ROYAUME DU MAROC

OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
---

(19)

المملكة المغربية
المكتب المغربي للملكية الصناعية و التجارية

(12) BREVET D'INVENTION

(11) N° de publication :
MA 67277 B1

(51) Cl. internationale :
B42D 25/305

(43) Date de publication :
29.11.2024

(21) N° Dépôt :
67277

(22) Date de Dépôt :
30.08.2021

(30) Données de Priorité :
02.09.2020 EP 20200194057

(86) Données relatives à la demande internationale selon le PCT:
PCT/EP2021/073864 30.08.2021

(71) Demandeur(s) :
SICPA HOLDING SA, Avenue de Florissant 41 1008 Prilly (CH)

(72) Inventeur(s) :
CALLEGARI, Andrea ; LOGINOV, Evgeny ; DORIER, Jean-Luc ; DINOEV, Todor ; RAEMY, Xavier Cédric ; CARNERO, Benito

(74) Mandataire :
CABINET DIANI

(86) N° de dépôt auprès de l'organisme de validation :21769961.0

(54) Titre : **MARQUAGE DE SÉCURITÉ, PROCÉDÉ ET DISPOSITIF DE LECTURE DE MARQUAGE DE SÉCURITÉ, DOCUMENT DE SÉCURITÉ MARQUÉ AVEC LE MARQUAGE DE SÉCURITÉ, ET PROCÉDÉ ET SYSTÈME PERMETTANT DE VÉRIFIER LEDIT DOCUMENT DE SÉCURITÉ**

(57) Abrégé : La présente invention concerne un marquage de sécurité (100), un procédé et un dispositif de lecture et de décodage du marquage de sécurité (100), un document de sécurité (150) marqué avec le marquage de sécurité (100), et un procédé et un système de vérification et d'authentification dudit document de sécurité (150). Le marquage de sécurité (100) comprend un marquage lisible par machine (130) se chevauchant avec une couche magnétiquement induite (120) d'un matériau comprenant des particules de pigment magnétiques ou magnétisables en forme de plaquettes réfléchissantes orientées magnétiquement avec deux zones (120a) et (120b) d'orientations distinctes des particules. Les données codées sur le marquage lisible par machine (130) peuvent être décodables uniquement après que les données lues séparément sur les deux zones (120a) et (120b) sont rassemblées.

REVENDICATIONS

1. Marquage de sécurité (100) comprenant :

un substrat plat (110) ;

une couche induite magnétiquement (120) d'un matériau comprenant des particules de pigment magnétiques ou magnétisables en forme de plaquettes réfléchissantes orientées magnétiquement, la couche induite magnétiquement étant appliquée sur le substrat (110), caractérisé en ce que la couche induite magnétiquement comprend une première zone (120a) dans laquelle lesdites particules de pigment magnétiques ou magnétisables en forme de plaquettes réfléchissantes orientées magnétiquement ont leurs faces planaires orientées dans une première direction et une seconde zone (120b), distincte de la première zone (120a), dans laquelle lesdites particules de pigment magnétiques ou magnétisables en forme de plaquettes réfléchissantes orientées magnétiquement ont leurs faces planaires orientées dans une seconde direction distincte de la première direction, les particules en forme de plaquettes dans la première zone (120a) ayant des faces planaires présentant un angle d'élévation γ_1 par rapport à un plan du substrat (110) et les particules en forme de plaquettes dans la seconde zone (120b) ayant des faces planaires présentant un angle d'élévation γ_2 par rapport au plan du substrat (110), chaque angle aigu des faces planaires par rapport au plan du substrat étant dans une plage d'environ 5° à environ 25° ;

un marquage lisible par une machine (130) comprenant un motif de référence (133) et un motif de code (134) représentant des données codées, le marquage lisible par une machine (130) étant respectivement appliqué soit sur une face supérieure (121) de la couche induite magnétiquement (120) soit sur le substrat (110) entre ledit substrat et une face arrière (122) de la couche induite magnétiquement (120), une première aire (134a) du motif de

code (134) étant disposée devant la première zone (120a) et une seconde aire (134b) restante du motif de code (134) étant disposée devant la seconde zone (120b).

2. Marquage de sécurité selon la revendication 1, dans laquelle
a) lesdites particules de pigment comprennent :
un métal magnétique choisi dans le groupe constitué du cobalt, du fer, du gadolinium et du nickel ;
un alliage magnétique de fer, de chrome, de manganèse, de cobalt, de nickel ou d'un mélange de deux ou plus de ceux-ci ;
un oxyde magnétique de chrome, de manganèse, de cobalt, de fer, de nickel ou d'un mélange de deux ou plus de ceux-ci ; ou
un mélange de deux ou plus de ceux-ci ; ou
b) le motif de code est l'un quelconque d'un code à barres unidimensionnel, d'un code à barres unidimensionnel empilé, d'un code à barres bidimensionnel et d'un code à barres tridimensionnel.

3. Marquage de sécurité selon l'une quelconque des revendications 1 et 2, dans lequel la première zone (120a) et la seconde zone (120b) de la couche induite magnétiquement (120) appartiennent à une même couche unique de matériau.

4. Marquage de sécurité selon l'une quelconque des revendications 1 et 2, dans lequel la première zone (120a) et la seconde zone (120b) de la couche induite magnétiquement (120) appartiennent respectivement à une première sous-couche et à une seconde sous-couche adjacente formant la couche induite magnétiquement (120).

5. Marquage de sécurité selon l'une quelconque des revendications 1 à 4, dans lequel le marquage lisible par une

machine (130) est appliqué sur la face supérieure (121) de la couche induite magnétiquement (120) et codé avec des symboles sombres et une couche primaire sombre (140) est appliquée sur le substrat (110), et la face arrière (122) de la couche induite magnétiquement (120) est appliquée sur une face supérieure (141) de la couche primaire sombre (140).

6. Marquage de sécurité selon l'une quelconque des revendications 1 à 4, dans lequel le marquage lisible par une machine (130) est appliqué sur la face supérieure (121) de la couche induite magnétiquement (120) et codé avec des symboles lumineux et une couche primaire sombre (140), de préférence une primaire noire, est appliquée sur le substrat (110), et la face arrière (122) de la couche induite magnétiquement (120) est appliquée sur une face supérieure (141) de la couche primaire sombre (140).

7. Marquage de sécurité selon l'une quelconque des revendications 1 à 4, dans lequel le marquage lisible par une machine (130) est appliqué sur le substrat (110) et codé avec des symboles sombres.

8. Procédé de lecture et de décodage du marquage de sécurité (100) selon l'une quelconque des revendications 1 à 7, avec un dispositif portable (200) équipé d'une source de lumière (201) servant à délivrer une lumière d'éclairage, d'un imageur (202), et d'un processeur équipé d'une mémoire et adapté pour effectuer des opérations de traitement d'image et de décodage, comprenant les étapes suivantes :

disposition du marquage de sécurité (100) à l'intérieur d'un champ de vision de l'imageur (202) ;

éclairage du marquage de sécurité (100) avec une lumière d'éclairage délivrée par la source de lumière (201) ;

acquisition d'une première image numérique du marquage de sécurité (100) avec l'imageur (202) à un premier angle de visualisation θ_1 associé au premier angle d'élévation γ_1, et stockage de la première image numérique acquise dans la mémoire ;

acquisition d'une seconde image numérique du marquage de sécurité (100) avec l'imageur à un second angle de visualisation θ_2 associé au second angle d'élévation γ_2, et stockage de la seconde image numérique acquise dans la mémoire ;

formation, par l'intermédiaire d'un traitement d'image avec le processeur, d'une image numérique composite du motif de code (134) à partir de la première image numérique stockée et de la seconde image numérique stockée par alignement par rapport au motif de référence (133), détecté dans la première image numérique et la seconde image numérique, d'une première partie du motif de code (134) correspondant à la première aire (134a) du motif de code détecté sur la première image numérique et d'une seconde partie du motif de code (134) correspondant à la seconde aire (134b) du motif de code détecté sur la seconde image numérique, et stockage de l'image numérique composite obtenue dans la mémoire ;

lecture et décodage avec le processeur du motif de code (134) à partir de l'image numérique composite stockée.

9. Dispositif portable (200) de lecture et de décodage du marquage de sécurité (100) selon l'une quelconque des revendications 1 à 7, comprenant :

une source de lumière (201) servant à délivrer une lumière d'éclairage ;

un imageur (202) ; et

un processeur équipé d'une mémoire,

caractérisé en ce que le dispositif portable est adapté pour réaliser les étapes suivantes :

éclairage du marquage de sécurité (100) avec une lumière d'éclairage délivrée par la source de lumière (201) ;

acquisition d'une première image numérique du marquage de sécurité (100) avec l'imageur (202) à un premier angle de visualisation θ_1 associé au premier angle d'élévation γ_1, et stockage de la première image numérique acquise dans la mémoire ;

acquisition d'une seconde image numérique du marquage de sécurité (100) avec l'imageur à un second angle de visualisation θ_2 associé au second angle d'élévation γ_2, et stockage de la seconde image numérique acquise dans la mémoire ;

formation, par l'intermédiaire d'un traitement d'image avec le processeur, d'une image numérique composite du motif de code (134) à partir de la première image numérique stockée et de la seconde image numérique stockée par alignement par rapport au motif de référence (133), détecté dans la première image numérique et la seconde image numérique, d'une première partie du motif de code (134) correspondant à la première aire (134a) du motif de code détecté sur la première image numérique et d'une seconde partie du motif de code (134) correspondant à la seconde aire (134b) du motif de code détecté sur la seconde image numérique, et stockage de l'image numérique composite obtenue dans la mémoire ;

lecture et décodage avec le processeur du motif de code (134) à partir de l'image numérique composite stockée.

10. Document de sécurité (150) délivré par une autorité à un utilisateur, caractérisé en ce qu'il comprend :

un marquage de sécurité (100) selon l'une quelconque des revendications 1 à 7 appliqué sur le document de sécurité (150), dans lequel des données codées dans le motif de code (134) du marquage de sécurité (100) contiennent des données numériques

d'identité correspondant à l'utilisateur et une signature numérique desdites données numériques d'identité de l'utilisateur, la signature numérique délivrée par l'autorité étant obtenue par signature des données numériques d'identité de l'utilisateur avec une clé cryptographique.

11. Procédé de vérification d'un document de sécurité (150) d'un utilisateur selon la revendication 10, avec un dispositif portable (200) selon la revendication 9 en outre équipé d'une unité de communication servant à envoyer et recevoir des données sur le réseau de communication (CN) à un serveur (S) de l'autorité connecté à une base de données (DB) stockant la clé cryptographique et une clé de déchiffrement correspondante, comprenant les étapes suivantes :

disposition du marquage de sécurité (100) à l'intérieur d'un champ de vision de l'imageur (202) ;

éclairage du marquage de sécurité (100) du document de sécurité (150) avec la source de lumière (201) ;

acquisition d'une première image numérique du marquage de sécurité (100) éclairé avec l'imageur (202) à un premier angle de visualisation θ_1 associé au premier angle d'élévation γ_1, et stockage de la première image numérique acquise dans la mémoire ;

acquisition d'une seconde image numérique du marquage de sécurité (100) éclairé avec l'imageur (202) à un second angle de visualisation θ_2 associé au second angle d'élévation γ_2, et stockage de la seconde image numérique acquise dans la mémoire ;

formation, par l'intermédiaire d'un traitement d'image avec le processeur, d'une image numérique composite du motif de code (134) à partir de la première image numérique stockée et de la seconde image numérique stockée par alignement par rapport au motif de référence (133), détecté dans la première image numérique et la seconde image numérique, d'une première partie du motif de code

(134) correspondant à la première aire (134a) du motif de code détecté sur la première image numérique et d'une seconde partie du motif de code (134) correspondant à la seconde aire (134b) du motif de code détecté sur la seconde image numérique ;

lecture et décodage du motif de code (134) à partir de l'image numérique composite, et extraction à partir de données décodées du motif de code de données d'identité d'un utilisateur et d'une signature numérique desdites données d'identité de l'utilisateur, par l'intermédiaire d'opérations de traitement d'image et de décodage avec le processeur, et stockage des données d'identité et de la signature numérique extraites de l'utilisateur dans la mémoire ;

envoi d'un premier message (M1) contenant les données d'identité et la signature numérique extraites de l'utilisateur stockées dans la mémoire par l'intermédiaire de l'unité de communication (CN) au serveur (S) ;

déchiffrement au niveau du serveur (S) de la signature numérique extraite reçue dans le premier message (M1) à partir du dispositif portable (200) avec la clé de déchiffrement stockée dans la base de données (DB), et fait de contrôler si les données d'identité extraites de l'utilisateur reçues dans le premier message (M1) correspondent à la signature numérique reçue extraite ; et

en cas de correspondance, renvoi au dispositif portable (200) d'un message de serveur (SM) indiquant une vérification réussie des données d'identité de l'utilisateur.

12. Procédé selon la revendication 11, comprenant, avant l'étape de renvoi d'un message de serveur au dispositif portable (200), les étapes préliminaires de :

éclairage de la couche induite magnétiquement (120) avec la source de lumière (201) et acquisition d'une pluralité d'images

numériques de la couche induite magnétiquement (120) éclairée avec l'imageur (202), l'imageur (202) étant pour chaque image numérique différente à un angle de visualisation θ distinct correspondant par rapport à ladite couche induite magnétiquement (120), par déplacement de l'imageur (202) relativement à la couche induite magnétiquement (120) parallèlement au plan du substrat (110) ;

pour chaque image numérique acquise, calcul, avec le processeur, respectivement de l'intensité I correspondante de la lumière réfléchie par la couche induite magnétiquement (120) et collectée par l'imageur (202) à un angle de visualisation θ correspondant, et stockage des intensités calculées de la lumière réfléchie et des angles de visualisation correspondants pour obtenir une courbe d'intensité de la lumière réfléchie I(θ) correspondante ;

envoi avec l'unité de communication d'un second message (M2) au serveur (S) par l'intermédiaire du réseau de communication (CN) contenant la courbe d'intensité de la lumière réfléchie I(θ) obtenue ;

comparaison au niveau du serveur (S) de la courbe d'intensité de la lumière réfléchie I(θ) reçue dans le second message (M2) avec une courbe d'intensité de la lumière réfléchie de référence $I_{ref}(\theta)$ pour ladite couche induite magnétiquement (120) stockée dans la base de données (DB) ;

fait de déterminer au niveau du serveur (S) si la couche induite magnétiquement (120) est authentique sur la base d'un résultat de la comparaison ; et

dans le cas où la couche induite magnétiquement (120) est déterminée comme étant authentique, renvoi au dispositif portable (200) du message de serveur (SM) indiquant une vérification réussie des données d'identité de l'utilisateur conjointement avec une indication que le marquage de sécurité (100) est authentique, et envoi par le serveur (S) par l'intermédiaire du réseau de

communication (CN) d'un message d'autorisation de serveur (SAM) à un dispositif de communication de l'utilisateur contenant des données d'accès accordant à l'utilisateur un accès à un service.

13. Procédé selon la revendication 11, comprenant, dans le cas d'une délivrance par le serveur (S) d'un message de serveur (SM) indiquant une vérification réussie des données d'identité de l'utilisateur, les étapes supplémentaires de :

éclairage de la couche induite magnétiquement (120) avec la source de lumière (201) et acquisition d'une pluralité d'images numériques de la couche induite magnétiquement (120) éclairée avec l'imageur (202), l'imageur (202) étant pour chaque image numérique différente à un angle de visualisation θ distinct correspondant par rapport à ladite couche induite magnétiquement (120), par déplacement de l'imageur (202) relativement à la couche induite magnétiquement (120) parallèlement au plan du substrat (110) ;

pour chaque image numérique acquise, calcul, avec le processeur, respectivement de l'intensité I correspondante de la lumière réfléchie par la couche induite magnétiquement (120) et collectée par l'imageur (202) à un angle de visualisation θ correspondant, et détermination avec les intensités calculées de la lumière réfléchie et des angles de visualisation correspondants d'une courbe d'intensité de la lumière réfléchie I(θ) correspondante ;

comparaison par l'intermédiaire du processeur de la courbe d'intensité de la lumière réfléchie I(θ) avec une courbe d'intensité de la lumière réfléchie de référence $I_{ref}(\theta)$ pour ladite couche induite magnétiquement (120) stockée dans la mémoire ;

fait de déterminer si la couche induite magnétiquement (120) est authentique sur la base d'un résultat de la comparaison, et, dans le cas où la couche induite magnétiquement (120) est

déterminée comme étant authentique, envoi au serveur (S), avec l'unité de communication par l'intermédiaire du réseau de communication (CN), d'un message (M) indiquant que le marquage de sécurité (100) est authentique ; et

en cas de réception au niveau du serveur (S) d'un message (M) à partir du dispositif portable (200) indiquant que le marquage de sécurité (100) est authentique, renvoi par le serveur (S) par l'intermédiaire du réseau de communication (CN) d'un message d'autorisation de serveur (SAM) à un dispositif de communication de l'utilisateur contenant des données d'accès accordant à l'utilisateur un accès à un service.

14. Système de vérification d'un document de sécurité (150) selon la revendication 10 délivré par une autorité à un utilisateur, comprenant :

un serveur (S) de l'autorité connecté à une base de données (DB) stockant la clé cryptographique et une clé de déchiffrement correspondante, et servant à envoyer et recevoir des données par l'intermédiaire d'un réseau de communication (CN) ; et

un dispositif portable (200) selon la revendication 9 pour la lecture et le décodage d'un marquage de sécurité (100) selon l'une quelconque des revendications 1 à 7 appliqué sur le document de sécurité (150), comprenant :

une source de lumière (201) servant à délivrer une lumière d'éclairage ;

un imageur (202) ;

une unité de communication servant à envoyer et recevoir des données sur le réseau de communication (CN) au serveur (S) ; et

un processeur équipé d'une mémoire et adapté pour effectuer des opérations de traitement d'image et de décodage, et adapté pour réaliser les étapes suivantes :

éclairage du marquage de sécurité (100) avec une lumière d'éclairage délivrée par la source de lumière (201) ;

acquisition d'une première image numérique du marquage de sécurité (100) avec l'imageur (202) à un premier angle de visualisation θ_1 associé au premier angle d'élévation γ_1, et stockage de la première image numérique acquise dans la mémoire ;

acquisition d'une seconde image numérique du marquage de sécurité (100) avec l'imageur à un second angle de visualisation θ_2 associé au second angle d'élévation γ_2, et stockage de la seconde image numérique acquise dans la mémoire ;

formation, par l'intermédiaire d'un traitement d'image avec le processeur, d'une image numérique composite du motif de code (134) à partir de la première image numérique stockée et de la seconde image numérique stockée par alignement par rapport au motif de référence (133), détecté dans la première image numérique et la seconde image numérique, d'une première partie du motif de code (134) correspondant à la première aire (134a) du motif de code détecté sur la première image numérique et d'une seconde partie du motif de code (134) correspondant à la seconde aire (134b) du motif de code détecté sur la seconde image numérique, et stockage de l'image numérique composite obtenue dans la mémoire ;

lecture et décodage avec le processeur du motif de code (134) à partir de l'image numérique composite stockée ;

dans lequel le système est en outre adapté pour réaliser les étapes suivantes :

extraction à partir de données décodées du motif de code de données d'identité d'un utilisateur et d'une signature numérique desdites données d'identité de l'utilisateur, par l'intermédiaire d'opérations de traitement d'image et de décodage avec le processeur, et stockage des données d'identité et de la signature numérique extraites de l'utilisateur dans la mémoire ;

envoi d'un premier message (M1) contenant les données d'identité et la signature numérique extraites de l'utilisateur stockées dans la mémoire par l'intermédiaire de l'unité de communication (CN) au serveur (S) ;

déchiffrement au niveau du serveur (S) de la signature numérique extraite reçue dans le premier message (M1) à partir du dispositif portable (200) avec la clé de déchiffrement stockée dans la base de données (DB), et fait de contrôler si les données d'identité extraites de l'utilisateur reçues dans le premier message (M1) correspondent à la signature numérique reçue extraite ; et

en cas de correspondance, renvoi au dispositif portable (200) d'un message de serveur (SM) indiquant une vérification réussie des données d'identité de l'utilisateur.

15. Système selon la revendication 14, dans lequel

le serveur (S) est en outre adapté pour envoyer des données par l'intermédiaire du réseau de communication (CN) à un dispositif de communication de l'utilisateur ; et

le serveur (S) et le dispositif portable (200) sont en outre adaptés pour réaliser les étapes du procédé selon l'une quelconque des revendications 12 et 13 de vérification du document de sécurité (150) de l'utilisateur.