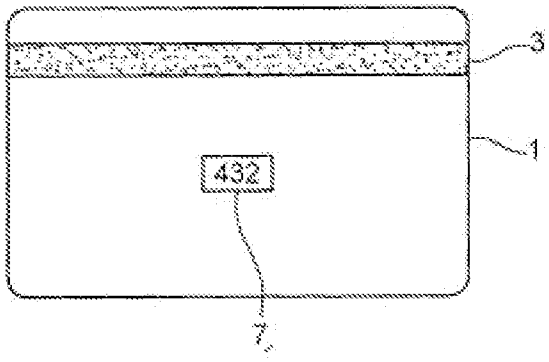


Fig. 2a

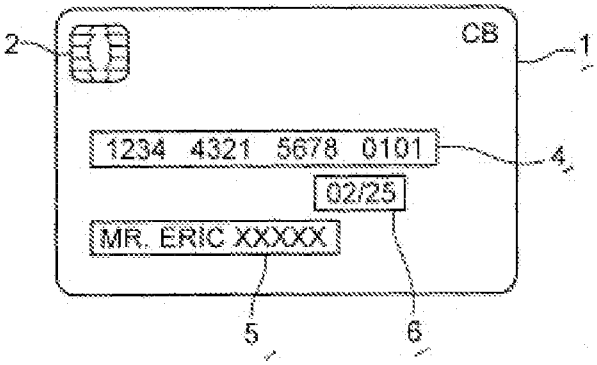


Fig. 2b

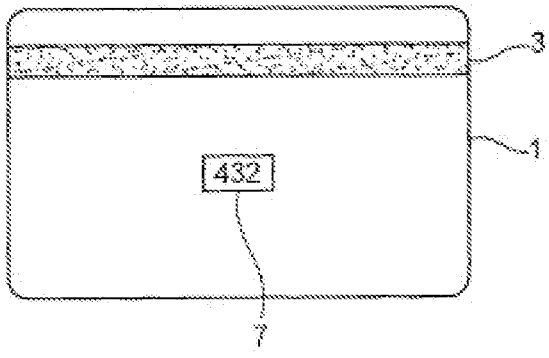


Fig. 3a

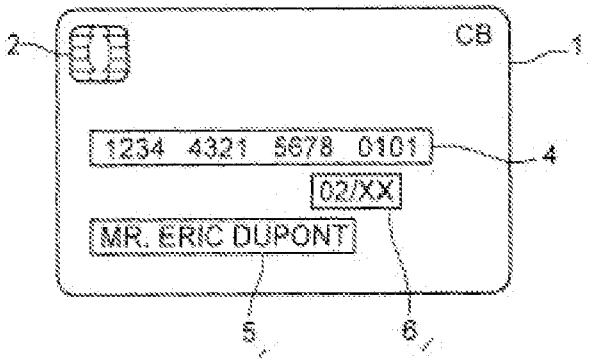


Fig. 3b

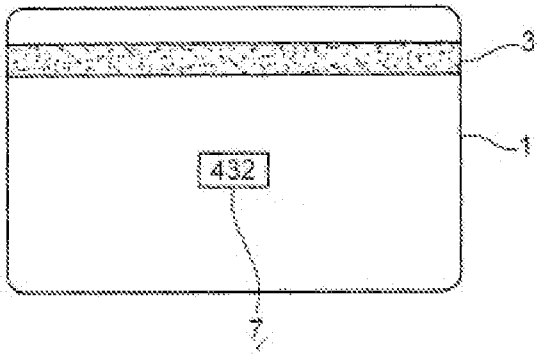


Fig. 4a

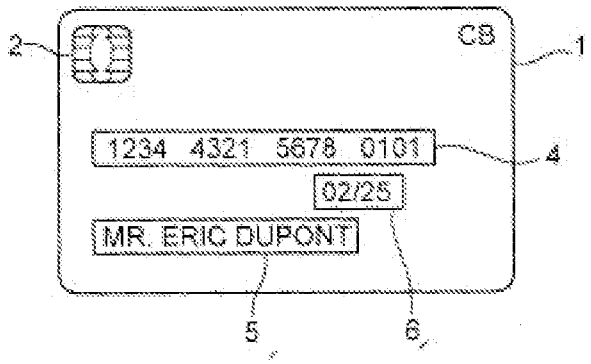


Fig. 4b

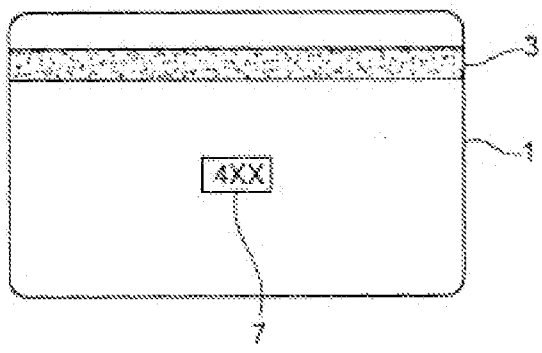


Fig. 5a

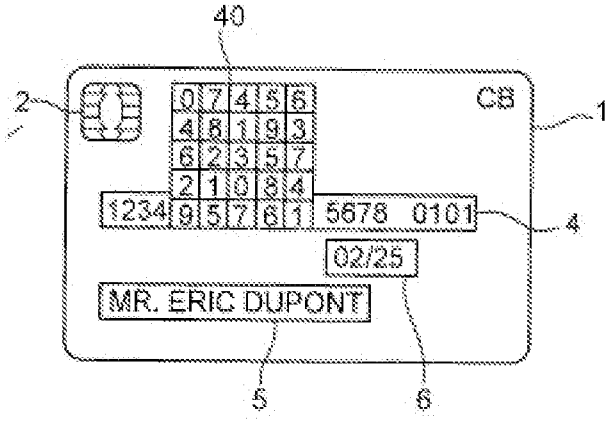


Fig. 5b

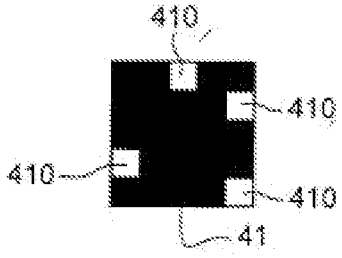


Fig. 5c

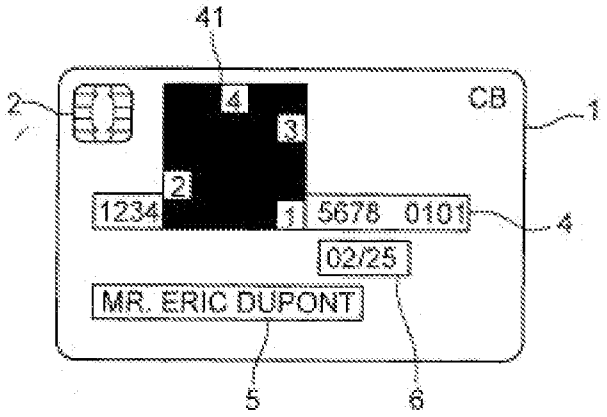


Fig. 5d

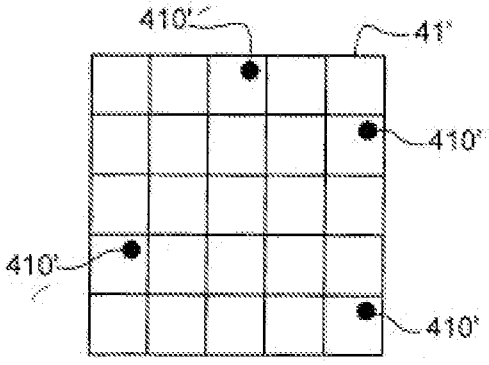


Fig. 5e

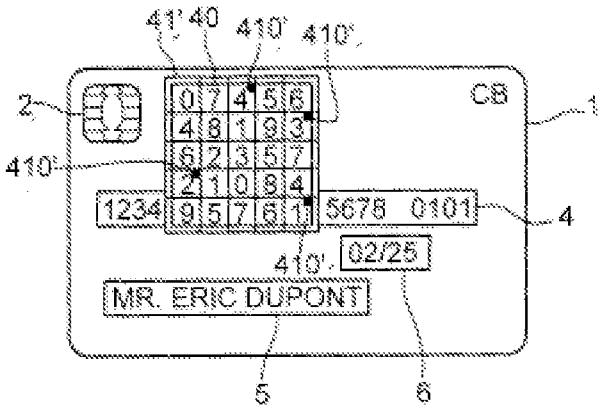

41'
40
410'
410'
2
CB
1
410'
0 7 4 5 6
4 8 1 9 3
6 2 3 5 7
2 1 0 8 4
1234
9 5 7 6 1
5678 0101
4
410'
02/25
MR. ERIC DUPONT
5
6

Fig. 6a

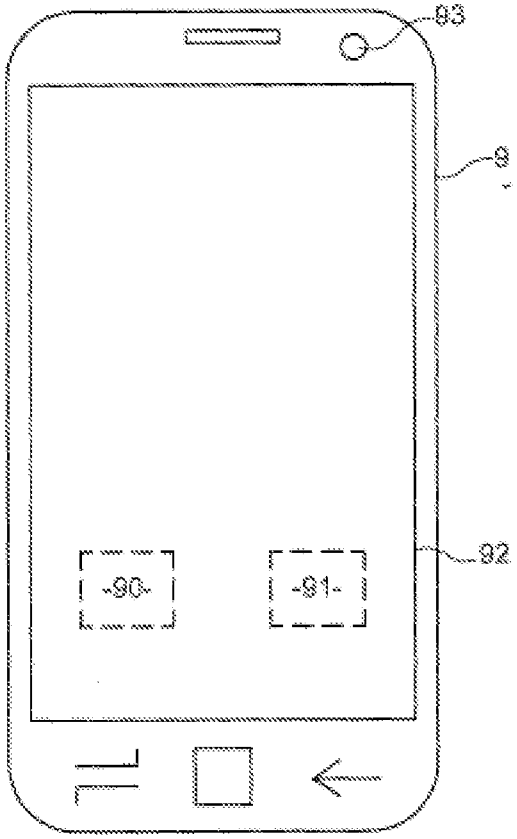

93
9
92
-90-
-91-

Fig. 6b

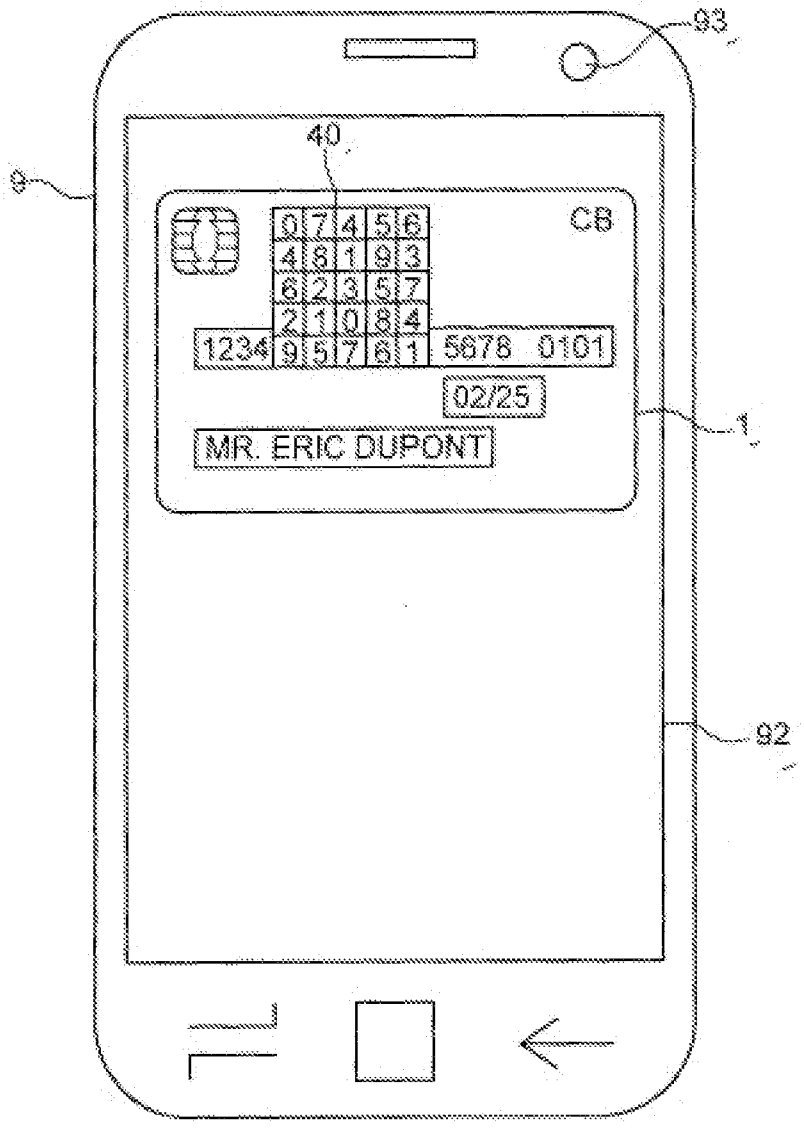

93
40
9
0 7 4 5 6
4 6 1 9 3
6 2 3 5 7
2 1 0 8 4
CB
1234 9 5 7 6 1
5678 0101
02/25
MR. ERIC DUPONT
1
92

Fig. 6c

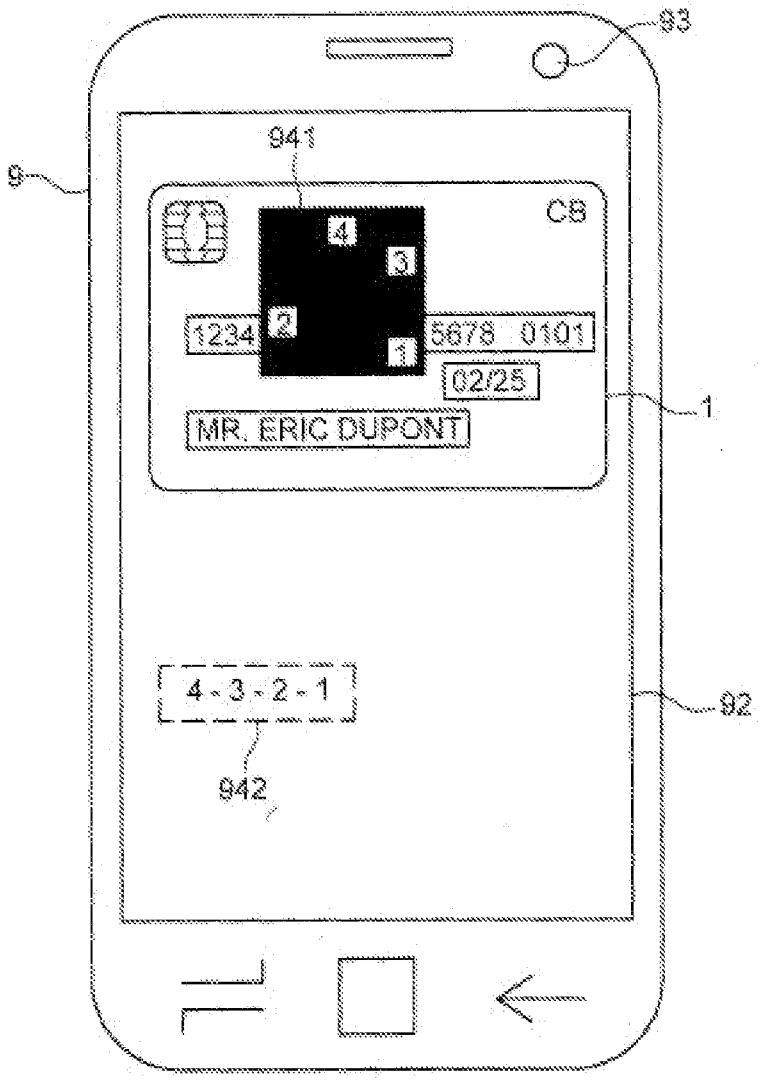
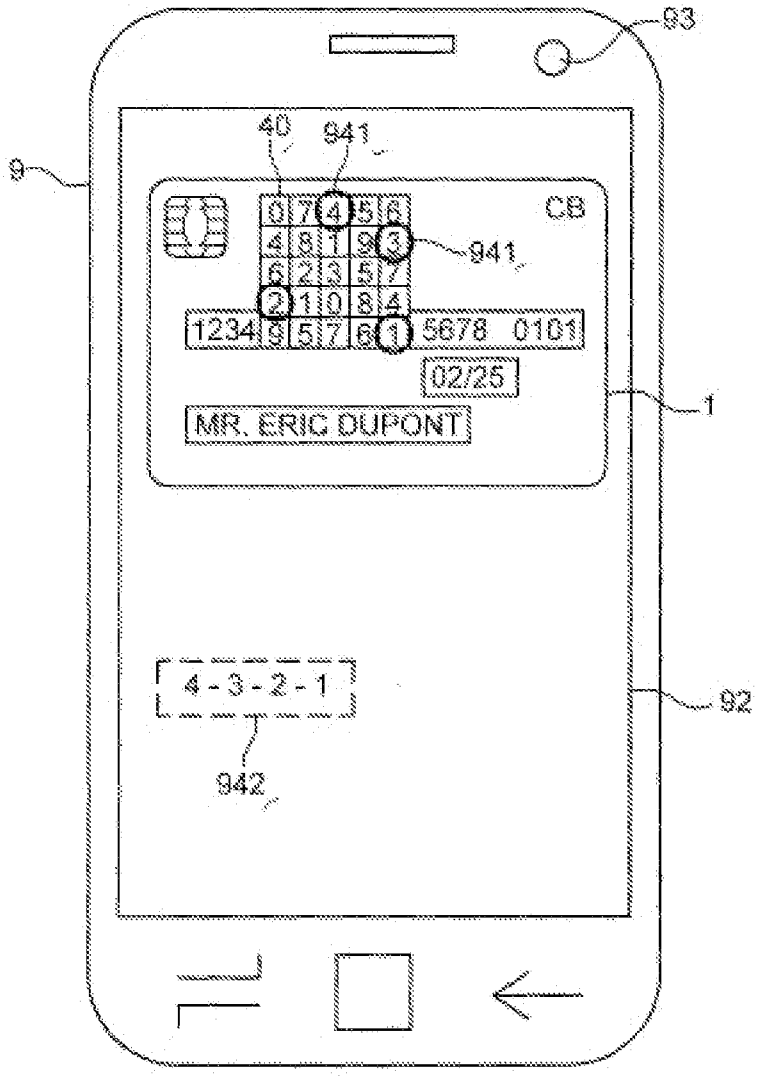

93
941
9
CB
4
3
2
1
1234
5678 0101
02/25
MR. ERIC DUPONT
1
4 - 3 - 2 - 1
92
942

Fig. 6d


93
40
941
9
0 7 4 5 6
4 8 1 9 3
6 2 3 5 7
2 1 0 8 4
941
CB
1234 9 5 7 6 1 5678 0101
02/25
MR. ERIC DUPONT
1
4 - 3 - 2 - 1
92
942