(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 784 535**

(21) Número de solicitud: 201930266

(51) Int. CI.:

G07F 7/12 (2006.01)

(12) SOLICITUD DE PATENTE A1

(22) Fecha de presentación:

25.03.2019

(43) Fecha de publicación de la solicitud:

28.09.2020

(71) Solicitantes:

UNIVERSIDAD DE VALLADOLID (100.0%)
Plaza de Santa Cruz, 5 bajo
47002 Valladolid ES

(72) Inventor/es:

GARCÍA ESCARTÍN, Juan Carlos;
GONZÁLEZ MORALES, Mª Jesús y
MARTÍN DÍEZ, Pablo

(74) Agente/Representante:

PONS ARIÑO, Ángel

(54) Título: **DISPOSITIVO Y PROCEDIMIENTO DE ENTRENAMIENTO E IDENTIFICACIÓN DE TARJETAS SIN CONTACTO POR CARACTERIZACIÓN EN RADIOFRECUENCIA**

(57) Resumen:

El dispositivo y procedimiento de entrenamiento e identificación de tarjetas sin contacto por caracterización en radiofrecuencia comprende un soporte (1) para posicionamiento de tarjeta en el que se coloca la tarjeta que va a ser identificada, un elemento emisor (2) de señal de radiofrecuencia que envía la señal y el consiguiente campo electromagnético, hacia el soporte (1), un elemento dispersor (4) reconfigurable que junto con la tarjeta, dispersa el campo electromagnético, un elemento receptor (3) que recoge el campo dispersado por la tarjeta, y un controlador (5) que da la orden de enviar la señal de radiofrecuencia al elemento emisor (2), reconfigura el elemento dispersor (4), recibe la señal recogida por el elemento receptor (3) y realiza la clasificación de la tarjeta, logrando una identificación única asociada a cada tarjeta, de forma que se logran evitar los ataques que tratan de suplantar su identidad.

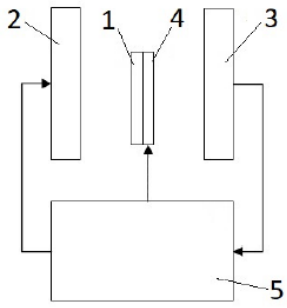

FIG.1

ES 2 784 535 A1

D E S C R I P C I Ó N

DISPOSITIVO Y PROCEDIMIENTO DE ENTRENAMIENTO E IDENTIFICACIÓN DE TARJETAS SIN CONTACTO POR CARACTERIZACIÓN EN RADIOFRECUENCIA

OBJETO DE LA INVENCIÓN

La invención se refiere a un dispositivo y procedimiento de entrenamiento e identificación de tarjetas sin contacto por caracterización en radiofrecuencia, que consigue una identificación única asociada a cada tarjeta, de forma que se logran evitar los ataques que tratan de suplantar su identidad.

ANTECEDENTES DE LA INVENCIÓN

Los dispositivos de identificación de tarjetas por radiofrecuencia (RFID), como por ejemplo aquellas que se usan para facilitar la entrada a zonas de acceso restringido, en general se basan en la identificación de estas a partir de alguna información única que contienen, tal como una clave secreta almacenada en su chip. Pero surge el problema de que existen mecanismos para crear una copia de las tarjetas extrayendo, por ejemplo, la clave del chip, que se replica en otra tarjeta, pudiendo engañar así a los dispositivos de identificación y suplantando la identidad de la tarjeta original.

Para resolver esta problemática, se plantea que las tarjetas puedan ser identificadas, además de por las claves secretas almacenadas en los chips, por alguna de sus características físicas únicas que se pueda evaluar. En el estado actual de la técnica son conocidas diversas formas de implementar este tipo de identificación individualizada.

Existe una propuesta que consiste en añadir elementos a las tarjetas, tales como virutas metálicas, de forma aleatoria, de tal forma que se genera una identificación tipo huella dactilar, que permite identificar las tarjetas, tal y como se describe en el documento de Vasileios Lakafosis en *“RFID-CoA: The RFID tags as Certificates of Authenticity”,* 2011 IEEE International Conference on RFID-Technologies and Applications. De esta forma se logra que cada tarjeta sea diferente a cualquier otra. El inconveniente de esta propuesta es que implica modificar las tarjetas físicamente al añadir los elementos mencionados posteriormente a su proceso de fabricación.

Existen además varias propuestas para identificar las tarjetas de forma unívoca a partir de sus particularidades físicas, basándose en que la respuesta de las tarjetas ante ciertas señales varía de una a otra. Un análisis detallado puede encontrarse en la publicación de Danev, B., Zanetti, D., Capkun, S: *"On physical-layer identification of wireless devices (Review)"* ACM Computing Surveys, Vol. 45, No. 1, Artículo 6, noviembre de 2012.

Por otra parte, existen protocolos desafío-respuesta que se emplean en procesos de autenticación basados en las características físicas de diferentes dispositivos y sistemas ópticos. Este es el caso, por ejemplo, del documento WO2010105993 (A2) *"System and method for security purposes"* y del documento EP2693685 (B1) *"Quantum secure device, system and method for verifying challenge-response pairs using a physically unclonable function (PUF) ".*

DESCRIPCIÓN DE LA INVENCIÓN

El dispositivo y procedimiento de entrenamiento e identificación de tarjetas sin contacto por caracterización en radiofrecuencia que propone la presente invención soluciona los problemas o inconvenientes anteriormente señalados, ya que mediante la incorporación de una identificación única asociada a cada tarjeta se logran evitar los ataques que tratan de suplantar la identidad de esta.

El dispositivo objeto de esta invención consta de un soporte para posicionamiento de la tarjeta, un elemento emisor, un elemento receptor, un elemento dispersor reconfigurable y un controlador; y el procedimiento de identificación de tarjetas sin contacto que propone la presente invención consta de una etapa de entrenamiento, un protocolo desafío-respuesta y un método de clasificación de tarjetas.

De manera concreta, lo que la invención propone es, en primer lugar, un soporte en el que se posiciona la tarjeta que se va a identificar, es decir, se va a determinar si la tarjeta pertenece al grupo de las registradas por el controlador.

El elemento emisor, cuando recibe la orden por parte del controlador, envía una señal de radiofrecuencia hacia el soporte donde se encuentra la tarjeta.

Las tarjetas normalmente se diseñan para operar en un cierto intervalo de frecuencias de la señal de radiofrecuencia. Al someter a las tarjetas a la señal en dicho intervalo de frecuencia, las tarjetas fabricadas en serie no muestran ninguna diferencia apreciable entre ellas en su respuesta física. Sin embargo, el elemento emisor del dispositivo de la siguiente invención emite una señal de radiofrecuencia en un intervalo de frecuencias que está muy por encima del intervalo para el que se diseñan las tarjetas, mencionado anteriormente. Al recibir esta señal de radiofrecuencia a una frecuencia más elevada, las tarjetas actúan como dispersores electromagnéticos que en este caso sí muestran diferencias apreciables entre sí en su respuesta física ante la señal. Estas diferencias entre las respuestas físicas de las tarjetas son debidas a la variabilidad natural en el proceso de fabricación, que introduce imperfecciones en alguno de los elementos de la tarjeta, particularmente en su antena, provocando que el campo electromagnético dispersado tenga ciertos rasgos propios y únicos en cada tarjeta.

Una vez que el elemento emisor emite la señal de radiofrecuencia que constituye un campo electromagnético, este atraviesa la tarjeta que actúa como dispersor electromagnético, generando una respuesta única respecto a las demás tarjetas. Se va a denominar a la dispersión del campo electromagnético escenario dispersor.

A continuación, el elemento receptor, recibe y registra el campo dispersado por la tarjeta y lo envía al controlador. Este campo será por tanto el que permita identificar cada tarjeta.

Además de suplantar la identidad de la tarjeta mediante la sustracción de la clave de su chip, tal y como se ha expuesto en el apartado anterior, también se puede suplantar su identidad por medio de un elemento externo que reproduce la respuesta a la señal de radiofrecuencia que se espera recibir por parte de la tarjeta auténtica. Para evitar este problema, la invención incluye el elemento dispersor reconfigurable antes citado, que se sitúa junto al soporte para posicionamiento de la tarjeta. Su finalidad es alterar el escenario dispersor, de modo que el campo electromagnético que genera el transmisor es dispersado de manera diferente por la tarjeta junto con el elemento dispersor para cada configuración de este. De esta forma, el receptor mide una respuesta diferente para cada configuración del elemento dispersor. Así se pueden generar distintas alternativas mediante la combinación de la señal de radiofrecuencia enviada, que es siempre la misma, con el elemento dispersor reconfigurable, que provoca una alteración del escenario dispersor. El objetivo final es que no se pueda prever cuál será la configuración del elemento dispersor, y por tanto, cómo será

el campo dispersado por la tarjeta junto con el elemento dispersor. Así será imposible que un elemento externo proporcione la respuesta que se espera recibir por parte de la tarjeta auténtica, evitando así que se pueda suplantar su identidad.

La realización del elemento dispersor reconfigurable consiste en una base en la que unas piezas metálicas se reparten por su superficie y se conectan al controlador, de modo que este puede cambiar su potencial eléctrico. Al variar el potencial eléctrico se altera la configuración del elemento dispersor, y como consecuencia, se modifica también el escenario dispersor. Si hay n elementos metálicos y m valores de voltaje, se puede lograr de este modo obtener m^n configuraciones diferentes, y por tanto m^n escenarios dispersores que pueden caracterizar la tarjeta.

Este procedimiento de modificación del escenario dispersor se ha denominado protocolo desafío-respuesta. En este protocolo por tanto, se lanzan ‘preguntas’, es decir, se envía a la tarjeta, una señal de radiofrecuencia con el consiguiente campo electromagnético, seleccionando una configuración del elemento dispersor reconfigurable, y se registra el campo dispersado o ‘respuesta’ a esa pregunta, que genera la combinación del elemento dispersor y la tarjeta. En cada identificación se modifica el escenario dispersor y por tanto la respuesta esperada. Esto protege, como se ha explicado anteriormente, frente a ataques en los que, mediante un elemento externo, se pretende reproducir el campo dispersado que se espera recibir de la tarjeta.

Finalmente, una vez que el elemento emisor ha enviado la señal, se ha dispersado el campo electromagnético mediante el elemento dispersor reconfigurable y la tarjeta, y el elemento receptor ha recogido la respuesta, esta se envía al controlador. Por tanto el controlador es el que da la orden de enviar la señal de radiofrecuencia al elemento emisor, es el que lleva a cabo la reconfiguración del elemento dispersor reconfigurable, y es el que recibe la respuesta de la tarjeta recogida por el elemento receptor.

Para terminar, una vez registrada la respuesta por el controlador se lleva a cabo la clasificación, que consiste en determinar si la respuesta que ha dado la tarjeta corresponde con alguna de las tarjetas registradas, y en caso afirmativo, a cuál de ellas corresponde. Para poder realizar la clasificación, hay que comparar la respuesta que proporciona la tarjeta con todas las respuestas registradas en el dispositivo. Por lo tanto, antes de poner en funcionamiento el dispositivo, se lleva a cabo una etapa previa de entrenamiento, que

consiste en colocar cada una de las tarjetas en el soporte para tarjetas y someterlas a todos los posibles escenarios de dispersión que puede generar el dispositivo, y que como se ha explicado, son generados por una combinación de la señal que envía el elemento emisor con el elemento dispersor reconfigurable. En consecuencia, durante el entrenamiento se generan los datos de respuesta de las tarjetas, que se almacenan en la memoria del controlador. Al leer la información de una tarjeta individual, disponiendo de los datos generados durante el entrenamiento, el dispositivo será capaz de determinar si se trata de una de las registradas y cuál de ellas, o si no es una de las tarjetas registradas. El algoritmo de clasificación empleado se puede realizar mediante aprendizaje autónomo utilizando, por ejemplo, la técnica de los k-vecinos más próximos o SVM (Support Vector Machine).

En la realización de la invención, cabe la posibilidad de utilizar, bien una antena emisora como medio emisor y una antena receptora como medio receptor, que pueden situarse una frente a otra a ambos lados del soporte, o bien una única antena que actúa como medio emisor y medio receptor, y situar el soporte para la tarjeta, seguido del elemento dispersor reconfigurable, enfrente de dicha antena.

DESCRIPCIÓN DE LOS DIBUJOS

Para complementar la descripción que se está realizando y con objeto de ayudar a una mejor comprensión de las características de la invención, de acuerdo con un ejemplo preferente de realización práctica de la misma, se acompaña como parte integrante de dicha descripción, un juego de dibujos en donde con carácter ilustrativo y no limitativo, se ha representado lo siguiente:

Figura 1.- Muestra una representación esquemática del dispositivo de entrenamiento e identificación de tarjetas sin contacto.

Figura 2.- Muestra una representación esquemática del elemento dispersor.

REALIZACIÓN PREFERENTE DE LA INVENCIÓN

A continuación, y a la vista de las figuras se describe un modo de realización preferente del dispositivo y procedimiento de entrenamiento e identificación de tarjetas sin contacto por caracterización en radiofrecuencia.

El dispositivo de entrenamiento e identificación de tarjetas sin contacto por caracterización en radiofrecuencia que se describe, mostrado en la figura 1, comprende un soporte (1) en el que se posiciona la tarjeta que se va a identificar, un elemento emisor (2) enfrentado al soporte, que cuando recibe la orden por parte de un controlador (5), envía una señal de radiofrecuencia hacia el soporte. (1). Una vez el elemento emisor (2) ha emitido la señal de radiofrecuencia con el consiguiente campo electromagnético, esta atraviesa la tarjeta que actúa como dispersor electromagnético y que produce una dispersión del campo electromagnético como respuesta. El dispositivo incorpora así mismo un elemento receptor (3), que se localiza al otro lado del soporte (1), opuesta al elemento emisor (2), y el cual recibe y registra el campo dispersado por la tarjeta y lo envía al controlador (5). Este campo es el que permite identificar la tarjeta.

Junto al soporte (1) para tarjeta y entre este y el elemento receptor (3) se encuentra un elemento dispersor (4) reconfigurable que, junto con la tarjeta (1), dispersan el campo electromagnético. Como se muestra con detalle en la figura 2, el elemento dispersor (4) comprende una base (6) en la que se reparten por su superficie unas piezas metálicas (7) y se conectan al controlador (5) de modo este puede cambiar su potencial eléctrico.

La modificación del campo electromagnético que le llega a la tarjeta se efectúa mediante el protocolo desafío-respuesta, en el que se envía a la tarjeta y al elemento dispersor (4), una señal de radiofrecuencia con el consiguiente campo electromagnético, que se denomina ‘pregunta’, y se registra el campo dispersado o ‘respuesta’ a esa pregunta que generan, siendo este diferente para cada configuración del elementos dispersor (4).

El controlador (5) del dispositivo es el que da la orden de enviar la señal de radiofrecuencia al elemento emisor (2), el que lleva a cabo la reconfiguración del elemento dispersor (4) reconfigurable, y el que recibe la respuesta de la tarjeta recogida por el elemento emisor (3).

Es también el controlador (5) el que lleva a cabo la clasificación de la tarjeta, determinando si la respuesta que ha dado corresponde con alguna de las tarjetas registradas, y en caso afirmativo, a cuál de ellas. Para poder realizar la clasificación, se compara la respuesta que proporciona la tarjeta con todas las respuestas registradas en el controlador (5).

Estas respuestas que están registradas se obtienen antes de poner en funcionamiento el dispositivo en una etapa previa de entrenamiento. Durante esta etapa se coloca cada una de

las tarjetas en el soporte (1) y se somete a todos los escenarios dispersores que puede generar el dispositivo. En consecuencia, se generan los datos de respuesta de las tarjetas, que se almacenan en la memoria del controlador (5).

Un ejemplo concreto de realización del dispositivo y procedimiento de entrenamiento e identificación de tarjetas por caracterización en radiofrecuencia se da a continuación.

Las tarjetas elegidas para caracterizar son RFID a 13.56 MHz según el estándar *ISO*/IEC 18092. La banda RF elegida para caracterizar las diferencias entre tarjetas es la banda Wi-Fi de uso libre: 2.4 GHz. Como elemento emisor (2) y elemento receptor (3) de señal se utilizan sendas unidades Wi-Fi. La tarjeta se posiciona entre ambas en el soporte (1) para posicionamiento de la tarjeta. El elemento dispersor (4) reconfigurable se posiciona junto a la tarjeta. Sus piezas metálicas (7) se configuran mediante el controlador (5) que modifica el potencial eléctrico aplicado a cada pieza metálica (7), modificando así el escenario dispersor. Por ejemplo, si hay n piezas metálicas (7) y dos valores de voltaje, se pueden lograr 2^{n} escenarios diferentes. El controlador (5) se encarga de hacer la clasificación y determinar si la tarjeta está registrada. La clasificación se realiza (con los datos almacenados previamente en la fase de entrenamiento) mediante un algoritmo de aprendizaje automático supervisado como por ejemplo el algoritmo de los k-vecinos más próximos o el SVM (Support Vector Machine).

R E I V I N D I C A C I O N E S

1. Dispositivo de entrenamiento e identificación de tarjetas sin contacto por caracterización en radiofrecuencia caracterizado por que comprende:
   - un soporte (1) para posicionamiento de tarjeta en el que se coloca la tarjeta que va a ser identificada,
   - un elemento emisor (2) de señal de radiofrecuencia que envía la señal y el consiguiente campo electromagnético, hacia el soporte (1),
   - un elemento dispersor (4) reconfigurable que junto con la tarjeta, dispersa el campo electromagnético,
   - un elemento receptor (3) que recoge el campo dispersado por la tarjeta, y
   - un controlador (5) que da la orden de enviar la señal de radiofrecuencia al elemento emisor (2), reconfigura el elemento dispersor (4), recibe la señal recogida por el elemento receptor (3) y realiza la clasificación de la tarjeta.

2. Dispositivo de entrenamiento e identificación de tarjetas sin contacto por caracterización en radiofrecuencia de acuerdo con la reivindicación 1 caracterizado por que el medio emisor (2) es una antena emisora y el medio receptor (3) es una antena receptora.

3. Dispositivo de entrenamiento e identificación de tarjetas sin contacto por caracterización en radiofrecuencia de acuerdo con la reivindicación 2 caracterizado por que la antena emisora está situada a un lado del soporte (1) para posicionamiento de la tarjeta, y la antena receptora está situada enfrente de la antena emisora, al otro lado del soporte (1).

4. Dispositivo de entrenamiento e identificación de tarjetas sin contacto por caracterización en radiofrecuencia de acuerdo con la reivindicación 1 caracterizado por que el medio emisor (2) y el medio receptor (3) están implementados en una única antena.

5. Dispositivo de entrenamiento e identificación de tarjetas sin contacto por caracterización en radiofrecuencia de acuerdo con la reivindicación 1 caracterizado por que el elemento dispersor (4) reconfigurable comprende:
   - una base (6),
   - unas piezas metálicas (7) situadas sobre la base, que provocan la modificación del campo dispersado al ser modificado su potencial eléctrico con respecto a un voltaje de referencia.

6. Procedimiento de entrenamiento e identificación de tarjetas sin contacto por caracterización en radiofrecuencia, que hace uso del dispositivo descrito en cualquiera de las reivindicaciones 1 a 5, caracterizado por que comprende las etapas de:

- entrenamiento para someter a la tarjeta a todas las configuraciones posibles del elemento dispersor (4) reconfigurable y registrar sus respuestas,
- ejecución de un protocolo desafío-respuesta en el que mediante el elemento dispersor (4) reconfigurable se modifica el campo electromagnético dispersado de forma que cada tarjeta puede identificarse por el campo que dispersa como respuesta,
- clasificación de tarjetas, para evaluar si la tarjeta leída está registrada o se trata de una tarjeta fraudulenta, mediante un algoritmo de clasificación.

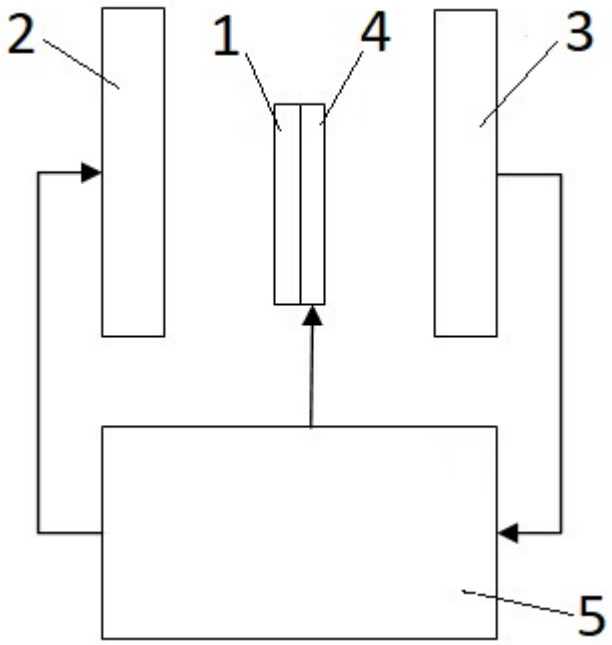

FIG.1

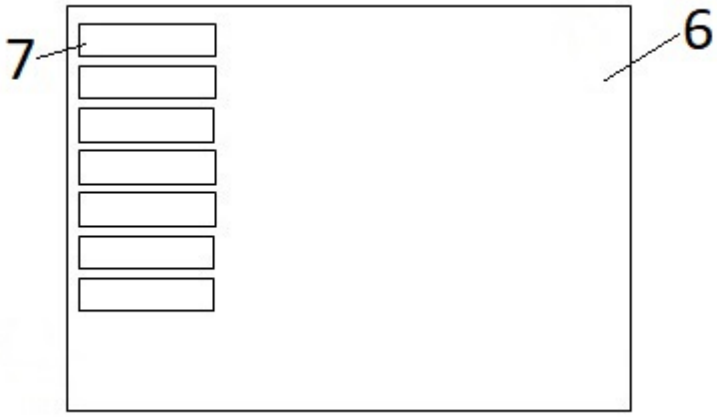

FIG. 2

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 201930266

(22) Fecha de presentación de la solicitud: 25.03.2019

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl. :** ***G07F7/12*** (2006.01)

DOCUMENTOS RELEVANTES

Categoría	(56) **Documentos citados**	**Reivindicaciones afectadas**
A	JP H0916834 A (NHK SPRING CO LTD) 17/01/1997, Resumen de la base de datos EPODOC. Recuperado de EPOQUE resumen; figuras.	1-6
A	EP 2693685 A1 (UNIV TWENTE et al.) 05/02/2014, Párrafos [0011] - [0071]; figuras 1-6.	1-6
A	WO 2007046018 A1 (KONINKL PHILIPS ELECTRONICS NV et al.) 26/04/2007, Página 2, línea 27 a página 10, línea 26; figuras 1-3.	1-6

Categoría de los documentos citados

X: de particular relevancia
Y: de particular relevancia combinado con otro/s de la misma categoría
A: refleja el estado de la técnica
O: referido a divulgación no escrita
P: publicado entre la fecha de prioridad y la de presentación de la solicitud
E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	**Examinador**	**Página**
16.01.2020	J. Botella Maldonado	1/2

Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)

G07F

Bases de datos electrónicas consultadas durante la búsqueda (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

INVENES, EPODOC, WPI, NPL, XPESP, XPAIP, XPI3E, INSPEC.