

(12) DEMANDE INTERNATIONALE PUBLÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



(10) Numéro de publication internationale
WO 2012/017161 A1

(43) Date de la publication internationale
9 février 2012 (09.02.2012)

(51) Classification internationale des brevets :
G07D 7/00 (2006.01) **G07D 7/20** (2006.01)

avenue de la châtaigneraie, F-92500 Rueil-Malmaison (FR).

(21) Numéro de la demande internationale :
PCT/FR2011/051727

(74) Mandataire : **SCHMIT-CHRETIEN**; 836, rue du Mas de Verchant, F-34000 Montpellier (FR).

(22) Date de dépôt international :
19 juillet 2011 (19.07.2011)

(81) États désignés (sauf indication contraire, pour tout titre de protection nationale disponible) : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1055826 19 juillet 2010 (19.07.2010) FR

(71) Déposants (pour tous les États désignés sauf US) :
ADVANCED TRACK & TRACE [FR/FR]; 99, avenue de la châtaigneraie, F-92500 Rueil-Malmaison (FR).
FOUCOU, Alain [FR/FR]; c/o Advanced Track & Trace, 99, avenue de la châtaigneraie, F-92500 Rueil-Malmaison (FR).
SAGAN, Zbigniew [FR/FR]; c/o Advanced Track & Trace, 99, avenue de la châtaigneraie, F-92500 Rueil-Malmaison (FR).

(84) États désignés (sauf indication contraire, pour tout titre de protection régionale disponible) : ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK,

(72) Inventeur; et

(75) Inventeur/Déposant (pour US seulement) : **MASSICOT, Jean Pierre** [FR/FR]; c/o Advanced Track & Trace, 99,

[Suite sur la page suivante]

(54) Title : METHODS AND DEVICES FOR MARKING AND AUTHENTICATING A PRODUCT BY A CONSUMER

(54) Titre : PROCÉDÉS ET DISPOSITIFS DE MARQUAGE ET D'AUTHENTIFICATION D'UN PRODUIT PAR UN CONSOMMATEUR

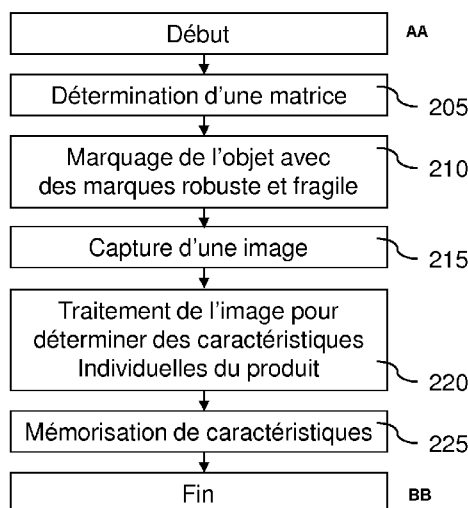


Figure 2

(57) Abstract : The product marking method comprises: a step of forming, on or in said product, a copy-robust mark with a first resolution; a step of forming, on or in said product, a copy-fragile mark, with a second resolution greater than the first resolution; a step of capturing an image of said robust mark, of said fragile mark and of another portion of the product; and a step of storing information representative of the image of said robust mark, of said fragile mark and of said other portion. In certain embodiments, during at least one forming step, the position of the mark formed during this forming step, relative to the other image portion, is random.

(57) Abrégé : Le procédé de marquage de produit comporte; une étape de formation, sur ou dans ledit produit, d'une marque robuste à la copie, avec une première résolution, une étape de formation, sur ou dans ledit produit, d'une marque fragile à la copie, avec une deuxième résolution supérieure à la première résolution, une étape de capture d'une image de ladite marque robuste, de ladite marque fragile et d'une autre partie du produit et une étape de mémorisation d'une information représentative de l'image de ladite marque robuste, de ladite marque fragile et de ladite autre partie d'image. Dans des modes de réalisation, au cours d'au moins une étape de formation, la position de la marque formée au cours de cette étape de formation, par rapport à l'autre partie d'image, est aléatoire.

WO 2012/017161 A1



SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG). **Publiée :**

— avec rapport de recherche internationale (Art. 21(3))

PROCÉDÉS ET DISPOSITIFS DE MARQUAGE ET D'AUTHENTIFICATION D'UN PRODUIT PAR UN CONSOMMATEUR

La présente invention concerne un procédé et un dispositif de marquage de produits et un procédé et un dispositif d'authentification d'un produit par un consommateur. Elle s'applique à tout type de produit, avec ou sans emballage.

5 Les dispositifs d'authentification de produit connus dans l'art antérieur sont réservés à des professionnels munis de matériels spécifiques onéreux. Il n'est donc pas possible, pour un consommateur, de vérifier l'authenticité d'un produit avant de l'acheter, par exemple dans un magasin, ou de le consommer, par exemple au restaurant. La contrefaçon de produits onéreux, notamment alcools, médicaments et parfums, s'étend ainsi facilement.

La présente invention vise à remédier à tout ou partie de ces inconvénients.

10 A cet effet, selon un premier aspect, la présente invention vise un procédé de marquage de produit, qui comporte :

- une étape de formation, sur ou dans ledit produit, d'une marque robuste à la copie, avec une première résolution,

- une étape de formation, sur ou dans ledit produit, d'une marque fragile à la copie, avec 15 une deuxième résolution supérieure à la première résolution,

- une étape de capture d'une image de ladite marque robuste, de ladite marque fragile et d'une autre partie du produit et

- une étape de mémorisation d'une information représentative de l'image de ladite 20 marque robuste, de ladite marque fragile et de ladite autre partie d'image.

20 Grâce à ces dispositions, en cas de copie illégale du produit, il peut être identifié grâce à la marque robuste et authentifié grâce, d'une part, à la marque fragile et, d'autre part, à l'image de la partie du produit. Ainsi, la destruction ou l'altération de la marque fragile n'empêchent pas l'authentification du produit. De plus, en comparant l'information représentative de l'image mémorisée avec une information représentative d'une image prise avec un capteur d'image 25 grand public, on peut authentifier le produit même si la qualité d'image ne permet pas le traitement de la marque fragile.

La présente invention permet ainsi l'authentification de produits par un consommateur muni d'un terminal mobile communiquant, par exemple un assistant personnel numérique ou un téléphone mobile, doté d'un capteur d'image, ou appareil photo.

Selon des caractéristiques particulières, au cours d'au moins une étape de formation, la position de la marque formée au cours de cette étape de formation, par rapport à l'autre partie d'image, est aléatoire.

Grâce à ces dispositions, des caractéristiques géométriques entre les positions de la
5 marque robuste, de la marque fragile et de l'autre partie du produit permettent aussi d'authentifier le produit.

Selon des caractéristiques particulières, ladite marque robuste est un code à barres en deux dimensions.

Par exemple, ce code à barres en deux dimensions est un DataMatrix (marque
10 déposée). On peut ainsi stocker une importante quantité d'information sur le produit (par exemple, le nom de son fabricant et le lieu et la date de fabrication).

Selon des caractéristiques particulières, ladite marque fragile à la copie est un code numérique authentifiant, le procédé objet de la présente invention comporte une étape de
15 détermination d'une information représentative des erreurs d'impression de ladite marque fragile à la copie et au cours de l'étape de mémorisation, on mémorise ladite information représentative des erreurs d'impression.

Selon des caractéristiques particulières, au cours de chacune des étapes de formation de marques, la position de ladite marque par rapport à un élément du produit est variable et, lors de l'étape de capture d'une image, on capte une image dudit élément.

20 Selon des caractéristiques particulières, au cours des étapes de formation de marques, on décale, entre deux produits différents, différemment les marques formées.

Selon un deuxième aspect, la présente invention vise un dispositif de marquage de produit, qui comporte :

- un moyen de formation, sur ou dans ledit produit, d'une marque robuste à la copie,
25 avec une première résolution,

- un moyen de formation, sur ou dans ledit produit, d'une marque fragile à la copie, avec une deuxième résolution supérieure à la première résolution,

- un capteur d'image adapté à capté une image de ladite marque robuste, de ladite
marque fragile et d'une autre partie du produit et

30 - un moyen de mémorisation d'une information représentative de l'image de ladite marque robuste, de ladite marque fragile et de ladite autre partie d'image.

Selon un troisième aspect, la présente invention vise un procédé d'authentification de produit, qui comporte :

- une étape de capture, sur ledit produit d'une image d'une marque robuste et d'une marque fragile à la copie de résolution plus élevée que la marque robuste et d'une autre partie du produit,

- une étape de transmission d'une information représentative de l'image de ladite marque robuste, de ladite marque fragile et de ladite autre partie d'image,

- une étape de comparaison de ladite information représentative de l'image de ladite marque robuste, de ladite marque fragile et de ladite autre partie d'image avec au moins une information mémorisée à distance et

- en fonction du résultat de ladite étape de comparaison, une étape d'affichage de données relatives au produit dont une image a été captée.

Dans des modes de réalisation, au cours de l'étape de comparaison, on effectue, d'abord, une étape de détermination de qualité de l'image de la marque fragile à la copie et :

- si la qualité est supérieure à une valeur prédéterminée, une comparaison d'une information représentative de la marque fragile à la copie et,

- sinon, une comparaison d'une information représentative de l'autre partie du produit.

Ainsi, même si l'image de la marque fragile à la copie n'est pas de qualité suffisante, par exemple du fait des conditions ou matériels de prise d'image, on peut néanmoins estimer l'authenticité du produit.

Selon un quatrième aspect, la présente invention vise un dispositif d'authentification de produit, qui comporte :

- un moyen de capture, sur ledit produit d'une image d'une marque robuste et d'une marque fragile à la copie de résolution plus élevée que la marque robuste et d'une autre partie du produit,

- un moyen de transmission d'une information représentative de l'image de ladite marque robuste, de ladite marque fragile et de ladite autre partie d'image,

- un moyen de comparaison de ladite information représentative de l'image de ladite marque robuste, de ladite marque fragile et de ladite autre partie d'image avec au moins une information mémorisée à distance et

- un moyen d'affichage de données relatives au produit dont une image a été captée, en fonction du résultat fourni par le moyen de comparaison.

Les avantages, buts et caractéristiques de ce dispositif de marquage, de ce procédé d'authentification et de ce dispositif d'authentification étant similaires à ceux du procédé de marquage objet de la présente invention, ils ne sont pas rappelés ici.

D'autres avantages, buts et caractéristiques de la présente invention ressortiront de la description qui va suivre faite, dans un but explicatif et nullement limitatif, en regard des dessins annexés, dans lesquels :

- 5 - la figure 1 représente, schématiquement, en vue de face, un premier mode de réalisation particulier des dispositifs objets de la présente invention,
- la figure 2 représente, sous forme d'un logigramme, des étapes mises en œuvre dans un mode de réalisation particulier du procédé objet de la présente invention
- la figure 3 représente, en vue agrandie, un motif numérique identifiant mis en œuvre dans des modes de réalisation particuliers du procédé objet de la présente invention,
- 10 - la figure 4 représente, en vue agrandie, le motif numérique identifiant de la figure 3, une fois imprimé sur une carte, lors d'une première impression d'une série,
- la figure 5 représente, en vue agrandie, le motif numérique identifiant de la figure 3, une fois imprimé sur une carte, lors d'une deuxième impression d'une série,
- la figure 6 représente une transformée cosinus discrète d'une image captée de l'un des motifs identifiants imprimés représentés dans les figures 4 et 5,
- 15 - les figures 7A et 7B représentent, sous forme de logigrammes, des étapes mises en œuvre dans des modes de réalisation particuliers du procédé objet de la présente invention,
- la figure 8 représente une distribution des scores pour deux groupes de motifs identifiants mis en œuvre dans des modes de réalisation particuliers du procédé objet de la présente invention,
- 20 - la figure 9 illustre en courbe obtenue lors de la détermination d'un taux optimale d'erreurs à obtenir à l'impression et
- la figure 10 représente une partie d'un produit mis en œuvre dans les modes de réalisation particuliers des procédés et dispositifs objet de la présente invention illustrés en figures 1 et 2.
- 25

Avant de donner le détail de différents modes de réalisation particuliers de la présente invention, on donne, ci-après, des définitions qui seront utilisées dans la description :

- « matrice d'informations » : il s'agit d'une représentation physique d'un message, généralement apposée sur une surface unie (à la différence des watermarks ou filigranes numériques qui modifient les valeurs de pixels d'un décor à imprimer), lisible par une machine (en anglais « machine-readable representation of information »). La définition de la matrice d'informations englobe, par exemple, les codes à barres 2D, les codes à barres à une dimension et d'autre moyens de représentation de l'information qui sont moins intrusifs, tel que les « Dataglyphs » (marquage de données) ;
- 30

- « marquage » ou « impression » : tout processus par laquelle on passe d'une image digitale (incluant préférentiellement une matrice d'information) à sa représentation dans le monde réel, cette représentation étant généralement faite sur une surface : ceci inclut, de manière non-exclusive, l'impression à jet d'encre, laser, offset, thermique, ainsi que l'embossage, la gravure laser, la génération d'hologrammes. Des processus plus complexes, tel que le moulage, dans lequel l'image digitale est d'abord gravée dans le moule, puis moulée sur chaque produit, sont également inclus. Notons qu'une image « moulée » peut être vue comme ayant trois dimensions dans le monde physique même si sa représentation digitale en comporte deux. Notons encore que plusieurs des procédés mentionnés incluent plusieurs transformations, par exemple l'impression offset classique (contrairement au offset « computer-to-plate »), inclut la création d'un film, ledit film servant à créer une plaque, ladite plaque étant utilisée dans l'impression. D'autres procédés permettent également d'imprimer une information dans le domaine non-visible, soit en utilisant des fréquences à l'extérieur du spectre visible, ou encore à inscrivant l'information à l'intérieur de la surface, etc,

- « Empreinte » ou « information représentative d'une image » : ensemble de valeurs de caractéristique mesurées, permettant de représenter une marque et de la comparer à d'autres représentations de marques,

- « Capture » : tout processus par lequel on obtient une représentation digitale du monde réel, incluant la représentation digitale de la surface externe d'un produit ou de son épaisseur (par rétro-éclairage),

- « Cellule » : il s'agit d'une zone régulière d'un motif de points à caractéristiques variables (« MPCV »), généralement rectangulaire, voire carrée, dans laquelle se trouve, au maximum, un nombre prédéterminé de points, le nombre prédéterminé valant généralement un ;

- « Pixel de génération » : la plus petite zone considérée pour la génération d'un MPCV,

- « Point » : une zone imprimée élémentaire de très petite dimension, éventuellement variable, faisant contraste avec un arrière-plan, le point étant généralement la représentation d'un ou plusieurs pixels de génération,

- « Pixel de capture » ou « pixel d'image » : une zone dont l'image correspondant à un point photosensible élémentaire, ou pixel, d'un capteur d'image,

Les codes numériques authentifiants, aussi appelés par la suite « CNA » ou marques fragiles à la copie, sont des images numériques qui, une fois marquées sur un support, par exemple par impression ou modification locale du support, sont conçues de façon à ce que certaines de leurs propriétés, en général mesurables automatiquement à partir d'une image

captée, soient modifiées si une image marquée est copiée. Les codes numériques authentifiants se basent généralement sur la dégradation d'un ou plusieurs signaux sensibles à la copie lors de l'étape de copie, un signal étant porté par des éléments d'image aux caractéristiques mesurables sensibles à la copie. Certains types de codes numériques authentifiants peuvent également contenir de l'information permettant d'identifier ou tracer le produit qui le contient.

Il existe plusieurs types de codes numériques authentifiants. Les motifs de détection de copie, aussi appelés par la suite « MDC », sont des images denses, en général de nature pseudo-aléatoire. Leur principe de lecture est basé sur une comparaison d'image pour mesurer un indice de similitude (ou de dissimilitude) entre le motif de détection de copie d'origine et le motif de détection de copie capturé, par exemple par un capteur d'image : si ce motif capturé est une copie, l'indice de similitude sera moins élevé que si c'est un original.

Les matrices d'information sécurisées, aussi appelés par la suite « MIS », sont, tout comme les codes à barre à deux dimensions, des images conçues pour transporter une grande quantité d'information de manière robuste. Cependant, contrairement aux codes à barre en deux dimensions, les matrices d'information sécurisées sont sensibles à la copie. A la lecture, on mesure un taux d'erreur du message codé extrait de la matrice, taux qui est plus élevé pour les copies que pour les originaux, ce qui permet de distinguer ces copies des impressions originales.

On observe, en figure 1, un mode de réalisation du dispositif de marquage 11 objet de la présente invention adapté à une machine traitant des produits à marquer 20 qui ont pu être imprimés en d'autres sites ou à d'autres dates. Dans d'autres modes de réalisation, ce dispositif 11 objet de la présente invention est adapté à une chaîne d'impression et traite les produits dès l'impression initiale de leur surface externe ou dans leur épaisseur.

Par exemple, le produit à marquer 20 est une étiquette ou un emballage pour un produit industriel.

Le dispositif d'identification de produits 11 comporte :

- un dépileur 15, connu en soi, qui dépile des produits 20,
- un convoyeur 16, de type connu,
- un empileur 17 qui forme une pile des produits 20 traitées par le dispositif 11,
- un moyen 18 de formation, sur ou dans ledit produit, d'une marque robuste à la copie, avec une première résolution,
- un moyen 19 de formation, sur ou dans ledit produit, d'une marque fragile à la copie, avec une deuxième résolution supérieure à la première résolution,

- un moyen 25 de capture d'une image de la marque robuste, de la marque fragile à la copie et d'une autre partie du produit (voir figure 10), sur chaque produit 20,

- un moyen 30 de génération d'une empreinte individuelle, variable d'un produit à un autre et fonction de l'image fournie par le moyen de capture 25 et

5 - un moyen 40 de mise en mémoire distante pour stocker ladite empreinte correspondant, individuellement, au produit 20, par exemple une base de données.

Dans le cas où la présente invention est adaptée à une chaîne d'impression, le dépileur 15 est en amont de la chaîne d'impression et ce n'est qu'après impression que les produits 20 portent, d'une part, une marque robuste et, d'autre part, une marque fragile à la
10 copie, ou anti-copie.

Dans des modes de réalisation, la marque anti-copie est un CNA comme exposé ci-dessus.

Le moyen 25 de capture d'image comporte une caméra 26 et au moins une source de lumière 27, éventuellement par rétro-éclairage si la marque anti-copie est formée dans
15 l'épaisseur du produit 20 ou si le produit 20 est suffisamment transparent pour au moins une longueur d'onde lumineuse. Le moyen de capture d'image 25 comporte aussi un moyen de détection 28 d'arrivée d'un produit 20, par exemple une cellule optoélectronique placée, sur le chemin suivi par les produits 20, en amont du moyen de lecture 25.

Le moyen de génération d'empreinte 30 effectue un traitement de l'image captée par la
20 caméra 26, qui détermine des caractéristiques de l'image de la marque robuste, de la marque fragile à la copie et d'une partie du produit 20. Ainsi, pour réaliser l'appairage entre le produit et l'empreinte qui est générée individuellement pour chaque produit 20, un système de vision lit en dynamique une image de la partie du produit qui porte les marques robuste et fragiles à la copie, puis transmet l'information au moyen de génération 30 de l'empreinte.

25 Dans des modes de réalisation, l'empreinte est formée d'une partie de l'image captée préférentiellement normalisée en proportion des dimensions des marques robuste et fragile. Dans d'autres modes de réalisation, tels que ceux détaillés ci-dessous, on effectue un traitement d'une partie de l'image captée entourant les marques robuste et fragile.

Par exemple, comme illustré en figure 10, la partie d'image 100 traitée correspond à
30 trois fois la hauteur de la marque robuste 105 sur trois fois la largeur de la marque robuste 105 et est centrée sur le coin inférieur droit de la marque fragile 110. Cette partie d'image comporte une autre partie 115 du produit, par exemple un logo ou une écriture dont la position est, préférentiellement, variable par rapport aux marques robuste et fragile, d'un produit 20 à un autre.

On donne, ci-dessous, un exemple de méthode pour la génération de l'empreinte.

- à partir du sous-ensemble « ICNA » des informations de l'image, on calcule une valeur associative « VA » par une fonction de calcul de valeur associative « F », ou d'une fonction « F' » qui utilise optionnellement un ou plusieurs autres paramètres dénotés « K »,
- 5 - on obtient un horodatage « T »,
- on obtient un identifiant « ID » de la machine génératrice d'empreintes,
- on obtient une clé de chiffrement « KCV » de l'empreinte,
- avec une fonction « CONC », on concatène, de préférence en représentation binaire, « VA », « T » et « ID » pour obtenir la concaténation « C » et
- 10 - on chiffre la concaténation « C » avec une fonction de chiffrement « ENCRYPT » et la clé de chiffrement KCV, pour obtenir « CENC ».

En ce qui concerne la fonction « F », celle-ci est, de façon non limitative, une fonction qui calcule une valeur « VA » à partir du sous-ensemble « ICNA ».

- En ce qui concerne la fonction « F' », dans le cas où on utilise la fonction « F' » avec
- 15 paramètre(s) « K », « F' » peut être, par exemple, une fonction de chiffrement (par exemple connue sous le nom de « Triple-DES » ou d'« AES »). « F' » peut également être une fonction de hachage en combinaison avec une clé, ici le paramètre « K » qui doit être tenu secret.

- En ce qui concerne la fonction « CONC », les valeurs « VA », « T » et « ID » peuvent être des entiers ou avoir une valeur appartenant à un ensemble déterminé (par exemple il existe
- 20 quatre machines génératrices d'empreintes, donc quatre valeurs possibles pour « ID »). Dans le second cas, on détermine le nombre de bits nécessaires pour représenter l'ensemble des valeurs possibles. Dans le premier, les entiers sont en général représentés sur un ensemble déterminé d'octets.

- En ce qui concerne la fonction « ENCRYPT », elle peut être une fonction de
- 25 chiffrement symétrique, par exemple connus sous le nom de « Triple DES », « AES » ou « RC4 » ou une fonction de chiffrement asymétrique, par exemple connue sous le nom de « RSA ».

Dans les modes de réalisation de la présente invention décrits ci-dessous en regard des figures 3 à 8, on met en œuvre :

- 30 - des étapes 301 à 303 de conception numérique des marques robuste et fragile,
- des étapes 311 à 314 de calcul d'empreinte,
- des étapes 320 à 326 d'optimisation de l'impression des marques et
- des étapes 331 à 334 de stockage en mémoire distante d'empreintes ou caractéristiques uniques de produits.

En ce qui concerne la conception numérique d'une marque fragile et la détermination des paramètres d'impression d'une marque fragile, à l'origine de certaines caractéristiques particulières de la présente invention, il a été découvert que, si l'on imprime plusieurs fois une même image source d'une matrice d'information sécurisée, celle-ci sera affectée d'erreurs différentes à chaque impression. Le même effet a également été constaté pour les motifs de détection de copie. De manière plus générale, il a été constaté que, pour toute image possédant une densité suffisante :

- l'impression de l'image résultera en une dégradation de l'image, et
- l'impression sera affectée d'une dégradation différente à chaque impression.

Pour être plus précis, ce phénomène n'est pas limité aux codes numériques authentifiants CNA. En effet, quelle que soit la densité d'une image numérique, chacune des impressions de celle-ci différera de toutes les autres impressions, étant donnés les processus aléatoires à l'œuvre durant l'impression. Cependant, pour des images de faibles densités, les différences seront beaucoup moins nombreuses et significatives. Il faut alors une résolution de capture beaucoup plus importante afin de capter les différences qui sont parfois minimes. A l'inverse, pour les codes numériques authentifiants imprimés avec la résolution adéquate il n'est pas nécessaire d'utiliser une résolution de capture particulièrement élevée (un scanner à 1 200 points par pouce se révèle suffisant). De plus, comme les différences sont très significatives, l'extraction des caractéristiques uniques ne doit pas être faite avec une précision très élevée, ce qui est avantageux au niveau du coût et de la stabilité des algorithmes de lecture.

Les marques fragiles à la copie, ou motifs identifiants, sont des images conçues et imprimées de façon à maximiser les différences entre chaque impression d'un même motif identifiant source. Ces images sont préférentiellement conçues de manière pseudo-aléatoires (par exemple avec une ou plusieurs clés cryptographiques), mais elles peuvent être complètement aléatoires (la différence étant que, dans le deuxième cas, il n'existe pas de clé cryptographique, ou la clé n'est pas conservée). Cependant, on note que le motif identifiant numérique d'origine peut être connu sans compromettre la sécurité. En effet, seul le motif identifiant répertorié (ayant leur empreinte) en mémoire est légitime, et il n'est, par principe, pas possible de contrôler les aléas de l'impression. Donc, la possession de l'image d'origine ne donne pas d'avantage réel au contrefacteur : ceci est un autre avantage, en termes de sécurité, des motifs identifiants.

Comme les dégradations sont de nature aléatoire et produisent un résultat différent pour chaque impression d'une même image source, chaque impression d'un motif identifiant recèle des caractéristiques uniques, non reproductibles et non transférables. Ainsi, chacune des

impressions d'un même motif identifiant diffère de toutes les autres, et recèle donc intrinsèquement les moyens de l'identifier sans équivoque. On peut donc calculer une empreinte d'un motif identifiant, et l'utiliser de différentes façons afin d'augmenter la sécurité du produit qui la contient, notamment en modes identification et vérification.

5 Les motifs identifiants peuvent être de simples rectangles, éventuellement encadrés d'une bordure facilitation leur détection, mais peuvent également avoir une forme particulière, tel qu'un logo, etc. Cependant, la forme rectangulaire se révèle avantageuse du point de vue de la lecture (elle est facilement repérable) et de sa compatibilité avec les formes habituelles des codes numériques authentifiants ou autre codes tels que le code barre en une ou deux
10 dimensions.

On décrit, ci-dessous, un algorithme de conception d'un motif identifiant :

- au cours d'une étape 301, on reçoit une clé cryptographique, par exemple une séquence de 32 octets (256 bits),
- au cours d'une étape 302, en utilisant une fonction de hachage ou de chiffrement de
15 manière récursive, l'algorithme étant initialisé avec la clé cryptographique, on génère le nombre requis de bits aléatoires. Le lecteur pourra s'inspirer des normes FIPS (acronyme de « Federal information processing standard » pour standard de traitement d'information fédéral) et AES (acronyme de « Advanced Encryption Standard » pour standard de chiffrement avancé) et
- au cours d'une étape 303, on assemble les bits en une image, par exemple de 100
20 x100 points, éventuellement complétée par une bordure.

La Figure 3 montre un tel motif identifiant, avant l'impression. Les Figures 4 et 5 montrent deux impressions différentes du motif identifiant illustré en figure 3.

Les codes numériques authentifiants (ou « anti-copie ») sont des images conçues et imprimées de façon à maximiser les différences entre l'impression originale et une copie
25 obtenue en utilisant une capture d'une image de l'impression originale et une seconde impression de cette image mettant en œuvre les mêmes valeurs de paramètres d'impression, notamment en termes de résolution, que la première impression.

Les fonctionnalités d'un code numérique authentifiant peuvent être combinées à celles d'un motif identifiant, car les caractéristiques de conception et d'impression des codes
30 numériques authentifiants sont proches de celles requises pour les motifs identifiants. Par exemple, les algorithmes de conception des motifs de détection de copie, qui nécessitent une clé cryptographique, s'apparentent à l'algorithme décrit précédemment, bien que le but recherché soit très différent. Les algorithmes de conception des matrices d'information

sécurisées, eux, nécessitent à la fois une ou plusieurs clés cryptographiques, et un ou plusieurs messages. Le résultat est cependant similaire, soit une image aux valeurs pseudo aléatoires.

Comme on le verra plus loin, il s'avère que les conditions idéales d'impression des motifs identifiants sont proches des conditions idéales d'impression des codes numériques authentifiants. Ainsi, il est possible, autant sur le plan de la conception que du résultat imprimé, de combiner les fonctionnalités des codes numériques authentifiants à celle des matrices d'information.

En ce qui concerne les méthodes d'extraction et, lors de la vérification d'un produit, de comparaison, de l'empreinte d'un motif identifiant, on décrit, d'abord, ci-dessous une méthode d'extraction et de comparaison d'empreinte générique, qui consiste à extraire les valeurs d'un ensemble de points d'un motif identifiant capturé :

- au cours d'une étape 311, on détermine la position des marques robuste 105 et fragile 110 dans l'image du produit marqué. Pour des marques de formes rectangulaires, on peut, par exemple, extraire les positions (hauteur, largeur) des quatre extrémités de chaque marque, Puis, on détermine la zone d'intérêt 100 dans l'image captée,

- au cours d'une étape 312, pour un nombre déterminé de points à extraire, on détermine la position dans l'image capturée et extraire la valeur de chacun des points. La détermination de la position des points peut se faire en utilisant des techniques géométriques standards, connues de l'art antérieur. Les valeurs obtenues pour chaque point du capteur d'image sont, par exemple, sur une échelle de 0 à 255, de même que l'image capturée. Comme les positions peuvent être fractionnaires, la valeur du point prise peut être celle « du plus proche voisin », méthode peu coûteuse mais peu précise ou une valeur interpolée. Le résultat est une matrice 256 x 256 de valeurs entières (plus proche voisin) ou en virgule flottante (interpolation),

- au cours d'une étape 313, on calcule les transformées en cosinus discrètes en deux dimensions de

- la matrice de points correspondant à la marque robuste 105,
- la matrice de points correspondant à la marque fragile 110 et
- la matrice de points correspondant à la partie d'image prédéterminée 115.

La transformée en cosinus discrète est avantageuse car elle permet de compresser fortement l'énergie du signal sur un faible nombre de composants. Au cours de cette même étape 313, on détermine les ratios des distances des centres des éléments 105, 110 et 115 ou les angles du triangle qu'ils forment.

- au cours d'une étape 314, on sélectionne un nombre déterminé de coefficients de chaque transformée, par exemple les 10 x 10 coefficients de fréquence la plus basse, et

éventuellement éliminer le coefficient constant, connu sous le nom de coefficient « DC » à la position (0,0) puis on réordonne les coefficients en un vecteur, qui constitue l'empreinte de la matrice d'information sécurisée.

On note que la méthode décrite précédemment ne met en œuvre aucun secret, et, par conséquent, permet à quiconque de calculer l'empreinte. Ceci peut être souhaitable dans certains cas, où on considère que cela ne pose pas de risque de sécurité. Par contre, dans d'autres cas, il est souhaitable que seules les personnes autorisées puissent calculer l'empreinte. Pour cela, on met en œuvre une clé cryptographique tenue secrète qui permet de déterminer les coefficients constituant l'empreinte. Cette clé n'est divulguée qu'aux personnes ou entités autorisées à reconstituer l'empreinte. Des techniques issues de l'art antérieur sont disponibles à l'homme du métier afin de sélectionner les coefficients à partir de la clé, mettant généralement en œuvre un algorithme de hachage ou un algorithme de chiffrement.

Deux empreintes correspondant à des captures distinctes peuvent alors être comparées de multiples manières, afin d'obtenir une mesure de similarité ou, inversement, une mesure de distance. En mesurant, par exemple, un coefficient de corrélation entre elles, on obtient une mesure de similarité, que l'on dénommera « score » par la suite.

On note que, même si l'image de la marque fragile 110 est inexploitable, les autres éléments de l'empreinte, 105 et 115 ainsi que les relations géométriques (ratios de distances ou angles) permettent d'estimer l'authenticité du produit 20 dont une image a été captée, par comparaison avec les parties correspondantes des empreintes mémorisées à distance.

Pour valider cette méthode d'extraction de caractéristiques uniques, on a généré un motif identifiant de 100 x 100 pixels que l'on a imprimé 100 fois, sur une imprimante laser à 600 points par pouce. Un scanner « flatbed » à 1200 points par pouce a été utilisé pour réaliser trois captures de chaque motif identifiant imprimé. On a ensuite calculé une empreinte pour chacune des 300 captures effectuées. On mesure alors un score pour chacun des 44 850 couples d'empreintes (nombre calculé comme suit : $300 \times (300-1)/2$). On sépare ces 44 850 couples d'empreinte en deux groupes :

- un groupe « A » de 600 couples d'empreintes correspondant à différentes captures du même motif identifiant imprimé et
- un groupe « B » de 44 250 couples d'empreintes correspondant à des captures de différents motifs identifiants imprimés.

Le score est compris entre 0,975 et 0,998 pour le groupe « A », et est compris entre 0,693 et 0,945 pour le groupe « B ». La Figure 8 montre la distribution des scores pour le groupe « A » et pour le groupe « B ». Sur la base de ces scores, il n'y a aucune confusion possible

entre les couples des deux groupes. Ainsi, en utilisant la méthode de calcul d'empreinte décrite précédemment, on peut déterminer sans ambiguïté laquelle des 100 impressions est à l'origine de l'image capturée.

On mesure un « degré de séparation des empreintes », qui consiste à calculer la
5 différence des moyennes des scores pour les groupes « A » et « B » (ici respectivement de 0,992 et 0,863) et à la normaliser par l'écart type des scores du groupe « A », ici de 0,005. On obtient une valeur de 25,8. Comme on le verra plus bas, cet index est utile pour déterminer les paramètres d'impressions et de conceptions donnant les meilleurs résultats.

On décrit, ci-dessous, une deuxième méthode d'extraction d'empreinte concernant les
10 matrices d'information sécurisées. Cette méthode, qui s'applique en particulier lorsque le motif identifiant a également les fonctionnalités d'une matrice d'information sécurisée. Il y est expliqué comment le message brouillé d'une matrice d'information sécurisée captée est extrait. Ce message brouillé possède un taux d'erreur non-nuls et la structure des erreurs est utilisée comme empreinte.

15 Un avantage de cette méthode est qu'elle permet d'utiliser un logiciel conçu pour la lecture des matrices d'information sécurisées, Cela minimise le coût des calculs nécessaires.

Cependant, la lecture précise d'une matrice d'information sécurisée nécessite la clé servant à générer les blocs d'aligner, s'il y a lieu. On ne souhaite pas forcément divulguer cette clé dans tous les cas. De plus, les variations d'alignement interne, spécifiques à chaque
20 impression sont autant que possibles éliminées. Ceci n'est pas forcément souhaitable, car ces variations participent à la différenciation des différentes impressions d'une matrice d'information sécurisée.

En ce qui concerne la méthode de détermination des paramètres de génération et d'impression optimaux des motifs identifiants, il existe un taux de dégradation optimal
25 permettant de séparer le plus aisément possible les différentes impressions d'un même motif identifiant source. Ainsi, si le taux de dégradation à l'impression est très faible, par exemple 1% ou 2% (1 ou 2% des cellules ou pixels du motif identifiant sont mal lues à partir d'une capture parfaite), les différentes impressions d'un même motif identifiant sont très proches l'une de l'autre, et il est difficile de les identifier de manière fiable, à moins d'avoir une capture très
30 précise de l'image et/ou un algorithme d'analyse très précis. Similairement, lorsque le taux de dégradation est très élevé, par exemple 45 à 50 % (45 ou 50 % des cellules de la matrice d'information sécurisée sont mal lues à partir d'une capture parfaite, 50 % signifiant qu'il n'y a aucune corrélation statistique entre la matrice lue et la matrice d'origine), les motifs identifiants imprimées sont quasi indistinctes les unes des autres. En réalité, le taux de dégradation optimal

est proche de 25 %, et si les conditions de l'application le permettent, il est préférable de s'en approcher. En effet, pour 25 % de dégradation, en supposant que les variations d'impression et donc les dégradations soient de nature probabiliste, on maximise, en chacun des points du motif identifiant imprimé, les chances qu'il diffère des autres motifs identifiants imprimés.

5 On donne, ci-dessous, un deuxième analyse des taux d'erreur à rechercher au moment de la génération d'une image à imprimer en fonction des moyens d'impression à mettre en œuvre.

Afin de déterminer comment on peut générer des MPCV permettant d'optimiser la détection de copie, nous présentons ci-dessous un modèle basé sur la théorie de la décision.

10 Les caractéristiques mesurées sur les images (ou points) sont représentées par des signaux. Pour simplifier l'analyse, on y fait l'hypothèse que les signaux numériques, avant impression, ont des valeurs binaires, correspondant à des caractéristiques pouvant avoir des valeurs binaires (par exemple deux tailles de points, deux positions, etc.). Cette hypothèse se justifie par le fait que la plupart des procédés d'impression traitent des images binaires. Evidemment, les

15 conclusions de l'analyse peuvent être étendues à des cas plus complexes, notamment avec plusieurs valeurs possibles de caractéristiques de point. L'impression du MPCV est modélisée par l'ajout de bruit gaussien. Il est également supposé que les copies sont réalisées avec le même procédé d'impression, de sorte que l'impression de la copie est modélisée également par l'ajout de bruit gaussien de même énergie. De plus, le contrefacteur, qui capte le signal avant

20 d'en imprimer une copie est forcé de reconstruire un signal binaire en faisant un estimé de la valeur initiale qui minimise sa probabilité d'erreur.

Ce modèle correspond directement à des MPCV pouvant avoir des tailles de point de 1x1 pixel ou 1x2 pixels (imprimé, par exemple, à 2 400 dpi), pour lequel le contrefacteur doit nécessairement choisir une des tailles de point dans l'image reconstruite à partir d'un scan, en

25 fonction d'un niveau de gris mesuré ou d'une surface estimée du point. Le modèle correspond également à des MPCV avec des positions variant de 1 pixel, par exemple.

A partir de ce modèle, nous dérivons le détecteur optimal, la distribution statistique des valeurs du détecteur, et les valeurs de paramètre qui maximisent la détection de copie.

Le tableau suivant résume les différentes variables.

s	Signal source
n, n_c	Bruit, bruit copie
x	Signal reçu

Sans perte de généralité, le signal source est équiprobable, c'est-à-dire $s[i] : \{+a, -a\}$, pour $i = 0, 1, \dots, N-1$, et $a > 0$. Le bruit d'impression est distribué selon une loi gaussienne $N(0, \sigma^2)$.

Les hypothèses du modèle se résument ainsi:

$$(H0)x[i] : \{+a, -a\} \quad (1)$$

$$(H1)n[i] : N(0, \sigma^2) \quad (2)$$

$$(H2)n_c[i] : N(0, \sigma^2) \quad (3)$$

On peut facilement vérifier que le contrefacteur minimise sa probabilité d'erreur en restaurant le signal à la valeur la plus proche entre $+a, -a$.

Par conséquent, le problème de détection consiste à distinguer les deux hypothèses suivantes :

$$H_0 : x[i] = s[i] + n[i] \quad (4)$$

$$H_1 : x[i] = a \cdot \text{sign}(s[i] + n[i]) + n_c[i] \quad (5)$$

où H_0 et H_1 sont les hypothèses que le signal reçu est un original, respectivement,

une copie.

La probabilité que le contrefacteur a correctement estimé la valeur est :

$$p(\text{sign}(s[i] + n[i]) = s[i]) = p(s[i] + n[i] > 0) \quad (6)$$

$$= p(N(a, \sigma^2) > 0) \quad (7)$$

$$= p(N(0, 1) > -a/\sigma) \quad (8)$$

$$= Q(-a/\sigma) \quad (9)$$

$$\text{où } Q(x) = (2\pi)^{-1/2} \int_{-a/\sigma}^{+\infty} \exp^{-x^2/2} dx.$$

Nous avons les distributions de probabilité suivantes pour le signal reçu, où dans l'hypothèse H_1 nous avons une mixture de deux distributions Gaussiennes.

$$p(x; H_0) = \frac{1}{(2\pi\sigma^2)^{N/2}} \exp\left[-\frac{1}{2\sigma^2} \sum_{n=0}^{N-1} (x[n] - s[n])^2\right] \quad (10)$$

$$p(x; H_1) = (1 - Q(-a/\sigma)) \frac{1}{(2\pi\sigma^2)^{N/2}} \exp\left[-\frac{1}{2\sigma^2} \sum_{n=0}^{N-1} (x[n] + s[n])^2\right] + \quad (11)$$

$$Q(-a/\sigma) \frac{1}{(2\pi\sigma^2)^{N/2}} \exp\left[-\frac{1}{2\sigma^2} \sum_{n=0}^{N-1} (x[n] - s[n])^2\right] \quad (12)$$

Nous allons vérifier qu'un simple corrélateur donne une fonction de classification optimale. Un test de Neyman-Pearson detector décide H_1 si le rapport de vraisemblance excède un seuil t :

$$L(\mathbf{x}) = \frac{p(\mathbf{x}; H_1)}{p(\mathbf{x}; H_0)} > t \quad (13)$$

5 Le rapport de vraisemblance est donné par:

$$L(\mathbf{x}) = Q(-a/\sigma) + (1 - Q(-a/\sigma)) \exp\left[-\frac{1}{2\sigma^2} \left(\sum_{n=0}^{N-1} (x[n] + s[n])^2 + \frac{1}{2\sigma^2} \sum_{n=0}^{N-1} (x[n] - s[n])^2\right)\right] \quad (14)$$

Prenant le logarithme, et un nouveau seuil t' , on obtient :

$$T'(x, s) = \sum_{n=0}^{N-1} x[n]s[n] < t' \quad (15)$$

10 La fonction de classification est donc un simple corrélateur T' , dont la valeur doit être inférieure à un seuil t' pour classer le signal comme copie.

Déterminons les statistiques de T' pour les deux hypothèses. Nous pouvons supposer que T' suit une gaussienne (vrai pour N élevé) dont nous nous dérivons les moyennes et variances pour les deux hypothèses :

$$E[T'; H_0] = Na^2 \quad (16)$$

$$15 \quad E[T'; H_1] = Q(-a/\sigma)Na^2 - (1 - Q(-a/\sigma))Na^2 = (2Q(-a/\sigma) - 1)Na^2 \quad (17)$$

$$Var[T'; H_0] = Na^2\sigma^2 \quad (18)$$

$$Var[T'; H_1] = N(a^2\sigma^2 + a^4Q(-a/\sigma)(1 - Q(-a/\sigma))) \quad (19)$$

20 Le deuxième terme de la variance pour l'hypothèse H_1 , $(a^4Q(-a/\sigma)(1 - Q(-a/\sigma)))$, peut être éliminé si les copies viennent du même original. En pratique, le contrefacteur minimise son travail en n'utilisant qu'un original pour produire un grand nombre copies, il est raisonnable d'éliminer le terme.

Dans le cas où les variances sont égales, on peut caractériser la performance de détection par le coefficient de déflexion d^2 , qui correspond à la différence entre les moyenne de la fonction T' pour les deux hypothèses, normalisée par la variance de T' :

$$25 \quad d^2 = \frac{(E[T'; H_0] - E[T'; H_1])^2}{Var[T'; H_0]} \quad (22)$$

$$= \frac{2N^2a^4(1 - Q(-a/\sigma))^2}{Na^2\sigma^2} \quad (23)$$

$$= \frac{2Na^2(1-Q(-a/\sigma))^2}{\sigma^2} \quad (24)$$

$$= 2N(\gamma(1-Q(\gamma)))^2 \quad (25)$$

où $\gamma = a/\sigma$ est la racine carrée du rapport signal sur bruit.

La performance de détection croissant avec le coefficient de déflexion, l'objectif est

- 5 de déterminer la valeur de γ maximisant l'expression $(\gamma(1-Q(\gamma)))^2$.

La Figure 9 représente la valeur de l'expression en fonction de γ . On peut interpréter cette figure comme suit. Les valeurs de γ proche de zéro correspondent à un bruit très élevé par rapport au signal : lorsque le bruit est très élevé, le signal est trop dégradé dès la première impression, le contrefacteur introduit un nombre d'erreurs d'estimation trop faible. A l'inverse, pour des valeurs de γ trop élevées, le signal n'est pas suffisamment dégradé, et dans une trop grande proportion des cas le contrefacteur n'introduira pas d'erreur d'estimation. Entre les deux extrêmes, l'expression passe par une valeur optimale, dont on estime numériquement la valeur à $\gamma \approx 0.752$.

Il est intéressant de noter que pour cette valeur, la probabilité que le contrefacteur n'ait pas déterminé correctement la valeur, est d'environ 22,6%.

En pratique, il s'agit d'obtenir un rapport signal sur bruit γ^2 aussi proche que possible de $0,752^2$, soit 0,565.

Prenons un exemple pour mieux comprendre comment viser cette valeur de rapport. Supposons que nous générons un MPCV avec deux tailles de point (exprimées en nombre de pixels) possibles, la taille de point étant de l'ordre de neuf pixels (par exemple, 3x3 pixels). On note que la taille de point peut être mesurée en mettant en œuvre une multitude d'algorithmes, par exemple par seuillage adaptatif local du niveau de gris et dénombrement des pixels en dessous du seuil. On imprime un nombre suffisant de fois des points de neuf pixels. On mesure, dans une image capturée, la moyenne et l'écart-type du nombre de pixels de chaque point. Supposons qu'on obtient une moyenne de douze (on observe un gain physique moyen de 33 %), et un écart-type de quatre. Cet écart-type correspond à la valeur σ décrivant le bruit dans les formules de notre modèle. On visera alors une valeur de notre signal a de l'ordre de trois, pour obtenir un rapport $\gamma = 0.75$, soit très près de l'optimum. Pour obtenir cette valeur de signal, on peut par exemple définir deux tailles de points de quinze et de six pixels.

On décrit, ci-dessous, un algorithme possible d'optimisation des paramètres d'impression :

- au cours d'une étape 320, on reçoit la surface disponible pour le motif identifiant, par exemple un carré dont le côté mesure 1/6 de pouce,

5 - au cours d'une étape 321, on génère plusieurs images numériques de motifs identifiants de dimensions numériques différentes, correspondant aux différentes résolutions d'impression possibles, par exemple un motif identifiant de 66 x 66 pixels à 400 points par pouce, un de 100 x 100 pixels à 600 points par pouce, un de 133 x 133 pixels à 800 points par pouce, un de 200 x 200 pixels à 1200 points par pouce,

10 - au cours d'une étape 322, on imprime plusieurs fois chacun des motifs identifiants de dimensions numériques différentes, par exemple 100 fois, avec la résolution adéquate de façon à ce que les dimensions de l'impression correspondent à la surface disponible.

- au cours d'une étape 323, pour chaque type, on capture plusieurs fois chacun des motifs identifiants imprimés, par exemple trois fois,

- au cours d'une étape 324, on calcule l'empreinte de chaque motif identifiant,

15 - au cours d'une étape 325, on calcule les scores de similarité pour toutes les paires de motif identifiant capturés de même résolution d'impression et

- au cours d'une étape 326, on suit la méthode décrite dans l'expérimentation de la méthode extraction d'empreinte générique exposée plus haut pour mesurer le « degré de séparation des empreintes », pour chacune des résolutions d'impression, et choisir la résolution d'impression donnant la valeur maximale de ce degré.

20 En variante, on imprime plusieurs matrices d'information sécurisées à différentes résolutions d'impression, et on détermine la résolution d'impression résultant en un taux d'erreur de 25 %, tel que calculé avec un des algorithmes décrits par ailleurs.

25 En variante, on choisit la résolution d'impression dont la différence est la plus élevée entre la plus basse valeur de score calculée sur la comparaison entre les empreintes correspondant à des impressions identiques, et la plus haute valeur de score calculée sur la comparaison entre les empreintes correspondant à des impressions différentes.

30 En ce qui concerne la méthode de représentation et stockage des caractéristiques, il est avantageux de réduire, autant que possible, le volume de données de l'empreinte. Dans le cas de l'identification, il s'agit de comparer une empreinte à un grand nombre d'empreintes stockées sur une base de données, ce qui est très coûteux. On réduit ce coût en réduisant la taille des empreintes à comparer, notamment en évitant d'utiliser des nombres en virgule flottante.

Prenons le cas de la méthode générique d'extraction d'empreinte. Le vecteur de données initial extrait d'un motif identifiant capté est la matrice de valeurs extraites 256 x 256, et

sa représentation par une transformée en cosinus discrète après sélection de coefficients, possède 10 x 10 valeurs. Il est avantageux de représenter la matrice de valeurs avec un octet par valeur, soit 100 octets.

5 Au cours d'une étape 327, on imprime au moins un produit avec un motif identifiant pour former un produit sécurisé.

En revanche, les coefficients de la transformée en cosinus discrète peuvent prendre des valeurs tant positives que négatives, et ne sont en principe pas limitées. Afin de représenter de telles valeurs avec une quantité d'information fixée, les valeurs doivent être quantifiées afin d'être représentées en valeurs binaires. Une approche possible est la suivante :

10 - au cours d'une étape 331, on détermine, à l'avance, une valeur minimale et une valeur maximale pour chaque coefficient. En général, les valeurs minimales et maximales ont la même valeur absolue,

- au cours d'une étape 332, on détermine le nombre de bits ou octets permettant de représenter chaque valeur et

15 - au cours d'une étape de normalisation 333, pour chaque coefficient de la transformée en cosinus discrète, on soustrait la valeur minimale, puis on divise le reste par la valeur maximale,

- au cours d'une étape 334, on multiplie le résultat par le nombre de valeurs possible des données quantifiées, soit 256 si un octet est disponible pour chaque valeur. La valeur
20 entière du résultat correspondant à la valeur d'origine quantifiée.

En variante, les pas de quantifications sont optimisés de façon à minimiser l'erreur de quantification.

Pour vérifier l'authenticité d'un produit, un consommateur prend une image comportant au moins la marque robuste, la marque fragile à la copie et une autre partie du produit.

25 Dans des modes de réalisation, on met en œuvre les étapes suivantes :

- au cours d'une étape 340, on détermine l'empreinte de la marque fragile, ou motif identifiant, contenue dans l'image captée,

- au cours d'une étape 341, on détermine si cette empreinte est de qualité suffisante, par exemple, en déterminant combien de valeurs de l'empreinte sont supérieures une valeur
30 prédéterminée (en effet, une image floue ou ne présentant pas une résolution suffisante aura pour ses coefficient de haute fréquence, des valeurs très faibles),

- si oui, au cours d'une étape 342, on calcule le score, ou similarité, de l'empreinte obtenue à l'étape 340, avec chacune des empreintes stockées dans la base de données distante 40,

- au cours d'une étape 343, on détermine la similarité maximale obtenue, en comparant l'empreinte calculée avec toutes les empreintes correspondant au même type de produit conservées à distance, par exemple dans une base de données,

- au cours d'une étape 344, si la similarité maximale est supérieure à une valeur seuil, le motif identifiant est jugé valide, c'est-à-dire que le produit 20 est authentique et, au cours d'une étape 345, on retrouve les informations de traçabilité associées,
- sinon, au cours d'une étape 346, le motif identifiant est jugé comme non-valide.

En variantes :

- au cours d'une étape 347, si le motif identifiant possède également les fonctionnalités d'un code numérique authentifiant, on extrait les informations de traçabilité,
- au cours d'une étape 348, les informations de traçabilité permettant de réduire l'espace de recherche peuvent également provenir d'une autre source, par exemple code barre associé, renseignement par le contrôleur, lecture de mémoire non volatile du produit, etc et
- au cours d'une étape 349, on exploite ces informations afin de réduire l'espace de recherche dans la base de données. Par exemple, l'information de l'ordre de fabrication permet d'effectuer une présélection des empreintes à comparer parmi le sous-ensemble d'empreintes correspondant à cet ordre de fabrication.

Si le résultat du test 341 est négatif, au cours d'une étape 351, on détermine la similarité de la marque robuste 105, de l'autre partie d'image 115 et des données géométriques (ratios de distances ou angles), comme exposé ci-dessus, en référence à la base de données 40. Puis, au cours d'une étape 352, on détermine si le produit 20 est authentique en fonction de la similarité maximale trouvée.

Au cours d'une étape 353, on effectue les étapes 347 à 349.

En ce qui concerne la méthode de vérification sans base de données, elle nécessite que l'empreinte pré-calculée du motif identifiant soit stockée sur le produit 20. Par exemple, lors de l'étape du calcul de l'empreinte de chacun des produits légitimes, celles-ci peuvent être à la fois destinées à être stockées dans une base de données 40, et à être stockées de manière sécurisée sur le produit 20 par exemple dans une marque robuste supplémentaire formée sur le produit 20.

En ce qui concerne un usage combiné d'un motif identifiant avec fonctionnalités d'un code numérique authentifiant, les méthodes de caractérisation unique des produits de l'art antérieur utilisent des caractéristiques non interprétables sans appel à une base de données. Par contre, si les motifs identifiants peuvent être de simples images sans significations, comme on l'a vu, ils peuvent également être des images comportant d'autres fonctionnalités.

Notamment, ils peuvent être des codes numériques authentifiants, auquel cas ils peuvent comporter des informations sécurisées (une ou plusieurs clés sont nécessaires pour les lire), et/ou avoir des propriétés authentifiantes (distinguer un original d'une copie).

On observe, en figure 2 :

- 5 - une étape 205 de détermination d'une matrice de points représentative d'une information associée à un produit à authentifier,
- une étape 210 d'apposition au produit d'une marque robuste 105 et d'une marque 110 fragile à la copie, de telle manière que la marque fragile présente des erreurs imprévisibles du fait des caractéristiques physiques des moyens mis en œuvre au cours de l'étape de
- 10 marquage,
- une étape 215 de capture d'une image de la marque robuste 105, de la marque fragile 110 et d'une autre partie 115 du produit 20 (voir figure 10), avec éventuellement, une étape d'extraction de la partie 100 de l'image,
- une étape 220 de détermination de caractéristiques physiques de l'image ou de la
- 15 partie d'image 100 par traitement d'image et
- une étape 225 de mémorisation, en mémoire distante, par exemple sur un serveur accessible par Internet, d'une information représentative des caractéristiques physiques des erreurs imprévisibles, ou empreinte.

 Au cours de l'étape 205, on détermine les marques robuste 105 (par exemple un

20 Datamatrix) et fragile à la copie 110 (par exemple un CNA ou un MPCV), par exemple sous la forme d'une matrice de zones comportant, chacune, des centaines de points et représentatives, pour au moins une partie, d'une information binaire. L'information associée au produit 20 dans l'une et/ou l'autre de ces marques 105 et 110 est, par exemple, le nom de son fabricant, l'ordre de fabrication du produit et/ou la date de fabrication.

25 Au cours de l'étape 210, on appose la marque robuste 105. On appose conjointement la marque fragile 110, formée d'une matrice de points, avec une résolution telle qu'au moins deux, préférentiellement au moins cinq, pour cent des points de la marque fragile à la copie 110 soient erronés, préférentiellement de manière individuellement imprévisible, en comparaison avec la matrice de points originale. Par exemple, on utilise la résolution maximale d'une

30 imprimante. Cette résolution a, notamment, pour effet, que la copie du produit, qui impose une copie de la marque fragile à la copie 110, par exemple par des procédés optiques ou photographiques, augmente d'au moins cinquante pour cent le taux d'erreurs dans la marque copiée, en comparaison avec la marque initiale.

Préférentiellement, au cours de l'étape 210, les positions respectives de l'autre partie d'image 115 et d'au moins l'une des marques 105 et 110 est aléatoire.

5 Au cours de l'étape 220, on détermine, comme caractéristiques physiques ou empreinte du produit 20, des caractéristiques représentatives de la répartition des erreurs dans la marque fragile 110 et de la partie 115 du produit 20 extérieure aux marques 105 et 110. Par exemple, on détermine le vecteur allant du centre de la partie 115 au barycentre des erreurs portées par la marque fragile 110, puis on affecte les erreurs d'un poids dépendant de leur position et on détermine un nouveau vecteur et ainsi de suite sur plusieurs itérations. On effectue la même succession d'étapes sur la marque robuste 105 pour obtenir une empreinte
10 indépendante de la marque fragile à la copie mais dépendant de la marque robuste 105 et de la partie 115 du produit 20.

Grâce à la mise en œuvre de la présente invention, bien que le même processus de marquage soit mis en œuvre, sans modification, par exemple par gravure ou impression, sur de nombreux produits 20, les caractéristiques physiques des marques et de l'élément 115
15 permettent de donner au moins une identification unique, ou empreinte, à chaque produit 20. A défaut, les éléments 105 et 115 et, éventuellement, des données géométriques, permettent d'estimer l'authenticité du produit 20.

Lorsqu'un consommateur veut vérifier l'authenticité du produit 20, une nouvelle capture d'image est effectuée par lui sur ce produit marqué 20. Un nouveau traitement d'image est
20 appliqué et le résultat de ce traitement d'image est comparé à l'information mémorisée en mémoire distante pour vérifier l'authenticité du produit 20.

La quantité d'erreur est importante et permet une identification unique de la marque et du produit. Même au cas où l'image de la marque fragile à la copie n'est pas exploitable, en mettant en œuvre des informations liées à la marque robuste 105 et à la partie 115 de l'image,
25 on peut vérifier l'authenticité du produit 20.

La lecture des données relatives au produit qui porte la marque robuste 105 fournit une origine et/ou des moyens d'accès à une base de données de caractéristiques physiques des erreurs.

Quelles que soient les conditions de capture d'une nouvelle image de ladite marque,
30 les caractéristiques du produit peuvent être retrouvées.

REVENDEICATIONS

1. Procédé de marquage de produit, caractérisé en ce qu'il comporte :

- une étape de formation, sur ou dans ledit produit, d'une marque robuste à la copie, avec une première résolution,

5 - une étape de formation, sur ou dans ledit produit, d'une marque fragile à la copie, avec une deuxième résolution supérieure à la première résolution,

- une étape de capture d'une image de ladite marque robuste, de ladite marque fragile et d'une autre partie du produit et

- une étape de mémorisation d'une information représentative de l'image de ladite marque robuste, de ladite marque fragile et de ladite autre partie d'image.

10 2. Procédé selon la revendication 1, dans lequel, au cours d'au moins une étape de formation, la position de la marque formée au cours de cette étape de formation, par rapport à l'autre partie d'image, est aléatoire.

3. Procédé selon l'une quelconque des revendications 1 ou 2, dans lequel ladite marque robuste est un code à barres en deux dimensions.

15 4. Procédé selon l'une des revendications 1 à 3, dans lequel ladite marque fragile à la copie est un code numérique authentifiant, ledit procédé comportant une étape de détermination d'une information représentative des erreurs d'impression de ladite marque fragile à la copie et au cours de l'étape de mémorisation, on mémorise ladite information représentative des erreurs d'impression.

20 5. Procédé selon l'une des revendications 1 à 4, dans lequel, au cours de chacune des étapes de formation de marques, la position de ladite marque par rapport à un élément du produit est variable et, lors de l'étape de capture d'une image, on capte une image dudit élément.

25 6. Procédé selon l'une des revendications 1 à 5, dans lequel, au cours des étapes de formation de marques, on décale, entre deux produits différents, différemment les marques formées.

7. Dispositif de marquage de produit, caractérisé en ce qu'il comporte :

- un moyen de formation, sur ou dans ledit produit, d'une marque robuste à la copie, avec une première résolution,

- un moyen de formation, sur ou dans ledit produit, d'une marque fragile à la copie, avec une deuxième résolution supérieure à la première résolution,

- un capteur d'image adapté à capté une image de ladite marque robuste, de ladite marque fragile et d'une autre partie du produit et

5 - un moyen de mémorisation d'une information représentative de l'image de ladite marque robuste, de ladite marque fragile et de ladite autre partie d'image.

8. Dispositif selon la revendication 7, dans lequel, au moins l'un des moyens de formation est adapté à ce que la position de la marque formée par rapport à l'autre partie d'image, soit aléatoire.

10 9. Dispositif selon l'une quelconque des revendications 7 ou 8, dans lequel le moyen de formation de ladite marque robuste est adapté à ce que ladite marque robuste soit un code à barres en deux dimensions.

15 10. Dispositif selon l'une des revendications 7 à 9, dans lequel le moyen de formation de ladite marque fragile est adapté à ce que ladite marque fragile à la copie soit un code numérique authentifiant, ledit dispositif comportant un moyen de détermination d'une information représentative des erreurs d'impression de ladite marque fragile à la copie et le moyen de mémorisation étant adapté à mémoriser ladite information représentative des erreurs d'impression.

20 11. Dispositif selon l'une des revendications 7 à 10, dans lequel, chacun des moyens de formation de marques est adapté à ce que la position de la marque par rapport à un élément du produit est variable et le moyen de capture d'une image est adapté à capter une image dudit élément.

25 12. Dispositif selon l'une des revendications 7 à 11, dans lequel, chaque moyen de formation de marque est adapté à décale, entre deux produits différents, différemment les marques formées.

13. Procédé d'authentification de produit, caractérisé en ce qu'il comporte :

- une étape de capture, sur ledit produit d'une image d'une marque robuste et d'une marque fragile à la copie de résolution plus élevée que la marque robuste et d'une autre partie du produit,

30 - une étape de transmission d'une information représentative de l'image de ladite marque robuste, de ladite marque fragile et de ladite autre partie d'image,

- une étape de comparaison de ladite information représentative de l'image de ladite marque robuste, de ladite marque fragile et de ladite autre partie d'image avec au moins une information mémorisée à distance et

- en fonction du résultat de ladite étape de comparaison, une étape d'affichage de données relatives au produit dont une image a été captée.

14. Procédé selon la revendication 13, dans lequel, au cours de l'étape de comparaison, on effectue, d'abord, une étape de détermination de qualité de l'image de la marque fragile à la copie et :

- si la qualité est supérieure à une valeur prédéterminée, une comparaison d'une information représentative de la marque fragile à la copie et,

- sinon, une comparaison d'une information représentative de l'autre partie du produit.

15. Dispositif d'authentification de produit, caractérisé en ce qu'il comporte :

- un moyen de capture, sur ledit produit d'une image d'une marque robuste et d'une marque fragile à la copie de résolution plus élevée que la marque robuste et d'une autre partie du produit,

- un moyen de transmission d'une information représentative de l'image de ladite marque robuste, de ladite marque fragile et de ladite autre partie d'image,

- un moyen de comparaison de ladite information représentative de l'image de ladite marque robuste, de ladite marque fragile et de ladite autre partie d'image avec au moins une information mémorisée à distance et

- un moyen d'affichage de données relatives au produit dont une image a été captée, en fonction du résultat fourni par le moyen de comparaison.

16. Dispositif selon la revendication 15, dans lequel le moyen de comparaison est adapté à effectuer, d'abord, une étape de détermination de qualité de l'image de la marque fragile à la copie et :

- si la qualité est supérieure à une valeur prédéterminée, une comparaison d'une information représentative de la marque fragile à la copie et,

- sinon, une comparaison d'une information représentative de l'autre partie du produit.

1/8

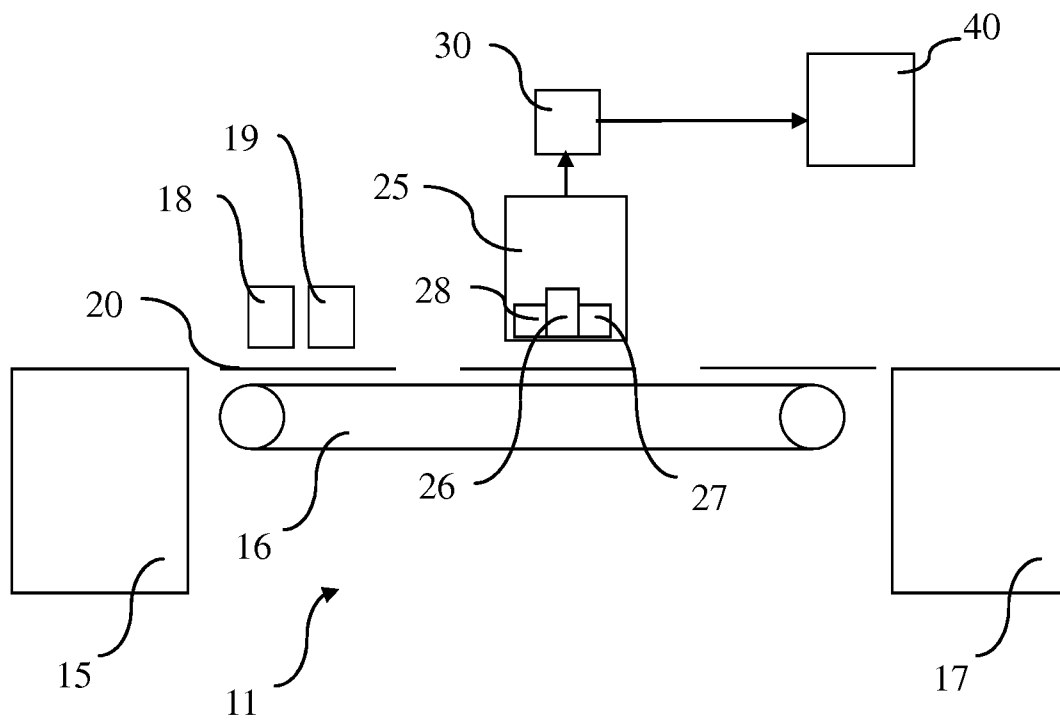


Figure 1

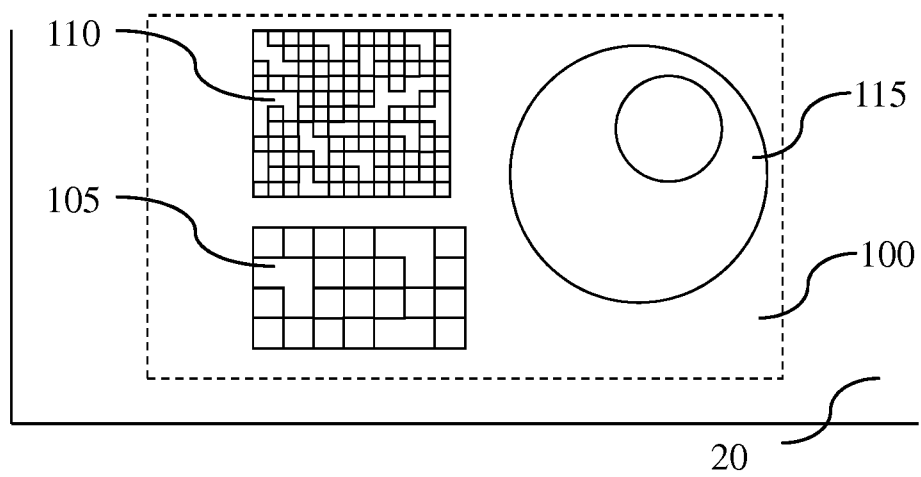


Figure 10

2/8

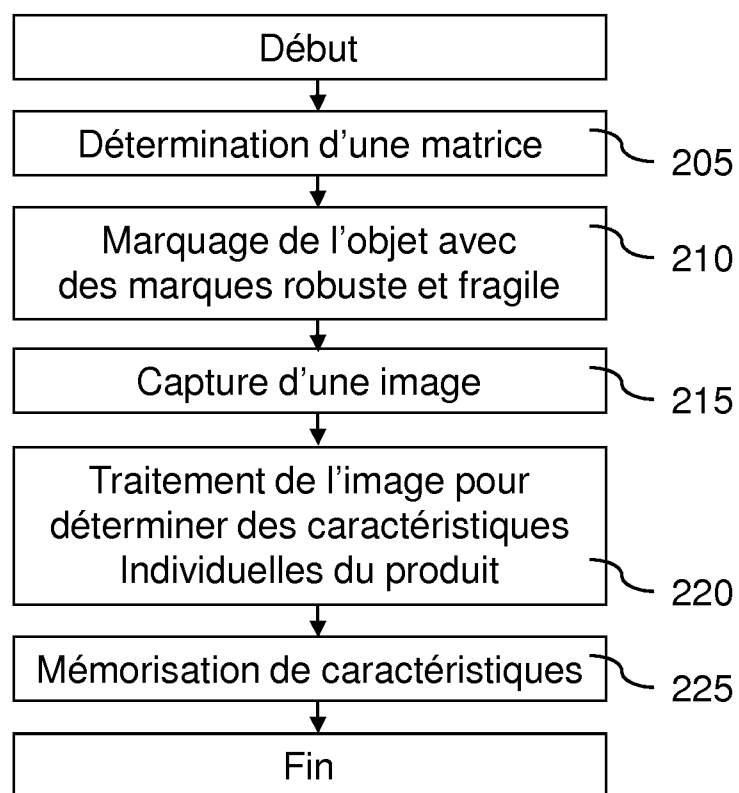


Figure 2

3/8

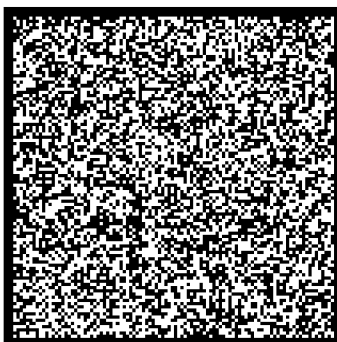


Figure 3

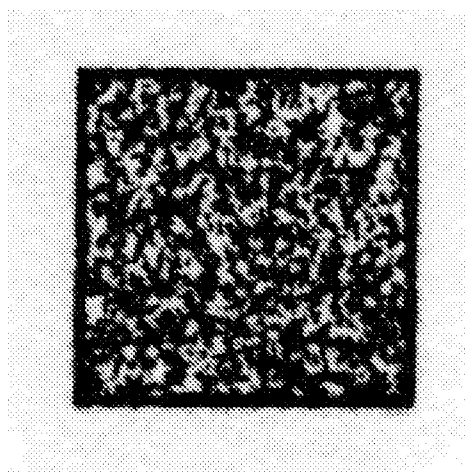


Figure 4

4/8

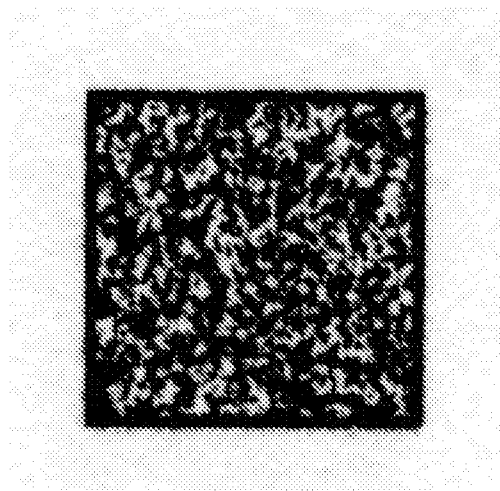


Figure 5

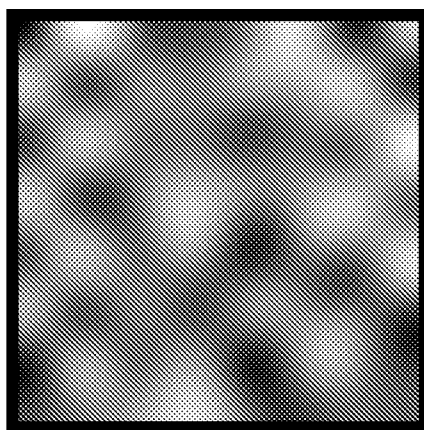


Figure 6

5/8

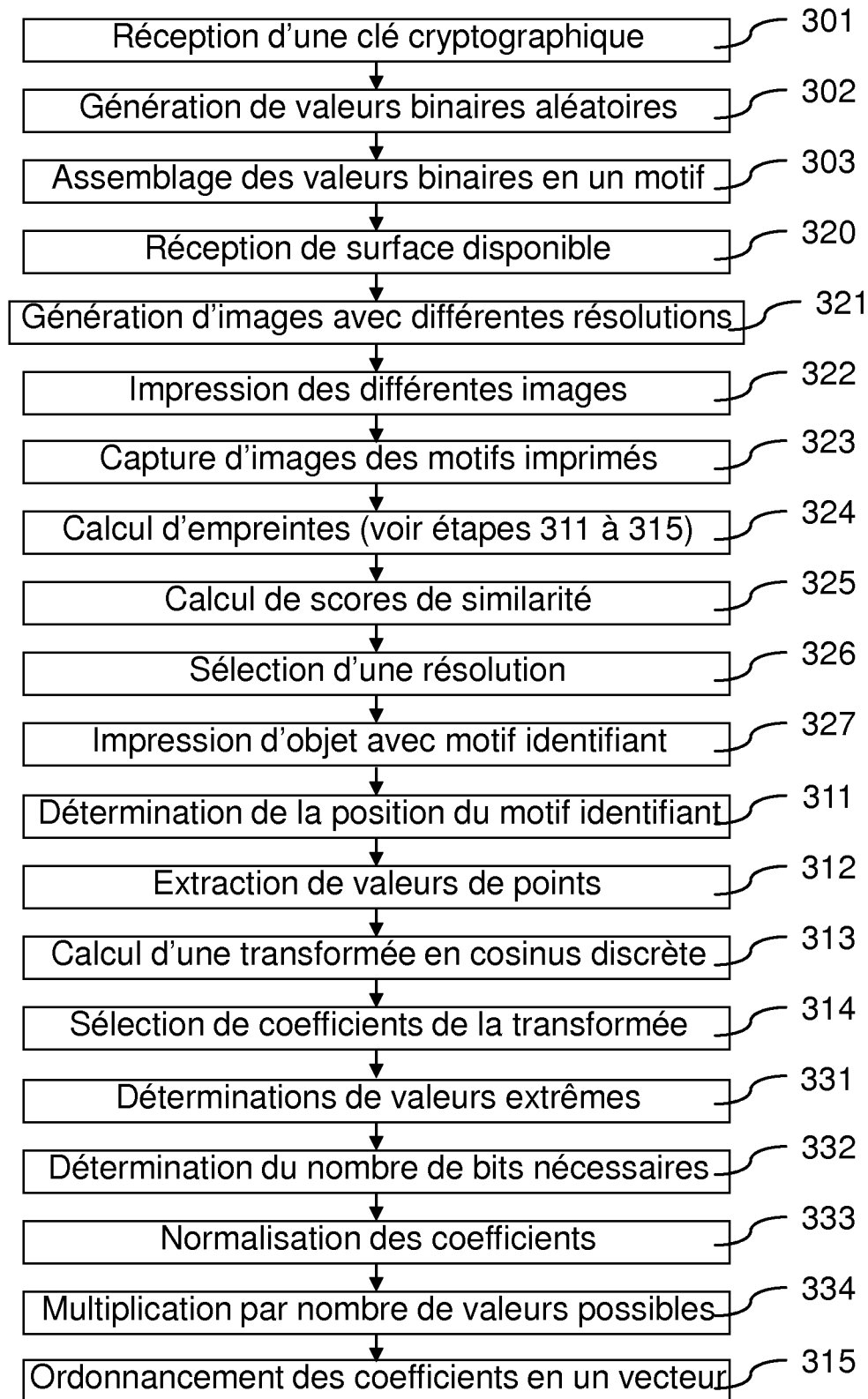


Figure 7A

6/8

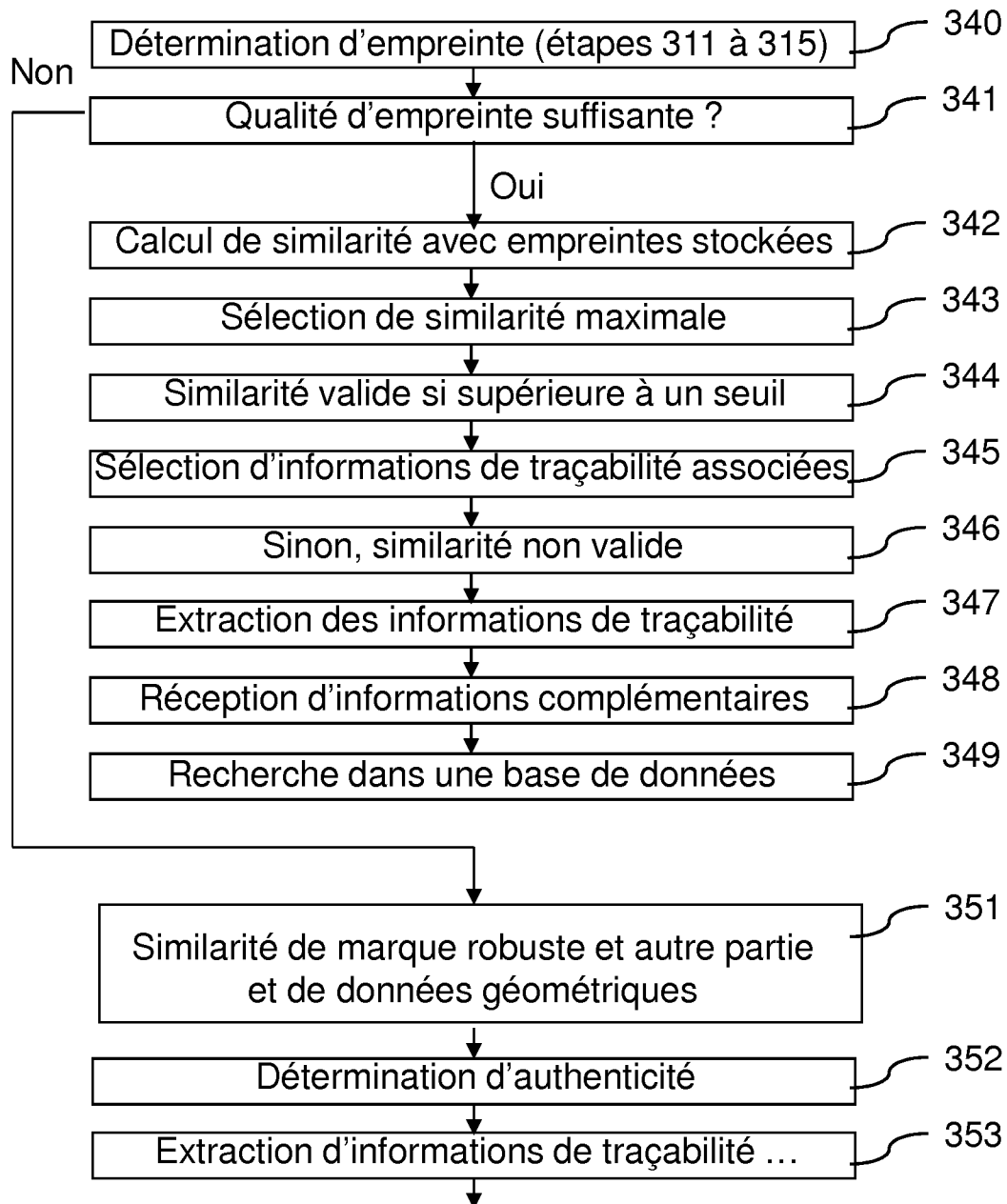


Figure 7B

7/8

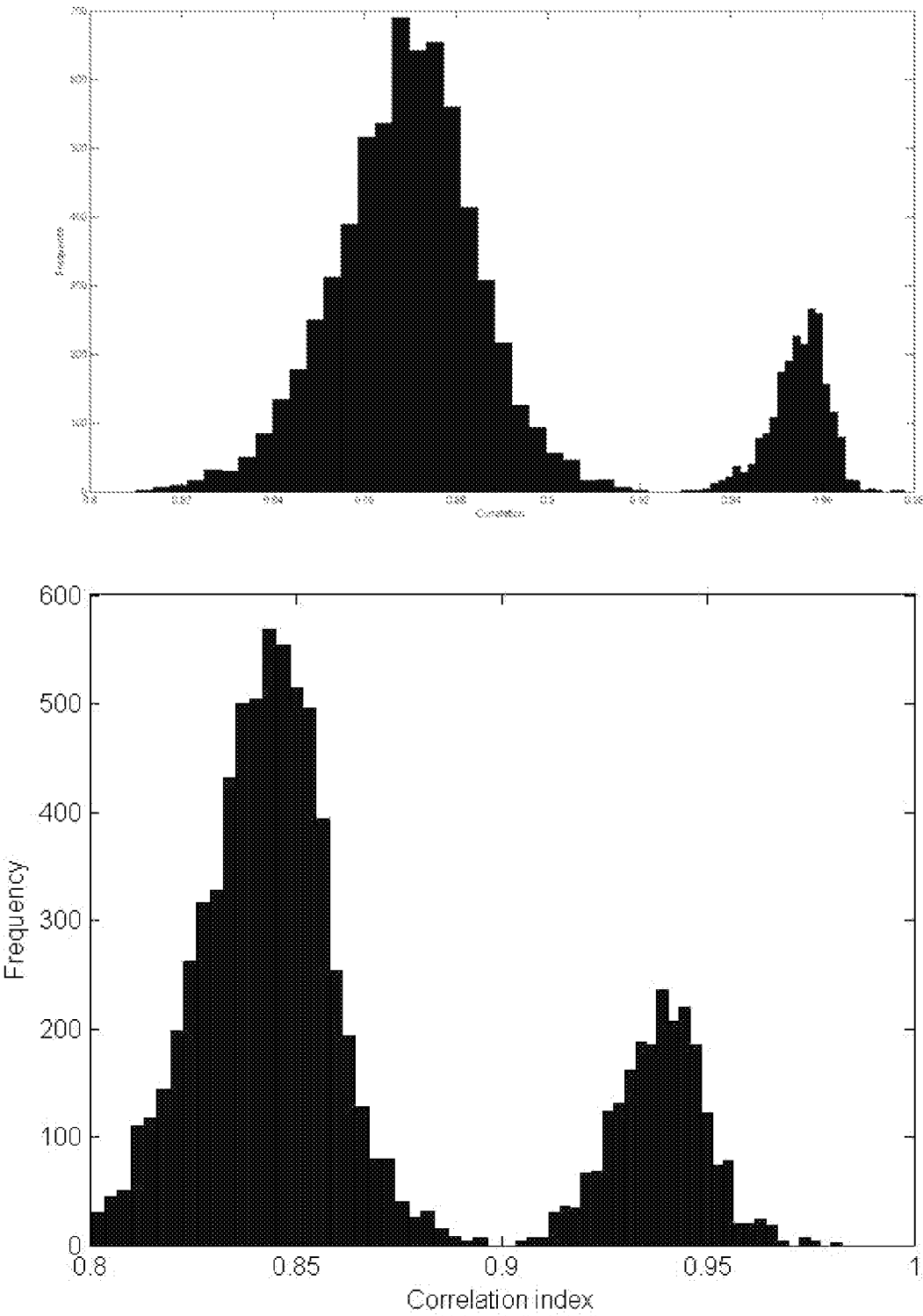


Figure 8

8/8

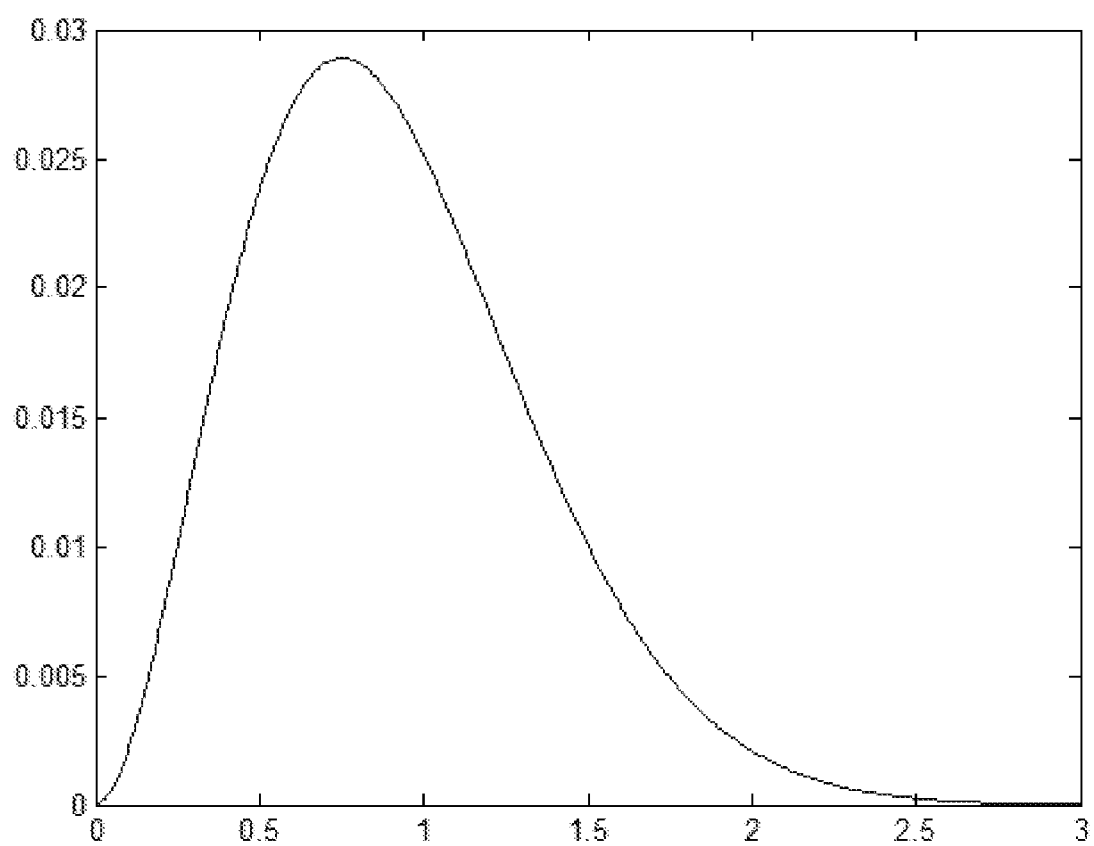


Figure 9

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2011/051727

A. CLASSIFICATION OF SUBJECT MATTER INV. G07D7/00 G07D7/20 ADD.		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) G07D		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practical, search terms used) EPO-Internal, WPI Data		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 1 672 593 A2 (PITNEY BOWES INC [US]) 21 June 2006 (2006-06-21) paragraph [0008] - paragraph [0010] paragraph [0032] - paragraph [0054] figures 1-10 -----	1-16
A	DE 102 24 256 A1 (HAASE BERND [DE]; MAEDER ANDREAS [DE]) 24 December 2003 (2003-12-24) the whole document -----	1-16
A	WO 2008/009826 A2 (ADVANCED TRACK & TRACE [FR]; MASSICOT JEAN-PIERRE [FR]; FOUCOU ALAIN []) 24 January 2008 (2008-01-24) abstract; figures page 1, line 10 - page 20, line 17 -----	1-16
☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.		
* Special categories of cited documents :		
"A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art. "&" document member of the same patent family		
Date of the actual completion of the international search	Date of mailing of the international search report	
8 November 2011	22/11/2011	
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Authorized officer Bocage, Stéphane	

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/FR2011/051727

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
EP 1672593	A2	21-06-2006	EP 1672593 A2	21-06-2006
			US 2006126094 A1	15-06-2006

DE 10224256	A1	24-12-2003	NONE	

WO 2008009826	A2	24-01-2008	EP 2054836 A2	06-05-2009
			WO 2008009826 A2	24-01-2008

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°

PCT/FR2011/051727

A. CLASSEMENT DE L'OBJET DE LA DEMANDE INV. G07D7/00 G07D7/20 ADD.		
Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB		
B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE Documentation minimale consultée (système de classification suivi des symboles de classement) G07D		
Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche		
Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés) EPO-Internal, WPI Data		
C. DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	EP 1 672 593 A2 (PITNEY BOWES INC [US]) 21 juin 2006 (2006-06-21) alinéa [0008] - alinéa [0010] alinéa [0032] - alinéa [0054] figures 1-10 -----	1-16
A	DE 102 24 256 A1 (HAASE BERND [DE]; MAEDER ANDREAS [DE]) 24 décembre 2003 (2003-12-24) le document en entier -----	1-16
A	WO 2008/009826 A2 (ADVANCED TRACK & TRACE [FR]; MASSICOT JEAN-PIERRE [FR]; FOUCOU ALAIN []) 24 janvier 2008 (2008-01-24) abrégé; figures page 1, ligne 10 - page 20, ligne 17 -----	1-16
☐ Voir la suite du cadre C pour la fin de la liste des documents ☒ Les documents de familles de brevets sont indiqués en annexe		
* Catégories spéciales de documents cités: "A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent "E" document antérieur, mais publié à la date de dépôt international ou après cette date "L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée) "O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens "P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée "T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention "X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément "Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier "&" document qui fait partie de la même famille de brevets		
Date à laquelle la recherche internationale a été effectivement achevée 8 novembre 2011		Date d'expédition du présent rapport de recherche internationale 22/11/2011
Nom et adresse postale de l'administration chargée de la recherche internationale Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Fonctionnaire autorisé Bocage, Stéphane

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°

PCT/FR2011/051727

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 1672593	A2	21-06-2006	EP 1672593 A2	21-06-2006
			US 2006126094 A1	15-06-2006

DE 10224256	A1	24-12-2003	AUCUN	

WO 2008009826	A2	24-01-2008	EP 2054836 A2	06-05-2009
			WO 2008009826 A2	24-01-2008
