(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 955 288**

(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **10 00176**

(51) Int Cl[8] : ***B 42 D 15/10*** *(2006.01), G 07 D 7/20, G 06 K 19/04*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 18.01.10.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 22.07.11 Bulletin 11/29.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *HOLOGRAM INDUSTRIES Société anonyme* — FR.

(72) **Inventeur(s) :** SOUPARIS HUGUES et LE LIBOUX KRISTEN.

(73) **Titulaire(s) :** HOLOGRAM INDUSTRIES Société anonyme.

(74) **Mandataire(s) :** NOVAGRAAF TECHNOLOGIES.

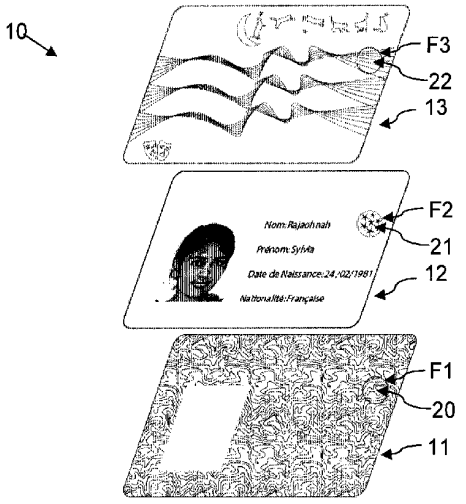
(54) PROCEDE DE SECURISATION D'UN OBJET, ET OBJET CORRESPONDANT.

(57) L'invention concerne notamment un procédé de sécurisation d'un objet comprenant des étapes consistant à:

- créer une signature graphique multicouche (23), par superposition en transparence partielle ou totale d'un premier élément graphique (20) aléatoire sur une première couche (11) à un deuxième élément graphique (21) sur une deuxième couche (12), et
- stocker ladite signature graphique sur ou dans l'objet (10).

Le procédé selon l'invention est essentiellement caractérisé en ce que:

- la position relative du premier élément graphique (20) et du deuxième élément graphique (21) est aléatoire.



FR 2 955 288 - A1

PROCEDE DE SECURISATION D'UN OBJET, ET OBJET CORRESPONDANT.

La présente invention concerne le domaine de la sécurisation d'objets, incluant éventuellement la vérification, l'authentification de ceux-ci.

Plus précisément, l'invention concerne selon un premier de ses objets, un procédé de sécurisation d'un objet comprenant des étapes consistant à :

- créer une signature graphique multicouche, par superposition en transparence partielle ou totale d'un premier élément graphique sur une première couche et d'un deuxième élément graphique sur une deuxième couche, dont au moins élément graphique comprend un élément graphique aléatoire, et
- stocker ladite signature graphique sur ou dans l'objet.

Selon l'invention, le procédé est essentiellement caractérisé en ce que :

- la position relative du premier élément graphique et du deuxième élément graphique est aléatoire.

Grâce à cette caractéristique, la signature graphique est unique.

De préférence, la création de la signature graphique multicouches comprend en outre la superposition en transparence partielle ou totale d'un troisième élément graphique sur une troisième couche, distincte des première et deuxième couche, la position relative dudit troisième élément graphique et dudit premier élément graphique et/ou dudit deuxième élément graphique étant aléatoire, ledit troisième élément graphique pouvant comprendre un élément graphique aléatoire.

Grâce à cette caractéristique, l'objet portant la signature graphique est très sécurisé.

La signature graphique multicouche selon l'invention comprend donc par superposition au moins deux éléments graphiques. Chaque élément graphique comprend par exemple au moins l'un des éléments suivants :

un ensemble de lignes ou points,

un ensemble de dessins, armoiries, logos,

un ensemble d'images en couleurs / niveaux de gris,

un ensemble d'effets holographiques,

un ensemble d'effets de dé-métallisation.

Dans un mode de réalisation, l'étape de stockage comprend une étape consistant à apposer ladite signature graphique multicouche sur ledit objet, ou à intégrer ladite signature graphique multicouche audit objet. Ceci permet de sécuriser l'objet : dans la masse de celui-ci lors de sa fabrication, par apposition par exemple sous forme d'étiquette, ou encore en utilisant également son emballage.

Par exemple dans un mode de réalisation, ledit objet est un objet multicouches, l'intégration de ladite signature graphique multicouches audit objet étant effectuée dans l'une au moins des couches dudit objet.

Dans un mode de réalisation, chaque couche de la signature est une couche respective dudit objet.

De préférence, le procédé comprend en outre des étapes consistant à :

- réaliser une première prise de vue de la signature graphique multicouche,
- calculer une première signature numérique de ladite prise de vue et enregistrer ladite signature numérique dans une

base de données, de sorte à constituer une partie au moins d'une signature numérique de référence, et

- enregistrer dans ladite base de données un identifiant numérique ou alpha-numérique, associé à ladite première signature numérique.

L'identifiant numérique ou alpha-numérique peut être dépendant ou indépendant de l'objet ou de la signature. L'identifiant numérique ou alpha-numérique permet d'indexer la signature numérique. A cet effet il peut être un index, un numéro d'enregistrement séquentiel, ou correspondre à au moins un élément distinctif ou nominatif de l'objet.

Ceci permet la vérification ultérieure de l'authenticité de l'objet.

De préférence, la réalisation de la première prise de vue de la signature graphique multicouche est effectuée lors de la fabrication de l'objet, par exemple grâce à un capteur CCD, de sorte que la signature numérique de référence soit créée à partir de la première prise de vue avant la mise dans le commerce de l'objet.

De préférence, le procédé comprend en outre des étapes consistant à :

- créer un identifiant graphique, optionnellement multicouche, à partir d'une prise de vue de l'ensemble superposé desdits premier et deuxième éléments graphiques, et dudit troisième élément graphique lorsqu'il existe ; et/ou à partir dudit au moins un élément distinctif ou nominatif de l'objet, et
- stocker ledit identifiant graphique sur ou dans l'objet, optionnellement sur l'une des couches de ladite signature multicouche.

Ceci permet de sécuriser à nouveau l'objet, et de faciliter le traitement de sa vérification. Par exemple l'identifiant graphique est un datamatrix.

Dans un mode de réalisation, ledit identifiant graphique est imprimé sur l'une des couches de ladite signature multicouche.

De préférence, le procédé comprend en outre des étapes consistant à :

- réaliser une deuxième prise de vue numérique de la signature graphique multicouche de l'objet,
- calculer une deuxième signature numérique de ladite prise de vue,
- comparer la première et la deuxième signature numérique, et
- authentifier ou non la signature graphique en fonction du résultat de la comparaison.

De préférence, la deuxième prise de vue numérique de la signature graphique multicouche est réalisée après la fabrication de l'objet, de sorte que la deuxième signature numérique est créée après la mise dans le commerce de l'objet.

De préférence, la comparaison de la première et de la deuxième signature numérique comprend des étapes consistant à :

- lire l'identifiant graphique,
- en extraire l'identifiant numérique correspondant, et
- sélectionner la signature numérique de référence associée.

Ceci permet d'augmenter la vitesse de traitement, donc de faciliter la vérification de l'authenticité de l'objet.

Avantageusement, le procédé comprend en outre une étape de détermination du type de signature/d'objet.

L'invention concerne également un programme d'ordinateur, comprenant des instructions de code de programme pour

l'exécution des étapes d'un procédé tel que défini ci-avant lorsque ledit programme est exécuté sur un ordinateur.

Selon un autre de ses objets, l'invention concerne un objet sécurisé, comprenant :

- une signature graphique multicouche, par superposition en transparence partielle ou totale d'un premier élément graphique aléatoire sur une première couche et d'un deuxième élément graphique sur une deuxième couche, stockée sur ou dans ledit objet, de préférence dont au moins élément graphique comprend un élément graphique aléatoire.

Selon l'invention, l'objet est essentiellement caractérisé en ce que la position relative du premier élément graphique et du deuxième élément graphique est aléatoire.

De préférence, l'objet comprend en outre un troisième élément graphique pouvant comprendre un élément graphique aléatoire sur une troisième couche, distincte des première et deuxième couche, et dans lequel la position relative dudit troisième élément graphique et dudit premier élément graphique et/ou dudit deuxième élément graphique est aléatoire.

Dans un mode de réalisation, l'objet comprend en outre un identifiant graphique, optionnellement multicouche, à partir d'une prise de vue de l'ensemble superposé desdits premier et deuxième éléments graphiques, et dudit troisième élément graphique lorsqu'il existe ; et/ou à partir dudit au moins un élément distinctif ou nominatif de l'objet. L'identifiant graphique permet de désigner de manière univoque l'objet sécurisé dans une base de données grâce à son identifiant numérique correspondant, en vue de l'authentification dudit objet.

Avantageusement, ledit identifiant graphique est imprimé sur l'une des couches de ladite de signature multicouche, de préférence sous forme de datamatrix.

Dans un mode de réalisation, ledit objet est un objet multicouches, dont l'une des couches supporte ou contient le premier élément graphique, une autre couche supporte ou contient le deuxième élément graphique, et éventuellement une autre couche encore supporte ou contient, lorsqu'il existe, le troisième élément graphique.

Dans un mode de réalisation, l'objet et la signature graphique comprennent le même nombre de couches, de sorte que chaque couche de la signature est une couche respective dudit objet.

Dans un mode de réalisation, l'objet comprend en outre un emballage, dont la ou l'une des couches est la première, deuxième, ou troisième couche lorsqu'elle existe.

L'invention assure l'unicité et la non reproductibilité de la signature, donc de la sécurité de l'objet. En effet, s'il est théoriquement possible de régénérer informatiquement le même code (même(s) élément(s) graphique(s)) et de le réimprimer sur un objet, à cause des tolérances mécaniques des processus mis en œuvre, cet(s) élément(s) graphique(s) ne sera(ont) jamais situé(s) exactement à la même place, ce qui rend en pratique la reproduction de la signature quasiment impossible.

L'invention présente également l'avantage que l'association de la signature à l'objet peut ne pas nécessiter l'emploi de matériaux exogènes audit objet. Sa longévité est donc la même qu'un objet auquel n'est pas associé de telle signature.

D'autres caractéristiques et avantages de la présente invention apparaîtront plus clairement à la lecture de la

description suivante donnée à titre d'exemple illustratif et non limitatif et faite en référence aux figures annexées dans lesquelles :

- la figure 1 illustre une vue éclatée d'un mode de réalisation d'un objet de type carte d'identité selon l'invention,
- la figure 2A illustre un mode de réalisation d'une signature graphique selon l'invention,
- la figure 2B illustre un mode de réalisation d'un objet comprenant une signature graphique et un identifiant graphique selon l'invention,
- la figure 2C illustre en gros plan un mode de réalisation d'une signature graphique et d'un identifiant graphique selon l'invention,
- les figures 3A à 3H illustrent des modes de réalisation d'éléments graphiques aléatoires selon l'invention,
- la figure 4 illustre un mode de réalisation du procédé selon l'invention, et
- la figure 5 illustre un mode de réalisation d'une signature graphique selon l'invention, en vue de l'authentification de l'objet.

Pour plus de clarté de la présente description, on décrira essentiellement le mode de réalisation dans lequel l'objet 10 à sécuriser est un objet multicouche, en l'espèce un document, document officiel (carte) d'identité par exemple, dans lequel la signature multicouche 23 selon l'invention est intégrée.

L'homme du métier transposera ce mode de réalisation à d'autres objets multicouche à couches partielles, dans lesquels la signature graphique multicouche selon l'invention est réalisée sur au moins l'une des couches partielles ; et/ou encore à des objets comprenant un emballage dans lesquels l'emballage constitue l'une au moins des couches.

Par couche partielle on entend une couche dont la surface est inférieure à la surface de l'objet sur laquelle celle-ci est superposée, par exemple une étiquette.

Dans le cas d'un document ou d'une carte multicouche, l'objet 10 comprend typiquement une première couche 11, dite couche de base, sur laquelle est imprimée un premier graphisme, par exemple sous forme de guilloches (figure 1). Pour une carte d'identité par exemple, la carte consiste en un assemblage de plusieurs couches produites de manière indépendantes. La première couche est en général imprimée en offset, en sérigraphie ou autres techniques d'impression utilisées pour la réalisation de graphismes de sécurité. Lors de la fabrication, les couches indépendantes sont assemblées par planches comportant par exemple 24 ou 48 cartes et chaque carte est ensuite découpée individuellement.

Sur la première couche 11 est apposée une deuxième couche 12, par exemple en polycarbonate, par exemple personnalisable par marquage laser, dans laquelle est imprimé un deuxième graphisme, différent du premier graphisme. Dans le cas de carte d'identité, le deuxième graphisme est imprimé lors de l'étape de personnalisation de la carte, une fois la carte assemblée.

Dans un mode de réalisation, sur cette deuxième couche est apposée une troisième couche 13, servant éventuellement de protection, sur laquelle peut être inscrit ou imprimé un troisième graphisme, en l'espèce un élément optiquement variable. Par optiquement variable, on entend un élément dont au moins un des ses aspects change lorsqu'il est soumis à un mouvement relatif par rapport à la ligne de visée d'un observateur (être humain, caméra).

Le mouvement relatif peut être un mouvement de translation, et/ou un mouvement de rotation, autour d'un axe horizontal (axe des X), d'un axe vertical (axe des Y), et/ou de rotation dans le plan de l'objet sécurisé (axe des Z).

Les changements d'aspects peuvent porter notamment sur tout ou partie des éléments suivants :

- changement de couleur en fonction de l'orientation,
- changement d'angles de vues d'un hologramme 3D
- déplacement d'un élément d'image
- changement d'aspect de l'image
- effacement d'une image et remplacement par une autre
- etc...

Selon l'invention, la signature graphique 23 est multicouche. Chaque élément graphique 20, 21, 22 de la signature graphique multicouche est compris dans une fenêtre graphique F1, F2, F3 respective, les formes et dimensions des fenêtres F1, F2, F3 étant de préférence identiques entre elles. Ainsi, la signature graphique au sens de la présente invention est la résultante graphique de la superposition desdites fenêtres, par transparence partielle ou totale d'un ensemble d'éléments graphiques répartis sur une pluralité de couches, comme illustré figure 2. Les fenêtres graphiques correspondent par exemple à tout ou partie d'une face de l'objet 10.

Pour simplifier la présente description, on ne décrira que le mode de réalisation dans lequel chaque couche comprend un élément graphique unique respectif.

On a donc au moins un premier élément 20 de signature graphique sur une première couche 11 et au moins un deuxième élément 21 de signature graphique sur une deuxième couche 12.

Le premier élément 20 de signature graphique peut être un élément de graphisme prédéterminé (image, logo ou autre) ou un élément graphique aléatoire.

Par élément graphique aléatoire, on entend, dans une fenêtre graphique donnée, un graphisme comprenant un ensemble d'au moins un élément, dont au moins l'une des caractéristiques suivantes de chaque élément est aléatoire :

- la forme,
- le motif,
- la(les) couleur(s), ou les niveaux de gris,
- la position dans la fenêtre graphique,
- la taille.

La population d'éléments uniques générés par l'algorithme utilisé pour la création de l'élément graphique aléatoire est de préférence supérieure au million.

L'objet analysé pour la vérification / authentification de la signature est le motif global obtenu par superposition des couches.

Or, le motif global est lui-même imprimé avec une tolérance de positionnement par rapport au(x) support(s) d'impression que représentant les couches, dont l'une au moins de préférence comporte au moins un élément fixe (non aléatoire) analysable.

Ainsi, la combinaison de l'aléa graphique généré par l'algorithme et de l'aléa de positionnement des fenêtres graphiques F1, F2, F3 (voir ci-après) assure une réelle source aléatoire dans le motif global à analyser, c'est-à-dire dans la signature graphique 23.

L'algorithme ci-dessous est un exemple basique de génération aléatoire, en l'espèce pseudo aléatoire.

1. Création d'une matrice radiale (figure 3A, 3B), circulaire (figure 3C, 3D), carrée ou rectangulaire (figure 3E, 3F), en nid d'abeille (figure 3G, 3H), ou de forme quelconque, maillée par une grille de forme prédéterminée : carrée, triangulaire, radiale, ou autre.

2. Détermination d'un nombre aléatoire N de motifs que comporte la signature graphique (par exemple généré par une fonction RAND() rapportée à un domaine allant typiquement de 10 à 30). A titre d'exemple purement illustratif, les motifs sont des polygones (figures 3B, 3D, 3F, 3H).

3. Détermination des emplacements des N motifs sur la grille définie par la matrice choisie la coordonnée de chaque motif M_i est donné par la formule :

$$(XM_i ; YM_i) = (RAND(1 ; X_{max}) ; RAND(1 ; Y_{max}))$$

Où X_{max} est la taille horizontale du tableau discret. Y_{max} la taille verticale.

Pour chaque motif Mi on peut déterminer une taille aléatoire comprise entre des bornes prédéfinies ($t_{min}<t_i<t_{max}$) et une orientation α sur la plage [0, 360°] ou sur une plage plus restreinte ($\alpha_{min}<\alpha_i<\alpha_{max}$).

Chaque motif aléatoire Mi est donc caractérisé notamment par son abscisse (Mi(xi)), son ordonnée (Mi(yi)) sur la grille, sa taille, et son orientation.

Un autre paramètre peut être la couleur du motif qui peut aussi être déterminée de façon aléatoire dans une palette de couleurs prédéfinies.

L'utilisation de cette diversité de paramètres permet d'augmenter le caractère aléatoire d'une fonction RAND() appliquée à un seul paramètre.

Dans le mode de réalisation illustré figure 1 ou figure 2, le premier élément 20 de signature graphique est un extrait du premier graphisme de la première couche 11 de l'objet, en l'espèce un extrait de guilloches, imprimé sur l'objet à sécuriser / authentifier.

Le deuxième élément graphique 21 de signature sur la deuxième couche peut également être un élément de graphisme prédéterminé (image, logo ou autre) ou un élément graphique aléatoire tel que décrit ci-dessus.

Pour des objets tels que les documents officiels (carte d'identité par exemple), il est classique que la deuxième couche 12 de l'objet comprenne des éléments distinctifs ou nominatifs de l'objet, en l'espèce des informations personnelles relatives au porteur de l'objet, par exemple le nom, prénom, date de naissance, etc.

Dans les cas où l'objet est équipé d'une puce électronique, celle-ci est munie d'un numéro de série pouvant servir d'élément distinctif ou nominatif de l'objet, la puce étant généralement insérée dans une autre couche (non illustrée) de l'objet 10.

Dans un mode de réalisation, l'objet comprend en outre un identifiant graphique 30, optionnellement multicouche, à partir d'une prise de vue de la signature graphique 23 ; et/ou à partir dudit au moins un élément distinctif ou nominatif de l'objet, par exemple l'identifiant graphique est généré par un moteur algorithmique à partir notamment des informations personnelles et/ou du numéro de puce.

De préférence, l'identifiant graphique 30 est créé lors de la personnalisation ou de la sérialisation de l'objet.

Pour des raisons de qualité notamment, lors de la réalisation de la signature par la superposition desdites fenêtres graphiques, il est souhaitable que l'erreur de position relative entre les fenêtres F1, F2, F3 soit la plus petite possible, c'est-à-dire inférieure à un seuil, par exemple pour donner une uniformité d'aspect à l'ensemble des objets produits.

Toutefois, les procédés de fabrication et/ou d'assemblage (superposition) desdites fenêtres impliquent des tolérances mécaniques inévitables dont il résulte une erreur aléatoire de position relative desdites fenêtres.

Contrairement à un *a priori* consistant à chercher à minimiser l'erreur, soit la valeur du seuil, l'invention utilise au contraire avantageusement l'erreur aléatoire de position relative.

En effet, la position relative du premier élément graphique 20 (par la première couche 11) et du deuxième élément graphique 21 (par la deuxième couche 12) étant aléatoire, la signature est donc unique.

De préférence, dans un mode de réalisation on prévoit en outre la superposition en transparence partielle ou totale d'un troisième élément graphique 22 sur une troisième couche 13, distincte des première et deuxième couche, où la position relative dudit troisième élément graphique et dudit premier élément graphique et/ou dudit deuxième élément graphique est aléatoire, pour les mêmes raisons.

Par exemple, le troisième élément graphique 22 est un hologramme porté par un laminat (couche laminaire), et appliqué après personnalisation de l'objet 10.

La signature multicouche 23 comprend donc en superposition totale ou partielle le premier 20, deuxième 21 et optionnellement troisième 22 élément graphique (figure 2A).

Pour la sécurisation de l'objet 10, on prévoit avantageusement de réaliser, de préférence à la création de l'objet 10 ou peu après celle-ci, une prise de vue de la signature graphique multicouche 23.

Cette prise de vue est par exemple enregistrée dans une base de données. A partir de cette prise de vue, on calcule une signature numérique, et on enregistre cette signature numérique dans une (éventuellement la même) base de données, de sorte à constituer une partie au moins d'une signature numérique de référence. De préférence, on utilise deux bases de données : une qui contient l'image de la prise de vue, et une qui contient la signature calculée, pour des raisons de place et de sécurité.

La signature numérique est calculée à partir de la prise de vue de la signature graphique de préférence par un algorithme spécifique faisant notamment appel au domaine du traitement d'images.

Dans un mode de réalisation, la prise de vue numérique est prétraitée afin d'en éliminer les bruits, redressée à partir d'un point de repère préétabli devant obligatoirement figurer sur l'une des couches de façon à corriger les effets éventuels de distorsion ou de rotation dus à la prise de vue, puis analysée pour produire des descripteurs qui constitueront ladite signature, ou empreinte numérique.

Par exemple, les descripteurs peuvent consister en tout ou partie des éléments suivants :

- les coordonnées exactes de certains éléments graphiques attendus sur l'image prétraitée,
- les moments mathématiques locaux ou globaux :
  - de l'image prétraitée (décrite en niveaux de gris ou en couleurs dans un espace de représentation particulier, par exemple tel que RGB ou HSV), ou
  - de l'image obtenue après extraction des contours de celle-ci, tels que les moments statistiques classiques (moyenne, variance, etc), les moments de Zernike, etc...
- d'autres descripteurs de forme calculés à partir de points stables de l'image tels que décrits dans la littérature

scientifique (SURF - Speeded Up Robust Features par exemple)

- d'autres descripteurs de couleurs ou de textures calculés localement ou globalement sur l'image prétraitée, tels que des histogrammes de couleurs ou des descripteurs dérivés de l'utilisation des filtres de Gabor,
- etc...

Une fois la signature calculée, on associe alors un identifiant numérique audit enregistrement de la signature numérique, de sorte à faciliter les recherches ultérieures, par indexation.

L'identifiant numérique peut être un index, ou correspondre à au moins un élément distinctif ou nominatif de l'objet, par exemple un numéro de série, le nom et/ou prénom du porteur de l'objet 10, etc.

L'identifiant numérique est stocké à distance sur le même serveur (base) de données que la signature de référence, accessible de préférence de manière sécurisée, éventuellement via l'Internet.

L'identifiant numérique permet d'indexer la signature graphique. Dans un mode de réalisation, l'identifiant numérique est une fonction, par exemple de hachage, de l'image numérique de la signature graphique 23.

L'identifiant graphique 30, quant à lui, est un code graphique unique, généré par logiciel. Il correspond typiquement à un numéro de série unique. Généralement il s'agit du numéro du document, ce numéro servant à nommer et indexer le fichier de signature correspondant *a posteriori*. Il peut en outre porter des informations relatives à la biographie du titulaire de l'objet : par exemple les lignes de la zone dite MRZ (Machine

Readable Zone) pour une carte d'identité ou un passeport, située au verso de l'objet.

On peut ainsi coder sur le recto d'un objet des informations situées sur le verso (ou une autre face pour des objets non plans), ce qui permet de ne pas avoir à manipuler l'objet ultérieurement pour des phases de vérification / authentification notamment, donc faciliter le traitement et d'augmenter grandement la vitesse de traitement de l'objet.

De préférence, l'identifiant graphique 30 est imprimable et codé sous forme de symbole code-barres bidimensionnel. En l'espèce, l'identifiant numérique 30 est un Datamatrix (figures 2B, 2C).

Dans un mode de réalisation, l'identifiant graphique 30 est en outre stocké en local sur l'objet, par apposition, impression, collage, insertion ou autre. Par exemple, le Datamatrix est imprimé sur la carte 10 après la lamination de l'une au moins des première 11, deuxième 12 et optionnellement troisième 13 couche de la carte si l'identifiant graphique est un index ; et après la lamination de toutes les couches sinon.

La sécurisation de l'objet 10 est assurée car il est ainsi possible d'authentifier ledit objet 10 porteur de la signature graphique 23 y associée.

A cet effet, la vérification / authentification de la signature peut être mise en œuvre de la manière suivante.

Une prise de vue numérique de la signature graphique multicouche 23 est réalisée, par exemple par un appareil photo ou tout équipement muni d'un capteur CCD et d'une mémoire.

La prise de vue numérique de la signature graphique multicouche 23 est alors comparée à la signature numérique de référence.

De préférence, on effectue une comparaison 1:1 entre l'objet 10 à analyser et la signature numérique de référence (de l'objet ou document original) portant un même numéro ou un même identifiant, plutôt qu'une recherche 1 parmi N qui pourrait être perturbée par la présence de plusieurs motifs semblables dans une base de plusieurs millions.

La comparaison peut être mise en œuvre par étude de ressemblances ou par étude de différences entre une signature à analyser, dite « suspecte » stockée sur ou dans un objet « suspect », et une signature de référence, dite « authentique ».

Dans un mode de réalisation, la comparaison est effectuée de manière connue en soi, notamment en analyse d'images, par la caractérisation de formes (détection de points saillants, extraction de contours...), de texture (matrices de cooccurrences, etc...) et de couleurs, combinées. Numériquement, elle peut consister par exemple à calculer un taux d'erreur bit à bit (BER, bit error-rate) entre les deux signatures, et à renvoyer "Vrai" lorsque ce taux est inférieur à un seuil donné, "Faux" dans le cas contraire. Le seuil est choisi de préférence de telle sorte que la probabilité statistique que la réponse est erronée soit négligeable.

A cet effet, on prévoit de préférence d'extraire par lecture optique l'identifiant graphique 30 de l'objet, par exemple par la réalisation d'une prise de vue numérique dudit au moins un élément distinctif ou nominatif de l'objet 10.

Il suffit alors de sélectionner dans la base de données la signature de référence associée à l'identifiant extrait et de comparer l'image de la signature de référence et l'image de la signature graphique 23 de l'objet 10.

Dans un autre mode de réalisation, la comparaison des signatures graphiques se ramène à la comparaison des signatures numériques par un algorithme connu en soi, faisant notamment appel au domaine du traitement d'images. Selon l'algorithme choisi pour le calcul de la signature numérique, la comparaison peut comprendre par exemple les étapes suivantes :

- la signature numérique suspecte est calculée exactement comme si il s'agissait de la signature de référence,
- la signature numérique de référence correspondante est recherchée dans la base de données, grâce à l'index numérique ou alphanumérique déduit du suspect,
- les deux signatures numériques sont comparées selon un ou plusieurs critères prédéterminés,
- si tous les critères sont validés, l'algorithme renvoie "vrai", sinon "faux".

Les critères prédéterminés pour la comparaison de deux signatures numériques dépendent de préférence de la nature des informations stockées dans celles-ci. Par exemple, un critère peut se baser sur le calcul d'une distance entre deux descripteurs appariés (c'est-à-dire calculés aux mêmes coordonnées ou sur les mêmes éléments graphiques de la prise de vue de la signature graphique du suspect d'une part, et de celle de la référence d'autre part) selon une formule adaptée à la nature du descripteur. L'utilisation d'un seuil permet alors d'accepter ou de rejeter le critère selon que la distance se trouve en dessous ou au dessus de celui-ci.

Le processus de décision est choisi de préférence de telle sorte que la probabilité d'une fausse réponse soit négligeable.

On peut également prévoir en outre, et de préférence au préalable, une étape de détermination du type de signature/d'objet, pour augmenter la vitesse de recherche de la signature de référence.

Cette étape comprend la localisation de l'identifiant graphique 30 (DataMatrix par exemple) et la détermination de son orientation et de son échelle dans l'image numérique.

Par exemple, la lecture de l'image de l'identifiant graphique 30 peut permettre de déterminer que l'objet est du type carte d'identité, du type passeport, du type objet manufacturé, etc. De ce type, on peut effectuer la recherche de la signature de référence correspondante uniquement sur la partie de la base de données dans laquelle sont stockées ce type de signatures, et non sur l'ensemble de la base. On peut également prévoir plusieurs bases de données, une par type d'objet, afin d'augmenter la sécurité du procédé.

On peut utiliser aussi les coordonnées de l'identifiant graphique 30 et le facteur d'échelle obtenus pour extraire l'image de la signature graphique 23, dont l'emplacement est de préférence relatif à celui-ci de façon prédéfinie. L'image est alors redressée de façon à annuler les effets éventuels de rotation dus à d'éventuelles manipulations, et normalisée à une résolution d'image standard pré-établie suffisante pour les étapes d'analyse suivantes.

Par exemple, on peut prévoir une étape de vérification dite bas niveau qui consiste à s'assurer que l'image extraite à l'étape précédente présente certaines caractéristiques communes avec le type d'objet. Par exemple, si la signature graphique comprend un imprimé sur fond constant présentant un graphisme spécifique (guilloches par exemple), cette étape peut consister à s'assurer que le fond en question est bien présent sur l'image, au moyen de toute technique d'analyse d'image connue.

Si tel n'est pas le cas, le programme peut se terminer en renvoyant un message adéquat à l'utilisateur.

La présente description n'est pas limitée aux modes de réalisation précédemment décrits.

Par exemple, l'objet 10 peut comprendre un emballage, une couche dudit emballage constituant en l'espèce la première 11 et/ou deuxième couche 12 de l'objet 10.

On peut ainsi prévoir que l'objet 10 comprenne un substrat muni d'une impression de fond et éventuellement une information de personnalisation pouvant comporter des éléments aléatoires.

Au moment de l'emballage du substrat, la position de l'emballage par rapport à l'impression de fond, voire à l'information de personnalisation est donnée avec une certaine tolérance, donc avec un aléa, pour les raisons mécaniques évoquées ci-avant.

Sur l'emballage, on peut alors prévoir d'apposer par exemple un hologramme au moins partiellement transparent, de manière à chevaucher au moins partiellement l'information de personnalisation.

Ce mode de réalisation est particulièrement avantageux pour la sécurisation de produit sensibles, par exemple pour des produits pharmaceutiques, par exemple des médicaments, emballés dans une boîte pré-imprimée, puis personnalisés avec un numéro de lot et une date (de fabrication, péremption, consommation etc) ; boîte sur laquelle on peut ensuite appliquer un hologramme sous forme d'étiquette auto-adhésive transparente avant de faire l'acquisition numérique de la signature graphique en fin de chaîne d'emballage.

REVENDICATIONS

1. Procédé de sécurisation d'un objet (10) comprenant des étapes consistant à :

- créer une signature graphique multicouche (23), par superposition en transparence partielle ou totale d'un premier élément graphique (20) sur une première couche (11) et d'un deuxième élément graphique (21) sur une deuxième couche (12), dont au moins élément graphique (20, 21) comprend un élément graphique aléatoire, et
- stocker ladite signature graphique sur ou dans l'objet (10),

caractérisé en ce que

- la position relative du premier élément graphique (20) et du deuxième élément graphique (21) est aléatoire.

2. Procédé selon la revendication 1, dans lequel la création de la signature graphique multicouche (23) comprend en outre la superposition en transparence partielle ou totale d'un troisième élément graphique (22) sur une troisième couche (13), distincte des première (11) et deuxième (12) couche, et dans lequel la position relative dudit troisième élément graphique (22) et dudit premier (20) élément graphique et/ou dudit deuxième (21) élément graphique est aléatoire, ledit troisième élément graphique (22) pouvant comprendre un élément graphique aléatoire.

3. Procédé selon l'une quelconque des revendications précédentes, dans lequel l'étape de stockage comprend une étape consistant à apposer ladite signature graphique multicouche (23) sur ledit objet (10), ou à intégrer ladite signature graphique multicouche à une partie au moins dudit objet.

4. Procédé selon l'une quelconque des revendications précédentes, comprenant en outre des étapes consistant à :

- réaliser une première prise de vue de la signature graphique multicouche (23),

- calculer une première signature numérique de ladite prise de vue et enregistrer ladite signature numérique dans une base de données, de sorte à constituer une partie au moins d'une signature numérique de référence, et
- enregistrer dans ladite base de données un identifiant numérique ou alpha-numérique, associé à ladite première signature numérique.

5. Procédé selon l'une quelconque des revendications précédentes, comprenant en outre des étapes consistant à :

- créer un identifiant graphique (30), optionnellement multicouche, à partir d'une prise de vue de l'ensemble superposé desdits premier (20) et deuxième (21) éléments graphiques, et dudit troisième (22) élément graphique lorsqu'il existe ; et/ou à partir d'au moins un élément distinctif ou nominatif de l'objet, et
- stocker ledit identifiant graphique (30) sur ou dans l'objet (10), optionnellement sur l'une des couches de ladite signature multicouche.

6. Procédé selon l'une quelconque des revendications 4 à 5, comprenant en outre des étapes consistant à :

- réaliser une deuxième prise de vue numérique de la signature graphique multicouche (23),
- calculer une deuxième signature numérique de ladite prise de vue,
- comparer la première et la deuxième signature numérique, et
- authentifier ou non la signature graphique en fonction du résultat de la comparaison.

7. Procédé selon les revendications 5 et 6, dans lequel, pour l'étape de comparaison, le procédé comprend en outre des étapes consistant à :

- lire l'identifiant graphique,

- en extraire l'identifiant numérique correspondant, et
- sélectionner la signature numérique de référence associée.

8. Programme d'ordinateur, comprenant des instructions de code de programme pour l'exécution des étapes du procédé selon l'une quelconque des revendications précédentes, lorsque ledit programme est exécuté sur un ordinateur.

9. Objet sécurisé (10), comprenant :

- une signature graphique multicouche (23) stockée sur ou dans ledit objet (10), réalisée par superposition en transparence partielle ou totale d'un premier élément graphique (20) sur une première couche (11) et d'un deuxième élément graphique (21) sur une deuxième couche (12), dont au moins élément graphique (20, 21) comprend un élément graphique aléatoire,

caractérisé en ce que

- la position relative du premier élément graphique (20) et du deuxième élément graphique (21) est aléatoire.

10. Objet sécurisé selon la revendication 9, comprenant en outre un troisième élément graphique (22), pouvant comprendre un élément graphique aléatoire, sur une troisième couche (13) distincte des première (11) et deuxième (12) couche, et dans lequel la position relative dudit troisième élément graphique (22) et dudit premier élément graphique (20) et/ou dudit deuxième élément graphique (22) est aléatoire.

11. Objet sécurisé selon l'une quelconque des revendications 9 ou 10, comprenant en outre un identifiant graphique (30), optionnellement multicouche, à partir d'une prise de vue de l'ensemble superposé desdits premier (20) et deuxième (21) éléments graphiques, et dudit troisième (22)

élément graphique lorsqu'il existe ; et/ou à partir dudit au moins un élément distinctif ou nominatif de l'objet.

12. Objet sécurisé selon la revendication 11, dans lequel ledit identifiant graphique (30) est imprimé sur l'une des couches de ladite de signature multicouche (23), de préférence sous forme de datamatrix.

13. Objet sécurisé selon l'une quelconque des revendications 9 à 12, dans lequel ledit objet (10) est un objet multicouches, dont l'une des couches supporte le premier élément graphique, une autre couche supporte le deuxième élément graphique, et éventuellement une autre couche encore supporte, lorsqu'il existe, le troisième élément graphique.

14. Objet sécurisé selon la revendication 13, dans lequel chaque couche (20, 21, 22) de la signature (23) est une couche respective (11, 12, 13) dudit objet (10).

15. Objet sécurisé selon l'une quelconque des revendications 9 à 12, comprenant en outre un emballage, dont la ou l'une des couches est la première (11), deuxième (12), ou troisième couche (13) lorsqu'elle existe.

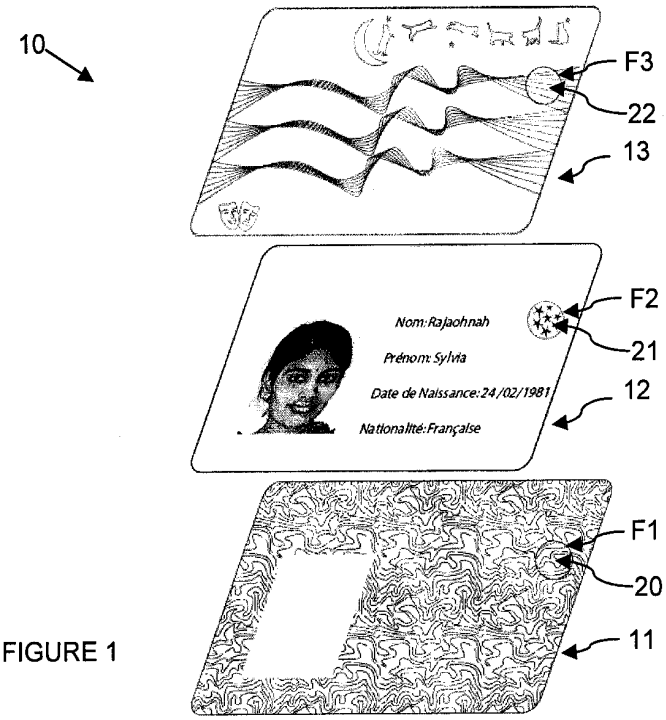


FIGURE 1

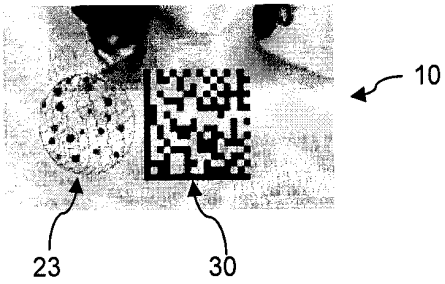


FIGURE 2C

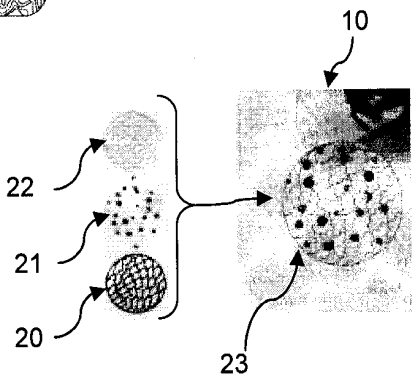


FIGURE 2A

FIGURE 2B

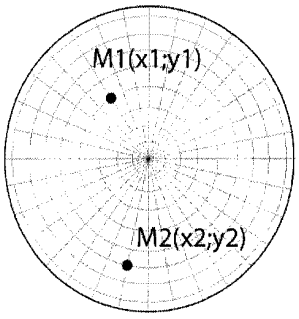


FIGURE 3A

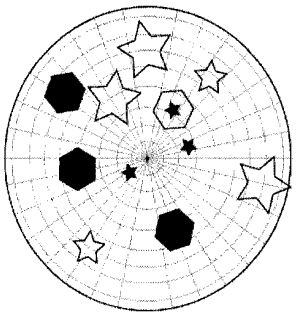


FIGURE 3B

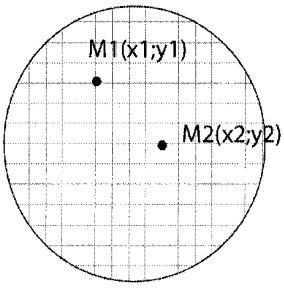


FIGURE 3C

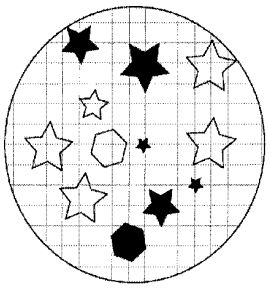


FIGURE 3D

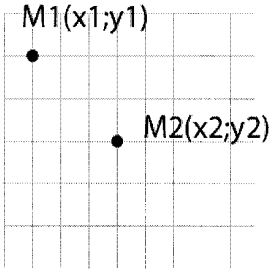


FIGURE 3E

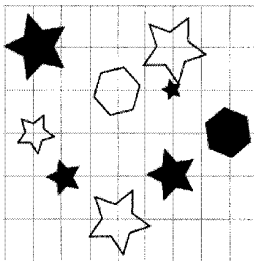


FIGURE 3F

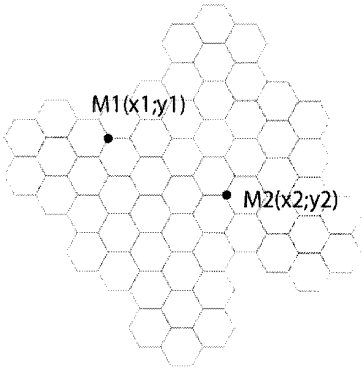


FIGURE 3G

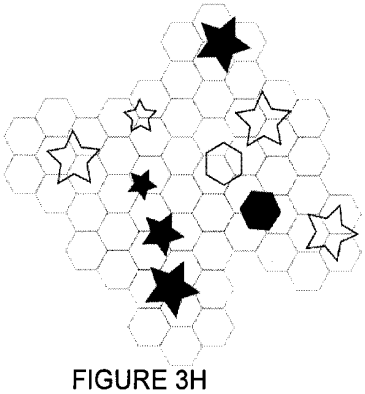


FIGURE 3H

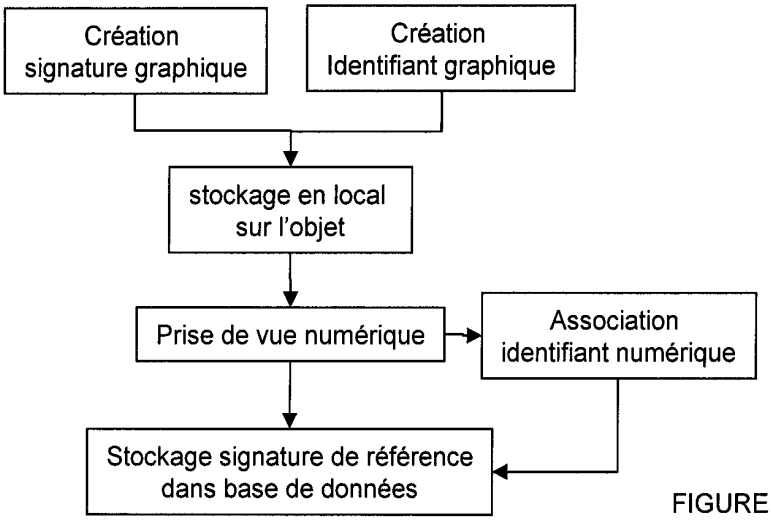


FIGURE 4

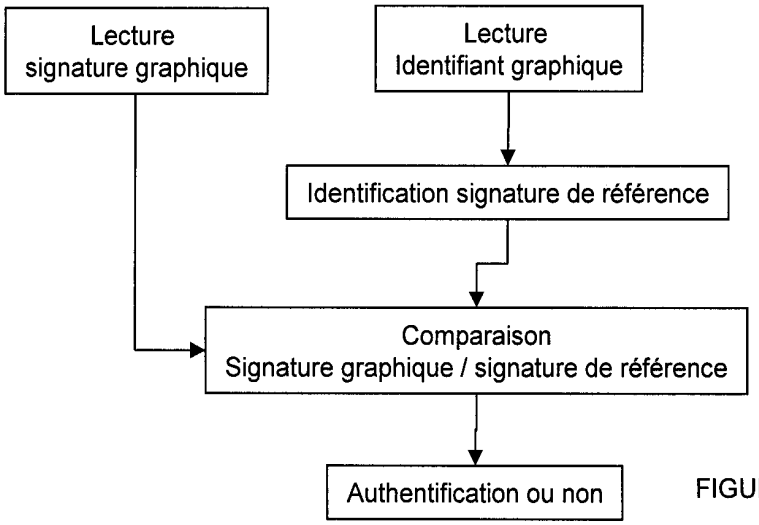


FIGURE 5

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 733342
FR 1000176

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
A	WO 2004/089649 A2 (IVY TRUST [CH]; OAKES ALISTAIR [GB]) 21 octobre 2004 (2004-10-21) * page 1 - page 5 * * page 7 - page 13 * * figures *	1-15	B42D15/10 G07D7/20 G06K19/04
A	FR 2 890 666 A1 (ARJOWIGGINS SECURITY SOC PAR A [FR]) 16 mars 2007 (2007-03-16) * page 9, ligne 3 - ligne 30 * * page 14, ligne 16 - page 22, ligne 30 * * figures 1-3,5-11 *	1-15	
A	WO 2006/053685 A2 (GIESECKE & DEVRIENT GMBH; GIERING THOMAS [DE]; MAYER KARLHEINZ [DE]; P) 26 mai 2006 (2006-05-26) * page 12, ligne 22 - page 22, ligne 25 * * figures 1,4 *	1-15	
A	WO 2005/010814 A1 (TBS HOLDING AG [CH]; HAUKE RUDOLF [DE]; NOTHAFT HANS-PETER [DE]) 3 février 2005 (2005-02-03) * page 6, ligne 8 - page 9, ligne 4 * * page 10; figures *	1-15	DOMAINES TECHNIQUES RECHERCHÉS (IPC) G07D G07F B42D B44F

Date d'achèvement de la recherche	Examinateur
13 juillet 2010	Bocage, Stéphane

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 1000176 FA 733342

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 13-07-2010
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 2004089649 A2	21-10-2004	AP 1947 A	28-02-2009
		AU 2004228474 A1	21-10-2004
		BR PI0409220 A	28-03-2006
		CN 1802264 A	12-07-2006
		EG 23773 A	08-08-2007
		EP 1610960 A2	04-01-2006
		JP 2006521943 T	28-09-2006
		MX PA05010844 A	09-03-2006
		US 2007164557 A1	19-07-2007
		ZA 200508956 A	28-02-2007
FR 2890666 A1	16-03-2007	CA 2622493 A1	22-03-2007
		EP 1951957 A1	06-08-2008
		WO 2007031694 A1	22-03-2007
		US 2009033914 A1	05-02-2009
WO 2006053685 A2	26-05-2006	EP 1815443 A2	08-08-2007
WO 2005010814 A1	03-02-2005	AU 2003250760 A1	14-02-2005

EPO FORM P0465