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

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
8 novembre 2012 (08.11.2012)

WIPO | PCT

(10) Numéro de publication internationale
WO 2012/150411 A1

(51) Classification internationale des brevets :
G07F 7/08 (2006.01) *G06T 1/00* (2006.01)

(21) Numéro de la demande internationale :
PCT/FR2012/050968

(22) Date de dépôt international :
30 avril 2012 (30.04.2012)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1153713 1 mai 2011 (01.05.2011) FR
1101548 19 mai 2011 (19.05.2011) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **SIGNOPTIC TECHNOLOGIES** [FR/FR]; 5 Allee du Lac d'Aiguebelette, F-73370 Le Bourget du Lac (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **BOUTANT, Yann** [FR/FR]; 147 rue du Champ Collomb, F-73310 Chindrieux (FR). **FOURNEL, Thierry** [FR/FR]; 12 rue Blériot, F-42330 Saint-Galmier (FR).

(74) Mandataire : **LE CACHEUX, Samuel**; CAPISTEL, 10 montée des lilas, F-69300 Caluire (FR).

(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, QA, RO, RS, RU, RW, 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.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, 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, 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))*

(54) Title : METHOD OF UNITARY AUTHENTICATION OF A HARDWARE OBJECT COMPRISING VISUAL CRYPTOGRAPHY AND MATERIAL SIGNATURE

(54) Titre : PROCEDE D'AUTHENTIFICATION UNITAIRE D'UN OBJET MATERIEL COMBINANT CRYPTOGRAPHIE VISUELLE ET SIGNATURE MATIERE

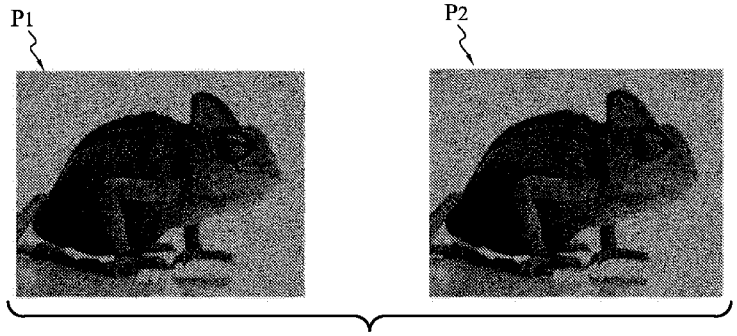


FIG.4

(57) Abstract : The invention relates to a method of unitary authentication of a hardware object comprising a phase of constructing an authenticator system comprising at least: a step of selecting a message image, a step of selecting a support image, a step of transforming the message and support images so as to generate at least two shared images according to a method of transformation implementing at least one random sequence, the message image not being accessible in each shared image taken individually, a step of recording at least one shared image. According to the invention, in the phase of constructing an authenticator each random sequence, termed a material signature, is extracted or generated from at least one structural characteristic of a region at least of the hardware object and able to be generated on demand and identically on the basis of the hardware object.

(57) Abrégé : L'invention concerne un procédé d'authentification unitaire d'un

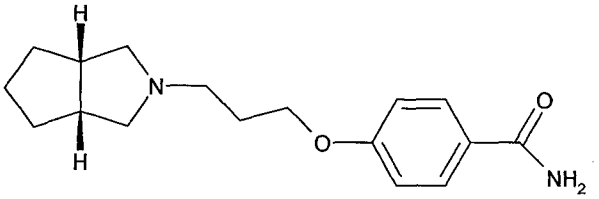
[Suite sur la page suivante]

WO 2012/150411 A1

objet matériel comprenant une phase de construction d'un système authentificateur comprenant au moins: une étape de sélection d'une image message, une étape de sélection d'une image support, une étape de transformation des images message et support pour générer au moins deux images partagées selon un procédé de transformation mettant en œuvre au moins une séquence aléatoire, l'image message n'étant pas accessible dans chaque image partagée prise individuellement, une étape d'enregistrement d'au moins une image partagée. Selon l'invention, dans la phase de construction d'un authentificateur chaque séquence aléatoire, dite signature matière, est extraite ou générée à partir d'au moins une caractéristique structurelle d'une région au moins de l'objet matériel et susceptible d'être générée à la demande et à l'identique à partir de l'objet matériel.

NOUVELLE ASSOCIATION ENTRE LE 4-{3-[*CIS*-HEXAHYDROCYCLOPENTA[*C*]PYRROL-2(1*H*)-YL]PROPOXY}BENZAMIDE ET UN INHIBITEUR DE L'ACETYLCHOLINESTERASE ET LES COMPOSITIONS PHARMACEUTIQUES QUI LA CONTIENNENT

La présente invention concerne une nouvelle association entre le 4-{3-[*cis*-hexahydrocyclopenta[*c*]pyrrol-2(1*H*)-yl]propoxy}benzamide de formule (I) :



(I)

ou un de ses sels d'addition à un acide ou à une base pharmaceutiquement acceptable, et un inhibiteur de l'acétylcholinesterase pour l'obtention de compositions pharmaceutiques utiles dans le traitement des troubles cognitifs associés au vieillissement cérébral et aux maladies neurodégénératives.

Le 4-{3-[*cis*-hexahydrocyclopenta[*c*]pyrrol-2(1*H*)-yl]propoxy}benzamide présente la particularité d'interagir avec les systèmes histaminergiques centraux in vivo. Ces propriétés lui confèrent une activité dans le système nerveux central et plus particulièrement dans le traitement des déficits cognitifs associés au vieillissement cérébral et aux maladies neurodégénératives.

Le 4-{3-[*cis*-hexahydrocyclopenta[*c*]pyrrol-2(1*H*)-yl]propoxy}benzamide, sa préparation et son utilisation en thérapeutique ont été décrits dans la demande de brevet WO2005/089747.

La demanderesse a présentement découvert que le 4-{3-[*cis*-hexahydrocyclopenta[*c*]pyrrol -2(1*H*)-yl]propoxy}benzamide de formule (I), ou ses sels d'addition à un acide ou à une base pharmaceutiquement acceptable, utilisé en association avec un inhibiteur de l'acétylcholinesterase, possédait des propriétés intéressantes pour le traitement des troubles cognitifs associés au vieillissement cérébral et aux maladies neurodégénératives.

Les maladies neurodégénératives liées au vieillissement cérébral telles que la maladie d'Alzheimer sont caractérisées par des troubles de la mémoire et des dysfonctionnements cognitifs. Les troubles cognitifs sont généralement associés à une diminution de la capacité

image permettant par superposition avec l'image de fond incorporant le message crypté de révéler le message crypté pour s'assurer de l'authenticité des informations constitutives du billet. Un tel procédé permet effectivement d'authentifier les informations associées à un billet dans le cadre d'une transaction en partie dématérialisée mais ne permet pas d'authentifier un produit qui serait associé à ce billet.

[05] Les procédés connus à ce jour s'avèrent ainsi adaptés à l'authentification de processus en partie dématérialisés ou encore d'objets dont le destinataire est connu. En revanche, les procédés connus apparaissent inadaptés pour une authentification forte d'objets matériels dont l'origine doit pouvoir être assurée et garantie à l'utilisateur final à partir de la mise dans un circuit de distribution ou d'acheminement quelque soit la chaîne de distribution ou d'acheminement et cela bien avant que le destinataire ou l'utilisateur final ne soit connu.

[06] Il est donc apparu le besoin d'un système qui soit en mesure de permettre une authentification d'un objet matériel de manière que son destinataire puisse être certain que l'objet en lui-même, pas seulement le dispositif d'authentification, est authentique et/ou que l'information associée à l'objet est authentique. Il est également apparu le besoin d'un système d'authentification qui puisse être mis en œuvre sans que le producteur ou l'émetteur de l'objet ait à connaître le destinataire final et/ou à personnaliser l'objet en fonction du destinataire ou utilisateur final.

[07] Afin d'atteindre cet objectif l'invention concerne un procédé d'authentification d'un objet matériel comprenant une phase de construction d'un système authentificateur comprenant au moins :

- une étape de sélection d'une image message,
- une étape de sélection d'une image support,
- une étape de transformation des images message et support pour générer au moins deux images partagées selon un procédé de transformation mettant en œuvre au moins une séquence aléatoire, l'image message n'étant pas accessible dans chaque image partagée prise individuellement,
- une étape d'enregistrement d'au moins une image partagée,

Selon l'invention, le procédé d'authentification unitaire est caractérisé en ce que dans la phase de construction d'un authentificateur chaque séquence aléatoire, dite signature matière, est extraite ou générée à partir d'au moins une caractéristique structurelle d'une région au moins de l'objet matériel et se trouve susceptible d'être générée ou extraite à la demande et obtenue à l'identique ou quasi-identique à partir de l'objet matériel.

[08] L'invention permet de créer un lien bi-univoque entre l'image message et l'objet matériel par mise en œuvre la signature matière pour la construction des images partagées.

[09] Au sens de l'invention, il faut entendre par séquence aléatoire une séquence de nombres qui sont la réalisation indépendante d'une variable uniformément distribuée, c'est à dire équiprobable. Parmi les séquences aléatoires utilisables dans le cadre de l'invention il est possible de citer les séquences aléatoires binaires constituées d'une série de valeurs binaires indépendantes les unes des autres. Une séquence aléatoire générée au moyen d'une caractéristique structurelle d'un élément ou objet matériel comme décrit dans FR 2 870 376 ou FR 2 895 543 correspond à la définition de séquence aléatoire au sens de l'invention.

[10] Au sens de l'invention, le fait que la séquence aléatoire utilisée, dite signature matière, puisse être générée à la demande et à l'identique ou quasi-identique à partir de l'objet matériel correspond au fait que cette signature matière est stable tout en étant aléatoire. Une signature aléatoire stable extraite d'une caractéristique structurelle d'un élément matériel, comme décrit par FR 2 895 543, est une signature matière, au sens de l'invention, qui peut être recalculée ou régénérée par une nouvelle mise œuvre de l'algorithme utilisé sur une même région de l'élément ou objet matériel. Lors de la construction du système authentificateur et à chaque fois que cela est nécessaire, la signature matière est générée ou extraite par lecture de l'élément matériel via un dispositif d'extraction de signature matière. De part la nature aléatoire de la signature matière, chaque valeur de signature matière est différente d'un élément matériel à l'autre ou d'une famille d'éléments matériels à l'autre et chaque valeur de signature ne peut être prédite même en présence de l'élément ou objet matériel sauf, bien entendu, à connaître l'algorithme mis en œuvre et, dans le cas de l'algorithme décrit par

FR 2 895 543, la base de décomposition utilisée et/ou les paramètres d'extraction de la signature matière tels que la forme de la fenêtre d'acquisition et/ou son sens de lecture. Dans ce dernier cas, la base de décomposition et/ou les paramètres d'extraction peuvent être chacun considérés comme une clé secrète pour l'extraction de la signature matière.

[11] A chaque extraction la signature matière est identique ou quasi identique à celle utilisée lors de la construction du système authentificateur. Quasi identique signifie qu'il existe une faible variation ou différence entre les signatures matière extraites à partir d'une même région d'un même objet matériel.

[12] De même au sens de l'invention, la caractéristique structurelle peut être une caractéristique propre de l'objet matériel en tant qu'individu ou dans le cas d'un objet issus d'un processus industriel visant à produire une famille d'objets matériels ayant des caractéristiques structurelles communes, la caractéristique structurelle peut être une caractéristique structurelle de la famille. Parmi ces processus industriels, il est possible de citer les procédés de moulages ou d'estampage de matières premières brutes pour obtenir des pièces en forme ou avec un relief. Il est également possible de citer les processus industriels qui consistent à assembler différentes pièces pour obtenir des objets manufacturés ou des ensembles fonctionnels ayant une apparence identique.

[13] Par ailleurs, au sens de l'invention, par enregistrement il faut entendre notamment :

- un enregistrement sous une forme imprimée ou analogue,
- un enregistrement sous une forme analogique comme, par exemple, sous une forme imprimée en tons continus,
- un enregistrement sous une forme numérique non électronique ou non magnétique comme, par exemple, sous une forme imprimée en demi-tons,
- un enregistrement sous une forme numérique, électronique, ou magnétique avec des moyens de stockage informatique

sans que cette liste soit limitative ou exhaustive.

[14] L'enregistrement par impression peut faire intervenir le dépôt d'encres ou de substances permettant d'obtenir des propriétés optiques du support d'impression adaptées à la réalisation des images partagées.

[15] Le procédé selon l'invention est qualifié de procédé d'authentification unitaire car il assure la combinaison d'une authentification et d'une identification.

[16] L'authentification peut être définie comme étant le fait d'établir qu'un objet est authentique c'est-à-dire qu'il peut être considéré comme ayant une origine connue et fiable. Le résultat d'une authentification et une réponse binaire : positive ou négative.

[17] L'identification est la possibilité de reconnaître ou d'individualiser soit un objet parmi une famille d'objets en circulation, soit une famille d'objets parmi un ensemble de familles en circulation. La manière la plus simple de procéder à une identification est d'associer ou attacher un nombre donné, appelé index, à un objet ou à une famille d'objets. Un tel index permet de connaître le rang de l'objet à l'intérieur de la famille d'objets ou le rang de la famille à l'intérieur de l'ensemble de familles. L'identification n'est pas en soi une mesure de sécurité ou une mesure visant à garantir une sécurité comme cela est le cas de l'authentification.

[18] Dans le cas de l'authentification unitaire d'un objet, la mise en œuvre d'une signature matière générée à partir de la structure en elle-même de l'objet à authentifier pour générer les images partagées crée un lien unique entre l'objet à authentifier et les images partagées servant à l'authentification de cet objet.

[19] De la même manière, dans le cas de l'authentification unitaire d'une famille d'objet, il sera mis en œuvre d'une signature matière générée à partir de la structure en elle-même d'un objet de la famille à authentifier, cette signature matière présentant la particularité d'être identique ou quasi-identique pour l'ensemble des objets appartenant à une même famille mais différente pour des objets appartenant à deux familles distinctes. L'utilisation de cette signature matière « de famille » pour générer les images partagées crée un lien unique entre la famille d'objets à authentifier et les images partagées servant à l'authentification de cette famille objet.

[20] Dans le cadre du procédé d'extraction tel que décrit dans la demande FR 2 895 543 dont l'enseignement doit être considéré comme faisant partie de la présente description, la distinction entre la signature matière individuelle d'un objet et la signature matière d'une famille d'objets peut être réalisée, par l'identification des composantes de la signature qui auront, d'une part, des valeurs identiques pour tous les objets appartenant à une même famille tout en ayant, bien entendu, des valeurs

différentes pour des objets n'appartenant pas à la même famille et, d'autre part, des valeurs différentes d'un objet à l'autre dans une même famille. La signature matière de la famille possède le caractère aléatoire propre aux signatures matière selon l'invention dans la mesure où la valeur de la signature matière ne peut être prédite d'une famille à l'autre et se trouve distincte d'une famille à l'autre.

[21] L'authentification unitaire effectuée au moyen du procédé selon l'invention présente une sécurité parfaite et, de plus, une très grande robustesse et fiabilité dans la mesure où il combine de la cryptographie visuelle, dont la sécurité parfaite est démontrée et reconnue, à la signature matière qui elle-même possède un caractère aléatoire démontré et peut être recalculé de manière fiable même après une certaine altération, notamment un vieillissement, de l'objet matériel. A cet égard, il convient de noter qu'à chaque nouvelle extraction la signature matière est identique ou quasi-identique à celle utilisée lors de la construction du système authentificateur. Par quasi-identique il faut comprendre que lors d'une nouvelle extraction un faible pourcentage, par exemple inférieure à 10% et, de préférence, inférieur à 5%, des valeurs des nombres constitutifs de la séquence aléatoire formant la signature matière peuvent d'être différentes des valeurs des nombres constitutifs de la séquence formant la signature matière utilisée lors de la construction du système authentificateur ou des valeurs des nombres constitutifs de la séquence formant d'une signature matière extraite précédemment. Dans le cadre de l'invention l'éventualité d'une telle légère variation de la signature matière n'est pas un obstacle à la fiabilité du procédé d'authentification selon l'invention dans la mesure où les éventuelles variations de la signature matière engendreront une éventuellement une altération d'une petite partie seulement de l'image partagée reconstruite avec la signature matière quasi-identique. Or, l'interprétation du résultat du contrôle par superposition des images partagées peut être effectuée par un utilisateur dont le système visuel humain est en mesure de lire ou reconnaitre l'image message et de l'interpréter même si cette image message est partiellement altérée. A cet égard, il convient de savoir que le système visuel humain permet de reconnaitre, à partir de fragments, des formes géométriques, des images ou des lettres alors qu'à partir des mêmes fragments un système de vision artificiel n'est pas en mesure d'effectuer une quelconque reconnaissance. Cette possibilité de

reconnaissance, malgré d'éventuelles altérations, offerte par le système visuel humain vaut également en cas de légères altérations d'une des images partagées. Ainsi, la combinaison de la génération de la séquence aléatoire nécessaire à l'algorithme de cryptographie visuelle au moyen de la signature matière et du contrôle au moyen du système visuel humain confère, au procédé selon l'invention, une grande résistance aux variations de l'objet matériel et de l'éventuelle image partagée qu'il porte.

[22] Par ailleurs, le fait que les images partagées sont construites au moyen de la signature matière générée en mettant en œuvre une clé secrète et/ou le fait que l'image message contienne éventuellement une marque secrète évite qu'un tiers puisse modifier subrepticement une image partagée ou générer une image partagée factice.

[23] Le procédé d'authentification unitaire selon l'invention peut être mis en œuvre pour des objets ou des produits formant un ensemble fonctionnel qui n'est pas destiné à être divisé de sorte que le procédé est mis en œuvre pour assurer l'authentification de l'ensemble sans nécessairement permettre une authentification individuelle des éléments qui le composent. Toutefois, l'invention peut également être mise en œuvre pour des objets ou des produits qui sont destinés à être divisés pour être intégré dans d'autres objets notamment. À titre d'exemple, il est possible de citer des matériaux en plaque ou en nappe qui sont produits en continu ou dans des dimensions très nettement supérieures à celles des objets ou des produits qui les incorporeront. Afin de permettre une authentification de ce type d'objets, selon une forme de mise en œuvre de l'invention, la phase de construction d'un système authentificateur comprend une étape de décomposition de l'image support en un nombre fini de zones et le procédé comprend pour certaines au moins des zones, une étape de transformation des images message et support pour générer au moins deux images partagées propres à chaque zone selon un procédé de transformation mettant en œuvre au moins une signature matière générée à partir d'au moins une caractéristique structurelle d'une région au moins de ladite zone de l'objet matériel. Ainsi, lors de la découpe des objets authentifiés au moyen il sera possible de retrouver sur une partie découpée une zone à laquelle il aura été associé au moins deux images partagées permettant d'en assurer une authentification. La taille des zones pourra être choisie pour correspondre à la plus

grande surface d'un seul tenant susceptible d'être trouvée sur un produit intégrant une partie de l'objet authentifié au moyen du procédé selon l'invention.

[24] Selon une forme de mise en œuvre de l'invention, la phase de construction d'un système authentificateur comprend une étape d'enregistrement de la localisation de la région de l'objet à partir de laquelle la signature matière est générée.

[25] Selon une caractéristique de l'invention, l'image message comprend une partie au moins de la signature matière ou de la valeur de la signature matière sous une forme alphanumérique ou graphique.

[26] Au sens de l'invention, un enregistrement ou une représentation sous forme alphanumérique signifie un enregistrement ou une représentation sous une forme graphique directement intelligible comprenant des caractères numériques et/ou alphabétiques et/ou des idéogrammes. Dans le cas par exemple, où la signature matière est extraite sous la forme d'une séquence binaire, la représentation alphanumérique de la signature matière peut-être une série de 0 et de 1 correspondant à ladite séquence binaire, une représentation dans une base décimale ou autre du nombre correspondant à cette séquence binaire. En cas de représentation graphique partielle de la valeur de la signature matière, il peut, par exemple, être retenu certains seulement des bits de la séquence binaire représentée par des zéros ou des uns ou encore par un nombre dans une base décimale ou autre correspondant aux bits sélectionnés de la signature matière.

[27] Selon l'invention, l'image support peut être de toute nature. Une image support peut être choisie parmi les types d'image suivants :

- image en couleurs,
- image en niveaux de gris,
- image binaire telle qu'une image à deux composantes visuelles comme deux couleurs distinctes ou encore deux composantes dont l'une possède un comportement spéculaire et l'autre possède un comportement diffusant,
- image en demi-tons,
- image résultant de l'assemblage de deux ou plus images des types ci-dessus,

sans que cette liste soit limitative ou exhaustive.

[28] L'image support peut être une image uniforme ne comprenant aucune information et, par exemple, une image monochrome telle qu'une image blanche ou une image noire ou encore une image uniforme en moyenne résultant d'une distribution aléatoire de pixels d'une couleur et de pixels d'une autre couleur. Selon l'invention, l'image support peut au contraire ne pas être uniforme et comprendre des éléments d'information et/ou des formes identifiables. Une telle image support peut alors permettre une indexation ou identification visuelle dans la mesure où les informations qu'elle véhicule sont visibles au niveau de l'une au moins des images partagées et peuvent être interprétées par le système visuel humain et/ou un système de lecture ou de reconnaissance optique artificiel.

[29] Selon une caractéristique de l'invention l'image support peut comprendre une image d'une région de l'objet matériel et/ou de la structure d'une région de l'objet matériel.

[30] Selon une autre caractéristique de l'invention, l'image message comprend une image d'une région de l'objet matériel et/ou de la structure d'une région de l'objet matériel.

[31] Au sens de l'invention, il faut entendre par image de la structure d'une région de l'objet matériel une représentation graphique, après éventuellement un traitement optique ou numérique, de la structure d'une région de l'objet matériel. Cette représentation graphique peut alors être à taille réelle ou alors faire intervenir un changement d'échelle telle qu'un agrandissement ou une réduction. La mise en œuvre d'un agrandissement permet alors de rendre plus facilement lisible des détails de la structure, tandis que la mise en œuvre d'un traitement optique peut permettre de faciliter la reconnaissance d'éléments caractéristiques de la structure.

[32] Selon l'invention, l'image message peut-être de toute nature appropriée tout en étant de préférence pour une partie au moins interprétable ou reconnaissable par le système visuel humain et, éventuellement, pour une partie au moins interprétable par un système de lecture ou de reconnaissance optique artificiel. L'image peut par exemple comprendre une partie intégrant un message dans une représentation graphique selon un système d'écriture humain et une partie intégrant un message graphique pour un système lecture de lecture artificiel comme un code barre et/ou un data Matrix.

[33] Selon une forme préférée de mise en œuvre, l'image message est une image binaire telle qu'une image à deux composantes visuelles. Les deux composantes peuvent alors être par exemple deux couleurs distinctes ou deux composantes dont l'une possède un comportement spéculaire et l'autre possède un comportement diffusant.

[34] Selon l'invention, l'enregistrement de l'une au moins des images partagées peut être réalisé de toute manière appropriée. Selon une forme de mise en œuvre de l'invention, la phase de construction d'un système authentificateur comprend une étape d'enregistrement de l'une au moins des images partagées sous forme numérique.

[35] Selon une caractéristique de cette forme de mise en œuvre, le procédé d'authentification selon l'invention comprend une étape d'enregistrement de l'une au moins des images partagées sous forme imprimée.

[36] Selon une variante de cette caractéristique, la phase de construction d'un système authentificateur comprend une étape d'impression de l'une au moins des images partagée sur l'objet matériel.

[37] Selon encore une autre caractéristique de l'invention, la phase de construction d'un système authentificateur comprend une étape d'enregistrement sous forme imprimée d'au moins une image partagée et une étape d'enregistrement sous forme numérique d'au moins une autre image partagée.

[38] Le procédé d'authentification selon l'invention permet à un utilisateur ou un destinataire de l'objet authentifié d'effectuer un contrôle visuel de l'authenticité par la mise en œuvre d'au moins deux images partagées. Ainsi selon une forme de mise en œuvre, le procédé d'authentification selon l'invention comprend, en outre, une phase de vérification par un utilisateur comprenant :

- une étape de présentation à la vue de l'utilisateur d'une image partagée
- et au moins une autre étape de présentation à la vue de l'utilisateur d'une autre image partagée,

les étapes de présentation étant conduites de manière que l'utilisateur perçoive les images partagées comme étant superposées pour permettre une lecture de l'image message par l'utilisateur.

[39] Selon une caractéristique de l'invention, les étapes de présentation sont conduites successivement de manière à mettre en œuvre un phénomène de persistance rétinienne chez l'utilisateur ou un autre phénomène de perception visuelle.

[40] Selon une autre caractéristique de l'invention les étapes de présentation sont conduites simultanément. Lorsque chaque image partagée présente l'image support qui par ailleurs intègre des formes identifiables, la présence de ces formes identifiables constitue une aide à une superposition des images partagées pour obtenir une révélation satisfaisante de l'image message. La présence de formes identifiables dans l'image support visibles dans chaque image partagée peut être utilisée pour permettre à l'utilisateur de choisir l'image support à utiliser dans les cadres des mises en œuvre de l'invention faisant intervenir la construction d'une image partagée dans la phase de vérification.

[41] Selon l'invention les étapes de présentation des images partagées peuvent être réalisées par tout moyen approprié.

[42] Selon une caractéristique de l'invention, une étape de présentation au moins est effectuée au moyen d'un dispositif électronique d'affichage ou de projection.

[43] Selon une autre caractéristique de l'invention, une étape de présentation au moins est effectuée au moyen d'au moins une image partagée imprimée. Cette impression peut alors être réalisée sur un support opaque, translucide ou transparent.

[44] Selon une caractéristique de l'invention, la phase de vérification comprend une étape d'extraction de la signature matière.

[45] Selon une autre caractéristique de l'invention, la phase de vérification comprend une étape de génération d'une image partagée.

[46] Selon encore une autre caractéristique de l'invention et lorsqu'une image partagée au moins aura été enregistrée sous une forme électronique, la phase de vérification comprend une étape de téléchargement d'une image partagée à partir d'un serveur distant.

[47] Le procédé de transformation des images support et message en images partagées s'apparente à un algorithme relevant de la cryptographie visuelle. Selon l'invention le procédé de transformation mis en œuvre pour transformer les images message et support en aux moins deux images partagées peut mettre en œuvre tout

algorithme de cryptographie visuelle adapté. Il est possible, par exemple, d'utiliser des algorithmes de cryptographie visuelle mettant en œuvre une image support décrits et référencés dans la publication « A Comprehensive Study of Visual Cryptography » de Jonathan Weir et WeiQi Yann [Y.Q. Shi (ed) : Transactions on DHMS V, LNCS 6010, pp. 70-105, 2010 ©Spinger-Verlag Berlin Heidelberg 2010]. Dans le contexte de cette publication:

- la notion d'image message, au sens de l'invention, correspond, notamment, à la terminologie « secret », « secret image »,
- la notion d'image support, au sens de l'invention, correspond notamment à la terminologie « cover image », « base image »,
- et la notion d'images partagées, au sens de l'invention, correspond notamment à la terminologie « share », « merged share » ou encore « secure mask ».

[48] L'invention vise également un procédé de transformation d'une image message et d'une image support en au moins deux images partagées au moyen d'au moins une séquence aléatoire, l'image message n'étant pas accessible dans chaque image partagée prise individuellement et étant révélée par superposition réelle et/ou virtuelle des images partagées. Selon l'invention chaque image partagée présente l'image support dans une forme altérée et lors de la superposition des images partagées il est obtenu une image comprenant l'image message et l'image support dans sa forme originale sauf dans les régions en partie au moins occultée par l'image message.

[49] Ainsi, l'invention vise donc aussi un procédé de transformation d'une image message binaire et d'une image support, comprenant au moins un plan couleur, en n images partagées qui partagent sans fuite d'information l'image message, reflètent l'image support, et sont destinées à révéler l'image message à la vue d'un utilisateur par présentation d'au moins k images partagées distinctes, k vérifiant la relation $2 \leq k \leq n$.

[50] Selon une caractéristique de l'invention, le procédé de transformation des images support et message comprend les étapes suivantes :

- choix d'un mode opératoire de présentation d'au moins k images partagées distinctes pour la visualisation de l'image support, k vérifiant la relation $2 \leq k \leq n$
- choix d'une valeur binaire de référence parmi les deux valeurs possibles pour les pixels de l'image message,

- division de l'image support en cellules supports chacune associées à un pixel de l'image message,
- mise en œuvre de deux collections de matrices booléennes de transformation, une première collection étant associée à la valeur binaire de référence et une deuxième collection étant associée à l'autre valeur binaire, les matrices booléennes étant telles que :
  - pour tout entier q tel que $1 \leq q < k \leq n$ les deux ensembles formés des sous-matrices à q lignes et m colonnes extraites des matrices booléennes dans chacune des deux collections sont indistinguables,
  - le mode opératoire appliqué à n'importe quel k-upplet de lignes d'une matrice booléenne quelconque d'une collection puisse révéler une différence avec la résultante du mode opératoire appliqué à n'importe quel k-upplet de lignes d'une matrice booléenne quelconque de l'autre collection,
- pour certaines au moins des cellules support, tirage au moyen d'une séquence aléatoire d'une matrice booléenne de transformation dans la collection correspondant à la valeur binaire du pixel message associé à la cellule support,
- assemblage des matrices booléennes sélectionnées éventuellement complétées par des valeurs neutres pour n images masque de même taille que l'image support.
- pour au moins un plan couleur, construction de n images partagées à partir des n images masques et/ou de l'image support.

[51] Selon l'invention, la construction des paires de collection de matrice booléennes peut mettre en œuvre un schéma binaire tel que décrit par le brevet US 5 488 664 ou encore dans la publication « Visual Cryptography » de M. Naor et A. Shamir, Adances in Cryptology – Eurocrypt' 94 Proceedings, LNCS vol.950, Springer-Verlag, 1995, pp. 1-12. Dans le contexte de cette publication:

- la notion d'image message, au sens de l'invention, correspond, notamment, à la terminologie « message » or « secret message »,
- la notion cellule, au sens de l'invention, correspond notamment à la terminologie « share »,
- et la notion de pixel de cellule, au sens de l'invention correspond à la terminologie « subpixel ».

[52] Selon une caractéristique de l'invention, au moins une image partagée est indépendante de l'image message et chaque autre image partagée dépend de l'image message. Cette caractéristique correspond au fait que dans le cadre de l'algorithme de construction des images partagées, exposé ci-dessus, au moins une image partagée résulte d'une image masque indépendante de l'image message et les autres images partagées résulte chacune d'une image masque dépendant de l'image message. A cet effet, les collections de matrices booléennes sont telles que pour un indice J prédéterminé et tout rang i, la ligne numéro J de la i-ème matrice de la première collection C_0 est égale à la J-ème ligne de la i-ème matrice de deuxième collection C_1 , les deux collections ayant le même nombre de matrices. (cf figure 6)

[53] Dans le cadre de cette caractéristique, l'image partagée résultant d'une image masque indépendante de l'image message peut être soit ladite image masque ou soit le résultat de l'application de l'image masque à l'image support.

[54] Selon une caractéristique de l'invention, le procédé de transformation comprend une étape de sélection d'une image support polychromatique ou non.

[55] Selon une caractéristique de l'invention, au moins une image partagée est indépendante de l'image support et résulte d'une image masque dépendant de l'image message, et les autres images partagées sont chacune obtenues par l'application d'une image masque, dépendant de l'image message, à l'image support.

[56] Selon une autre caractéristique de l'invention, chaque image partagée est obtenue par application d'une image masque à l'image support.

[57] Selon une forme de mise en œuvre du procédé de transformation selon l'invention, chaque séquence aléatoire utilisée provient d'une signature matière extraite d'au moins une caractéristique structurelle d'une région d'un objet matériel.

[58] Selon une variante de réalisation de cette forme de mise en œuvre, l'image message comprend une référence à l'origine du message. Cette référence peut notamment être une marque sécrète.

[59] Selon une autre caractéristique du procédé de transformation conforme à l'invention, chaque séquence aléatoire est enregistrée.

[60] Selon une caractéristique de l'invention, le procédé comprend une sélection des cellules supports pour lesquelles il est effectué un tirage d'une matrice booléenne de transformation.

[61] Selon une variante de cette caractéristique la sélection des cellules support est effectuée de manière aléatoire.

[62] Selon une autre variante de cette caractéristique la sélection des cellules support est effectuée selon des courbes ou lignes, virtuelles ou réelles, à l'intérieur de l'image support.

[63] Selon encore une autre variante de cette caractéristique, le nombre total des cellules support sélectionnées correspond à au moins 50% du nombre de pixels de l'image message de manière à garantir un possible déchiffrage du message par le système visuel humain.

[64] Le procédé de transformation selon l'invention peut comprendre une étape d'enregistrement de l'une au moins des images partagées sous forme numérique.

[65] Le procédé de transformation selon l'invention peut également comprendre une étape d'enregistrement de l'une au moins des images partagées sous forme imprimée.

[66] Selon une caractéristique de l'invention, le procédé de transformation selon l'invention comprend une étape d'impression d'au moins une image partagée et une étape d'enregistrement d'au moins une autre image partagée sous forme numérique.

[67] Selon une caractéristique de l'invention, l'image support comprend au moins deux plans couleur. Par plan couleur, il convient de comprendre la décomposition selon l'une des composantes constitutives de l'image support. Dans le cas d'une image en couleur, il y a au moins trois plans couleur, un pour chaque couleur primaire, dans le cas d'une image monochrome, il y a un plan couleur. Un plan couleur peut être binaire ou au contraire assurer un codage d'un niveau d'intensité sur plusieurs bits pour chaque pixel. Dans le cas d'une image en noir et blanc, il y a un seul plan couleur.

[68] Bien entendu, les différentes caractéristiques, variantes et formes de réalisation et de mise en œuvre du procédé d'authentification et du procédé de transformation conformes à l'invention peuvent être associées les unes avec les autres selon diverses combinaisons dans la mesure où elles ne sont pas incompatibles ou exclusives les unes des autres.

[69] Par ailleurs, diverses autres caractéristiques de l'invention ressortent de la description annexée effectuée en référence aux dessins qui illustrent des formes non limitatives de mise en œuvre des procédés conformes à l'invention.

- La figure 1 est une vue en perspective d'un produit susceptible d'être authentifié au moyen du procédé selon l'invention.
- La figure 2 est une image support qui correspond à une partie de l'image de la face supérieure de produit illustré figure 1 et qui est utilisée dans le cadre du procédé selon l'invention.
- La figure 3 est une image message qui est utilisée dans le cadre du procédé.
- La figure 4 montre deux images partagées qui forment un système authentificateur visuel et qui sont construites par la mise en œuvre du procédé selon l'invention avec les images support et message illustrées respectivement figure 3 et figure 4.
- La figure 5 montre un exemple deux collections de matrices booléennes mises en œuvre pour la construction des images partagées.
- La figure 6 illustre une autre notation des deux collections de matrices booléennes de la figure 5. La figure 7 illustre un dispositif pour l'extraction d'une signature matière, tel que décrit dans la demande FR 2 907 923, placé sur la face supérieure du produit illustré figure 1.
- La figure 8 illustre un schéma de mise en œuvre de l'invention avec enregistrement de la première image partagée dans une base de données accessible à distance.
- La figure 9 est le résultat de la superposition des images partagées de la figure 4.
- La figure 10 illustre la face arrière du produit représenté figure 1, l'une des deux images partagées représentées figure 4 est enregistrée par impression sur cette face arrière.
- La figure 11 est une autre image support utilisée dans le cadre du procédé selon l'invention.
- La figure 12 est une autre image message est utilisée dans le cadre du procédé.
- La figure 13 montre deux images partagées qui forment un système authentificateur visuel et qui sont construites par la mise en œuvre du procédé selon l'invention avec les images support et message illustrées respectivement figure 11 et figure 12.
- La figure 14 est le résultat de la superposition des images partagées de la figure 13.

– La figure 15 monte deux images partagées qui forment un système authentificateur et qui sont construites par la mise en œuvre du procédé selon l'invention avec les images support et message illustrées respectivement figure 3 et figure 4 et dont seule une image partagée, celle de gauche, reflète l'image support tandis que l'image partagée de droite ne reflète aucune information. La superposition des images partagées de la figure 15 permet d'obtenir le résultat illustré figure 5.

[70] L'invention propose de mettre en œuvre un système authentificateur qui permet à un utilisateur de procéder visuellement à une authentification, associée à une identification, d'un objet matériel en sa possession. Un tel objet O peut par exemple être une boîte ou un étui d'emballage tel qu'illustré à la figure 1. Bien entendu, il ne s'agit là que d'un exemple, l'invention pouvant être appliqué à tout type d'objet matériel sous réserve que ce dernier comprenne de la matière à l'état solide dont le processus d'évolution et/ou de dégradation spontanée est très nettement plus long que le délai entre la phase de construction du système authentificateur et la phase de vérification. Par « très nettement plus long », on entend que le délai, à partir duquel intervient les premières évolutions ou dégradations spontanées, est au moins deux fois supérieur, de préférence supérieur d'au moins un voire deux ordres de grandeur, au délai entre la phase de construction du système authentificateur et la phase de vérification. Une image selon un point de vue donné d'une scène naturelle comme un paysage, une rue, un monument, un bâtiment ou autre, peut constituer un objet matériel authentifiable par l'invention et susceptible de servir de base à une extraction d'une signature matière susceptible d'être extraite à l'identique ou quasi identique à partir d'une autre image de la même scène naturelle selon le même ou quasiment le même point de vue.

[71] Parmi les objets matériels susceptibles de faire l'objet d'un authentification unitaire par la mise en œuvre de l'invention il est également possible de citer :

– les produis industriels ou manufacturés en tant que tels quelque soit leur matière et/ou leur composants, notamment pour des applications du type protection des marques,

– l'emballage et/ou sur-emballage de ces produits,

- les documents officiels comme par exemple les titres d'identité, les titres fiduciaires, monnaies ou autres,
- les titres d'accès à un lieu, une machine ou un service,
- tout document nécessitant un authentification,
- sans cette liste soit limitative ou exhaustive.

[72] Afin de construire un système d'authentificateurs visuels, l'invention propose de mettre en œuvre une image support S, figure 2, et une image message M, figure 3, qui sont transformées au moyen d'un algorithme de cryptographie visuelle en au moins deux et, selon l'exemple illustré, exactement deux images partagées P1 et P2, figure 4. L'une des caractéristiques essentielles de l'invention réside dans le fait que l'aléa, appelé dans le cadre de l'invention séquence aléatoire, nécessaire à la mise en œuvre de l'algorithme de cryptographie visuelle est fourni par la signature matière extraite à partir d'au moins une caractéristique structurelle d'une région au moins de l'objet matériel O.

[73] Selon l'exemple illustré, l'image support S correspond à l'image d'une partie de la face supérieure 1 de l'objet O, étant entendu que toute autre image pourrait être utilisée en tant qu'image support.

[74] Toujours selon l'exemple illustré, l'image message M comprend un message M1 qui est susceptible d'être interprété par le système visuel humain et qui, dans le cas présent, correspond à une séquence binaire de zéros et de uns. L'image message M comprend également un message M2 qui est susceptible d'être interprété par un système de lecture ou de reconnaissance optique artificiel et qui, dans le cas présent, correspond à un data Matrix. Selon l'invention l'image message peut ne comprendre qu'un message M1 intelligible par le système visuel humain ou qu'un message M2 intelligible par un système de lecture ou de reconnaissance optique artificiel. L'image message peut également comprendre un message intelligible à la fois par le système visuel humain et par un système de lecture ou de reconnaissance optique artificiel.

[75] La construction du système d'authentificateurs visuels peut être réalisée de la manière suivante dans le cas d'un système d'authentificateurs à deux images partagées destinées à être superposées pour la lecture du message M.

[76] L'image message M comprend un nombre donné de pixels message, pour l'exemple illustré, 1872O pixels pour image de 5 cm par 6,5 cm (156 pixels x 120 pixels).

[77] L'image support est divisée en cellules chacune associées à un pixel de l'image message de sorte qu'il y a autant de cellules support que de pixels message. Chacune des cellules support comprend un nombre donné de pixels adjacents de préférence supérieur ou égal à deux et selon l'exemple illustré égal à quatre. Il doit être compris que la résolution de l'image support est choisie pour que, une surface égale à celle de l'image message, l'image support comprenne suffisamment de pixels pour être divisée en autant de cellules support qu'il existe de pixels image. Ainsi dans le cas de l'exemple illustré où chaque cellule support comprend quatre pixels, l'image support S comprendra 74 880 pixels soit une résolution de 312 pixels x 120 pixels pour une surface de 5 cm par 6,5 cm.

[78] Préalablement à la construction des images partagées en tant que telles, il convient de construire des images masque dans un nombre égal au nombre d'image partagées ici deux.

[79] Il est mis en œuvre deux collections C_0, C_1 de matrices booléennes dont un exemple est illustré à la figure 5 dans le cadre de la mise en œuvre de cellules support carrées de quatre pixels. Chaque collection correspond à une des deux valeurs possibles pour chaque pixel de l'image message M. Une première collection C_0 de matrice peut, par exemple, correspondre à la valeur 0 tandis que la deuxième collection C_1 peut correspondre à la valeur 1. Chaque collection comprend un certain nombre de sous collections qui comprennent chacune autant de matrices qu'il y aura d'images partagées.

[80] À la figure 5, les sous-collections correspondent aux colonnes de chaque collection C_0, C_1. Dans le cas présent, chaque collection comprend six sous-collections respectivement C_{01} à C_{06} et C_{11} à C_{16}. Chaque sous-collection comprend, selon l'exemple illustré, deux matrices correspondant à deux cellules support l'une de la première image masque Mq_1 et l'autre de la deuxième image masque Mq_2. Pour faciliter la représentation, sur la figure 5, dans chaque collection, la première ligne correspond aux valeurs possibles des cellules de la première image masque tandis que la deuxième ligne correspond aux valeurs possibles pour les cellules de la deuxième image masque.

[81] Il est en outre représenté au dessus des collections, les cellules masques correspondant aux matrices des sous-collections. Dans une forme préférée de mise en œuvre les deux collections comprennent le même nombre de sous-collection, toutefois cela n'est pas nécessaire à la mise en œuvre de l'invention.

[82] Pour chaque pixel message, il est alors procédé de la manière suivante :

- si la valeur du pixel message est 0 alors c'est la première collection C_0 qui est mise en œuvre. Il est alors choisi de manière aléatoire une sous-collection parmi les sous-collections C_{01}, C_{02}, C_{03}, C_{04}, C_{05}, C_{06}.
- si la valeur du pixel message est 1 alors c'est la deuxième collection C_1 qui est mise en œuvre et il est choisi de manière aléatoire une sous-collection parmi les sous-collections C_{11}, C_{12}, C_{13}, C_{13}, C_{14}, C_{15}, C_{16}.

[83] La matrice du haut de la sous-collection choisie est alors attribuée à la première image masque tandis que la matrice du bas est attribuée à la deuxième image masque.

[84] Il est procédé ainsi pour tous les pixels messages et toutes les matrices masques sont assemblées pour former les première et deuxième images masque.

[85] Pour l'image message M de 18720 pixels, il est nécessaire de disposer d'une séquence aléatoire qui comprenant 18720 valeurs chaque valeur permettant de choisir de manière aléatoire une sous-collection parmi six. Dans le cas d'un codage binaire, il faut donc trois bits pour chaque tirage. De sorte que dans le cas de notre exemple, il faut une séquence de 56160 bits, soit 7020 octets. Cette séquence aléatoire sera ensuite divisée en groupes de trois bits utilisés à chaque tirage ou choix de sous-collection.

[86] L'invention propose d'utiliser en tant que séquence aléatoire la signature matière par exemple d'une partie au moins de la structure du produit la signature matière extraite à partir d'au moins une caractéristique structurelle d'une région R au moins de l'objet matériel O. Selon l'exemple illustré, la région R est située sur la face supérieure de l'objet matériel O. L'extraction de la signature matière peut-être effectuée par tous moyens appropriés comme cela est décrit dans la demande FR 2 895 543. Selon l'exemple illustre à la figure 7, il est mis en œuvre un terminal communiquant portable SP équipé d'un accessoire ad hoc tel que décrit par la demande FR 2 895 923. Ainsi il est

obtenu une signature matière de 7 020 octets qui sont utilisés comme décrit précédement.

[87] Les images masques peuvent être utilisées directement pour révéler à un utilisateur l'image message en superposant les images masques. L'invention propose toutefois de mettre en œuvre l'image support pour construire les images partagées à partir des images masques. L'utilisation de l'image support permet une reconnaissance ou une indexation des images partagées ce qui n'est pas possible avec les images masque. Ainsi, les images partagées possèdent deux niveaux d'informations un premier niveau offert par l'image support accessible directement pour chaque image partagée seule. Le deuxième niveau d'information constitué par l'image message n'étant accessible qu'avec la réunion des deux images partagées De plus, l'image support permet de conférer un aspect plus esthétique aux images partagées.

[88] Chaque image partagée est construite en attribuant à chaque pixel de l'image partagée la valeur de la multiplication des valeurs des pixels correspondants de l'image masque et de l'image support. Par pixel correspondant il convient d'entendre un pixel ayant la même positon dans l'image masque ou support que le pixel dans l'image partagée.

[89] Une fois les images partagées P_1 et P_2 construites elles peuvent être enregistrées.

[90] Selon une première forme de mise en œuvre, l'invention propose, comme le montre la figure 8, d'enregistrer la première image partagée dans une base de donnée BD accessible à distance. La deuxième image partagée P_2 est, quant à elle, enregistrée sous une forme imprimée sur la face arrière de l'objet O comme le montre la figure 9.

[91] Lorsqu'un acheteur ou un utilisateur U de l'objet O souhaite vérifier l'authenticité de l'objet O, il interroge via un dispositif portable SP comme un téléphone intelligent, en anglais « smart-phone » la base de donnée BD en lui fournissant par exemple le code associé au code à barre C figurant également sur la face arrière de l'objet O. La base de données envoie en réponse la première image partagée P1. L'utilisateur réalise ensuite une photo de la deuxième image partagée P2 et le dispositif portable SP réalise la superposition des images partagées P1 et P2 qui si elles sont toutes deux authentiques offre l'image telle illustrée à la figure 10. L'utilisateur sait qu'il est présence d'un produit authentique par le fait qu'il peut lire le message M. Il peut de plus procéder à une

vérification supplémentaire en utilisant tout ou partie de l'information de l'image message pour interroger une base de données.

[92] Le dispositif utilisé pour assurer l'extraction de la signature matière lors de la construction des images partagées et/ou la phase de vérification peut comprendre tout type de système d'acquisition d'image comme par exemple un scanner à plat, un scanner USB linéaire, une caméra.

[93] Dans un deuxième exemple de mise en œuvre, l'invention propose de tirer partie du fait que l'aléa utilisé pour construire les images partagée est une signature matière qui possède la caractéristique de pouvoir être extraite à la demande en étant à chaque extraction identique ou quasi-identique à la signature matière utilisée pour la génération des images partagées P1 et P2. Cette caractéristique de la signature matière est également appelé caractère rejouable. Selon ce deuxième exemple, il est proposé d'enregistrer comme précédemment la deuxième image partagée P2 en l'imprimant sur l'objet O tandis que la première image partagée P1 est reconstruite au moment de la vérification par l'utilisateur. Pour ce faire, l'image message M doit être connue ou tout au moins générable au moment de la construction de la deuxième image partagée.

[94] A cet effet il peut être utilisé une partie de la signature matière qui par ailleurs est utilisée pour construire les images partagées P1 et P2. Par exemple, la partie M1 intelligible pour l'homme de l'image message peut correspondre aux 22 premiers bits de la signature matière tandis que la partie M2 interprétable par un système artificiel peut correspondre aux 576 premiers bits de la signature matière.

[95] Lorsque l'utilisateur est en possession de l'objet O sur lequel est imprimé la deuxième image partagée P2, il peut utiliser un terminal communiquant SP adapté pour extraire la signature matière de la région R indiquée sur la face supérieure 1 de l'objet O. Le terminal SP est en outre adapté pour générer avec cette signature matière l'image message M et la première image partagée P1. Le terminal communiquant est en outre adapté pour réaliser une photo de la deuxième image partagée P2 et pour superposer cette dernière avec la première image partagée qu'il aura reconstruite.

[96] Si l'utilisateur voit s'afficher l'image telle illustrée à la figure 10, il aura une première confirmation d'authenticité. Le terminal communicant SP peut en outre être adapté pour afficher les 22 premiers bits de la signature matière qu'il aura extraite.

L'utilisateur peut alors comparer les valeurs de la partie M1 de l'image message et les valeurs affichées pour vérifier la concordance. Il est ainsi offert un deuxième niveau d'authentification. La partie M2 de l'image message peut en outre être utilisée par le terminal communiquant pour effectuer un contrôle automatisé de la concordance entre la valeur de la signature matière incorporée à l'image message et la signature matière extraite lors du contrôle de l'authenticité par l'utilisateur.

[97] Selon une troisième variante de mise en œuvre, l'invention propose d'utiliser le caractère rejouable de la signature matière pour permettre une construction de la première image partagée sans connaissance du message. A cet effet, les collections C_0 et C_1 possède le même nombre de sous-collection ou colonne et une ligne d'un rang i de la première collection C_0 possède les mêmes matrices que la ligne de même rang i de la deuxième collection C_1. Ainsi l'image masque de rang i est indépendante de l'image message et dépend uniquement de la signature matière utilisée. Selon l'exemple de collections illustrées à la figure 5, la ligne Mq_1 de la première collection C_0 est identique à la ligne Mq_1 de la deuxième collection. La première image masque sera donc indépendante de l'image message et ne dépendra que de l'aléa utilisé lors de la construction des images masques, soit, dans le cadre de l'invention, la signature matière.

[98] Un scénario de mise en œuvre de cette troisième variante, consiste par exemple à enregistrer par impression la deuxième image partagée sur l'objet puis lors de la vérification à construire la première image partagée avec la signature matière extraite comme expliqué précédemment. L'image support utilisée pourra alors être une image d'une partie de l'objet ou une image prédéfinie stockée dans le dispositif assurant la reconstruction de la première image masque. Il doit être souligné que la possibilité de reconnaitre l'image support à partir de la deuxième image partagée permet à l'utilisateur de déterminer lui-même l'image support à mettre en œuvre. De plus, l'image support incorporée à la deuxième image partagée peut fournir à l'utilisateur une information sur la localisation de la région de l'objet d'où est extraite la signature matière.

[99] Un autre scénario possible de mise en œuvre de cette troisième variante peut aussi être le suivant. Les images partagées P_1 et P_2 sont construites avec les images

masques appliquées à une image support S comprenant un code identifiant pour un système de lecture automatique comme illustré à la figure 11. L'image message M, illustrée figure 12 comprend une image d'une partie de la structure matérielle de l'objet O. La deuxième image partagée P_2, figure 13, est alors enregistrée par impression sur une étiquette ou un certificat d'authenticité associé à l'objet O. Lorsque qu'un utilisateur ou un détenteur de l'objet souhaite en contrôler l'authenticité, il procède au moyen du dispositif portable SP à la construction de la première image partagée P_1, figure 13. Cette première image partagée P_1 est ensuite utilisée en association avec la deuxième image partagée P_2 pour présenter au détenteur l'image message M et l'image support S comme illustré figure 14. Le détenteur peut alors comparer l'image message M à l'image de la structure de la matière de l'objet dans une zone dont la position pourra être indiquée par l'image message ou repérée sur l'objet. Ce scénario de mise en œuvre est particulièrement adapté pour des objets qui ne doivent pas être altérés par l'enregistrement d'une image partagée sur leur surface.

[100] Dans les exemples décrits précédemment la construction des images partagées à partagée P_1 et P_2 partir des images masques Mq_1 ou Mq_2 et de l'image support S est assurée par la multiplication des valeurs des pixels correspondants de l'image masque Mq1 ou Mq2 et de l'image support S. Toutefois, la construction de chaque image partagée, résultant de l'application d'une image masque à l'image support, peut être effectuée par substitution par une valeur prédéfinie de la valeur de chaque pixel de l'image support selon la valeur du pixel correspondant de l'image masque correspondante. Par exemple, si la valeur du pixel de l'image masque est 0 il n'y aura pas substitution tandis que si la valeur du pixel de l'image masque est 1 il y a substitution de la valeur du pixel de l'image support par la valeur prédéfinie. Ce mode opératoire peut être avantageux dans le cadre d'une image en couleur. En effet, il peut être utilisé une première valeur de substitution pour la première image partagée et une deuxième valeur de substitution pour la deuxième image partagée. La première valeur de substitution peut correspondre à une première couleur tandis que la deuxième valeur de substitution correspond à une deuxième couleur. Les première et deuxième couleurs peuvent alors être choisies pour que lors de la présentation superposée des images partagées P_1 et P_2 l'image message M s'affiche dans une couleur cible résultant

du mélange des première et deuxième couleurs. La couleur cible peut alors être choisie pour faciliter la lecture de l'image message.

[101] Bien entendu divers autres scénarii pour la mise œuvre des différentes variantes de l'invention présentées ainsi que d'autre variantes de l'invention peuvent être envisagés dans le cadre des revendications annexées.

REVENDICATIONS

1. Procédé d'authentification unitaire d'un objet matériel (O) comprenant une phase de construction d'un système authentificateur comprenant au moins :

– une étape de sélection d'une image message (M),

– une étape de sélection d'une image support (S),

– une étape de transformation des images message (M) et support (S) pour générer au moins deux images partagées (P_1, P_2) selon un procédé de transformation mettant en œuvre au moins une séquence aléatoire, l'image message (M) n'étant pas accessible dans chaque image partagée(P_1, P_2) prise individuellement,

– une étape d'enregistrement d'au moins une image partagée (P_2),

caractérisé en ce que dans la phase de construction d'un authentificateur chaque séquence aléatoire, dite signature matière, est extraite ou générée à partir d'au moins une caractéristique structurelle d'une région (R) au moins de l'objet matériel (O) et susceptible d'être générée à la demande et à l'identique à partir de l'objet matériel (O).

2. Procédé d'authentification selon la revendication 1, caractérisé en ce que la phase de construction du système authentificateur comprend une étape de décomposition de l'image support (S) en un nombre finis de zones et en ce qu'il comprend pour certaines au moins des zones, une étape de transformation des images message (M) et support (S) pour générer au moins deux images partagées (P1, P2) propres à chaque zone selon un procédé de transformation mettant en œuvre au moins une signature matière générée à partir d'au moins une caractéristique structurelle d'une région au moins de ladite zone de l'objet matériel (O).

3. Procédé d'authentification selon l'une des revendications précédentes, caractérisé en ce que la phase de construction du système authentificateur comprend une étape d'enregistrement de la localisation de la région de l'objet à partir de laquelle la signature matière est générée.

4. Procédé d'authentification selon l'une des revendications précédentes, caractérisé en ce que l'image message (M) comprend une partie au moins de la signature matière sous une forme alphanumérique ou graphique.

5. Procédé d'authentification selon l'une des revendications précédentes, caractérisé en ce que l'image support (S) comprend une image d'une région de l'objet matériel et/ou de la structure d'une région de l'objet matériel.

6. Procédé d'authentification selon l'une des revendications précédentes, caractérisé en ce que l'image support (S) comprend des données graphiques d'indexation ou d'identification interprétables par le système visuel humain et/ou par un système de lecture ou de reconnaissance optique artificiel.

7. Procédé d'authentification selon l'une des revendications précédentes, caractérisé en ce que l'image message (M) comprend une image d'une région de l'objet matériel (O) et/ou de la structure d'une région de l'objet matériel.

8. Procédé d'authentification selon l'une des revendications précédentes, caractérisé en ce que l'image support (S) est choisie parmi les types d'image suivant :

- image en couleurs,
- image en niveaux de gris,
- image binaire telle qu'une image à deux composantes visuelles comme deux couleurs distinctes ou encore une composante ayant un comportement spéculaire et une composante ayant un comportement diffusant,
- image en demi-tons,
- image résultant de l'assemblage de deux ou plus images des types ci-dessus.

9. Procédé d'authentification selon l'une des revendications précédentes, caractérisé en ce que l'image message (M) est une image binaire, telle qu'une image à deux composantes visuelles.

10. Procédé d'authentification selon l'une des revendications précédentes, caractérisé en ce que la phase de construction du système authentificateur comprend une étape d'enregistrement de l'une au moins des images partagées (P1, P2) sous forme numérique.

11. Procédé d'authentification selon l'une des revendications précédentes, caractérisé en ce qu'il comprend une étape d'enregistrement de l'une (P_2) au moins des images partagées (P1, P2) sous forme imprimée.

12. Procédé d'authentification selon la revendication précédente, caractérisé en ce que la phase de construction d'un système authentificateur comprend une étape d'impression de l'une au moins des images partagée sur l'objet matériel (O).

13. Procédé d'authentification selon l'une des revendications précédentes, caractérisé en ce que la phase de construction d'un système authentificateur comprend une étape d'enregistrement sous forme imprimée d'au moins une image partagée (P_2) et une étape d'enregistrement d'au moins une autre image partagée (P_1) sous forme numérique.

14. Procédé d'authentification selon l'une des revendications précédentes, caractérisé en ce qu'il comprend une phase de vérification par un utilisateur comprenant :

- une étape de présentation à la vue de l'utilisateur d'une image partagée (P_1)
- et au moins une autre étape de présentation à la vue de l'utilisateur d'une autre image partagée (P_2),

les étapes de présentation étant conduites de manière que l'utilisateur perçoive les images partagées (P1, P2) comme étant superposées pour permettre une lecture de l'image message (M) par l'utilisateur.

15. Procédé d'authentification selon la revendication précédente, caractérisé en ce que les étapes de présentation sont conduites successivement de manière à mettre en œuvre un phénomène de persistance rétinienne chez l'utilisateur.

16. Procédé d'authentification selon la revendication 14, caractérisé en ce que les étapes de présentation sont conduites simultanément.

17. Procédé d'authentification selon l'une des revendications 14 à 16, caractérisé en ce qu'au moins une étape de présentation est effectuée au moyen d'un dispositif électronique d'affichage ou de projection.

18. Procédé d'authentification selon l'une des revendications 14 à 17, caractérisé en ce qu'au moins une étape de présentation est effectuée au moyen d'au moins une image partagée imprimée (P_2).

19. Procédé d'authentification selon l'une des revendications 14 à 18, caractérisé en ce que la phase de vérification comprend une étape d'extraction de la signature matière.

20. Procédé d'authentification selon l'une des revendications 14 à 18, caractérisé en ce que la phase de vérification comprend une étape de génération ou construction d'une image partagée (P_1).

21. Procédé d'authentification selon l'une des revendications 14 à 19, caractérisé en ce que la phase de vérification comprend une étape de téléchargement d'une image partagée (P_1) à partir d'un serveur distant (SD).

22. Procédé d'authentification selon l'une de revendication précédente caractérisé en ce qu'au moins une image partagée (P_1) est indépendante de l'image message (M) et chaque autre image partagée (P2) dépend de l'image message (M).

23. Procédé, pour la mise en œuvre du procédé selon la revendication 1, de transformation d'une image message (M) et d'une image support (S) en au moins deux images partagées (P1, P2) au moyen d'au moins une séquence aléatoire, l'image message (M) n'étant pas accessible dans chaque image partagée prise individuellement et étant révélée par superposition réelle et/ou virtuelle des images partagées (P1, P2), caractérisé en ce que chaque image partagée présente l'image support (S) dans une forme altérée et en ce que lors de la superposition des images partagées (P1, P2) il est obtenu une image comprenant l'image support (S) dans sa forme originale et l'image message (M)

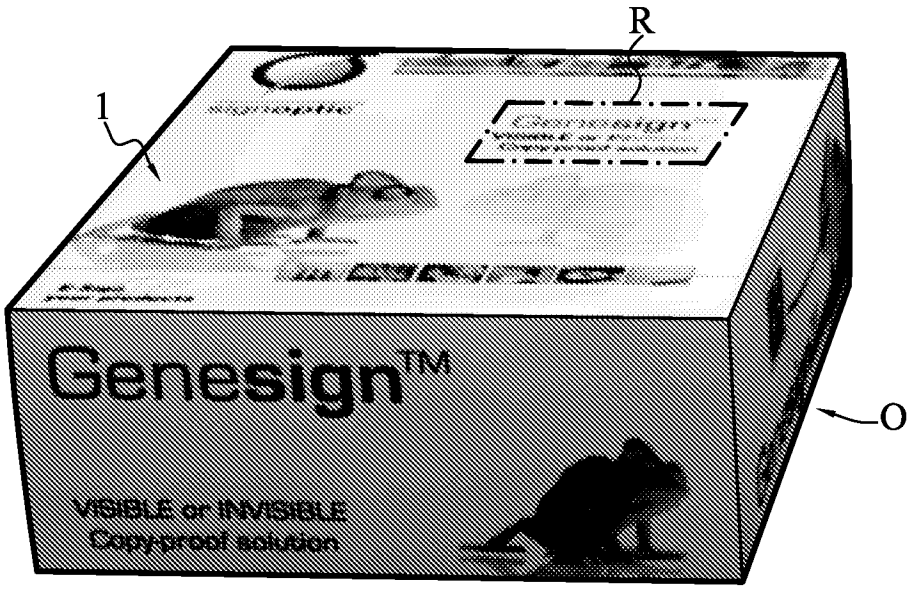

R
1
Genesign™
VISIBLE or INVISIBLE
Copyproof solution
O

FIG.1

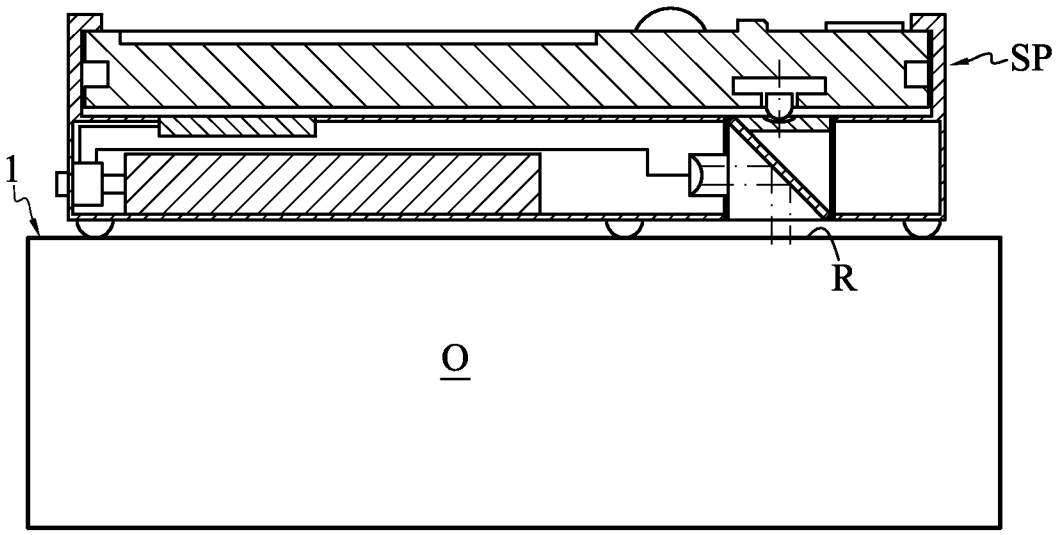

SP
1
R
O

FIG.7

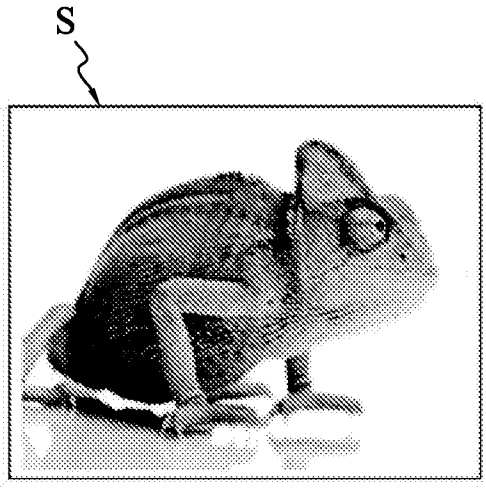


FIG.2

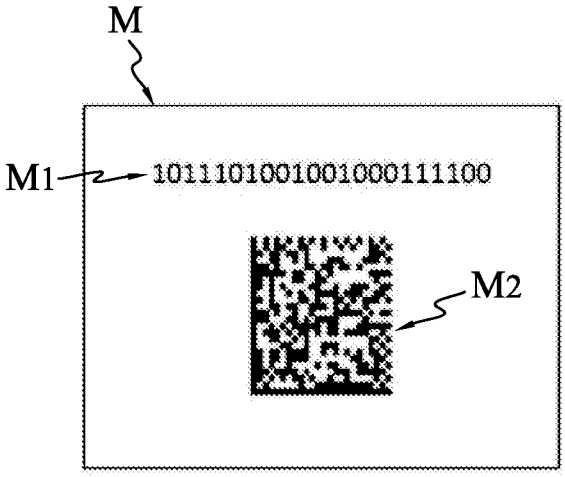


FIG.3

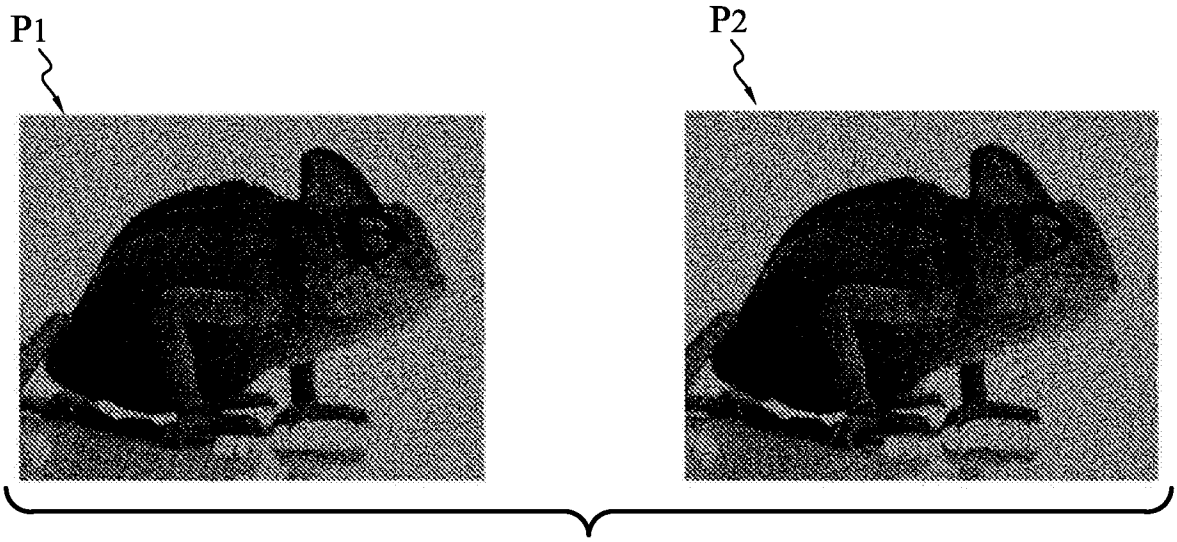


FIG.4

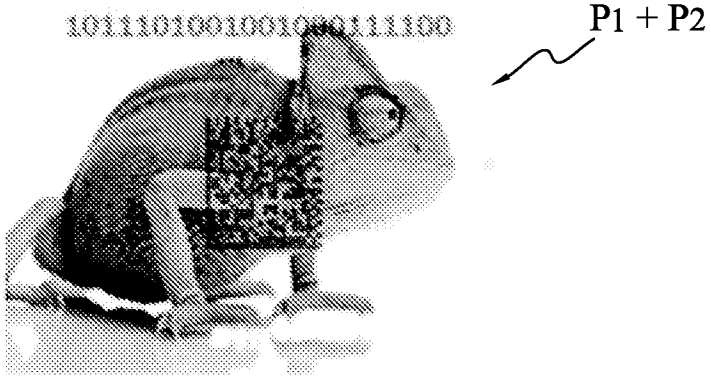


FIG.10

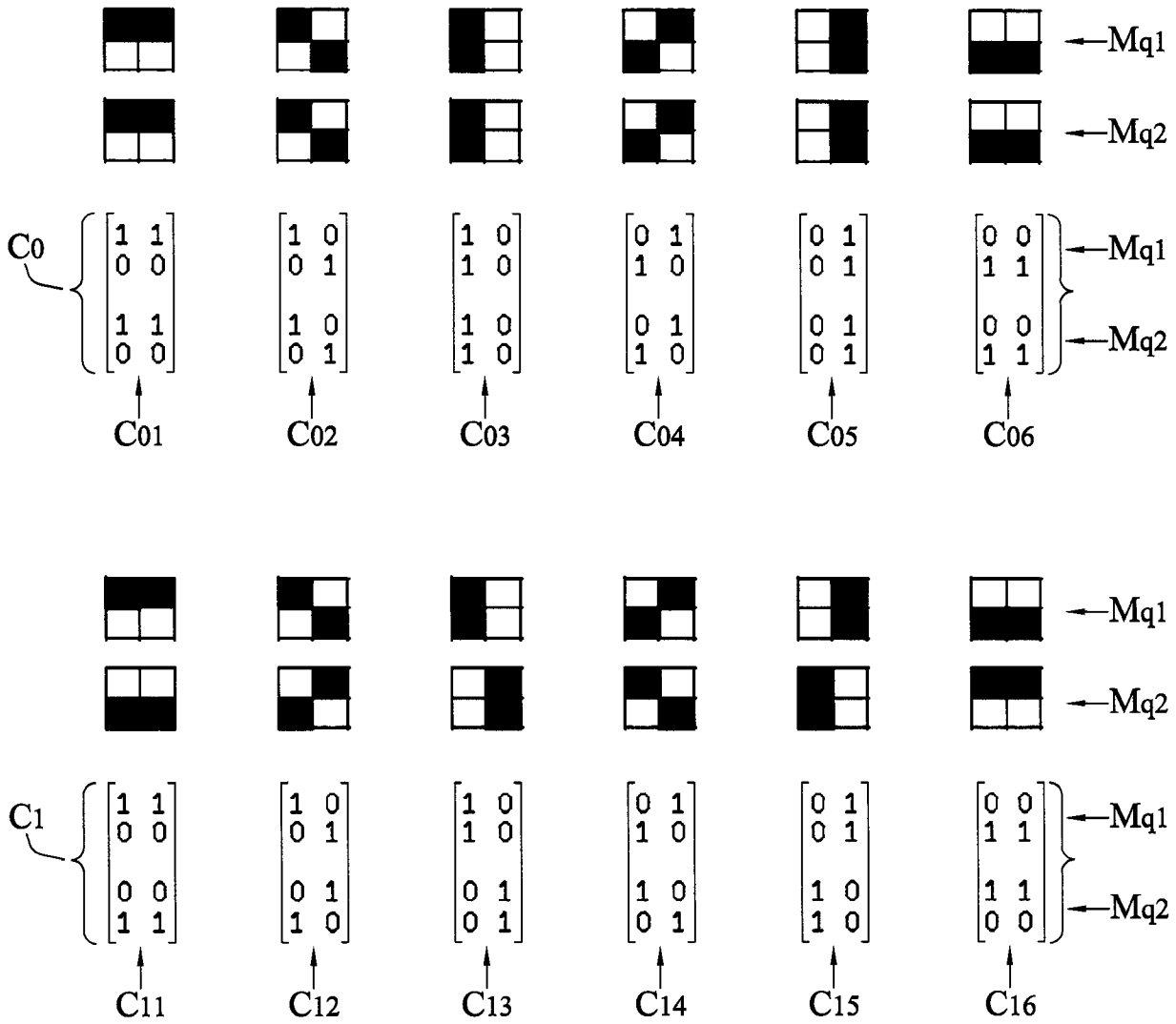

Mq1
Mq2
C0
C01
C02
C03
C04
C05
C06
C1
C11
C12
C13
C14
C15
C16

FIG.5

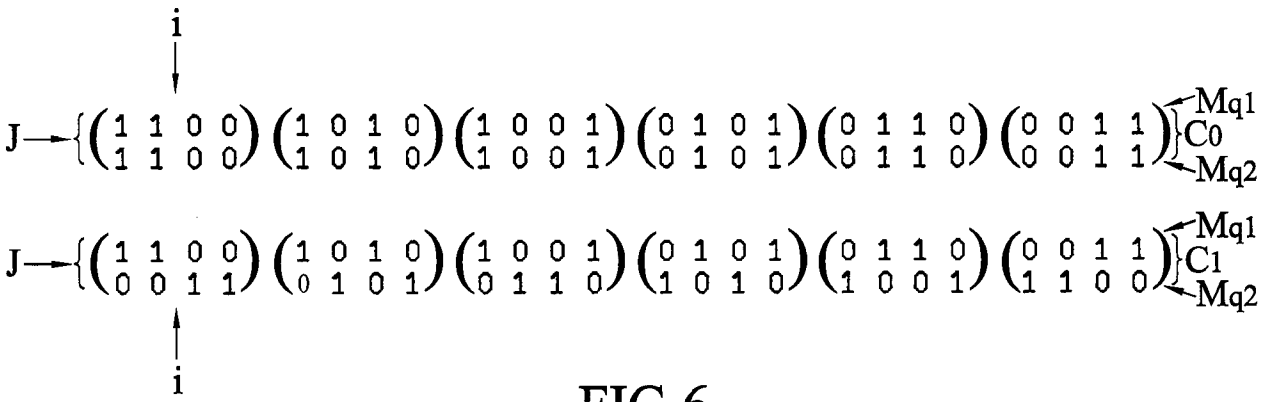

i
J
Mq1
C0
Mq2
Mq1
C1
Mq2
i

FIG.6

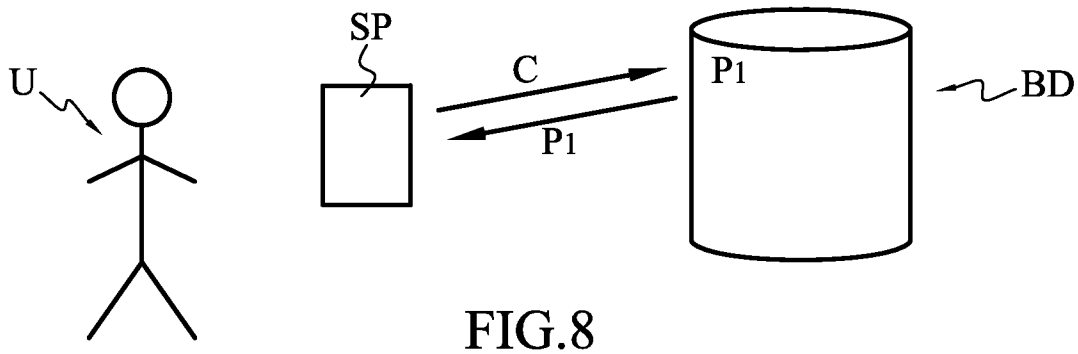


FIG.8

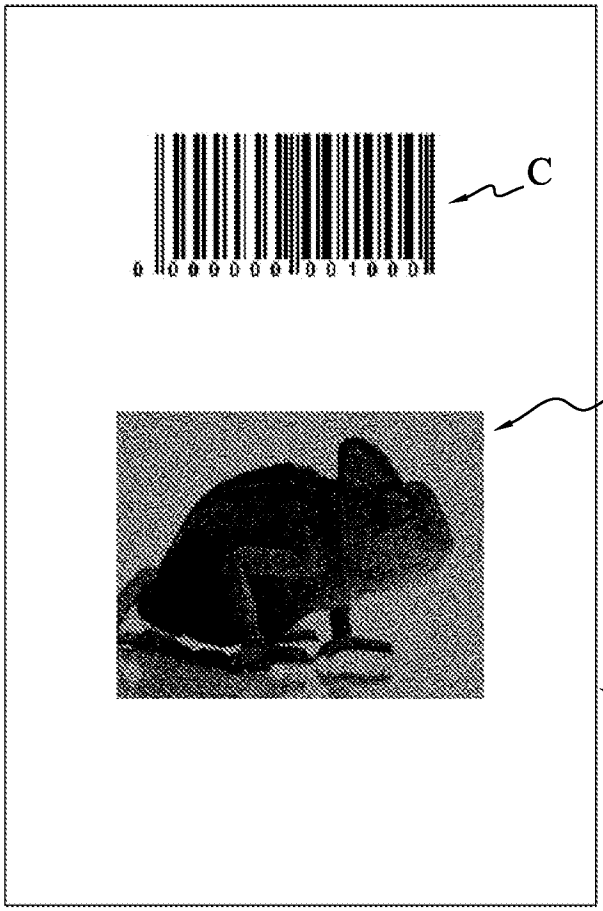


FIG.9

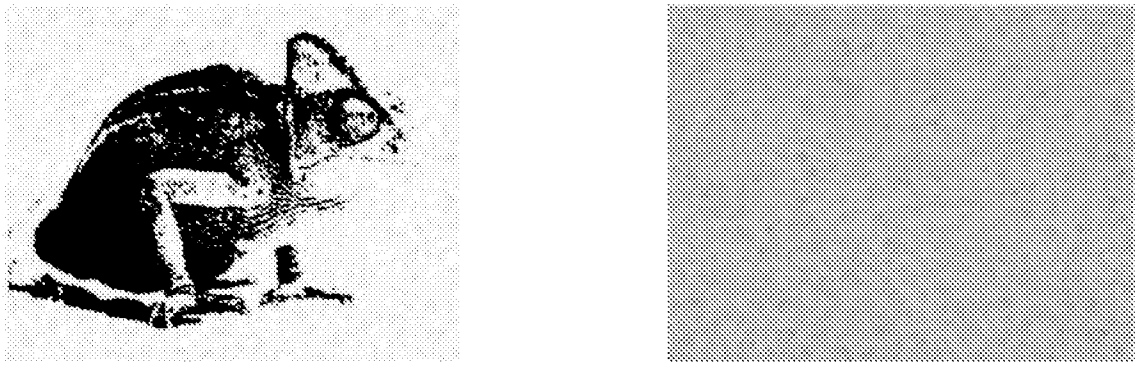


FIG.15

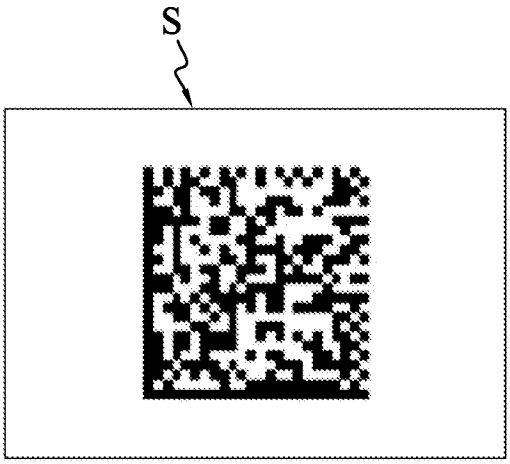


FIG.11

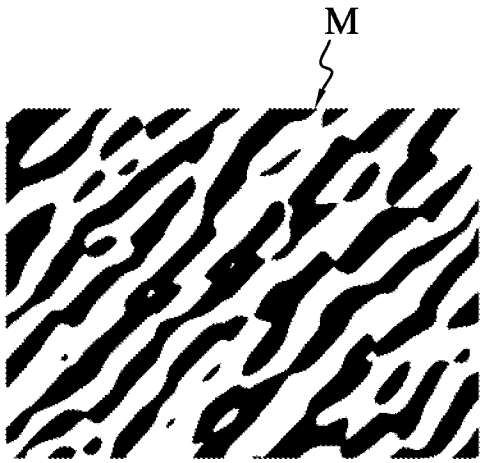


FIG.12

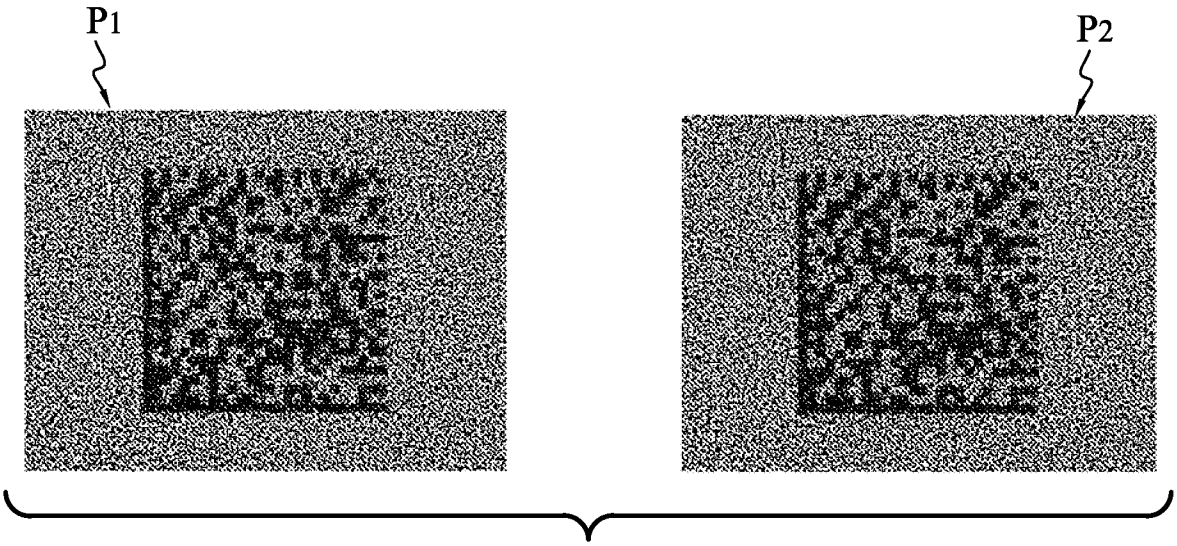


FIG.13

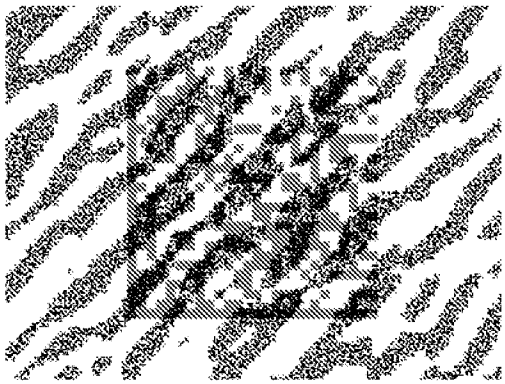


FIG.14

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2012/050968

A. CLASSIFICATION OF SUBJECT MATTER
INV. G07F7/08 G06T1/00
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)
G07F G06T

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 practicable, 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.
X	US 4 586 711 A (WINTERS SIMON N [US] ET AL) 6 May 1986 (1986-05-06) the whole document -----	1-23
X	GB 2 289 016 A (YEDA RES & DEV [IL]) 8 November 1995 (1995-11-08) abstract figures 1-3 -----	1-23
X	US 5 851 032 A (GREEN IAN MACDONALD [GB]) 22 December 1998 (1998-12-22) the whole document -----	1-23
X	EP 2 199 098 A1 (GEMALTO SA [FR]) 23 June 2010 (2010-06-23) abstract paragraph [0005] - paragraph [0025] -----	1-23

-/--

[X] Further documents are listed in the continuation of Box C.

[X] 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 application or patent 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
2 July 2012	06/07/2012

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Beugin, Anne

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2012/050968

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2009/257619 A1 (BOUTANT YANN [FR] ET AL) 15 October 2009 (2009-10-15) abstract paragraph [0121] - paragraph [0126]	1-23
A	EP 1 577 847 A1 (ELCA INF S A [CH]) 21 September 2005 (2005-09-21) paragraph [0008] - paragraph [0017] paragraph [0026]	1-23

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2012/050968

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 4586711 A	06-05-1986	NONE	
GB 2289016 A	08-11-1995	GB 2289016 A	08-11-1995
		US 5488664 A	30-01-1996
US 5851032 A	22-12-1998	AU 687447 B2	26-02-1998
		AU 7787994 A	01-05-1995
		CA 2173487 A1	13-04-1995
		DE 69404042 D1	07-08-1997
		DE 69404042 T2	05-02-1998
		EP 0722391 A1	24-07-1996
		GB 2282563 A	12-04-1995
		JP H09503172 A	31-03-1997
		NZ 273984 A	25-09-1996
		US 5851032 A	22-12-1998
		WO 9509731 A1	13-04-1995
EP 2199098 A1	23-06-2010	EP 2199098 A1	23-06-2010
		WO 2010070089 A1	24-06-2010
US 2009257619 A1	15-10-2009	AT 529826 T	15-11-2011
		BR PI0620363 A2	08-11-2011
		CA 2634603 A1	28-06-2007
		DK 1971960 T3	30-01-2012
		EP 1971960 A1	24-09-2008
		ES 2374975 T3	23-02-2012
		FR 2895543 A1	29-06-2007
		JP 2010514227 A	30-04-2010
		PT 1971960 E	01-02-2012
		SI 1971960 T1	30-03-2012
		US 2009257619 A1	15-10-2009
		WO 2007071788 A1	28-06-2007
EP 1577847 A1	21-09-2005	EP 1577847 A1	21-09-2005
		US 2007180248 A1	02-08-2007
		WO 2005091232 A1	29-09-2005

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2012/050968

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. G07F7/08 G06T1/00
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)
G07F G06T

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
X	US 4 586 711 A (WINTERS SIMON N [US] ET AL) 6 mai 1986 (1986-05-06) le document en entier	1-23
X	GB 2 289 016 A (YEDA RES & DEV [IL]) 8 novembre 1995 (1995-11-08) abrégé figures 1-3	1-23
X	US 5 851 032 A (GREEN IAN MACDONALD [GB]) 22 décembre 1998 (1998-12-22) le document en entier	1-23
X	EP 2 199 098 A1 (GEMALTO SA [FR]) 23 juin 2010 (2010-06-23) abrégé alinéa [0005] - alinéa [0025]	1-23

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] 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	Date d'expédition du présent rapport de recherche internationale
2 juillet 2012	06/07/2012

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Beugin, Anne

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2012/050968

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	US 2009/257619 A1 (BOUTANT YANN [FR] ET AL) 15 octobre 2009 (2009-10-15) abrégé alinéa [0121] - alinéa [0126] -----	1-23
A	EP 1 577 847 A1 (ELCA INF S A [CH]) 21 septembre 2005 (2005-09-21) alinéa [0008] - alinéa [0017] alinéa [0026] -----	1-23

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2012/050968

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 4586711 A	06-05-1986	AUCUN	
GB 2289016 A	08-11-1995	GB 2289016 A	08-11-1995
		US 5488664 A	30-01-1996
US 5851032 A	22-12-1998	AU 687447 B2	26-02-1998
		AU 7787994 A	01-05-1995
		CA 2173487 A1	13-04-1995
		DE 69404042 D1	07-08-1997
		DE 69404042 T2	05-02-1998
		EP 0722391 A1	24-07-1996
		GB 2282563 A	12-04-1995
		JP H09503172 A	31-03-1997
		NZ 273984 A	25-09-1996
		US 5851032 A	22-12-1998
		WO 9509731 A1	13-04-1995
EP 2199098 A1	23-06-2010	EP 2199098 A1	23-06-2010
		WO 2010070089 A1	24-06-2010
US 2009257619 A1	15-10-2009	AT 529826 T	15-11-2011
		BR PI0620363 A2	08-11-2011
		CA 2634603 A1	28-06-2007
		DK 1971960 T3	30-01-2012
		EP 1971960 A1	24-09-2008
		ES 2374975 T3	23-02-2012
		FR 2895543 A1	29-06-2007
		JP 2010514227 A	30-04-2010
		PT 1971960 E	01-02-2012
		SI 1971960 T1	30-03-2012
		US 2009257619 A1	15-10-2009
		WO 2007071788 A1	28-06-2007
EP 1577847 A1	21-09-2005	EP 1577847 A1	21-09-2005
		US 2007180248 A1	02-08-2007
		WO 2005091232 A1	29-09-2005