(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
12 septembre 2008 (12.09.2008)

PCT

(10) Numéro de publication internationale
WO 2008/107525 A2

(51) Classification internationale des brevets :
H04N 1/32 (2006.01)

(21) Numéro de la demande internationale :
PCT/FR2007/002085

(22) Date de dépôt international :
14 décembre 2007 (14.12.2007)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :

0610891	14 décembre 2006 (14.12.2006)	FR
0611402	26 décembre 2006 (26.12.2006)	FR
0703922	1 juin 2007 (01.06.2007)	FR
0704517	22 juin 2007 (22.06.2007)	FR

(71) Déposant *(pour tous les États désignés sauf US)* : **ADVANCED TRACK & TRACE** [FR/FR]; 99, avenue de la Châtaigneraie, F-92504 Rueil-Malmaison Cedex (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **MASSICOT, Jean-Pierre** [FR/FR]; c/o ATT, 99, avenue de la Châtaigneraie, F-92504 Rueil-Malmaison Cedex (FR). **FOUCOU, Alain** [FR/FR]; c/o ATT, 99, avenue de la Châtaigneraie, F-92504 Rueil-Malmaison Cedex (FR). **SAGAN, Zbigniew** [FR/FR]; c/o ATT, 99, avenue de la Châtaigneraie, F-92504 Rueil-Malmaison Cedex (FR).

(74) Mandataire : **CORNUEJOLS, Georges**; 31, avenue Charles de Gaulle, F-92200 Neuilly-sur-Seine (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, 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,

[Suite sur la page suivante]

(54) Title: METHOD AND DEVICE AGAINST FORGERY

(54) Titre : PROCEDE ET DISPOSITIF DE LUTTE CONTRE LA CONTREFAÇON

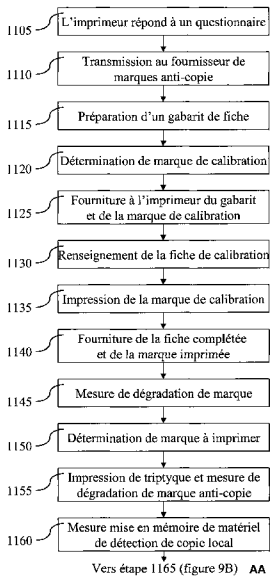

Figure 9A

1105 The printer fills in a form
1110 Transmission to the provider of anti-forgery marks
1115 Preparation of a card template
1120 Determination of a calibration mark
1125 Sending the template and the calibration mark to the printer
1130 Filling in the calibration card
1135 Printing the calibration mark
1140 Sending the filled-in card and the printed mark
1145 Mark degradation measurement
1150 Determining a mark to be printed
1155 Triptych printing and measurement of the degradation of the anti-forgery mark
1160 Memorising the measurement of the local copy detection hardware
AA To step 1165 (Figure 9B)

(57) Abstract: The method of the invention comprises : a step of determining characteristics of the printing hardware of said original document; a step of determining a mark for differentiating an original from a copy based on the characteristics of the printing hardware to be used for printing said mark on said document; a step of printing said mark using said printing hardware in order to create said original document; and a step of determining a first boundary value to be used by a copy detection hardware for discriminating the original document from a copy of the original document based at least on a print of said mark. In some embodiments, the method comprises the step of printing at least one printing reference representative of a maximal or minimal authorised inking for the printing of said document and, during the step for determining a first boundary value, determining a measure on at least said one printing reference and adding a tolerance thereto.

(57) Abrégé : Le procédé comporte : une étape de détermination de caractéristiques d'un matériel d'impression dudit document original; une étape de détermination d'une marque permettant de différencier un original d'une copie, en fonction des caractéristiques du matériel d'impression destiné à être mis en œuvre pour l'impression de ladite marque sur ledit document; une étape d'impression de ladite marque avec ledit matériel d'impression pour former ledit document original; et une étape de détermination d'une première valeur limite à utiliser par un matériel de détection de copie pour discriminer ledit document original d'une copie dudit document original, en fonction d'au moins une impression de ladite marque. Dans des modes de réalisation, le procédé comporte une étape d'impression d'au moins une référence d'impression représentatives d'un maximum ou d'un minimum d'encrage autorisé pour l'impression dudit document et, au cours de l'étape de détermination de la première valeur limite, on détermine une mesure sur au moins une dite référence d'impression et on y ajoute une tolérance.

WO 2008/107525 A2

MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

— *avec tous renseignements concernant une ou plusieurs revendications de priorité considérées comme nulles*

PROCEDE ET DISPOSITIF DE LUTTE CONTRE LA CONTREFACON

La présente invention concerne un procédé et un dispositif de lutte contre la contrefaçon. Elle concerne, en particulier, la production et l'exploitation des codes numériques authentifiants (« CNA »). Parmi ces codes numériques authentifiants, la présente invention applique, en particulier, des motifs de détection de copie (« MDC »), des matrices d'information sécurisées (« MIS »), des motifs de points dispersés et/ou des filigranes numériques (en anglais « watermarks ») à la production, au traçage et à l'authentification sécurisés et robustes de produits et pièces manufacturés, d'emballages, etc.

La contrefaçon et la falsification de certificats, billets de banque, éléments de monétique, passeports, attestations, chèques, diplômes, timbres de taxes, ou autres, existent depuis presque aussi longtemps que ces documents. En revanche, si les problèmes de contrefaçon et de marché « gris » ou parallèles de produits industriels existent depuis longtemps, depuis quelques années ils ont pris une ampleur considérable. Aujourd'hui, une partie significative des produits industriels sont soit contrefaits, soit détournés de leurs marchés autorisés par leurs distributeurs. Les détenteurs de droits de propriété intellectuelle sont relativement démunis pour faire face à ce problème : les législations sont inadaptées ou inégales dans les différentes zones géographiques, et il est difficile de retrouver la source ou de tracer, c'est-à-dire de reproduire le chemin, des produits contrefaits ou détournés.

Les détenteurs de ces droits de propriété intellectuelle souhaitent, avant tout, prendre la mesure du ou des problèmes auxquels ils sont confrontés : font-ils face à des problèmes de contrefaçon, de marché gris, une combinaison des deux, sur quels marchés, etc. ? Aussi, les propriétaires de droits de propriété intellectuelle, notamment des marques, modèles et dessins et les organismes qui génèrent des documents officiels et qui ont adopté les codes à barres en deux dimensions (« 2D ») chiffrés ou d'autres supports d'information, tels que les étiquettes électroniques RFID (acronyme de « radiofréquence identification » pour identification radiofréquence), pour les aider à résoudre les problèmes de falsification, doivent néanmoins utiliser des moyens d'authentification (des « authentifiants ») radicalement différents, tels que des hologrammes, des encres de sécurité, des micro-textes, ou des motifs dits « de guilloche » (lignes fines et courbes interférant avec les systèmes de reproduction numérique, par exemple par effet de Moiré), pour éviter ou détecter la contrefaçon servile.

Ces moyens ont cependant leurs limites, qui deviennent de plus en plus flagrantes avec la diffusion rapide de la technologie, permettant aux contrefacteurs de copier ces

authentifiants de mieux en mieux et dans un délai de plus en plus court. Ainsi, les hologrammes sont de mieux en mieux copiés par les contrefacteurs et les utilisateurs terminaux (en anglais « end-users ») n'ont pas les capacités ni la motivation de vérifier ces hologrammes. Les encres de sécurité, les motifs dits « de guilloche » et les micro-textes sont difficiles à insérer dans les chaînes de production ou d'information des entreprises et n'offrent pas le niveau de sécurité généralement requis. De plus, ils peuvent être difficiles à identifier et n'offrent pas de réelles garanties de sécurité contre les contrefacteurs déterminés.

La difficulté d'intégration de ces moyens d'authentification est également un frein à leur utilisation, en particulier lorsque la production est décentralisée. Ainsi, une multinationale a souvent des sites de production dans plusieurs pays, faisant souvent appel à plusieurs sous-traitants. Il est très difficile, et en tous cas très coûteux, d'assurer la logistique d'acheminement d'éléments de sécurité physique (encre de sécurité, marqueur DNA, etc.) vers chacun de ces sites de productions. Une mauvaise gestion des stocks ou un retard dans l'acheminement peut signifier une production suspendue ou non-protégée.

Les CNA offrent une alternative intéressante aux méthodes traditionnelles de sécurisation de documents. Dans l'ère du « tout numérique », ils offrent une solution de nature essentiellement numérique ayant l'ensemble des fonctionnalités désirées, c'est-à-dire traçabilité de produits, authentification (détection des copies) automatique, détection des falsifications. Ils dématérialisent le processus de production de documents sécurisés : on insère une marque en modifiant un fichier numérique d'un document, ou en y ajoutant une image qui est authenfiante (c'est-à-dire permettant de détecter automatiquement des copies) et, éventuellement, identifiante. La lecture se fait par le traitement automatique d'une capture d'image numérique d'un document, le lecteur pouvant éventuellement se connecter à une base de données sécurisée.

Les CNA sont particulièrement intéressants pour les détenteurs de droits sur les produits manufacturés qui ont des impératifs de production et de coût particulièrement sévères : en effet, la commande, l'envoi et la réception de fichiers images de CNA peuvent se faire instantanément.

Un autre avantage des CNA est la possibilité d'utiliser des capteurs d'images standards, tels des scanners ou des appareils photos numériques grand public, éventuellement intégrés dans des assistants personnels numériques (ou téléphones portables), pour la vérification des CNA. Ceci autorise le déploiement des CNA à grande échelle, étant donné le faible coût et la facilité qu'il y a à se procurer de tels capteurs. Par opposition, une encre de sécurité nécessite un lecteur dédié, souvent coûteux, et oblige le détenteur de droits à s'engager sur une solution vulnérable et coûteuse à mettre en place, avec les conséquences et risques que cela comporte.

Parmi les CNA, les MIS et les MDC sont des codes numériques authentifiants particuliers. D'autres CNA incluent les filigranes numériques, et les motifs de points dispersés, si ceux-ci ont des propriétés authentifiantes. Les codes numériques authentifiants CNA présentent la capacité, du moins en principe, de tracer individuellement chaque document ou produit.

Comme les codes à barres 2D, les matrices d'information sécurisées MIS sont une représentation d'information matricielle sur une surface, lisible par une machine à partir d'une capture d'image. Mais contrairement aux code à barres 2D (en deux dimensions), les MIS ne sont pas de simples « conteneurs » d'information : elles sont conçues de manière à assurer la sécurité des documents sur lesquels elles sont imprimées. En particulier, elles permettent de traiter de nombreux problèmes liés à la contrefaçon (copies à l'identique, reproductions) et à la falsification de documents (date de péremption d'un médicament, carte d'identité, etc.), et assurent leur traçabilité, ce qui permet notamment de lutter contre le marché gris. Certes, certains de ces problèmes peuvent être traités partiellement par des code à barres 2D ordinaires, telles que les Datamatrix (marque déposée), moyennant l'ajout d'une couche cryptographique protégeant l'écriture et la lecture des messages. Cependant, les MIS offrent un traitement beaucoup plus étendu des problèmes liés à la sécurité. Par exemple, les MIS permettent de détecter les cas de contrefaçon par copie conforme ou photocopie, ce qui n'est en principe pas possible avec les autres types de matrices d'information. En particulier, toute copie d'une MIS imprimée originale peut être détectée. En effet, comme exposé dans les documents PCT FR 2007/000918 et PCT FR 2007/001246, incorporés ici par référence, le taux d'erreur au décodage du message porté par la MIS copiée est plus élevé que le taux d'erreur maximum toléré pour une MIS imprimée originale. De plus, les MIS offrent la possibilité d'utiliser différents niveaux de permission d'écriture ou de lecture, verrouillés chacun par une clé cryptographique, chaque niveau de permission correspondant à une couche de sécurité : si une clé cryptographique est compromise, seule la couche de sécurité correspondante est affectée.

Grâce à leur capacité relativement importante en termes de quantité d'information et à la possibilité d'utiliser différents niveaux de permission d'écriture ou de lecture, les MIS permettent de stocker de façon sécurisée l'ensemble des valeurs associées à la traçabilité du document comme, par exemple, un numéro d'identité unique, une date de péremption, un ordre de fabrication, une provenance, un marché de destination, etc. Il est avantageux que chaque MIS soit unique, c'est-à-dire qu'une MIS comportant un message spécifique ne sera imprimée qu'une seule fois : on parle alors d'impression « sérialisée ». On s'assure ainsi de pouvoir identifier de façon unique chacun des documents existants. Les MIS sont en général utilisés de cette manière pour les méthodes d'impression de nature digitale, c'est-à-dire dans lesquels un processeur communique directement avec le moyen d'impression et peut faire

varier les contenus imprimés, notamment avec les moyens d'impression digitale, laser, à jet d'encre permettant l'impression sérialisée de MIS.

Les motifs de détection de copies (en anglais « copy detection patterns ») MDC sont un type de motifs d'authentification visibles, qui ont généralement l'apparence du bruit et sont générés à partir d'une clé, de manière pseudo-aléatoire. Ces motifs de détection de copie MDC sont essentiellement utilisés pour distinguer des documents imprimés originaux et des documents imprimés copies des premiers, par exemple par photocopie ou utilisation d'un scanner et d'une imprimante. Cette technique fonctionne en comparant une image captée d'un motif de détection de copie analogique, c'est-à-dire du monde réel, avec une représentation numérique originale de ce motif pour mesurer le degré de différence entre les deux. Le principe sous-jacent est que le degré de différence est plus élevé pour l'image captée d'un motif qui n'a pas été produit à partir d'un motif analogique original, du fait de la dégradation lors de la copie. Pour véhiculer de l'information, l'image du MDC est divisée en zones, et chaque zone peut contenir différentes configurations de valeurs de pixels (toutes ayant l'apparence du bruit), chaque configuration étant associée à une valeur binaire.

Leur principe de fonctionnement lors de la lecture peut souvent être assimilé à la mesure du niveau d'énergie d'un signal dans l'image captée, appelée par la suite « score », qui est comparé à une valeur de seuil, en général, prédéterminé : si le score est supérieur à cette valeur de seuil, on en déduit que l'image est un original. Sinon, on en déduit que c'est une copie. On peut également avoir une zone d'indécision « grise » dans la région de la valeur de seuil, pour laquelle la décision est ambiguë, et dans le cas où le score est situé dans cette zone, on demande une nouvelle capture d'image.

Pour les MIS, le score peut être, par exemple, mesuré comme une fonction décroissante du taux d'erreur du MIS capté. Pour les MDC il peut être mesuré comme l'indice de similarité entre le MDC d'origine et le MDC capté. Pour les filigranes numériques, le score peut être mesuré par le degré de corrélation entre le filigrane d'origine, soit le signal avant sa modulation dans l'image marquée, et l'image captée, une fois l'image filtrée dans le spectre de fréquence adéquat et la synchronisation des signaux effectuée. Finalement, pour les motifs de points dispersés, le score peut être mesuré par la valeur au pic de corrélation croisée entre le motif de points d'origine et le motif de points dans l'image captée. On note que de nombreuses autres mesures sont possibles, et notamment que les mesures de distance peuvent être inversées pour représenter des mesures de proximité ou de similarité.

La valeur de seuil (ou éventuellement les seuils si on utilise la zone d'indécision « grise » décrite précédemment) sont en général pré-calculées en se basant sur la distribution statistique des scores d'un échantillon représentatif de l'ensemble des impressions de CNA originaux. Des techniques connues de l'art antérieur sont utilisées pour l'estimation de la moyenne, de la variance ou de l'écart-type, et les probabilités à priori (on

peut par exemple supposer qu'un original est beaucoup plus probable qu'une copie) sont parfois utilisées. Des facteurs de coût peuvent être attribués aux types d'erreur du système de détection, auquel cas on détermine une valeur de seuil qui minimise ce risque. Par exemple, dans certaines applications on considère qu'il est plus acceptable qu'un original soit faussement détecté comme copie que l'inverse, car, pour une décision « copie », on peut faire une seconde lecture qui confirme ou dissipe les doutes.

On observe que les CNA peuvent être invisibles ou du moins difficiles à percevoir, par exemple un filigrane numérique fragile à la copie intégré à l'image, ou encore un motif de points pseudo-aléatoirement dispersés, également appelé « MSMA ». Les points répartis pseudo-aléatoirement présentent une certaine densité, suffisamment faible pour être difficile à repérer, par exemple de l'ordre de 1%. Un score s'apparentant au pic de corrélation croisée entre le MSMA de référence et le MSMA capturé correspond au niveau d'énergie du signal, et sera à priori plus faible pour les copies.

Si les avantages des CNA sont nombreux, la mise en œuvre d'un système de traçabilité basé sur les CNA pose cependant de nombreux problèmes non-résolus à ce jour, que ce soit pour leur intégration dans des documents ou pour leur exploitation pour lutter contre la contrefaçon.

Pour le calcul de la valeur de seuil, un problème vient du fait que la distribution statistique des scores des copies est une abstraction. On peut décider de « l'ignorer », auquel cas on peut fixer la valeur de seuil en considérant le taux d'erreurs acceptable si on lit que des originaux. Ainsi, pour une valeur de seuil égal à la moyenne moins trois écart-type (s=m-3*e), en faisant l'hypothèse d'une distribution gaussienne des scores, la probabilité qu'un original soit détecté comme copie est de 0.44%. Pour connaître la probabilité qu'une copie soit détectée comme original, beaucoup de méthodes sont possibles : on peut, par exemple, à partir d'une image d'un original, chercher à faire la meilleure copie possible en utilisant le même procédé d'impression pour la copie que pour l'original, on estime la distribution statistique des scores pour la copie, et on peut alors estimer la probabilité qu'une copie ait un score qui excède la valeur de seuil. On peut également faire l'hypothèse qu'un taux de dégradation similaire est appliqué lors de l'impression d'un original et lors de l'impression d'une copie : ainsi, si pour les originaux le score est inférieur de 20% au score dans le cas où l'image n'aurait pas été dégradée du tout, on peut faire l'hypothèse que le score d'une impression originale subira aussi une perte de 20% lors de la copie, auquel cas une copie aurait en moyenne 66% du score maximal. D'autres approches similaires sont possibles, et on peut également modéliser, par un filtrage spatial numérique, l'impression d'un original et d'une copie (par exemple : ajout de bruit et filtrage gaussien passe-bas).

On voit que la détermination de la valeur de seuil et la fiabilité du système (qu'elle soit mesurée en taux d'erreurs moyen, coût, ou autre) est fortement dépendante de la distribution

statistique du score des originaux, qui doit, idéalement, avoir un écart-type aussi petit que possible. En pratique, des instabilités d'impression en production peuvent causer une dispersion des scores des originaux telle que la fiabilité du système s'en trouve fortement réduite. A titre d'exemple, les figures 4 et 5 montrent deux distributions 905 et 915 de scores pour les impressions originales et deux distributions hypothétiques 910 et 920 pour les copies (en effet, comme on l'a dit il n'existe pas, à proprement parler, de distribution universelle de scores des copies), lorsque la production des documents originaux est bien contrôlée, comme illustré en figure 4, et lorsqu'elle est mal contrôlée, comme illustré en figure 5. Dans le premier cas, la distribution 905 des scores des originaux suit approximativement une distribution gaussienne, et la séparation avec les scores des copies 910 est nette : l'ensemble des impressions originales a été réalisée dans des conditions à l'identique. En revanche, dans le deuxième cas, la distribution des scores des originaux 915 est plus étalée et la capacité de séparer complètement des scores d'originaux 915 et des scores de copies 920 n'est plus assurée, la zone (a) pointée par une flèche correspondant aux valeurs de scores où on ne peut se fier au résultat du détecteur. L'étalement de la distribution des scores des originaux correspond à une combinaison des distributions illustrées en figures 4 et 5 avec des proportions respectives de ¾ et ¼ : ces distributions correspondent à des conditions de production qui seraient, en partie, différentes. On peut imaginer, par exemple, que les trois premiers quarts de la production ont été réalisés avec des conditions de densité d'encre constantes, puis, à la suite d'un changement d'opérateur, le nouvel opérateur n'a pas respecté les conditions initiales de densité d'encre, ce qui a provoqué une diminution du score du CNA.

Du côté de l'exploitation des CNA, plusieurs problèmes sont également non résolus, notamment la robustesse de lecture, la sécurité et la disponibilité des modules de lecture, et l'interopérabilité des systèmes de sécurité.

Dans la discussion précédente sur le score, il a été fait l'hypothèse implicite qu'il n'existait qu'un seul score possible pour une impression d'un CNA : ce serait effectivement le cas si la capture d'image était « parfaite » ou, du moins, identique à chaque fois. Or, la capture et la qualité d'image associée peuvent varier d'un outil de capture à l'autre, et même d'une capture à l'autre par un même capteur d'image. Et la qualité de la capture d'image peut avoir une influence considérable sur le score.

Les paramètres internes de l'outil de capture d'image ont également une influence. Par exemple, la qualité d'image, et donc le score d'un CNA, capturée avec un scanner peut varier en fonction de la résolution de capture d'image, du nombre de bits par pixel, etc. De plus, un capteur d'images peut réaliser de mauvaises captures d'images. Par exemple, si un objet contenant un CNA est mal positionné sur un scanner, l'image captée peut être floue. Si un outil portable est utilisé et si l'opérateur n'y prend pas garde, l'image peut avoir un

problème de netteté à cause d'un mouvement ou d'un positionnement du CNA hors du plan focal. Typiquement, le score du CNA peut être sensiblement moins élevé et un original peut alors être détecté comme copie.

On peut donc, d'une part, avoir des problèmes de mauvaise qualité de capture d'image avec un outil pouvant réaliser, autrement, des captures d'image de qualité requise. D'autre part, il peut exister des différences de qualité intrinsèque entre les outils de capture d'image, notamment l'outil de capture d'image utilisé pour initialement calculer la distribution statistique des scores, et l'outil de capture d'image utilisé en exploitation/lecture, qui peuvent se traduire par un décalage du score. Si on n'en tient pas compte, chaque valeur de seuil calculée initialement peut induire de nombreuses erreurs de détermination d'authenticité. La figure 6 montre, dans la partie haute, une distribution statistique des scores pour les originaux, 925, et les copies, 930, calculée sur la base d'images prises avec un outil de capture d'image de référence, une valeur de seuil calculée minimisant le taux d'erreurs moyen pour cette distribution. Dans la partie basse, cette figure montre la distribution statistique des scores pour les mêmes originaux, 935, et copies, 940, sur la base d'images capturées par un autre outil de capture d'image de qualité inférieure. On y indique, en 945, la valeur de seuil tel que calculée pour l'outil de capture d'image de référence. On voit clairement que la valeur de seuil utilisée n'est pas adéquate et mènerait à de nombreuses erreurs de décision. On note que le score représenté en figure 6 est, par rapport au score représenté en figures 4 et 5, divisé par cinq. Par exemple, la valeur limite qui vaut 12 en figure 6 correspond à un score de 60 en figures 4 et 5.

En ce qui concerne la sécurité relativement à la disponibilité des modules de lecture, les outils de vérification des CNA peuvent soit opérer localement, soit en liaison avec un serveur. Dans le premier cas, le danger est qu'un contrefacteur s'empare d'un module et en fasse le « reverse engineering », afin de déterminer les algorithmes de lecture utilisés, d'en déduire les algorithmes de génération correspondants (les algorithmes de lecture sont en général symétriques avec les algorithmes de génération de CNA), et surtout de s'emparer des clés cryptographiques stockées dans le module.

Un autre problème concerne le fait que les modules de lecture dédiés ne sont pas toujours disponibles, soit pour des raisons de sécurité, soit parce que leur nombre est limité, ou parce qu'ils sont trop coûteux.

En ce qui concerne l'interopérabilité des systèmes basés sur des CNA, rien n'est prévu actuellement. Or des inspecteurs mandatés par des associations de propriétaires des droits pourraient authentifier et tracer les produits aux différents points de vente. De même, des douaniers pourraient être munis de lecteurs pour vérifier les CNA sur les différents produits entrant dans un pays ou une zone géographique disposant d'un accord de libre-échange. Cependant, les propriétaires des droits sont en général très sensibles à la

confidentialité de leurs données, et ils ne souhaitent évidemment pas que d'autres propriétaires des droits, éventuellement des concurrents, puissent accéder à leurs informations. Par exemple, à leurs yeux, il serait catastrophique qu'un concurrent puisse vérifier leurs CNA et en déduire des informations sur leurs méthodes de distribution ou, pire encore, constater que des faux produits sont intégrés dans leur distribution. Ici, l'intérêt des propriétaires de droits ne converge pas forcément avec l'intérêt général qui est justement qu'un maximum de gens soient informés si des contrefaçons sont présentes dans les circuits de distributions.

Chacun des aspects de la présente invention vise à remédier à tout ou partie des inconvénients précités.

La présente invention vise ainsi, selon ses différents aspects, à remédier aux difficultés d'intégration et/ou aux difficultés d'exploitation des CNA, en particulier aux problèmes de sécurité, de stabilité, et de manque de souplesse d'intégration des CNA dans la production de documents sécurisés et/ou aux problèmes de sécurité, de stabilité, et de manque de souplesse d'exploitation des CNA dans la vérification de documents sécurisés.

Certains aspects de la présente invention visent à remédier à ces inconvénients.

A cet effet, selon un premier aspect, la présente invention vise un procédé de lecture d'un code numérique authentifiant, caractérisé en ce qu'il comporte :

- une étape de capture d'une image représentative d'un code numérique authentifiant,
- une étape de détermination de conditions de capture de ladite image,
- une étape de détermination d'un taux d'erreur dudit code numérique authentifiant représenté par ladite image captée et
- une étape de détermination d'authenticité du code numérique authentifiant en fonction du taux d'erreur et des conditions de capture de ladite image.

Grâce à ces dispositions, on peut, pour déterminer l'authenticité d'un document, mettre en œuvre différents moyens de capture d'image, différents moyens d'éclairage du CNA ou traiter une image partiellement floue ou de qualité insuffisante. Le procédé de lecture et d'authentification est ainsi beaucoup plus robuste que les procédés connus dans l'art antérieur.

Selon des caractéristiques particulières, l'étape de détermination de conditions de capture de ladite image comporte une étape de détermination d'une valeur représentative de la qualité de capture de ladite image.

Selon des caractéristiques particulières, l'étape de détermination de conditions de capture d'une image comporte une étape de détermination d'une valeur représentative du flou de capture de ladite image.

Selon des caractéristiques particulières, au cours de l'étape de détermination d'authenticité, on détermine, d'abord, si la valeur représentative de flou représente un flou inférieur à une valeur prédéterminé et, si oui, si le taux d'erreur est inférieur à une valeur prédéterminée.

Selon des caractéristiques particulières, si la valeur représentative de flou représente un flou supérieur à la valeur prédéterminée, on retourne à l'étape de capture d'image et on réitère les étapes de détermination de taux d'erreur et de détermination d'authenticité.

Ainsi, on est prévenu lorsque le flou ne permet pas une détermination d'authenticité suffisamment fiable et on peut réitérer les étapes du procédé.

Selon des caractéristiques particulières, si la valeur représentative de flou représente un flou inférieur à une valeur prédéterminée, on transmet au moins une partie de ladite image à un serveur distant et l'étape de détermination d'authenticité est effectuée par ledit serveur distant.

Des traitements plus complexes peuvent ainsi être réalisés par un système possédant plus de ressources en termes de capacités de traitement.

Selon des caractéristiques particulières, au cours de l'étape de détermination, on détermine, d'abord, si le taux d'erreur est inférieur à une valeur prédéterminée et, si non, si la valeur représentative de flou représente un flou inférieur à une valeur prédéterminé.

Selon des caractéristiques particulières, l'étape de détermination d'une valeur représentative du flou met en œuvre des valeurs représentatives des conditions d'impression du code numérique authentifiant.

On augmente ainsi la fiabilité du procédé car on tient compte de la qualité d'impression du code numérique authentifiant qui peut avoir un impact sur la valeur représentative du flou.

Selon des caractéristiques particulières, le procédé objet de la présente invention, tel que succinctement exposé ci-dessus comporte, à la suite de l'étape de capture d'image et avant l'étapes de détermination d'authenticité, une étape de détection de la présence d'un code numérique authentifiant dans ladite image, les étapes de détermination n'étant effectuées qu'en cas de présence d'un code numérique authentifiant dans ladite image et l'étape de capture d'image étant réitérée en cas d'absence de code numérique authentifiant dans ladite image.

Grâce à ces dispositions, le procédé peut s'appliquer sur une succession d'images captées, sans que l'utilisateur n'ait besoin de déclencher la capture d'une image.

Selon des caractéristiques particulières, au cours de l'étape de détection de présence d'un code numérique authentifiant, on détermine si l'image représente une forme géométrique caractéristique desdits codes.

Par exemple, on recherche, de manière automatique, une forme carrée ou rectangulaire.

Selon des caractéristiques particulières, au cours de l'étape de détermination d'une valeur représentative de flou, on détermine une valeur représentative d'un gradient dans un code numérique authentifiant.

On détermine ainsi facilement le flou représenté par ce gradient, notamment lorsque le flou provient d'un défaut de positionnement du code numérique authentifiant, par rapport au plan de netteté conjugué au plan capteur par l'objectif du moyen de capture d'image.

Selon des caractéristiques particulières, au cours de l'étape de détermination d'une valeur représentative de flou, on met en œuvre un filtre de Sobel.

Selon des caractéristiques particulières, au cours de l'étape de détermination d'une valeur représentative de flou, on met en œuvre un filtre gaussien.

Selon des caractéristiques particulières, le procédé objet de la présente invention, tel que succinctement exposé ci-dessus comporte :

- une étape de capture d'une image représentative d'une mire,
- une étape de détermination d'une valeur d'ajustement à partir de l'image représentative de la mire et
- une étape d'ajustement du taux d'erreur en fonction de ladite valeur d'ajustement,

l'étape de détermination d'authenticité du code numérique authentifiant mettant en œuvre le taux d'erreur ajusté.

Grâce à ces dispositions, on tient automatiquement compte des défauts de prise de vue et on mesure ceux-ci très précisément puisque la mire est, par nature, normalisée.

Selon des caractéristiques particulières, au cours de l'étape de capture d'une image représentative d'une mire, on capture une image d'une carte, le procédé objet de la présente invention, tel que succinctement exposé ci-dessus comportant une étape de lecture, sur ladite carte, d'un identifiant de porteur de carte et une étape de vérification d'autorisation audit porteur d'effectuer une étape de détermination d'authenticité.

On peut ainsi interdire qu'un utilisateur non autorisé ne disposant pas de la carte ne mette en œuvre le procédé objet de la présente invention.

Selon des caractéristiques particulières, l'étape de détermination de conditions de capture d'une image comporte une étape de détermination du nombre de points de ladite image qui correspondent à un code numérique authentifiant.

On peut ainsi tenir compte de la résolution de l'image du code numérique authentifiant, qui a une grande influence sur le taux d'erreurs.

Selon des caractéristiques particulières, l'étape de détermination du nombre de points de ladite image qui correspondent à un code numérique authentifiant comporte une

étape de détermination de la résolution du capteur d'image en nombre de points par unité de surface placée dans son plan de netteté.

Selon des caractéristiques particulières, au cours de l'étape de détermination de conditions de capture d'une image, on détermine une netteté d'impression du code numérique authentifiant.

Selon des caractéristiques particulières, on détermine ladite netteté par lecture, dans le contenu du code numérique authentifiant, d'un type d'impression utilisé pour imprimer ledit code numérique authentifiant.

Selon des caractéristiques particulières, le procédé objet de la présente invention, tel que succinctement exposé ci-dessus, comporte :

- une étape d'envoi à destination d'un serveur sécurisé distant de l'image captée, par l'intermédiaire d'un réseau informatique, l'étape de détermination d'un taux d'erreur et l'étape de détermination de l'authenticité du code numérique authentifiant étant réalisées par ledit serveur distant et
- une étape de renvoi d'un message par le serveur sécurisé indiquant si le code numérique authentifiant est authentique, une copie ou si une nouvelle image doit être capturée.

Selon un deuxième aspect, la présente invention vise un dispositif de lecture d'un code numérique authentifiant, caractérisé en ce qu'il comporte :

- un moyen de capture d'une image représentative d'un code numérique authentifiant,
- un moyen de détermination de conditions de capture de ladite image,
- un moyen de détermination d'un taux d'erreur dudit code numérique authentifiant représenté par ladite image captée et
- un moyen de détermination d'authenticité du code numérique authentifiant en fonction du taux d'erreur et des conditions de capture de ladite image.

Les avantages, buts et caractéristiques de ce dispositif, de ce programme d'ordinateur et de ce support d'information étant similaires à ceux du procédé objet de la présente invention, tel que succinctement exposé ci-dessus, ils ne sont pas rappelés ici.

Du côté de l'intégration des CNA dans la production de documents sécurisés, parmi les problèmes non résolus, on trouve notamment la sécurité des fichiers numériques et la stabilité du marquage. En ce qui concerne la sécurité des fichiers numériques, lorsqu'un CNA est imprimé ou marqué sur un produit, il est en principe quasiment impossible à copier avec une qualité suffisante pour confondre la copie et l'original. En revanche, initialement, un CNA se présente généralement sous forme d'un fichier image, qui permet de produire des CNA authentiques à volonté. Il apparaît donc essentiel de protéger ce fichier durant toute sa durée de vie. Cependant, un tel fichier d'image numérique peut transiter par plusieurs mains, être intégré dans un fichier de design de produit ou de prépresse, etc. Souvent, le détenteur

de droits se voit obligé de confier ce fichier au transformateur, par exemple un imprimeur, sur lequel il a peu de contrôle. De plus, pour de nombreux procédés de marquage, tels que l'offset, le fichier image n'est pas imprimé directement, mais passe par au moins une étape de transformation analogique, par exemple lors de la création de la plaque et parfois lors de la création du film servant à faire la plaque, etc. Ces plaques ou films doivent être également protégés car ils permettent de générer des CNA authentiques. Finalement, il n'y a pas de moyen de contrôle assurant que le transformateur mandaté par le détenteur de droits pour produire un nombre donné de documents, n'en a pas produit un excédent qu'il revendra à un tiers non autorisé.

En ce qui concerne la stabilité du marquage, les CNA nécessitent une grande stabilité du processus d'impression pour fonctionner correctement. En effet, leur principe de fonctionnement peut souvent être assimilé à la mesure du niveau d'énergie d'un signal dans l'image captée, appelé par la suite « score », ce score étant en règle générale supérieur pour les documents originaux que pour les copies (on peut également utiliser des mesures de distance telles que la distance sera en règle générale inférieure pour les documents originaux que pour les copies). Il est essentiel que ce score soit aussi « stable » que possible pour les impressions originales. En effet, plus la distribution statistique du score des impressions originales est étalée, moins ce score permet une différenciation efficace entre les originaux et les copies. Or, en pratique les moyens de marquage comportent de nombreux paramètres de réglage qui dépendent, par exemple, du produit à marquer, du substrat, de l'encrage, et qui peuvent fortement affecter le score du CNA. Pour une même fabrication, ces paramètres peuvent également évoluer dans le temps, être ajustés différemment par différents opérateurs, etc. Sans une maîtrise complète du moyen de production des documents, la capacité de détection des copies peut être fortement diminuée.

En ce qui concerne la souplesse d'intégration dans les procédés existants, lors de l'intégration d'un CNA dans un document, des échanges de données sécurisés (et traçables ou permettant des audits) doivent généralement être faits entre plusieurs parties. Typiquement, ces parties peuvent être le propriétaire des droits (par exemple, une compagnie pharmaceutique qui veut produire des médicaments protégés contre la copie), le ou les transformateurs (par exemple, l'imprimeur d'un emballage et/ou d'une étiquette), et le fournisseur des CNA, qui est souvent un tiers. Si les processus d'échange d'information ne sont pas automatisés, comment garantir que les CNA possédant les valeurs adéquates seront correctement imprimés sur les documents ou produits correspondants ? Ce problème est critique pour des applications à grandes échelles où le propriétaire des droits doit protéger des centaines voire des milliers de types de produits différents, et travaille avec des sous-traitants répartis dans différents pays ou continents. En effet, les erreurs d'intégration risquent d'être si nombreuses qu'elles peuvent rendre le système inutilisable, ou fortement

réduire sa crédibilité. A titre d'exemple d'erreur d'intégration, on peut imaginer un sous-traitant devant gérer l'insertion de plusieurs CNA dans plusieurs produits, qui insère un CNA dans un document qui ne lui correspond pas.

Certains aspects de la présente invention visent à remédier à ces inconvénients.

A cet effet, selon un troisième aspect, la présente invention vise un procédé de contrôle de qualité d'impression, caractérisé en ce qu'il comporte :

- une étape d'impression d'un support de code numérique authentifiant, en mettant en œuvre des valeurs de paramètres d'impression,

- une étape de capture d'une image du code numérique authentifiant imprimé sur ledit support,

- une étape de détermination d'une qualité d'impression du code numérique authentifiant en fonction de l'image du code numérique authentifiant et

- une étape d'impression d'au moins un autre support avec des paramètres d'impression fonctions de ladite qualité d'impression

Grâce à ces dispositions, on contrôle la qualité d'impression par traitement d'une image du code numérique authentifiant et on ne poursuit l'impression de support(s) avec les mêmes paramètres d'impression que si la qualité d'image est suffisante.

Selon des caractéristiques particulières, au cours de l'étape de détermination de qualité d'impression, on détermine la qualité d'impression en fonction d'un contenu d'information du code numérique authentifiant lu dans ladite image. Par exemple, le contenu d'information identifie un type de support (par exemple papier ou carton, couleurs, glaçage, ...).

Selon des caractéristiques particulières, au cours de l'étape de détermination de qualité d'impression, on détermine un taux d'erreur dans le code numérique authentifiant lu dans ladite image, la qualité d'impression étant fonction du dit taux d'erreur.

Grâce à ces dispositions, la mesure de qualité peut être normalisée. On note que, au cours d'une transformation ultérieure du support, le code numérique authentifiant peut être séparé de la partie utile, ce code numérique authentifiant servant alors uniquement à la détermination de qualité d'impression du support.

Selon des caractéristiques particulières, le procédé objet de la présente invention, tel que succinctement exposé ci-dessus comporte une étape de détermination si, à la fois, ladite image permet la lecture d'une valeur portée par le code numérique authentifiant imprimé et présente un taux d'erreur inférieur à une valeur limite prédéterminée,

- si ce n'est pas le cas, une étape de production d'un nouveau support et une itération de l'étape de lecture et de l'étape de détermination et

- si c'est le cas, une étape d'impression de codes numériques authentifiant en mettant en œuvre les paramètres d'impression dudit support.

Selon des caractéristiques particulières, le procédé objet de la présente invention tel que succinctement exposé ci-dessus comporte une étape de détermination de ladite valeur limite prédéterminée en fonction de la valeur représentée par le code numérique authentifiant.

Selon des caractéristiques particulières, le procédé objet de la présente invention tel que succinctement exposé ci-dessus comporte :

- une étape d'impression d'une pluralité de codes numériques authentifiants, en mettant en œuvre des valeurs de paramètres d'impression,

- une étape de capture d'images d'une pluralité de codes numériques authentifiants imprimés,

- une étape de détermination de qualité d'impression pour chacune d'une pluralité de dites images et

- une étape de mise en mémoire d'une valeur représentative de ladite qualité d'impression.

Grâce à ces dispositions, lorsque l'on détermine, ultérieurement, si un support est un original ou une copie, on peut tenir compte de la qualité d'impression initiale, ce qui augmente la fiabilité et la facilité de rendre opérationnel le procédé objet de la présente invention.

Selon des caractéristiques particulières, ladite étape de détermination de qualité d'impression comporte la détermination d'un taux d'erreur pour chacune d'une pluralité de dites images et au cours de l'étape de mise en mémoire, on mémorise une valeur limite de taux d'erreur, en fonction desdits taux d'erreurs déterminés.

Par exemple, on demande à l'opérateur un minimum de lecture, par exemple 30, prises de manière uniforme durant la production, de façon à déterminer les statistiques de taux d'erreurs, ou « score » de la production.

Selon des caractéristiques particulières, le procédé objet de la présente invention, tel que succinctement exposé ci-dessus comporte, réalisées par un serveur qui fournit des codes numériques authentifiants :

- une étape de transmission, de manière sécurisée, de codes numériques authentifiants à des systèmes d'impression pour intégration au design du document,

- une étape de réception de mesures de qualité de codes numériques authentifiants imprimés sur des documents,

- une étape de détermination si la production est valide à partir des mesures reçues et

- une étape de transmission d'un message indiquant si la production est valide.

Selon des caractéristiques particulières, au cours de l'étape de transmission de codes numériques authentifiants, le serveur transmet, d'abord, au moins un fichier de

contrôle permettant d'imprimer un code numérique authentifiant inutilisable, du fait de son contenu d'information, pour authentifier une production de supports et, si la production est valide, le serveur transmet au moins un autre code numérique authentifiant représentatif d'information liée à ladite production.

Selon des caractéristiques particulières, le procédé objet de la présente invention tel que succinctement exposé ci-dessus comporte :

- une étape d'impression d'un nombre prédéterminé de documents comportant un dit code numérique authentifiant,

- une étape de capture d'une image de chaque code numérique authentifiant imprimé et

- une étape de stockage d'une information représentative de chaque code numérique authentifiant imprimé.

Selon des caractéristiques particulières, le procédé objet de la présente invention, tel que succinctement exposé ci-dessus comporte une étape de détermination d'une signature de chaque image capturée d'un code numérique authentifiant, et une étape de stockage de ladite signature dans une base de données, avec les informations associées à la fabrication.

On peut ainsi retrouver, ultérieurement, par l'utilisation de la signature, pour chaque document imprimé, si sa fabrication a été autorisée ainsi que les informations associées permettant sa traçabilité.

Selon des caractéristiques particulières, le procédé objet de la présente invention, tel que succinctement exposé ci-dessus comporte une étape d'impression d'une matrice d'information représentant ladite signature, sur le document portant le CNA correspondant à ladite signature.

Selon des caractéristiques particulières, le procédé objet de la présente invention, tel que succinctement exposé ci-dessus comporte :

- une étape de capture d'images d'une partie des codes numériques authentifiants imprimés et de détermination, en mettant en œuvre des valeurs de paramètres d'analyse, d'une note représentative de la qualité d'impression dudit code numérique authentifiant et

- une étape de présentation, à l'opérateur, de ladite note représentative de qualité d'impression.

Selon des caractéristiques particulières, lesdites valeurs de paramètres d'analyse sont représentatives d'un taux d'erreur d'impression des codes numériques authentifiants et en ce que, au cours de l'étape de détermination d'une note, ladite note est représentative d'une différence entre le taux d'erreur représenté par les valeurs de paramètres d'analyse et le taux d'erreur déterminé à partir de ladite image.

Selon des caractéristiques particulières, le procédé objet de la présente invention, tel que succinctement exposé ci-dessus comporte une étape de détermination d'un taux

d'erreur moyen à partir d'au moins une image de code numérique authentifiant et, à partir d'un instant prédéterminé, au cours de l'étape de détermination d'une note, ladite note est représentative d'une différence entre ledit taux d'erreur moyen et le taux d'erreur déterminé à partir d'au moins une image d'un nouveau code numérique authentifiant.

Selon des caractéristiques particulières, le procédé objet de la présente invention, tel que succinctement exposé ci-dessus comporte une étape de transmission d'alarme lorsque ladite différence est supérieure à une valeur limite prédéterminée.

Selon des caractéristiques particulières, le procédé objet de la présente invention, tel que succinctement exposé ci-dessus comporte une étape d'association d'un microtexte au code numérique authentifiant, ledit microtexte étant imprimé avec le code numérique authentifiant qui lui est associé.

Selon un quatrième aspect, la présente invention vise un dispositif de contrôle de qualité d'impression, caractérisé en ce qu'il comporte :

- un moyen d'impression d'un support de code numérique authentifiant, en mettant en œuvre des valeurs de paramètres d'impression,
- un moyen de capture d'une image du code numérique authentifiant imprimé sur ledit support,
- un moyen de détermination d'une qualité d'impression du code numérique authentifiant en fonction de l'image du code numérique authentifiant et
- un moyen d'impression d'au moins un autre support avec des paramètres d'impression fonction de ladite qualité d'impression.

La présente invention concerne aussi un procédé et un dispositif de sécurisation de documents. Elle s'applique, en particulier à l'impression de marques permettant de différencier un original d'une copie.

On connaît deux grandes familles de telles marques : les images traitées par stéganographie, c'est-à-dire comportant, sur un décor, de manière indiscernable à l'œil, une empreinte (en anglais « watermark ») et les marques visibles formées d'une matrice de points présentant, chacun, l'une de deux couleurs, généralement noire et blanche.

Dans chacun de ces cas, une marque de détection de copie est fabriquée de telle manière que toute copie, que ce soit par photocopie ou par prise de vue puis impression de l'image captée, entraîne une dégradation de ses détails et permette, avec un système de lecture et de traitement adapté, de détecter cette dégradation. Pour déterminer si un document est un original ou une copie, le système de lecture effectue une mesure de la dégradation et la compare, généralement, à une valeur limite, ou seuil, prédéterminée.

Cependant, l'impression des originaux provoque une détérioration initiale de la marque imprimée et peut rendre impossible l'exploitation de la fonction anti-copie de cette marque.

Certains aspects de la présente invention visent à remédier à ces inconvénients.

A cet effet, selon un cinquième aspect, la présente invention vise un procédé de sécurisation d'un document dit « original », qui comporte :

- une étape de détermination de caractéristiques d'un matériel d'impression dudit document original,
- une étape de détermination d'une marque permettant de différencier un original d'une copie, en fonction des caractéristiques du matériel d'impression destiné à être mis en œuvre pour l'impression de ladite marque sur ledit document,
- une étape d'impression de ladite marque avec ledit matériel d'impression pour former ledit document original, et
- une étape de détermination d'une première valeur limite à utiliser par un matériel de détection de copie pour discriminer ledit document original d'une copie dudit document original, en fonction d'au moins une impression de ladite marque.

Grâce à ces dispositions, la marque est optimisée en fonction des caractéristiques du matériel d'impression et la valeur limite utilisée par le matériel de détection tient compte de la qualité d'impression effective de ce matériel d'impression.

Selon des caractéristiques particulières, le procédé tel que succinctement exposé ci-dessus comporte une étape d'impression d'au moins une référence d'impression représentative d'un maximum ou d'un minimum d'encrage autorisé pour l'impression dudit document et, au cours de l'étape de détermination de la première valeur limite, on détermine une mesure sur au moins une dite référence d'impression et on y ajoute une tolérance.

Grâce à ces dispositions, dans la plage d'encrage autorisée, pour un contexte d'impression, on est sûr que chaque document original sera considéré comme tel par le matériel de détection.

Selon des caractéristiques particulières, le procédé tel que succinctement exposé ci-dessus comporte une étape de mesure de détérioration de la marque sur la chaîne d'impression, une étape de comparaison de cette mesure avec une deuxième valeur limite prédéterminée et, en cas de dépassement de la deuxième valeur limite de détérioration, une étape d'alerte.

On observe que la deuxième valeur limite peut être identique à la première valeur limite. Grâce à ces dispositions, l'imprimeur peut être automatiquement informé quand la qualité d'impression se dégrade et rectifier les réglages de la machine d'impression.

Les caractéristiques essentielles et/ou particulières des différents aspects de la présente invention, tels que succinctement exposés ci-dessus, sont destinés à être combinés pour former un procédé et un dispositif de sécurisation présentant tout ou partie des avantages de ces différents aspects.

Selon un sixième aspect, la présente invention vise un programme d'ordinateur chargeable dans un système informatique, ledit programme contenant des instructions permettant la mise en œuvre du procédé objet de la présente invention tel que succinctement exposé ci-dessus.

Selon un septième aspect, la présente invention vise un support d'informations lisibles par un ordinateur ou un microprocesseur, amovible ou non, conservant des instructions d'un programme informatique, caractérisé en ce qu'il permet la mise en œuvre du procédé objet de la présente invention tel que succinctement exposé ci-dessus.

Les avantages, buts et caractéristiques de ce dispositif, de ce programme d'ordinateur et de ce support d'information étant similaires à ceux du procédé objet de la présente invention, tel que succinctement exposé ci-dessus, 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 :

- la figure 1 représente, schématiquement, un mode de réalisation particulier du dispositif de production de codes numériques authentifiants objet de la présente invention,
- les figures 2A et 2B représentent, sous forme d'un logigramme, des étapes mises en œuvre dans un mode de réalisation particulier du procédé de production de codes numériques authentifiants objet de la présente invention,
- les figures 3A à 3H représentent, sous forme d'un logigramme, des étapes mises en œuvre dans un mode de réalisation particulier du procédé de lecture de codes numériques authentifiants objet de la présente invention,
- les figures 4 et 5 représentent des distributions de scores de codes numériques authentifiants,
- la figure 6 représente des distributions statistiques de scores pour des originaux et des copies calculée sur la base d'images prises avec un outil de capture d'image de référence et avec un outil de capture d'image de qualité inférieure,
- les figures 7A et 7B représentent, sous forme de logigrammes, des étapes mises en œuvre dans un mode de réalisation particulier du procédé objet de la présente invention,
- la figure 8 représente, schématiquement, un mode de réalisation particulier d'un dispositif capable de mettre en œuvre le procédé objet de la présente invention,
- les figures 9A et 9B représentent, sous forme d'un logigramme, des étapes mises en œuvre dans un mode de réalisation particulier du procédé objet de la présente invention.

Dans toute la description, on applique la présente invention à des codes numériques authentifiants prenant la forme de zones carrées comportant des cellules carrées imprimées en noir sur fond blanc, les zones blanches présentant, dans l'image numérique initiale, la même surface, en nombre de points, ou pixels, que les zones noires. Cependant, la présente

invention ne se limite pas à ce type d'application mais s'étend, bien au contraire, à tout type d'image numérique CNA permettant de discerner (automatiquement) les impressions originales des copies sur la base de la mesure d'un score de l'image numérique imprimée puis numérisée, ledit score variant en fonction de la quantité de dégradation subie par l'image. En effet, tous les CNA ont les mêmes problématiques de fiabilité et de sécurité au niveau de la maîtrise du score et du contrôle de l'image source et :

- aux MIS, CDP, MSMA et filigranes numériques, certaines adaptations pouvant être nécessaires afin d'utiliser l'un ou l'autres des CNA ;

- aux formes quelconques, polygonales ou non, tant pour les cellules individuelles que pour l'ensemble des cellules

- aux couleurs quelconques,

- aux nombres de couleurs quelconques,

- aux densités de cellules quelconques sur une surface donnée et

- à l'intégration, ou non, du CNA dans une image existante.

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'une image 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 » ;

- « cellule » : il s'agit d'un élément du code numérique authentifiant qui représente une unité d'information ;

- « document » : il s'agit de n'importe quel objet (physique) portant une information ;

- « marquage » ou « impression » : tout processus par laquelle on passe d'une image digitale (incluant un code numérique authentifiant, un document..) 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 le code numérique authentifiant est d'abord gravé dans le moule, puis moulée sur chaque objet, sont également inclus (notons qu'un code numérique authentifiant « moulé » 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 transformation, par exemple l'impression offset

classique (contrairement au offset « computer-to-plate »), inclut la création d'un film, ledit film sevrant a 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, et

- « capture » : tout processus par lequel on obtient une représentation digitale du monde réel, incluant la représentation digitale d'un document physique contenant un code numérique authentifiant.

En guise d'introduction à la description de modes de réalisation particuliers du procédé et du dispositif objets de la présente invention, on rappelle que la dégradation d'un code numérique authentifiant a pour conséquence que les contenus de certaines cellules peuvent ne pas être correctement décodés.

Chaque étape de la création du code numérique authentifiant est effectuée dans le but que le message d'origine soit lisible sans erreur, même si, et c'est un effet désiré, l'impression initiale du code numérique authentifiant est entachée d'erreurs. En particulier, un des buts de cette création du code numérique authentifiant est d'utiliser le nombre ou le taux d'erreurs du message modulé, pour déterminer un score, puis l'authenticité d'une impression de ce code numérique authentifiant. En effet, une copie de l'impression initiale du CNA comportera généralement plus d'erreurs que cette impression initiale du CNA.

On rappelle ici que l'image du code numérique authentifiant est créée à partir d'un (ou éventuellement plusieurs) message et d'une (ou éventuellement plusieurs) clé : typiquement, le message source est transformé en représentation binaire, puis chiffré par la clé ; le message chiffré est encodé de façon à être robuste à un nombre d'erreurs élevé, puis le message encodé est brouillé par la clé avant d'être modulé sous forme d'image, chaque valeur binaire étant représentée par un pixel de l'image formant le code numérique authentifiant. L'image formant le code numérique authentifiant est imprimée à une résolution assurant, dès cette impression initiale, un taux d'erreurs important (soit un faible score) sans être trop élevé, de sorte que le décodage du message encodé contenant les erreurs soit garanti, ainsi que la détection d'une éventuelle copie du code numérique authentifiant, qui comporte nécessairement davantage d'erreurs.

En effet, le taux d'erreurs, ou le score, peuvent être ajustés en fonction des caractéristiques de l'impression, de telle sorte que la production d'une copie entraîne des erreurs supplémentaires, résultant en un taux d'erreurs en moyenne plus élevé, ou un score plus faible, lors de la lecture d'une copie, que lors de la lecture d'un original.

En pratique, un taux d'erreur de l'ordre de 20% lors de l'impression originale est adéquat, bien que des taux allant de 5% à plus de 30% puissent fonctionner. Notons que, pour un taux d'erreur trop faible, une copie parfaite et donc non-discernable des originaux

serait réalisable, alors que pour un taux d'erreur trop élevé, le code numérique authentifiant ne pourrait être décodée correctement et, il n'y aurait plus suffisamment d'information qui puisse être dégradée durant la copie.

Le message codé extrait d'un code numérique authentifiant copié capté a donc plus d'erreurs que le message codé extrait d'un code numérique authentifiant original capté. Le nombre ou le taux d'erreurs détectés sont, dans des modes de réalisation, utilisés pour différencier une copie d'un original, par l'intermédiaire du score qui est une fonction décroissante de ce taux d'erreurs. En pratique, un enjeu important consiste à déterminer un seuil de décision adéquat permettant de discriminer au mieux les originaux des copies.

Avant de décrire un mode de réalisation particulier du procédé de sécurisation, on donne, ci-dessous, une présentation générale du processus mis en œuvre. Tout d'abord, le détenteur de droits commande auprès d'un transformateur ou imprimeur mandaté, un nombre déterminé de documents ou produits sécurisés par un ou des CNA. Ce dernier télécharge un ou plusieurs CNA, respectivement pour une impression du même CNA sur tous les documents ou pour une impression de différents CNA sur les différents documents. Puis, le transformateur imprime le nombre prévu de documents, avec le ou les CNA prévus sur chaque document en mettant en œuvre au moins un aspect de la présente invention. Le nombre prévu de documents imprimés est envoyé au détenteur de droits. En variante, les documents sont envoyés à l'assembleur mandaté par le détenteur de droits. Le détenteur de droits ou l'assembleur assemble le produit fini (qui peut contenir plusieurs « documents » sécurisés par des CNA) et met en œuvre au moins un aspect de la présente invention.

Au cours de ce processus, dans un mode de réalisation particulier du procédé objet de la présente invention illustré en figures 7A et 7B qui ne concernent que la mise en œuvre de la fonction authentifiante des CNA, le détenteur de droits autorise le fournisseur de CNA à fournir au moins un CNA à l'imprimeur. Au cours d'une étape 805, le fournisseur de CNA fournit un CNA de test et une valeur de seuil prédéterminée qui peut dépendre des conditions d'impression (type de support, type d'impression, couleurs imprimées, conditions de capture d'image). On observe que la densité (c'est-à-dire le ratio des surfaces sombres sur les surfaces claires) de ce CNA de test et de chaque CNA définitif (voir plus loin) peut dépendre du document et des conditions d'impression.

Au cours d'une étape 810, l'imprimeur imprime une présérie de documents comportant le CNA de test. Au cours d'une étape 815, on détermine si la qualité d'impression des CNA de test est suffisante, par analyse d'images de CNA et comparaison de son score à la valeur de seuil. Si la qualité d'impression est insuffisante, on retourne à l'étape 810. Si la qualité d'impression est suffisante, au cours d'une étape 820, le fournisseur de CNA détermine des valeurs de seuil à mettre en œuvre au cours de la production, c'est-à-dire l'impression des documents à livrer, et au moins un CNA, qui représente,

éventuellement, au moins une valeur de paramètre de compensation à appliquer lors de la détermination si une image d'un CNA représente un CNA original, c'est-à-dire imprimé au cours de la production, ou une copie d'un CNA original. En variante, c'est une matrice d'information fournie par le fournisseur de CNA qui représente chaque valeur de paramètre de compensation. Lors de l'étape 820, le fournisseur de CNA détermine aussi des valeurs de seuil à appliquer au cours de la production.

Puis, au cours d'une étape 825, le fournisseur de CNA fournit à l'imprimeur au moins un CNA définitif et des valeurs de seuil à appliquer au cours de la production et, éventuellement, des valeurs de paramètres de compensation.

Au cours de la production, lors d'une étape 830, on réalise une capture d'image d'un CNA imprimé. Au cours d'une étape 835, on détermine si les conditions de capture d'image sont suffisantes. Sinon, on retourne à l'étape 830. Si oui, au cours d'une étape 840, on détermine le score de l'image, on fournit à l'opérateur une note représentative de ce score et on détermine si l'image du CNA correspond à une valeur de score, éventuellement compensé, qui se trouve entre les valeurs de seuil fournies au cours de l'étape 825. Si oui, on stocke ce score au cours d'une étape 845, la production se poursuit et on retourne à l'étape 830. Sinon, on déclenche une alarme au cours d'une étape 850 et on fait rejeter les documents en cours d'impression. Puis on retourne à l'étape 830, l'acceptation des documents ne reprenant que lorsque l'alarme est levée.

Lorsque la production est achevée, au cours d'une étape 855, on détermine au moins une valeur de paramètre de compensation (par exemple, additif ou multiplicatif) à appliquer au score des images de CNA de cette production en fonction de la qualité de capture d'image, en fonction des scores conservés en mémoire et on stocke, dans le serveur du fournisseur de CNA, chaque valeur de paramètre de compensation. Chaque valeur de paramètre représente les conditions et/ou la qualité d'impression des CNA.

Lors de l'exploitation des CNA, au cours d'une étape 860, on capture une image d'un CNA. Puis, au cours d'une étape 865, on détermine des conditions de capture d'image. Au cours d'une étape 870, on détermine si les conditions de capture d'image sont suffisantes, notamment en termes de flou, résolution et éclairage, pour permettre une interprétation du CNA. Sinon, on retourne à l'étape 860 et/ou on fournit l'image au serveur du fournisseur de CNA. Si les conditions de capture d'image sont suffisantes, au cours d'une étape 875, on détermine au moins une valeur de paramètre de compensation (par exemple, additif ou multiplicatif) à appliquer au score du CNA représenté par l'image, en fonction des conditions de capture d'image, notamment, le flou, la résolution et l'uniformité d'éclairage. Au cours d'une étape 875, on détermine au moins une valeur de paramètre de compensation lié à l'impression et une valeur de seuil à appliquer, soit en lisant une partie du contenu du CNA,

soit en lisant un contenu d'une matrice d'information, soit en demandant cette valeur au serveur du fournisseur de CNA.

Puis, au cours d'une 885, on détermine, en fonction des différentes valeurs de compensation et de la valeur de seuil, si l'image représente un CNA original ou une copie. Au cours d'une étape 890, on transmet le résultat de l'étape 885 au fournisseur de CNA et, éventuellement, au détenteur de droits et, éventuellement à l'opérateur ayant effectué la capture.

La mise en œuvre des différentes étapes illustrées en figure 7 est détaillée dans d'autres modes de réalisation particulier du procédé objet de la présente invention illustrés dans les figures 1 à 3H.

On observe, en figure 1, un mode de réalisation du dispositif d'identification 100 objet de la présente invention adapté à une machine, ou chaîne, d'impression de documents afin de traiter ces documents dès leur impression initiale.

Le dispositif d'identification de documents 100 comporte :

- un dépileur 105, connu en soi, qui dépile des objets, généralement des feuilles de carton ou de papier, ou « documents », 110,
- une chaîne d'impression 106, de type connu, pour imprimer au moins un CNA sur chaque document 110,
- un empileur 107, de type connu, qui forme une pile des documents 110 imprimés par le dispositif 100,
- un moyen 125 de lecture d'au moins un CNA 115 formé sur un document 110,

Le moyen 125 de lecture du CNA 115 comporte une caméra 126 et au moins une source de lumière 127.

Le moyen de lecture 125 comporte aussi un moyen de traitement 129 de l'image captée par la caméra 126, qui détermine des caractéristiques de l'image du CNA 115.

Dans un mode de réalisation particulier du dispositif illustré en figure 1, le moyen 125 de lecture du CNA commande un moyen de retrait (non représenté) de chaque document 100 portant un CNA de mauvaise qualité. Ainsi, la qualité de chaque CNA est vérifiée et tous les documents mis en circulation bénéficient de la protection conférée par la mise en œuvre de la présente invention. Le moyen de retrait de chaque document 100 portant un CNA de mauvaise qualité est, par exemple, constitué d'une « écluse », c'est-à-dire d'un volet commandé pour, dans l'une de ses positions, faire tomber les documents dans une poubelle et, dans une autre position, laisser passer les document vers l'empileur 107.

Le résultat de la vérification effectuée par le moyen 125 est transmis, pour stockage et exploitation ultérieure à un serveur 155.

Ce serveur 155 fournit des codes numériques authentifiants et possède les fonctionnalités suivantes :

- un moyen 160 de spécifier, les détenteurs de droits, les transformateurs autorisés, les imprimantes calibrées ou homologuées, les produits ou documents existant avec tous paramètres d'impression ou de génération de CNA relatifs à ces produits, ainsi que les imprimantes ou transformateurs ; de plus le moyen d'associer des produits à des clients, des imprimantes à des transformateurs ;

- un moyen 165 pour les détenteurs de droits de déclarer des ordres de fabrication relatifs à certains produits, indiquant notamment les quantités à produire de CNA et/ou produits ;

- un moyen 170 pour l'imprimeur de télécharger de manière sécurisée des CNA qui seront intégrés au design du produit, automatiquement (notamment dans le cas de l'impression variable) ou manuellement. Alternativement, une connexion sécurisée permettant à une machine contrôlant l'impression de télécharger les CNA à la demande. Alternativement, pour les CNA qui nécessitent l'image d'origine pour être générés (notamment les filigranes numériques), le moyen d'envoyer une image vers ledit serveur et recevoir en retour l'image marquée. De plus, un moyen de télécharger le ou les fichiers de contrôle utilisé par le logiciel de lecture de qualité de CNA sur la ligne de production ;

- un moyen 175 de recevoir des mesures de qualité du CNA, de conserver ces mesures de qualité, et de déterminer si la production est valide à partir de ces mesures de qualité. Voir plus bas pour les mesures de qualités, basées sur des images saisies sur la chaîne de fabrication. Si la production est jugée valide, un message est envoyé au transformateur lui permettant de clôturer la production et livrer les produits au détenteur de droits et

- un moyen 180 pour le responsable des CNA de déterminer les produits, machines, clients, imprimeurs et de modifier les valeurs de seuil mises en œuvre pour la détermination de qualité du CNA par le moyen 125 et

- une base de données 185 de seuils, ou valeurs limites, ou de statistiques de dégradation de CNA autorisées pour discerner un original, en correspondance avec des identifiants de documents imprimés. Comme on le verra par la suite, la base de données 185 est optionnelle, un CNA pouvant, dans des modes de réalisation, incorporer au moins une valeur limite de dégradation pour discriminer un document original d'une copie.

Un moyen mobile de lecture de CNA 190 est aussi représenté en figure 1. Le moyen de lecture fixe 125 et le moyen de lecture mobile 190 comportent, chacun, un moyen de communication à distance avec le serveur 155, par exemple, par l'intermédiaire d'un réseau de téléphonie, fixe ou mobile, ou du réseau Internet.

Préférentiellement, l'intégration des CNA pour la sécurisation de documents implique trois parties : le détenteur de droits souhaitant produire des documents sécurisés, le fournisseur du service de sécurisation des documents par CNA, et le transformateur ou

l'imprimeur produisant les documents sécurisés par CNA. Parfois, une partie peut avoir deux rôles à jouer, par exemple le détenteur de droits est également fournisseur du service de sécurisation, ou ce dernier est également responsable de l'impression des documents. Cependant, même dans ces cas particuliers, la séparation en trois parties est pertinente du point de vue fonctionnel car ce sont, en général, des services différents qui commandent, fournissent ou impriment les CNA.

Il est préférable de sécuriser au maximum les étapes menant à l'impression des CNA. D'une part, l'accès aux images de CNA à imprimer doit être limité aux personnes de confiance. D'autre part, le système doit garder un audit complet en cas de litige. Dans un contexte industriel, on peut avoir des millions de CNA à imprimer chaque jour, impliquant plusieurs détenteurs de droits qui traitent avec des dizaines de sous-traitants pour produire des centaines de type de produits différents. Préférentiellement, on minimise la complexité des opérations humaines qui sont sources d'erreur, on automatise les procédés et on garde des traces des opérations effectuées.

Conformément à au moins un aspect de la présente invention, au cours du processus d'impression, au moins une image de CNA imprimé est capturée. Préférentiellement, ce processus est fait automatiquement, les produits défilant sous l'objectif du moyen de lecture fixe 125. Ce moyen de lecture fixe 125 est déclenché automatiquement ou par une activation externe venant d'un capteur. En variante, le lecteur mobile 190 est mis en œuvre par un opérateur pour capter des images des CNA au cours de la production.

Chaque image capturée d'un CNA est stockée sur une base de donnée, avec les informations associées (ordre de fabrication, date, etc.).

Lorsque le CNA doit assurer une fonction d'identification de chaque produit ou document, en temps réel ou différé, une ou plusieurs signatures, ou empreintes, sont calculées pour chaque image valide de CNA capturée. Une signature permet d'identifier de manière unique une impression d'un CNA parmi les impressions des CNAs provenant d'une même image source (du même CNA).

Le site où sont capturées les images des CNA peut se trouver chez l'imprimeur, l'avantage étant qu'il peut être intégré à la production et le désavantage étant qu'il est en zone exposée. La machine servant au calcul et ou/stockage des signatures peut être sécurisée, par exemple déportée sur le serveur et traitant des images fournies par l'un des moyens de lecture 125 ou 190. Alternativement, le site peut se trouver chez le tiers parti mandaté par le détenteur de droits, généralement le même qui fournit le ou les CNA utilisés.

En ce qui concerne la fonction de détection de copie des CNA, la fiabilité de détection des copies dépend de la stabilité du score : d'un point de vue statistique, on cherche en premier lieu à avoir le score avec la plus petite variance. Ceci signifie que, du début à la fin

de la production de produits contenant un CNA donné, les conditions d'impression affectant le score des CNA ne doivent pas changer de manière significative.

Or, ce score est sensible à un grand nombre de paramètres, par exemple le type de papier, le type d'encre, et des paramètres généralement ajustables sur les machines d'impression tel que la densité d'encre. Les machines d'impression sont souvent très sensibles, et l'expérience montre que pour un même produit imprimé sur une même machine, les paramètres d'impression peuvent évoluer pour des séquences d'impression réalisées à des moments différents, avec un impact significatif sur le score des CNA. De plus, les paramètres d'impression peuvent changer au cours d'une même production, et on observe alors un décalage progressif du score. Il arrive même que le changement d'opérateur en cours de production ait un impact sur la qualité d'impression et donc le score des CNA. On cherche donc à minimiser ces effets notamment en prévoyant des compensations de scores.

Selon au moins un aspect de la présente invention, on contrôle les conditions de marquage durant la production, pour assurer la fonctionnalité essentielle de détection de copie des CNA. Egalement, il n'est pas rare que l'imprimeur ou le responsable de l'intégration des CNA dans les fichiers fasse une erreur d'association, de sorte qu'une mauvaise valeur de CNA se trouve assignée à un document à imprimer.

Ce type de problème doit évidemment être détecté le plus tôt possible. Si le moyen de lecture 125 est absent, on munit un opérateur d'un lecteur de CNA mobile 190, afin qu'il fasse des contrôles réguliers de la production sur la chaîne d'impression. Le lecteur peut être très proche d'un lecteur habituel de CNA. Cependant, il est préférable qu'il possède les caractéristiques suivantes : il est préférentiellement maniable, par exemple en prenant la forme d'un lecteur autonome, ou par connexion filaire avec un fil de longueur suffisante. Sa fonction principale est de contrôler la qualité de la production, donc une réponse binaire est, en général, peu appropriée ; les lecteurs étant situés sur des zones éloignées, c'est-à-dire des imprimeurs ou transformateurs sous-traitants, il vaut mieux stocker localement un minimum d'informations sensibles (algorithmes de lecture, paramètres de lecture) dans les moyens de lecture 125 et 190.

Dans une implémentation préférentielle, l'opérateur reçoit un fichier de jeux de paramètres de lecture des CNA (ces paramètres pouvant être transmis automatiquement via le réseau interne de l'imprimeur) et est muni d'un lecteur mobile 190, à communication filaire ou non.

Préférentiellement, le jeu de paramètres ne comporte pas les clés de lecture, car il y aurait un risque de sécurité à diffuser un tel jeu de paramètres. On stocke donc un sous-ensemble des valeurs du CNA, échantillonné au hasard et de taille suffisante pour permettre de mesurer un score représentatif pour le contrôle qualité, mais de taille insuffisante pour

recréer un CNA qui soit proche des impressions originales de CNA. Si un CNA comporte, par exemple, 12.000 valeurs, on stocke, par exemple, 2.000 de ces valeurs dans le fichier, choisies à des positions aléatoires mais connues du lecteur.

L'opérateur effectue une lecture de la plaque d'impression qui le porte (par exemple celle qui correspond à l'encre noire), pour s'assurer que le CNA possède la bonne valeur et est de bonne qualité. Si ce n'est pas le cas, il devra produire une nouvelle plaque, éventuellement avec de nouveaux CNA. Autrement, il peut lancer l'impression de produits en phase préliminaire d'ajustement des paramètres d'impression. Durant cette phase préliminaire, l'opérateur effectue plusieurs contrôles des CNA.

Comme on l'observe en figures 2A et 2B, le procédé de sécurisation de documents comporte d'abord, réalisées par un serveur qui fournit des codes numériques authentifiants :

- une étape 205 de spécification de détenteurs de droits, de transformateurs/imprimeurs autorisés,
- une étape 210 de spécification de systèmes d'impression et/ou de transformation calibrées ou homologuées,
- une étape 215 de spécification des produits/documents à imprimer avec des paramètres d'impression ou de génération de CNA relatifs à ces produits,
- une étape 220 d'association de produits à des détenteurs de droits et à des systèmes d'impression et/ou de transformation,
- une étape 225 de déclaration d'ordres de fabrication relatifs à des produits, indiquant notamment les quantités à produire de CNA et/ou de produits et
- une étape 230 de transmission, de manière sécurisée, de codes numériques authentifiants à des systèmes d'impression ou de transformation pour intégration au design du produit.

Dans des variantes, notamment dans le cas d'utilisation de CNA qui nécessitent l'image d'origine pour être générés, par exemple les filigranes numériques, l'image d'origine est envoyée au serveur avant l'étape 230 et au cours de cette étape, le serveur réalise le CNA et le transmet au site d'impression ou de transformation. On note que les codes numériques authentifiants transmis au cours de l'étape 230 sont des codes numériques authentifiants de test pour intégration au design du produit.

Puis, on effectue, sur la chaîne d'impression ou de transformation, une étape 235 d'impression d'un premier nombre prédéterminé de documents comportant un dit code numérique authentifiant.

Au cours d'une étape 240, on effectue une capture d'une image d'au moins un et, préférentiellement de chaque, code numérique authentifiant imprimé et le stockage d'une information représentative de chaque code numérique authentifiant imprimé. Cette capture

d'image peut être effectuée manuellement ou automatiquement, par un capteur d'images placé sur la chaîne considérée.

Au cours d'une étape 245, on transmet, depuis le site d'impression ou de transformation, des images capturées de codes numériques authentifiants imprimés au serveur ainsi que des valeurs de paramètres d'impression mis en œuvre pour imprimer le premier nombre prédéterminé de produits.

Au cours d'une étape 250, le serveur détermine un taux d'erreurs dans les codes numériques authentifiants représentés par les images, puis un score et une qualité d'impression du premier nombre prédéterminé de produits, avec une éventuelle compensation en fonction des conditions d'impression et des conditions de capture d'image. Puis, au cours d'une étape 255, le serveur détermine si la production est valide à partir des mesures reçues, en fonction d'une valeur limite prédéterminée, comme exposé en regard des figures 3A à 3D.

Si la production n'est pas valide, au cours d'une étape 260, le serveur le notifie à l'utilisateur ou à la chaîne d'impression, avec des indications sur les modifications à effectuer sur les paramètres d'impression (par exemple pour réduire l'encrage ou pour l'augmenter). Puis on retourne à l'étape 235.

Si la production est valide, au cours d'une étape 265, le serveur transmet au site d'impression ou de transformation un message indiquant que la production est valide ainsi qu'un code numérique authentifiant à mettre en œuvre pour la production à venir. Dans des modes de réalisation, une valeur limite de taux d'erreur ou de score, ou valeur de seuil, pour la validation de l'authenticité des CNA est déterminée par le serveur à partir des taux déterminés au cours de l'étape 250. Cette valeur est représentée, de manière sécurisée, par le CNA transmis au cours de l'étape 265. Par exemple, cette valeur limite correspond à la validation de l'authenticité de 98 % des CNA imprimés au cours de la dernière étape 235. Cette valeur, ainsi qu'une marge d'erreur, sont transmises au lecteur sur chaîne et/ou au lecteur manuel. Préférentiellement, ce CNA est aussi représentatif des paramètres d'impression mis en œuvre au cours de la dernière étape 235.

En variante, le taux d'erreurs, le score et la qualité d'impression sont déterminés localement par le lecteur effectuant les captures d'images et ils sont transmis au serveur 155.

Au cours d'une étape 270, on imprime ou transforme un deuxième nombre prédéterminé, spécifié dans l'ordre de fabrication, de produits en mettant en œuvre les paramètres d'impression de la dernière étape 235.

Puis, au cours d'une étape 275, pour chaque produit ou pour une partie des produits, on effectue, automatiquement ou manuellement, sur la chaîne d'impression, une capture d'image du CNA imprimé.

Au cours d'une étape 280, on détermine, pour chaque image capturée au cours de l'étape 275, un taux d'erreurs dans les codes numériques authentifiants représentés par les images, puis un score et une qualité d'impression du premier nombre prédéterminé de produits, avec une éventuelle compensation en fonction des conditions d'impression et des conditions de capture d'image, en fonction d'une valeur limite prédéterminée, comme exposé en regard des figures 3A à 3D. Puis, le lecteur local détermine si la production instantanée est valide en fonction de la marge d'erreur, attribue une note à la dernière image capturée et fournit, par affichage, cette note à l'opérateur de la chaîne d'impression.

Si la production n'est pas valide, c'est-à-dire si le taux d'erreur est supérieur à la valeur limite d'authenticité additionnée à la marge d'erreur, on déclenche une alarme pour que l'opérateur rétablisse les paramètres d'impression. Eventuellement, les produits pour lesquels la production n'est pas valide sont éliminés et décomptés du nombre de produits imprimés.

Au cours d'une étape 285, en temps réel ou différé, une ou plusieurs signatures sont calculées pour chaque image valide de CNA capturée. Une signature, généralement celle occupant le plus petit volume de donnée est quantifiée et/ou compressée de façon à obtenir une représentation compacte de celle-ci. L'ensemble des signatures calculées est envoyé, par lien sécurisé, au serveur sur lequel les inspecteurs se connectent afin de vérifier la validité des signatures.

En variante permettant de vérifier le CNA, une matrice d'information, préférablement sécurisée à l'aide d'une clé de chiffrement, est générée pour contenir la représentation de la signature et imprimée sur le document contenant le CNA, au cours de l'étape 285.

En variante, une valeur limite, ou valeur de seuil, de validité du CNA est déterminée au cours de la production, à partir des mesures réalisées au cours de l'étape 280, et représentée, de manière sécurisée par une matrice d'information imprimée au cours d'une étape 295.

Comme on le comprend, au cours de l'étape 265, le jeu de paramètres reçu par l'opérateur contient un score moyen visé pour le CNA, ainsi que des marges d'erreur. Par exemple, sur une échelle de 0 à 20, le score visé peut être de 15, et la marge d'erreur de +/- 2. Ainsi, tout score entre 13 et 17 est accepté, mais le score souhaité doit être aussi proche que possible de 15. Ce score n'est en général pas présenté à l'opérateur, mais une transformation de ce score, appelé la note, lui est présentée, au cours de l'étape 280, lors de la production. Cette note est plus facilement interprétable pour lui, et est comparable entre différentes fabrications qui auraient des scores visés différents. Une transformation possible consiste à transformer le score sur une échelle de -5 à +5, de la manière suivante :

- si Score < score visé-marge d'erreur : note=+5
- si Score > score visé+marge d'erreur: note=-5

- autrement : note= 5*(score visé-score)/2*marge d'erreur

Pour notre exemple:

- Score<13 : note=+5,
- Score>17 : note=-5
- autrement : note= 5*(15-score)/4.

L'objectif de l'opérateur est d'avoir autant que possible une note proche de 0, ce qui correspond à un score égal au score visé, ici de 15. Il lui faut à tout prix éviter une note -5 ou +5, qui correspond à un score inacceptable.

Ainsi, un score de 14.2 donne une note de +1, un score de 16 une note de -1.25. Pour simplifier, la note peut être quantifiée à l'entier le plus proche.

On demande à l'opérateur un minimum de lecture, par exemple 30, prises de manière uniforme durant la production, de façon à déterminer les statistiques de score de la production.

Lorsque l'imprimeur ou le transformateur souhaite clôturer la production, les mesures de qualité effectuées au cours de la production sont envoyées au serveur, et une décision sur la validité de la production est envoyée en retour.

Détermination de la validité de la production :

Plusieurs critères peuvent entrer en ligne de compte : le nombre de valeur égales à +5 ou -5, la moyenne des notes, la moyenne des notes en valeur absolue. Dans une implémentation préférentielle, la production est jugée valide si :

- le nombre de notes égal à +5 ou -5 est inférieur à 3 et
- la moyenne des notes en valeur absolue est inférieure à 4.

En variante, un score plus élevé que le score visé est en réalité plus acceptable qu'un score inférieur au score visé. Il y a donc une dissymétrie, qui peut donc être intégrée en attribuant une marge d'erreur supérieure dans le premier cas.

En variante, les notes affichées à l'opérateur sont transformées en notes sur une échelle de notation par lettre, par exemple A, B, C, D, E avec un signe + ou – selon que le score est au dessous ou au dessus du score visé. On quantifie préférablement la note au préalable. Ensuite +5, correspond à E+, +4 à D+,+3 à C+, +2 à B+, +1 à A+, 0 à A, -1 à A-, -2 à B-, -3 à C-,-4 à D-,-5 à E-. On peut éventuellement inverser la position du signe +/- et de la lettre, car le signe est davantage significatif.

On note que le score visé et la ou les marges d'erreurs sont en général pré-calculées lors d'une phase de calibrage de la machine d'impression et/ou de l'encre et du papier utilisés et/ou du produit cible, chacun pouvant avoir un impact sur le score du CNA.

On note que, pour augmenter la tolérance aux conditions spécifiques de l'impression, la phase d'ajustement peut servir de phase d'apprentissage : on peut tolérer une certaine variation dans la valeur du score visé, pour autant que toute la production soit aussi proche

que possible de ce score visé. Autrement dit, la priorité est de minimiser la variabilité du score, et tant que la variabilité est faible, il est acceptable que le score moyen de la production soit différent du score visé. A cet effet, un message peut être envoyé à l'opérateur en fonction de la note, par exemple recommandant d'augmenter ou diminuer la charge d'encre. En variante, on commande directement la machine d'impression pour que la note reste aussi proche que possible de la valeur « 0 ».

Les scores, ou taux d'erreurs, sont ainsi présentés à l'opérateur et comptabilisés dans les statistiques de la production.

En variante, il n'y a pas d'étape de transmission de paramètres d'analyse au transformateur, et le transformateur établit une connexion sécurisée avec un serveur d'analyse. Les images sont remontées au serveur et les résultats envoyés à l'application informatique du transformateur, en temps réel.

On observe que les statistiques et la valeur de seuil appliqué au score du CNA (pour la détermination des originaux/copies) peuvent être établies ou modifiées après la clôture de fabrication.

Comme on l'observe en figure 3A, pour contrôler la qualité de codes authentifiants, on réalise :

- une étape 305 de capture d'une image avec l'un des moyens de lecture fixe, 125 ou mobile 190,
- une étape 310 d'obtention de valeur limite, ou valeur de seuil, à appliquer au taux d'erreur pour déterminer l'authenticité d'un CNA, par exemple de lecture du contenu du CNA représenté par l'image, ou par interrogation d'une base de données en fonction du contenu du CNA ou d'un autre identifiant de la production,
- une étape 315 d'obtention des paramètres d'impression, par exemple de lecture du contenu du CNA représenté par l'image, ou par interrogation d'une base de données en fonction du contenu du CNA ou d'un autre identifiant de la production,
- une étape 320 d'ajustement de la valeur limite en fonction des conditions d'impression, si cette valeur limite n'en tient pas déjà compte comme exposé en regard des figures 2A et 2B,
- une étape 325 de détermination des conditions de capture d'image au cours de laquelle on détermine une résolution de l'image du CNA et/ou du flou de mauvaise focalisation et/ou de flou de mouvement au cours de la capture d'image, selon des techniques de traitement d'image connues et/ou en mettant en œuvre une mire, comme exposé par ailleurs,
- une étape 330 de détermination si les conditions de capture d'image sont suffisantes,

- si non, une étape 335 d'envoi de l'image au serveur 155 pour des traitements d'image complémentaires suivi d'un retour à l'étape 305,

- si oui, une étape 340 de détermination de taux d'erreur dans le CNA, taux d'erreur aussi appelé « score » du CNA,

- une étape 345 de détermination d'authenticité en comparant le taux d'erreur mesuré du CNA, éventuellement ajusté en fonction des conditions de capture d'image, avec une valeur de seuil,

- une étape optionnelle 350 de détermination de signature de chaque CNA dont une image a été capturée,

- une étape 355 de transmission de la signature et du résultat de l'étape 345 au serveur 155,

- une étape 360 de détermination d'identité du produit en comparant la signature trouvée au contenu d'une base de données de signatures permettant d'identifier les CNA et

- une étape 365 de transmission des résultats des traitements, depuis le serveur 155 vers le lecteur local de capture d'image, par exemple en vue d'un affichage d'une note, d'une identité et d'une authenticité, à l'opérateur, au détenteur de droits et/ou au fournisseur de CNA.

Comme on l'observe en figure 3B, pour contrôler la qualité de codes authentifiants, dans des modes de réalisation particuliers, on effectue les mêmes étapes que celles illustrées en figure 3A, à ceci près que les étapes 340 et 345 sont éliminées et au cours de l'étape 425, qui suit l'étape 320, on détermine le taux d'erreurs dans l'image du CNA, puis un score et, au cours d'une étape 430, on détermine l'authenticité du produit, comme exposé en regard des étapes 340 et 345 mais sans ajustement en fonction des conditions de capture d'image. Si on détermine que le produit est authentique, on passe à l'étape 350. Sinon, on effectue les étapes 325 et 330 et, si les conditions de capture d'image sont suffisantes, on passe à l'étape 350.

Dans le cas d'utilisation d'un outil de capture d'image non homologué, comme illustré en figure 3C, on effectue :

- une étape de capture d'image par un outil de capture, éventuellement non-homologué pour la mise en œuvre de la présente invention, en effectuant :

  - d'abord, dans le cas de la mise en œuvre d'un scanner, en effectuant un scan à basse résolution, par exemple à 150 dpi, au cours d'une étape 505,

  - un traitement d'image pour déterminer la position du CNA ou de chaque zone contenant potentiellement un CNA, dans l'image capturée au cours de l'étape 505, au cours d'une étape 510 puis

- en effectuant un scan local, pour chaque zone contenant potentiellement un CNA pour obtenir une image du CNA à haute résolution, par exemple à 1.200 dpi, au cours d'une étape 515,

- en déterminant, à partir de chaque image capturée au cours de l'étape 515, pour chaque candidat, s'il s'agit réellement d'un CNA (par opposition avec un carré noir non significatif ou un code à barres 2D), par exemple en en détectant le contour carré et sombre d'une largeur prédéterminée par rapport au côté du carré, au cours d'une étape 520,

- en effectuant une première mesure de netteté, sur la base de l'image de chaque CNA, par exemple par détermination de la moyenne des gradients locaux, en valeurs absolus, au cours d'une étape 525,

- en comparant cette première mesure de netteté avec une valeur représentant la valeur de seuil minimal de netteté, afin de déterminer si l'image du candidat CNA est à envoyer au serveur, au cours d'une étape 530,

- en envoyant au serveur chaque candidat CNA sélectionné, au cours d'une étape 535, par l'intermédiaire d'un réseau informatique (notamment, par courrier électronique, ou email),

- au cours d'une étape 540, lire chaque CNA, faire une seconde mesure de netteté et comparer le score du CNA et son score de netteté aux valeurs de seuil stockées en référence, comme exposé en regard de l'une des figures 3A ou 3B, toutes les étapes étant alors réalisées par le serveur 155,

- au cours d'une étape 545, en fonction du résultat, retourner un résultat à l'ordinateur client dans un message représentatif de l'authenticité, de l'identité du CNA et/ou d'une note et

- une étape 550 d'affichage du contenu de ce message à l'utilisateur ou opérateur, au détenteur de droits et/ou au fournisseur de CNA.

Ce mode de réalisation s'applique, par exemple aux images produites par les scanners à plat. Dans certaines applications, une image peut être générée par différents scanners à plats, qui ne sont pas forcément homologués ni même connus. Ces scanners produisent des images de qualité variable : il existe en effet une multitude de marques et de modèles de scanner à plat, et de plus, la plupart de ces scanners contiennent des réglages internes pouvant affecter la qualité de l'image capturée.

Connaître le modèle du scanner (celui-ci peut être contenu dans les métadonnées du fichier image, ou transmis simultanément par l'opérateur du scanner) ne signifie en général pas à déterminer la qualité d'image : en effet, pour un même scanner la résolution de capture (600 dpi, 1.200 dpi, 2.400 dpi) affecte la qualité de l'image, et ceci de manière différente sur différents modèles de scanners. Le type d'image (couleur, niveau de gris, binaire) affecte aussi la qualité d'image. Et même pour une résolution fixée d'un scanner

donné, on peut avoir d'importantes variations de qualité. Par exemple, l'option « lissage » de certains scanners correspond à l'application d'un filtre passe-bas de l'image qui peut éliminer de nombreux détails du CNA, dont le score peut alors être significativement réduit. Et d'autres options peuvent avoir l'effet contraire sur le score. Ainsi des options telles que « Accentuation de la netteté » correspondent à un filtrage passe-haut qui peut parfois augmenter ou diminuer le score du CNA. SI une application spécifique est installée sur le poste connecté au scanner, il serait en principe possible de « geler » les différents paramètres de capture afin de contrôler la qualité de l'image. Mais en pratique, cela n'est malheureusement pas possible de manière fiable, car les programmes de gestions des paramètres de scanner sont propriétaires, et ne donnent pas accès à une majorité de paramètres internes autrement que par une interface utilisateur, qui peuvent donc être changés à tout moment sans contrôle. Finalement, le document à vérifier peut simplement être mal apposé à la surface du scanner, de sorte que l'image du CNA n'est pas prise au point focal du scanner : son score peut alors s'en trouver fortement affecté.

Dans certaines applications, l'outil de capture d'image peut être d'origine inconnue. Par exemple, dans certains cas, une image peut être prise sur un scanner quelconque, puis envoyée à un serveur pour vérification. Le nom du scanner n'est pas transmis au serveur, et même s'il était transmis, ses propriétés de capture d'image pourraient être inconnues, étant donnée le grand nombre de modèles existant sur le marché.

Pour pallier ces difficultés, et ainsi permettre le déploiement à grande échelle d'applications de lecture de CNA sans forcément maîtriser tous les paramètres de la lecture ni installer d'application locale (lecture à distance), une solution consiste à distribuer des mires aux opérateurs des outils de capture d'image, au cours d'une étape 600, illustrée en figure 3D. Une mire est un objet, par exemple une carte, qui contient des structures d'image permettant d'évaluer la qualité de l'image produite par le capteur d'image de manière précise et stable.

L'opérateur muni d'une mire souhaitant authentifier un document place la mire et le document de manière adjacente dans le champ de vision du capteur d'image, de sorte qu'une seule capture d'image contienne à la fois le ou les CNA à analyser et la mire, au cours de l'étape 605.

Une image de la mire permet de calculer un ou plusieurs indicateurs de la qualité de l'image. Ces indicateurs sont mis en rapport avec des valeurs de référence pour la mire, afin d'ajuster le score du CNA en tenant compte de la mesure de qualité d'image, au cours d'une étape 610 et 615 et/ou de déterminer si l'image est de qualité suffisante pour déterminer l'authenticité du CNA.

La mire peut également être un autocollant qui est collé sur le document à vérifier, à côté du CNA. De cette façon, si le CNA est mal placé sur le scanner de sorte qu'il soit flou

dans l'image générée, il y a de fortes chances que la mire soit également floue. Il sera alors possible de déterminer que l'image ne permet pas d'authentifier le CNA. Dans un mode de réalisation préférentiel, la mire contient, elle-même, un CNA.

On donne ci-dessous, un exemple d'étapes de mise en œuvre de la mire :

- au cours de l'étape 610, on calcule un score du CNA,
- au cours de l'étape 615, on calcule un indicateur de qualité d'image à partir de la mire,
- au cours de l'étape 620, si l'indicateur de qualité est inférieur à une valeur de seuil prédéterminée, on rejette l'image, c'est-à-dire que l'on demande des analyses complémentaires,
- si l'indicateur de qualité est supérieur à la valeur de seuil considérée, au cours d'une étape 625, à partir de la valeur de l'indicateur, on calcule un coefficient d'ajustement multiplicatif ou un coefficient additif à appliquer au score du CNA et on calcule le score ajusté du CNA à partir de son score initial et du coefficient multiplicatif ou additif.

Le score ajusté est comparé à chaque valeur de seuil prédéterminée du CNA afin de prendre une décision sur son authenticité, sa signature, sa note et l'identité du produit, comme exposé en regard des figures 3A ou 3B.

Des problèmes de qualité d'image peuvent exister même avec des outils de lecture aux propriétés, en principe, connues. En effet, en pratique une flotte de lecteurs est distribuée chez les sous-traitants, unités d'assemblage, service qualité de différents détenteurs de droits, ainsi que chez les inspecteurs, douaniers, distributeurs. Ces lecteurs sont déplacés et manipulés avec des précautions variables, et parfois certains lecteurs sont déréglés. De plus, il peut arriver qu'un lecteur ne soit pas parfaitement réglé à sa sortie d'usine. Et en général, on ne peut garantir que tous les lecteurs aient exactement les mêmes performances de lecture, même s'ils sont produits de manière identique. Selon au moins un aspect de la présente invention, on ajuste les scores, ou les valeurs de seuil de décision, afin de tenir compte de la performance de l'outil. Préférentiellement, on prévoit des moyens de détection d'un problème de réglage sur un outil de lecture.

Une solution à ces problèmes consiste à intégrer de manière fixe une mire (telle que celles décrites précédemment) dans le champ de vision du moyen de capture d'image, de sorte que la mire soit contenue dans toute image capturée avec le moyen de capture. Ainsi, à chaque lecture d'une image, la lecture de la mire permet de mesurer la qualité de l'image. Cette qualité d'image peut être prise en compte afin d'ajuster le score mesuré pour le CNA, ou afin d'afficher un message avertissant l'opérateur du moyen de lecture qu'un réglage de ce moyen de lecture est nécessaire.

Les étapes mises en œuvre sont alors, comme illustré en figure 3E :

- une étape 635 de génération de CNA de référence servant de cale et de certification de lecteurs et

- une étape 640 d'apposition de ces CNA sur chacun des moyens de lecture autorisés, dans son champ de vision (par exemple par gravure ou collage 'un support de CNA de référence.

Lorsque les performances du moyen de capture d'image ne sont pas connues et qu'une mire n'est pas disponible, il est néanmoins possible de s'assurer qu'un document étudié est un original. En effet, on peut établir au préalable une valeur de seuil correspondant à la meilleure qualité de lecture qui peut être obtenue sur une gamme de moyen de lecture. Par exemple, la gamme de moyens de lecture peut correspondre à l'ensemble des scanners à plat opérant à 1.200 dpi. La valeur de seuil peut être établie par l'une des méthodes décrites précédemment. Lorsqu'on compare le score obtenu à cette valeur de seuil, le CNA est considéré comme un original si le score est supérieur à la valeur de seuil. En revanche, si le score est inférieur à la valeur de seuil, on ne peut conclure s'il s'agit d'une copie, ou d'un original capturé avec une qualité d'image inférieure. Dans ce cas, le message de réponse consiste généralement à recommander une vérification approfondie, à l'aide d'un moyen de capture d'image aux performances connues, ou sinon avec un moyen de capture d'image fournissant une qualité d'image supérieure.

La carte munie de la mire peut avoir d'autres fonctionnalités avantageuses. Par exemple, la mire peut contenir de l'information, par exemple dans un CNA ou MIS, permettant d'identifier son détenteur. Ainsi, on peut s'assurer que seules les personnes autorisées peuvent lire ou authentifier les CNA. On peut également déterminer les CNA lus pour une mire donnée, ou encore permettre un nombre maximal de lectures pour une mire donnée. Il en va de même si la mire est sur un autocollant, celui-ci pouvant être destructible si on essaie de le détacher.

Le moyen de lecture permet également d'établir un modèle de paiement du client du service de lecture de CNA basé sur le nombre de lectures faites.

Des méthodes de détection de copie peuvent être appliquées afin de détecter une éventuelle copie d'une carte de lecture.

Il est à noter que ces fonctionnalités peuvent être implémentées sans que la carte contienne une mire.

Les étapes mises en œuvre peuvent être celles illustrées en figure 3F :

- une étape 650 d'impression de documents servant à la fois de certificat de lecture, et de cale de lecture, contenant un CNA de référence et de certification servant à la fois comme certificat de lecture et comme cale de lecture,

- une étape 655 de distribution des certificats de lecture aux personnes autorisées.

- une étape 660 de capture d'image par un outil de capture non-homologué, ladite image contenant à la fois un document contenant un CNA et un document contenant le CNA de certification,

- une étape 665 d'envoi, vers un serveur sécurisé, de l'image captée, par l'intermédiaire d'un réseau informatique (notamment par courrier électronique),

- une étape 670 d'analyse du CNA de certification de l'image captée par le serveur sécurisé 155,

- une étape 675 d'analyse du CNA du document de l'image captée par le serveur sécurisé,

- une étape 680 de renvoi d'un message, par le serveur sécurisé, précisant si le CNA de certification autorise la lecture, si les conditions de capture d'image autorisent l'authentification, et si oui, si le CNA du document capté est authentique ou est une copie, éventuellement l'identité du produit et/ou une note.

On note que l'estimation de flou traité au cours du traitement d'image peut aussi être aussi due à une mauvaise qualité d'impression. On a alors des valeurs de netteté d'impression qui peuvent, par exemple, être pré-calculées lors de l'étape de contrôle d'impression et stockée par le serveur 155. Les étapes mises en œuvre comportent, comme illustré en figure 3G :

- une étape 705 de capture d'image, de lecture/extraction du message) et de mesure du score du CNA,

- une étape 710 de détermination de la valeur de seuil de score du CNA (par exemple stocké sur serveur ou dans le message),

- une étape 715 de comparaison du score du CNA à la valeur de seuil : si le taux d'erreurs est inférieur à la valeur de seuil, on détermine que le produit est original, et sinon :

  - une étape 720 de mesure d'une valeur de netteté du CNA (cette étape peut être faite automatique lors de l'étape de lecture du CNA),

  - une étape 725 de détermination de la valeur de seuil de netteté (par exemple, en fonction du message contenu dans le CNA, en fonction de l'identification du CNA),

  - une étape 730 de comparaison de la valeur de netteté à la valeur de seuil de netteté, et en sortie, une détermination si le produit est une « copie », si le CNA est suffisamment net ou si l'image est « non-conforme », si l'image n'est pas nette.

En variante, le degré de netteté peut, jusqu'à une certaine valeur tolérable, être utilisé pour ajuster le score du CNA.

En variante, on a une maîtrise complète du contexte d'impression, et on peut stocker la valeur attendue ou valeur de seuil de netteté (ainsi que la valeur de seuil du score) dans le

message porté par le CNA ; on peut également stocker ces valeurs dans un code barre 2D lors d'une impression par repiquage.

Dans le contexte d'un outil de lecture qui capture des images en série, on peut utiliser un algorithme présenté en figure 3H permettant la détermination en temps réel d'images floues. Si l'image contient un CNA et est jugée nette, le CNA peut être authentifié, sinon on poursuit. Notons qu'un certain nombre d'images bonnes mais rejetées peut éventuellement être tolérable. Par contre un rejet systématique d'image valide (par exemple d'une copie non-floue) n'est pas acceptable.

La valeur de seuil du score de netteté peut être absolue ou déterminée en fonction des conditions d'impressions si celles-ci sont connues. Par exemple, selon la mesure de netteté, on peut avoir des scores de valeurs différentes pour des CNA imprimés en offset, ou en impression à jet d'encre (typiquement moins élevés dans ce dernier cas). On note que la mesure de netteté peut également varier en fonction des propriétés de l'outil de capture d'image et de la résolution à laquelle il est utilisé. Si nécessaire, on convertit les mesures de netteté pour tenir compte de ces propriétés, et on peut également adapter les paramètres de l'algorithme de mesure de netteté (par exemple la taille du voisinage considéré, qui est typiquement plus grande si la résolution de capture est plus élevée).

Les étapes mises en œuvre sont alors les suivantes :

- une étape 755 de détermination si une image contient un CNA (par exemple par détection d'un carré si le CNA est carré),

- si oui, une étape 760 de mesure d'un indice de netteté, par exemple la mesure moyenne de la valeur absolue gradient sur la portion d'image contenant le CNA (certains CNA sont très texturés), et comparaison à une valeur de seuil prédéterminée,

- si la mesure de netteté est supérieure à une valeur de seuil prédéterminée, une étape 765 de transmission de l'image à un module de lecture du CNA (ce dernier peut se trouver sur une machine différente de celle mettant en œuvre les fonctions de mesure de netteté). En variante, l'opérateur peut forcer la lecture par pression d'un bouton prévu à cet effet, pour le cas où la mesure de netteté serait systématiquement inférieure à la valeur de seuil prédéterminée,

- en fonction du temps estimé d'analyse, une étape 770 de transmission d'un signal à l'opérateur indiquant qu'une image est lue et

- une étape 775 de détermination d'authenticité et/ou d'identité et/ou de note et affichage le résultat de la lecture à l'opérateur, au détenteur de droits et/ou au fournisseur de CNA, comme exposé en regard des figures 3A et 3B.

En variante, on mesure une différence d'image entre l'image reçue et l'image précédente, et on rejette l'image si la mesure de différence est supérieure à une valeur de seuil. En effet, une grande différence d'image peut indiquer que le produit ou document est

en mouvement et que sa position n'est pas stabilisée, ce qui augmente les chances que l'image soit floue.

En variante, on intègre la mesure d'un score de netteté sur la mire dans l'algorithme donné ci-dessus.

On note qu'il existe de nombreuses mesures de netteté qui peuvent être utilisée, dont plusieurs sont décrites dans « Autofocus survey: A comparison of algorithms » de Loren Shih. Le filtre de gradient de Sobel fournit de bons résultats, et est peu coûteux en calculs. Egalement, la soustraction d'une image et du résultat du filtrage passe-bas (par exemple par filtrage gaussien) de cette image résulte en une image de différences, ces différences étant d'autant plus marquées si l'image contenait à l'origine une énergie importante dans les hautes fréquences. La moyenne, de ces différences (prises en valeur absolue), ou une moyenne de ces différences sur une sélection de l'image contenant le plus grand nombre de différences, fournit un indicateur de netteté.

On a vu comment une application de lecture à distance par scanner peut vérifier la qualité d'image à l'aide de la mire. Cette application est avantageuse parce qu'aucun logiciel ne doit être installé chez l'utilisateur. Par contre, l'application exige plusieurs manipulations (fixer correctement les paramètres du scanner, éventuellement sélectionner la partie d'image à scanner, enregistrer l'image numérisée, ou « scan », dans un fichier, envoyer le fichier au serveur par courrier électronique). Or, de nombreux utilisateurs ne seront pas forcément familiers avec ce genre de manipulations, et de ce fait n'utiliseront pas l'application. De plus, une erreur de manipulation peut facilement être faite, résultant par exemple en un fichier image ne contenant pas de CNA, ou encore en une image n'ayant pas la qualité requise. Ces erreurs ne sont constatées qu'après la réponse du serveur, ce qui peut prendre un certain temps. De nombreux utilisateurs risqueront d'être découragés par la difficulté d'utilisation de l'application, et il est probable que plusieurs d'entre eux éviteront de l'utiliser.

L'installation d'un applicatif local permet de fortement simplifier la lecture. Cet applicatif local ne contient préférablement pas les algorithmes de lecture de CNA, ni les clés associées. En effet, ainsi on évite les problèmes de sécurité associés. D'autre part, on évite les problèmes de mise à jour des clés ou paramètres sur les applicatifs installés. En revanche, l'applicatif local gère les paramètres du scanner, détermine les zones à scanner, envoie les images des CNA au serveur, et affiche les réponses du serveur en retour. Il peut également détecter des problèmes avant l'envoi d'image au serveur, par exemple des images floues, et indiquer à l'utilisateur comment corriger ces problèmes.

Sur le serveur, le ou les CNA sont lus. Pour chaque CNA, une mesure de netteté peut être faite et comparée à une valeur de seuil stockée sur le serveur (cette valeur peut être retrouvée si le CNA est identifié). Si le score du CNA est inférieur à la valeur de seuil qui lui correspond et la mesure de netteté est également inférieure à la valeur de seuil qui lui

correspond, on peut, par exemple, envoyer un message à l'opérateur du scanner, au détenteur de droits et/ou au fournisseur de CNA, indiquant que l'image n'a pu être authentifiée.

On note que la valeur de seuil appliquée au score de netteté peut avoir été calculée au moment de la clôture de fabrication, à partir des images issues du contrôle qualité. La figure 3C illustre les étapes mises en œuvre dans ce mode de réalisation particulier.

Les scores de taux d'erreurs (ou qualité) et de netteté peuvent varier en fonction des caractéristiques de la capture d'image : qualité, résolution, éclairage, etc. Les mesures faites lors de la calibration (voir figures 2A et 2B), lors du contrôle de qualité en production ou lors de la livraison des produits au transformateur ou à tout destinataire désigné par le détenteur de droits, qui servent de référence pour les mesures attendues, doivent être adaptées aux conditions de la capture d'image si elles ont été effectuées avec un outil de capture d'image produisant des images de nature différente.

Pour effectuer une compensation des scores et/ou des valeurs de seuil en fonction des conditions de capture d'image et/ou des conditions de l'application, on choisit un CNA imprimé (ou plusieurs impressions du même CNA) qui sert de référence. De préférence, ce CNA est imprimé correctement sans particularité, par exemple sa charge d'encre n'est pas trop élevée. On effectue plusieurs captures d'images avec l'outil de capture d'image de référence, par exemple celui qui sert au contrôle qualité en production ou à réception des documents. On calcule une moyenne « m » et un écart-type « e » du score, par exemple, en utilisant des méthodes de statistique robuste. Pour une capture d'image avec cet outil, sans hypothèse sur le score des copies, on fixe la valeur de seuil à $s = m - n * e$, « n » étant une valeur positive qui dépend de la probabilité maximale de fausse détection d'une copie que l'on est prêt à accepter. Comme discuté précédemment, on peut créer un certain nombre de copies de bonne qualité en réimprimant dans les mêmes conditions, et effectuer plusieurs captures d'images pour déterminer la distribution statistique des scores, ou encore appliquer un modèle simple qui permet d'estimer le score obtenu lors d'une bonne copie, c'est-à-dire en mettant en œuvre des outils d'impression de qualité similaire à celle des outils d'impression de l'original.

Supposons que l'outil de capture d'image soit différent de l'outil de capture d'image utilisé lors du calcul de la distribution statistique des scores. En général, mais pas nécessairement, l'outil de capture d'image sera de qualité inférieure, de sorte que la moyenne « m' » des scores pour cet outil est inférieure à « m ». En tous les cas, on estime une fonction « f » de conversion des scores entre les deux outils de capture d'image : pour cela, on imprime des CNA avec différentes qualités d'impression. On en capture des images avec les différents outils de capture d'image utilisés, et on détermine la fonction conversion qu'il faut appliquer aux différents niveaux de score obtenus avec ces différents outils de

capture d'image. Par exemple, on considère que la fonction de conversion est de type additif ou multiplicatif, et on détermine le coefficient additionnel ou multiplicateur à appliquer. Par exemple, si la moyenne des scores est de 13 pour un échantillon de CNA avec l'outil de référence, et cette moyenne est de 11 pour l'outil utilisé en exploitation, on pourra utiliser un coefficient multiplicatif de 13/11 quel que soit le score. Par exemple, un score de 15 avec l'outil de capture d'image sera transformé en 15*13/11=17,72 avant d'être comparé à la valeur de seuil. Ainsi, on corrige le décalage des scores expliqué précédemment, et on minimise les risques de mauvaise classification des CNA qui peut en résulter.

Cependant, cette approche n'est pas toujours applicable car, comme discuté précédemment, on ne connaît pas toujours l'outil de capture d'image utilisé. Par contre, dans certains cas, une image d'une mire a également été capturée lors de la prise de vue et, préférentiellement, cette mire contient un autre CNA dont le score sur un outil de référence est connu. On a vu précédemment comment cette mire peut être utilisée pour déterminer si la qualité d'image est suffisante. On peut également utiliser cette mire pour ajuster le score obtenu pour le CNA à authentifier. Par exemple, si le CNA servant de mire obtient un score de 12, alors que ce score est de 13 en moyenne sur l'outil de capture d'image de référence, on peut appliquer un coefficient multiplicatif de 13/12 au score du CNA à authentifier. Par rapport à la méthode décrite précédemment qui juge simplement, d'après la mire, si la qualité de prise de vue est suffisante, cette nouvelle méthode permet, dans certaines limites (un score en dessous d'une limite préétablie pour le CNA de la mire menant à un rejet de l'image capturée), d'effectuer une compensation de score qui, si elle peut être approximative, permet néanmoins de réduire les risques d'erreurs (notamment les risques de considérer un original comme une copie sur un outil de capture d'image de qualité inférieure).

Cependant, dans certains cas, une mire n'est pas disponible au moment de la capture d'image. Dans ce cas, on peut estimer la qualité d'image de diverses façons, par exemple en appliquant un filtrage passe-bas, préférablement de type gaussien, à l'image, et en mesurant une différence, pour chaque pixel d'image entre l'image filtrée et l'image d'origine, puis en calculant une moyenne de la différence d'image. On peut également calculer une moyenne en privilégiant les zones du CNA de plus fort contraste. Plus cette différence sera faible, moins la qualité de prise sera grande en général. On note que d'autres méthodes analogues, par exemple se basant sur la mesure du spectre d'énergie en fréquence de l'image captée, peuvent être utilisées comme indicateur de netteté.

Dans cette méthode, on doit prédéterminer la relation entre l'indicateur de netteté et le facteur de correction de score. Par exemple, on choisit un ou plusieurs CNA imprimés de même qualité d'impression, et on calcule leur score et leur indicateur de netteté sur des outils de capture d'image de qualités différentes. On peut alors estimer, par des méthodes statistiques, la relation entre l'indicateur de netteté et le coefficient de correction du score.

On peut répéter la même procédure pour des CNA de différents niveaux de qualité d'impression, et donc de différents niveaux de score lors de capture d'image avec un outil de capture d'image de référence. On note que, pour de meilleurs résultats, il est préférable de tenir compte des possibles différences de résolutions de capture d'image dans le calcul de l'indicateur de netteté, ainsi que de la dynamique d'image.

Dans toute la suite de la description, on appelle « document » tout support d'information lisible avec un matériel de lecture et, parfois, à l'œil et on appelle « marque anticopie » ou « marque », une marque destinée à être faite, par impression ou par modification physique locale du support, sur un document, et dont la dégradation lors d'une copie de ce document est détectable et permet de différencier l'original de la copie. On rappelle qu'il y a deux grandes familles de telles marques : les images traitées par stéganographie, c'est-à-dire comportant, sur un décor, de manière indiscernable à l'œil, une empreinte (en anglais « watermark ») et les marques visibles formées d'une matrice de points présentant, chacun, l'une de deux couleurs, généralement noire et blanche.

La figure 8 n'est pas, non plus, représentée à l'échelle. On observe, en figure 8, un matériel d'impression 1005 muni d'un matériel de détection de copie 1010, un serveur 1015 de fourniture de marques anti-copie, un serveur 1020 de conservation d'une base de données de mesures de dégradation autorisées, un serveur 1025 de propriétaire des droits sur un document, des moyens d'alerte 1030, par exemple gyrophare, émetteur sonore ou ordinateur de contrôle de production et un matériel mobile de détection de copie 1035.

Le matériel d'impression 1005 est de type quelconque, par exemple flexographie, héliogravure, offset, typographie, impression numérique, impression laser ou jet d'encre.

Les matériels de détection de copie 1010 et 1035 comportent un moyen de prise d'image 1040 d'une marque sur un document, par exemple un capteur d'image à transfert de charges, connu sous le nom de « CCD » (acronyme de « charge coupled device » pour dispositif à transfert de charge), un processeur 1045 et une mémoire non volatile 1050 conservant un logiciel implémentant des étapes illustrées en figures 9A et 9B.

Le matériel de détection de copie 1010 comporte aussi un moyen de communication à distance 1055 avec le serveur 1020 et/ou avec le serveur 1015, par exemple sur un réseau de téléphonie, fixe ou mobile,

Le matériel de détection de copie 1035 comporte aussi un moyen de communication à distance 1060 avec les serveurs 1020 et 1025, par exemple sur un réseau de téléphonie mobile.

Le serveur 1015 de fourniture de marques anti-copie est adapté à implémenter l'étape 1165 illustrée en figures 9A et 9B pour fournir une marque anti-copie en fonction des caractéristiques du matériel d'impression.

Le serveur 1020 conserve une base de données de mesures de dégradation autorisées en correspondance avec des identifiants de documents imprimés. Comme on le verra par la suite, le serveur 1020 est optionnel, une marque anti-copie pouvant, dans des modes de réalisation, incorporer la ou les mesures de dégradation limites permettant de discriminer un document original d'une copie.

Le serveur 1025 de propriétaire des droits sur un document est adapté à archiver et à traiter des informations provenant du matériel mobile de détection de copie 1035 pour déterminer le chemin d'un document, notamment dans le cas où une copie est détectée.

Au cours d'une étape 1105, un imprimeur remplit un questionnaire décrivant, notamment, le type et la marque d'un matériel d'impression destiné à être utilisé pour imprimer des documents comportant une marque anti-copie, et, l'ensemble des paramètres de la chaîne graphique, par exemple du système de « PAO » (acronyme de « publication assistée par ordinateur ») du système de « RIP » (acronyme de « rastering image process » pour processus de traduction d'image) qui traduit en fichier « bitmap », c'est-à-dire représentant séparément chaque point de l'image pour chaque couleur, et le système « CTP » (acronyme de « computer to plate » pour ordinateur à plaque) ou « FTP » (acronyme de « film to plate » pour filme à plaque), qui grave les plaques d'impression.

Au cours d'une étape 1110, le questionnaire renseigné est fournit par l'imprimeur à un fournisseur de marques anti-copie.

Au cours d'une étape 1115, le fournisseur prépare et fournit un gabarit de fiches de calibration à l'imprimeur, en fonction du contenu du questionnaire renseigné qui représente la configuration physique de la machine d'impression. Par exemple, à partir de la laize, le fournisseur détermine où placer le gabarit (par exemple d'une dimension de 105 x 210), sachant que ce gabarit est à reproduire plusieurs fois sur des feuilles de test. Préférentiellement, on prévoit que le gabarit permette d'identifier chaque couleur imprimée (chaque groupe d'impression) car on intègre une marque anti-copie pour chaque groupe d'impression. Dans d'autres modes de réalisation, on ne prévoit de marque anti-copie que pour la couleur, préférentiellement le noir, avec laquelle cette marque sera imprimée.

Au cours d'une étape 1120, le fournisseur de marques détermine une marque de calibration, en fonction du contenu du questionnaire renseigné. Connaissant la résolution native du matériel d'impression, généralement 2400 points par pouce, on choisit la résolution de la marque anti-copie de telle manière que l'impression de l'original comporte, elle-même, une dégradation de marque suffisante, par exemple supérieure à une valeur prédéterminée.

Au cours d'une étape 1125, le fournisseur fournit le gabarit de fiche et la marque de calibration à l'imprimeur, préférentiellement par attachement à un courrier électronique.

Au cours d'une étape 1130, l'imprimeur complète une fiche de calibration, c'est-à-dire, lors de la conception d'une feuille de test comportant plusieurs fiches destinées à être

imprimées en différents endroits et en différentes couleurs, il ajoute une marque, par exemple un croix, dans une case correspondant à la position et à la couleur d'impression. De même, il identifie le matériel utilisé pour l'impression. Au cours de cette étape 1130, l'imprimeur associe une marque anti-copie fournie au cours de l'étape 1125, à chaque fiche réalisée selon le gabarit.

Au cours d'une étape 1135, l'imprimeur imprime la marque de calibration avec le matériel d'impression, préférentiellement en différentes zones centrales et latérales d'impression du matériel d'impression et préférentiellement pour la référence carton la plus répandue en fabrication. En variante, l'imprimeur imprime la marque sur différents types de papier ou carton, de différents grammages.

Au cours d'une étape 1140, l'imprimeur fournit la fiche de calibration complétée et la ou les marques imprimées par le matériel d'impression, au fournisseur de marques.

Au cours d'une étape 1145, le fournisseur effectue une mesure de dégradation d'au moins une marque anti-copie imprimée avec le matériel d'impression en vue d'un traitement statistique pour déterminer un écart standard entre les impressions de fiches.

Au cours d'une étape 1150, le fournisseur de marque détermine les caractéristiques d'une marque à imprimer, en fonction de la dégradation d'au moins une marque imprimée avec le matériel d'impression à utiliser et fournit une marque possédant ces caractéristiques, à l'imprimeur, qui les intègre dans la matrice du document à imprimer, par exemple les films offset. Par exemple, le fournisseur détermine, statistiquement, un écart-type du nombre d'erreurs d'impression de la marque anti-copie imprimée au cours de l'étape 1135. En fonction de cet écart-type, on vérifie la capacité d'utilisation du matériel d'impression et de son contexte. Eventuellement, le fournisseur ajuste, au cours de l'étape 1150, la résolution d'impression des marques anti-copie.

Lors du lancement d'une fabrication de documents originaux, l'imprimeur met en œuvre un triptyque imprimeur. On rappelle, ici, qu'un triptyque est un échantillon physique d'impression du document, accepté par le donneur d'ordre en terme de la qualité d'exécution. Il est signé par le client et sert d'étalon de référence ou de calage du matériel d'impression au début de chaque fabrication. C'est un outil de travail très répandu et utilisé systématiquement dans le monde d'impression. Le triptyque correspond à trois situations d'impression :

- l'impression avec la charge d'encre minimale acceptable,
- l'impression avec la charge d'encre idéale et
- l'impression avec la charge d'encre maximale acceptable.

Au cours d'une étape 1155, un matériel de détection de copie est mis en œuvre pour mesurer, sur au moins l'un des volets extrêmes du triptyque correspondant à un encrage extrême, la dégradation de la marque anti-copie. L'encrage standard, représenté par le volet

central du triptyque, définit, par l'intermédiaire du matériel de détection de copie, un taux d'erreurs, ou mesure de dégradation, standard. Préférentiellement, on effectue la mesure au moins sur le volet du triptyque présentant l'encrage minimum autorisé par le client. Préférentiellement, chaque volet est l'objet d'une mesure de dégradation et on sélectionne la mesure de dégradation la plus élevée. On rappelle qu'une mesure de dégradation peut déterminer le nombre de points de la marque qui ne possèdent pas la couleur de l'original numérique. Cette mesure peut être effectuée par comparaison d'une image de la marque analysée avec une image numérique sans dégradation, par exemple.

Au cours d'une étape 1160, on met en mémoire d'un matériel de détection de copie installé sur le matériel d'impression, une information représentative de la mesure de dégradation obtenue au cours de l'étape 1155. Cette information est, par exemple, la mesure du taux d'erreur pour chaque encrage extrême autorisé.

Au cours d'une étape 1165, on ajoute une marge de sécurité, par exemple un multiple de l'écart type, à la mesure de dégradation obtenue au cours de l'étape 1155 pour l'encrage standard et on met le résultat en mémoire. Dans des modes de réalisation, on détermine deux valeurs limites, en ajoutant ou en retranchant la marge de sécurité du taux d'erreur obtenu avec l'encrage standard.

Dans des modes de réalisation, la mise en mémoire est effectuée dans une base de données distante (voir serveur 1020 illustré en figure 8), en mémorisant la ou les valeurs limites, en association avec un identifiant du document dans la base de données.

Dans d'autres modes de réalisation, la mise en mémoire est effectuée dans une nouvelle marque anti-copie fournie par le fournisseur de marque anti-copie pour la fabrication de documents originaux. La marque anti-copie possède alors un codage ou un chiffrement de la ou des valeurs limites. Dans ce mode de réalisation, la marque anti-copie intègre, de manière connue, une information représentative de la ou des valeurs limites.

Au cours d'une étape 1170, on fabrique le document, généralement en grande série. Au cours d'une étape 1175, pour au moins une partie des documents fabriqués, on mesure, avec le matériel de détection installé sur le matériel d'impression, la dégradation des marques anti-copie. Au cours d'une étape 1180, on détermine si la mesure effectuée au cours de l'étape 1175 est supérieure à la mesure effectuée au cours de l'étape 1155. Si oui, au cours d'une étape 1185, on émet un signal d'alerte, par exemple un signal numérique destiné à un ordinateur de contrôle de production, un signal sonore et/ou un signal lumineux. Sinon, on retourne à l'étape 1170. En fonction de ce signal, l'imprimeur peut modifier l'encrage et revenir dans les limites autorisées par le client.

Lorsque la fabrication est achevée, au cours d'une étape 1190, si la marque anti-copie ne représente pas, elle-même, la ou les valeurs limites, on met en mémoire de matériels de détection de copie mobiles, une information représentative de la mesure de

dégradation conservée en base de données en correspondance avec un identifiant du document produit.

Lorsqu'un matériel mobile est utilisé, par exemple en douane, au cours d'une étape 1195, on identifie le document, soit à partir d'information contenue dans la marque anti-copie ou dans un support d'information associé à cette marque, par exemple un code à barres, éventuellement en deux dimensions, par exemple un datamatrix (marque déposée), soit par saisie de l'information visible qui lui est attachée (modèle et fabricant, par exemple).

Au cours d'une étape 1200, on met en œuvre le matériel de détection de copie pour mesurer une dégradation d'une marque sur un document identifié au cours de l'étape 1195. On observe que les étapes 1195 et 1200 peuvent ne former qu'une étape, en particulier lorsque la lecture d'un identifiant du document est effectuée par traitement d'image de la marque anti-copie.

Au cours d'une étape 1205, on détermine si la mesure effectuée au cours de l'étape 1200 est supérieure à la mesure mise en mémoire au cours de l'étape 1190. Si oui, au cours d'une étape 1210, on transmet à distance, de l'information concernant la marque analysée ou le produit concerné, afin que le propriétaire des droits puisse agir contre une éventuelle contrefaçon de son produit associé au document. Par exemple, cette communication est effectuée en mettant en œuvre un réseau de téléphonie mobile. Sinon, à intervalles de temps réguliers, par exemple une fois par jour, au cours d'une étape 1215, on transmet à distance, de l'information concernant les documents analysés, afin que le propriétaire des droits puisse faire de la traçabilité de ses produits.

A la fin de l'une des étapes 1210 ou 1215, on retourne à l'étape 1195.

On observe que les étapes 1160 et 1190 peuvent être éliminées dans le cas où la marque anti-copie représente, dans l'information qu'elle incorpore, la ou les valeurs limites qui, pour l'étape 1175, représente le ou les seuils de déclenchement de signal d'alerte et, pour l'étape 1205, représente le ou les seuils de discrimination d'un document original d'une copie.

Ainsi, les deux situations extrêmes représentées par le triptyque définissent la valeur maximum du taux d'erreurs, ou mesure de dégradation, autorisé pour constater qu'une document est un original, à une marge de tolérance près.

On observe que, au cours de la fabrication des documents originaux, pour effectuer un calage du matériel d'impression, le conducteur dispose, grâce à la mise en œuvre de certains aspects de la présente invention, de deux possibilités d'assistance technique :

- la mesure densitométrique classique pour déterminer la qualité ou l'encrage de l'impression et/ou
- la mesure de la dégradation de la marque anti-copie effectuée par un matériel de détection de copie associé à la chaîne d'impression.

REVENDICATIONS

1 - Procédé de sécurisation d'un document dit « original », caractérisé en ce qu'il comporte :

- une étape de détermination de caractéristiques d'un matériel d'impression dudit document original,
- une étape de détermination d'une marque permettant de différencier un original d'une copie, en fonction des caractéristiques du matériel d'impression destiné à être mis en œuvre pour l'impression de ladite marque sur ledit document,
- une étape d'impression de ladite marque avec ledit matériel d'impression pour former ledit document original, et
- une étape de détermination d'une première valeur limite à utiliser par un matériel de détection de copie pour discriminer ledit document original d'une copie dudit document original, en fonction d'au moins une impression de ladite marque.

2 – Procédé de sécurisation selon la revendication 1, caractérisé en ce qu'il comporte une étape d'impression d'au moins une référence d'impression représentatives d'un maximum ou d'un minimum d'encrage autorisé pour l'impression dudit document et, au cours de l'étape de détermination de la première valeur limite, on détermine une mesure sur au moins une dite référence d'impression et on y ajoute une tolérance.

3 – Procédé selon l'une quelconque des revendications 1 ou 2, caractérisé en ce qu'il comporte une étape de mesure de détérioration de la marque sur la chaîne d'impression, une étape de comparaison de cette mesure avec une deuxième valeur limite prédéterminée et, en cas de dépassement de la deuxième valeur limite de détérioration, une étape d'alerte.

4 - Procédé selon l'une quelconque des revendications 1 à 3, caractérisé en ce qu'il comporte :

- une étape de capture d'une image représentative d'un code numérique authentifiant,
- une étape de détermination de conditions de capture de ladite image,
- une étape de détermination d'un taux d'erreur dudit code numérique authentifiant représenté par ladite image captée et
- une étape de détermination d'authenticité du code numérique authentifiant en fonction du taux d'erreur et des conditions de capture de ladite image.

5 - Procédé selon la revendication 4, caractérisé en ce que l'étape de détermination de conditions de capture de ladite image comporte une étape de détermination d'une valeur représentative de la qualité de capture de ladite image.

6 – Procédé selon l'une quelconque des revendications 4 ou 5, caractérisé en ce que l'étape de détermination de conditions de capture d'une image comporte une étape de détermination d'une valeur représentative du flou de capture de ladite image.

7 – Procédé selon la revendication 6, caractérisé en ce que, au cours de l'étape de détermination d'authenticité, on détermine, d'abord, si la valeur représentative de flou représente un flou inférieur à une valeur prédéterminé et, si oui, si le taux d'erreur est inférieur à une valeur prédéterminée.

8 – Procédé selon la revendication 7, caractérisé en ce que, si la valeur représentative de flou représente un flou supérieur à la valeur prédéterminée, on retourne à l'étape de capture d'image et on réitère les étapes de détermination de taux d'erreur et de détermination d'authenticité.

9 – Procédé selon l'une quelconque des revendications 7 ou 8, caractérisé en ce que, si la valeur représentative de flou représente un flou inférieur à une valeur prédéterminée, on transmet au moins une partie de ladite image à un serveur distant et l'étape de détermination d'authenticité est effectuée par ledit serveur distant.

10 – Procédé selon l'une quelconque des revendications 6 à 9, caractérisé en ce que l'étape de détermination d'une valeur représentative du flou met en œuvre des valeurs représentatives des conditions d'impression du code numérique authentifiant.

11 - Procédé selon l'une quelconque des revendications 4 à 10, caractérisé en ce qu'il comporte :

- une étape de capture d'une image représentative d'une mire,
- une étape de détermination d'une valeur d'ajustement à partir de l'image représentative de la mire et
- une étape d'ajustement du taux d'erreur en fonction de ladite valeur d'ajustement,

l'étape de détermination d'authenticité du code numérique authentifiant mettant en œuvre le taux d'erreur ajusté.

12 – Procédé selon l'une quelconque des revendications 4 à 11, caractérisé en ce que l'étape de détermination de conditions de capture d'une image comporte une étape de détermination du nombre de points de ladite image qui correspondent à un code numérique authentifiant.

13 – Procédé selon l'une quelconque des revendications 4 à 12, caractérisé en ce que, au cours de l'étape de détermination de conditions de capture d'une image, on détermine une netteté d'impression du code numérique authentifiant.

14 - Procédé selon l'une quelconque des revendications 1 à 13, caractérisé en ce qu'il comporte :

- une étape d'impression d'un support de code numérique authentifiant, en mettant en œuvre des valeurs de paramètres d'impression,
- une étape de capture d'une image du code numérique authentifiant imprimé sur ledit support,

- une étape de détermination d'une qualité d'impression du code numérique authentifiant en fonction de l'image du code numérique authentifiant et

- une étape d'impression d'au moins un autre support avec des paramètres d'impression fonctions de ladite qualité d'impression

15 – Procédé selon la revendication 14, caractérisé en ce que, au cours de l'étape de détermination de qualité d'impression, on détermine la qualité d'impression en fonction d'un contenu d'information du code numérique authentifiant lu dans ladite image.

16 – Procédé selon l'une quelconque des revendications 14 ou 15, caractérisé en ce que, au cours de l'étape de détermination de qualité d'impression, on détermine un taux d'erreur dans le code numérique authentifiant lu dans ladite image, la qualité d'impression étant fonction du dit taux d'erreur.

17 – Procédé selon l'une quelconque des revendications 14 à 16, caractérisé en ce qu'il comporte une étape de détermination si, à la fois, ladite image permet la lecture d'une valeur portée par le code numérique authentifiant imprimé et présente un taux d'erreur inférieur à une valeur limite prédéterminée,

- si ce n'est pas le cas, une étape de production d'un nouveau support et une itération de l'étape de lecture et de l'étape de détermination et

- si c'est le cas, une étape d'impression de codes numériques authentifiant en mettant en œuvre les paramètres d'impression dudit support.

18 – Procédé selon la revendication 17, caractérisé en ce qu'il comporte une étape de détermination de ladite valeur limite prédéterminée en fonction de la valeur représentée par le code numérique authentifiant.

19 – Procédé selon l'une quelconque des revendications 14 à 18, caractérisé en ce qu'il comporte :

- une étape d'impression d'une pluralité de codes numériques authentifiants, en mettant en œuvre des valeurs de paramètres d'impression,

- une étape de capture d'images d'une pluralité de codes numériques authentifiants imprimés,

- une étape de détermination de qualité d'impression pour chacune d'une pluralité de dites images et

- une étape de mise en mémoire d'une valeur représentative de ladite qualité d'impression.

20 – Procédé selon l'une quelconque des revendications 14 à 19, caractérisé en ce qu'il comporte, réalisées par un serveur qui fournit des codes numériques authentifiants :

- une étape de transmission, de manière sécurisée, de codes numériques authentifiants à des systèmes d'impression pour intégration au design du document,

- une étape de réception de mesures de qualité de codes numériques authentifiants imprimés sur des documents,

- une étape de détermination si la production est valide à partir des mesures reçues et

- une étape de transmission d'un message indiquant si la production est valide.

21 – Procédé selon l'une quelconque des revendications 1 à 8, caractérisé en ce que, au cours de l'étape de transmission de codes numériques authentifiants, le serveur transmet, d'abord, au moins un fichier de contrôle permettant d'imprimer un code numérique authentifiant inutilisable, du fait de son contenu d'information, pour authentifier une production de supports et, si la production est valide, le serveur transmet au moins un autre code numérique authentifiant représentatif d'information liée à ladite production.

22 – Procédé selon l'une quelconque des revendications 1 à 21, caractérisé en ce qu'il comporte :

- une étape d'impression d'un nombre prédéterminé de documents comportant un dit code numérique authentifiant,

- une étape de capture d'une image de chaque code numérique authentifiant imprimé et

- une étape de stockage d'une information représentative de chaque code numérique authentifiant imprimé.

23 – Procédé selon l'une quelconque des revendications 1 à 22, caractérisé en ce qu'il comporte une étape de détermination d'une signature de chaque image capturée d'un code numérique authentifiant, et une étape de stockage de ladite signature dans une base de données, avec les informations associées à la fabrication.

24 – Procédé selon la revendication 23, caractérisé en ce qu'il comporte une étape d'impression d'une matrice d'information représentant ladite signature, sur le document portant le CNA correspondant à ladite signature.

25 – Procédé selon l'une quelconque des revendications 1 à 24, caractérisé en ce qu'il comporte :

- une étape de capture d'images d'une partie des codes numériques authentifiants imprimés et de détermination, en mettant en œuvre des valeurs de paramètres d'analyse, d'une note représentative de la qualité d'impression dudit code numérique authentifiant et

- une étape de présentation, à l'opérateur, de ladite note représentative de qualité d'impression.

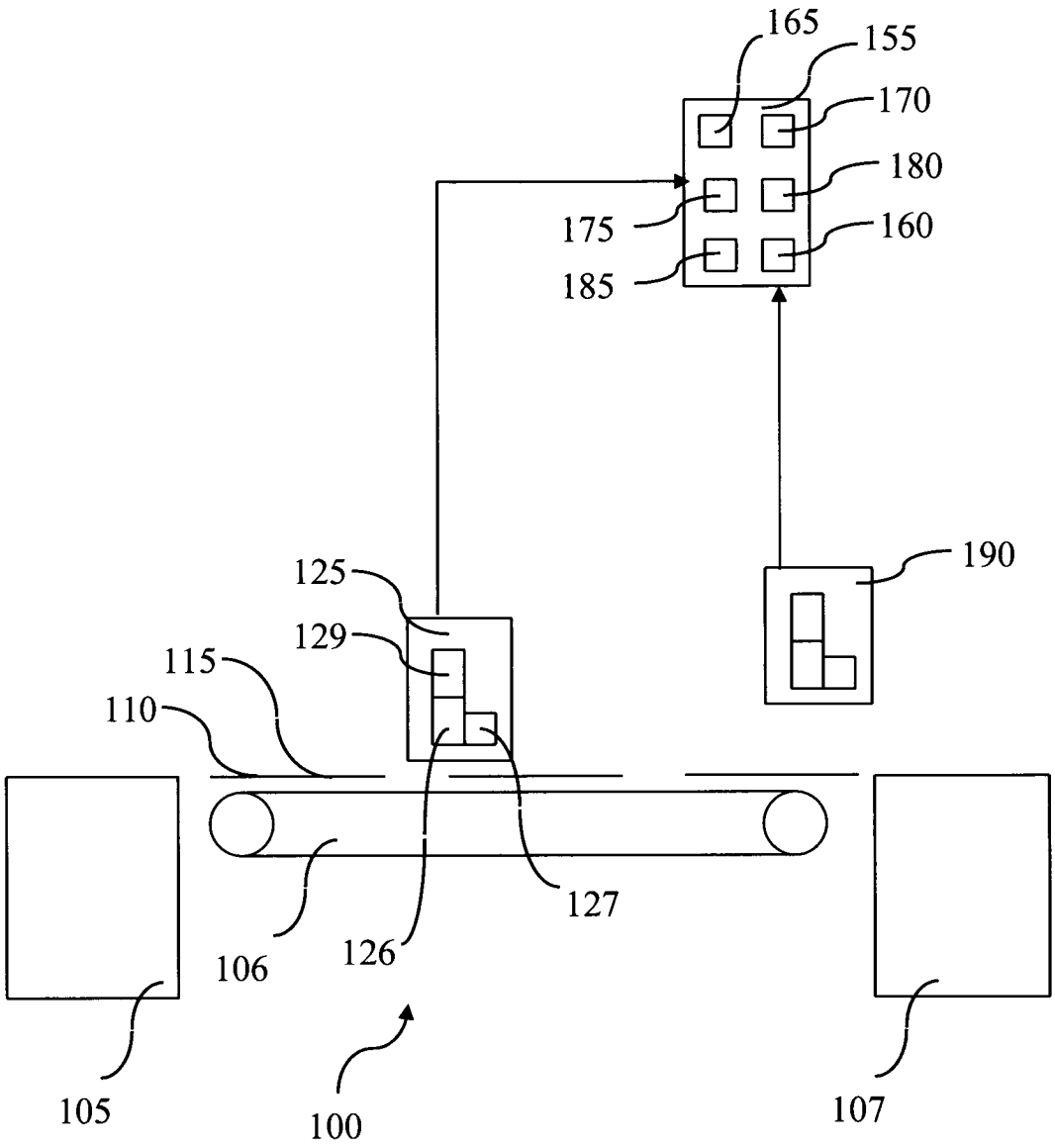
165
155
170
180
175
160
185
190
125
129
115
110
127
106
126
105
100
107

Figure 1

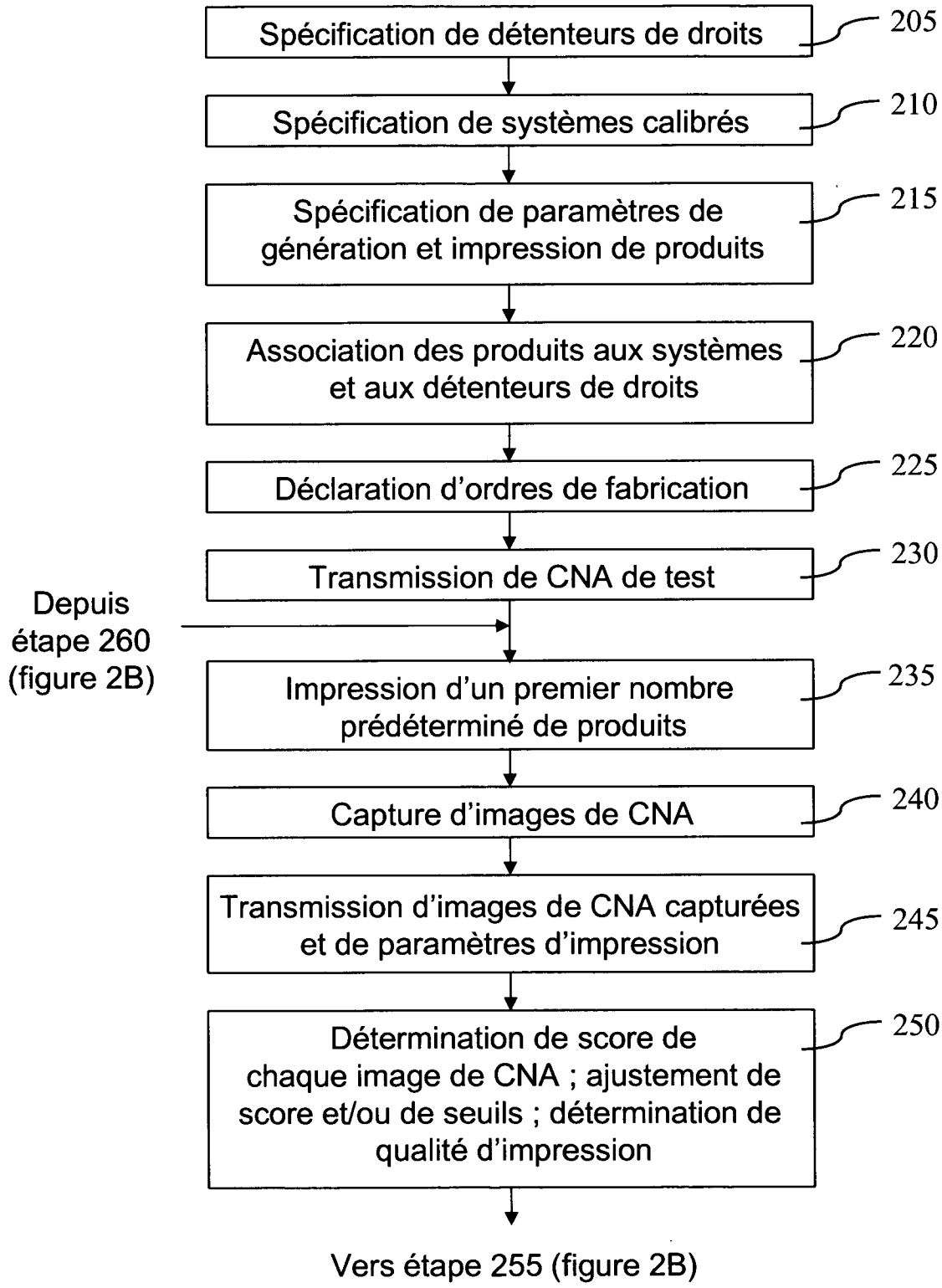
Spécification de détenteurs de droits
205
Spécification de systèmes calibrés
210
Spécification de paramètres de génération et impression de produits
215
Association des produits aux systèmes et aux détenteurs de droits
220
Déclaration d'ordres de fabrication
225
Transmission de CNA de test
230
Depuis étape 260 (figure 2B)
Impression d'un premier nombre prédéterminé de produits
235
Capture d'images de CNA
240
Transmission d'images de CNA capturées et de paramètres d'impression
245
Détermination de score de chaque image de CNA ; ajustement de score et/ou de seuils ; détermination de qualité d'impression
250
Vers étape 255 (figure 2B)

Figure 2A

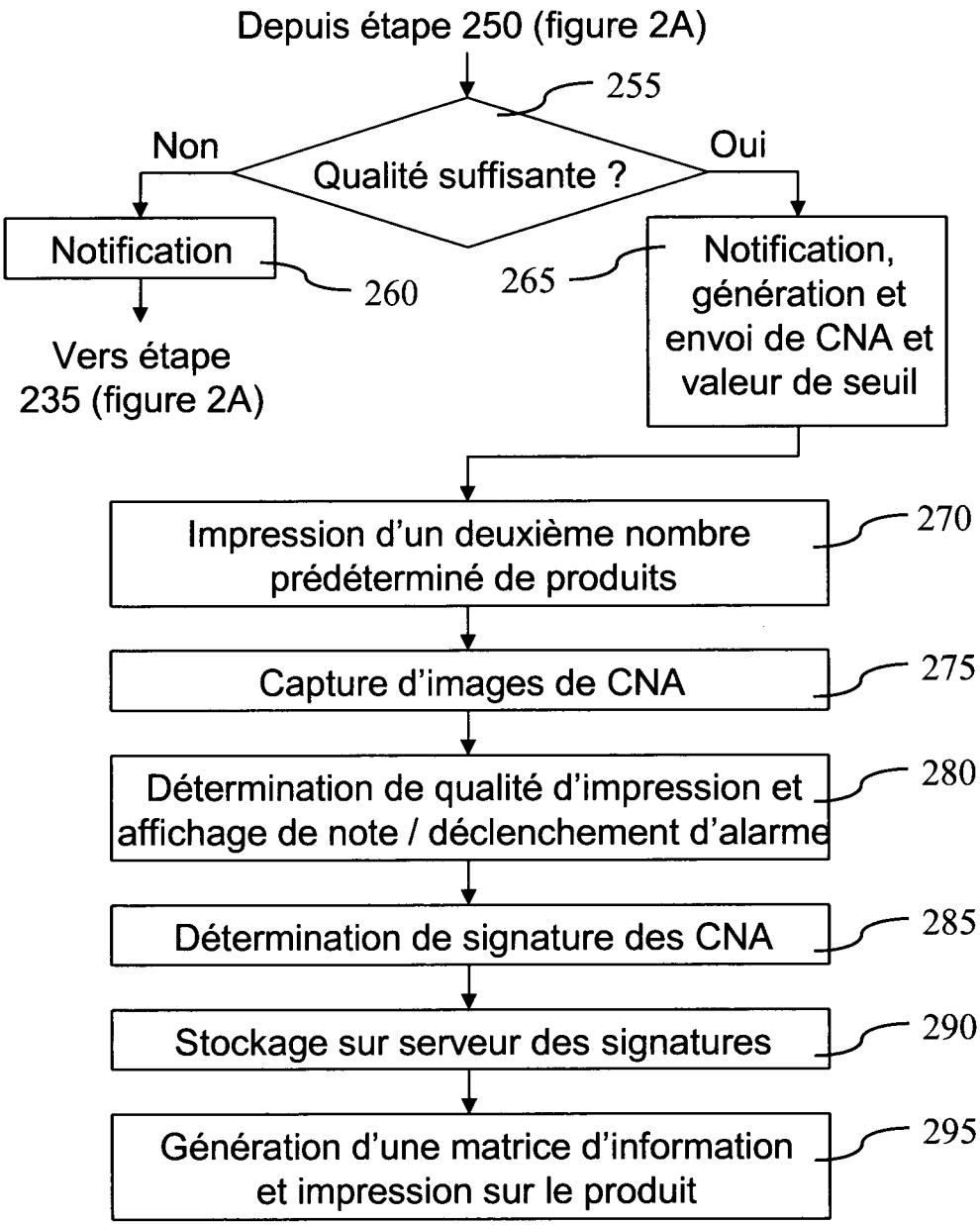
Depuis étape 250 (figure 2A)
255
Qualité suffisante ?
Non
Oui
Notification
260
Vers étape 235 (figure 2A)
265
Notification, génération et envoi de CNA et valeur de seuil
Impression d'un deuxième nombre prédéterminé de produits
270
Capture d'images de CNA
275
Détermination de qualité d'impression et affichage de note / déclenchement d'alarme
280
Détermination de signature des CNA
285
Stockage sur serveur des signatures
290
Génération d'une matrice d'information et impression sur le produit
295

Figure 2B

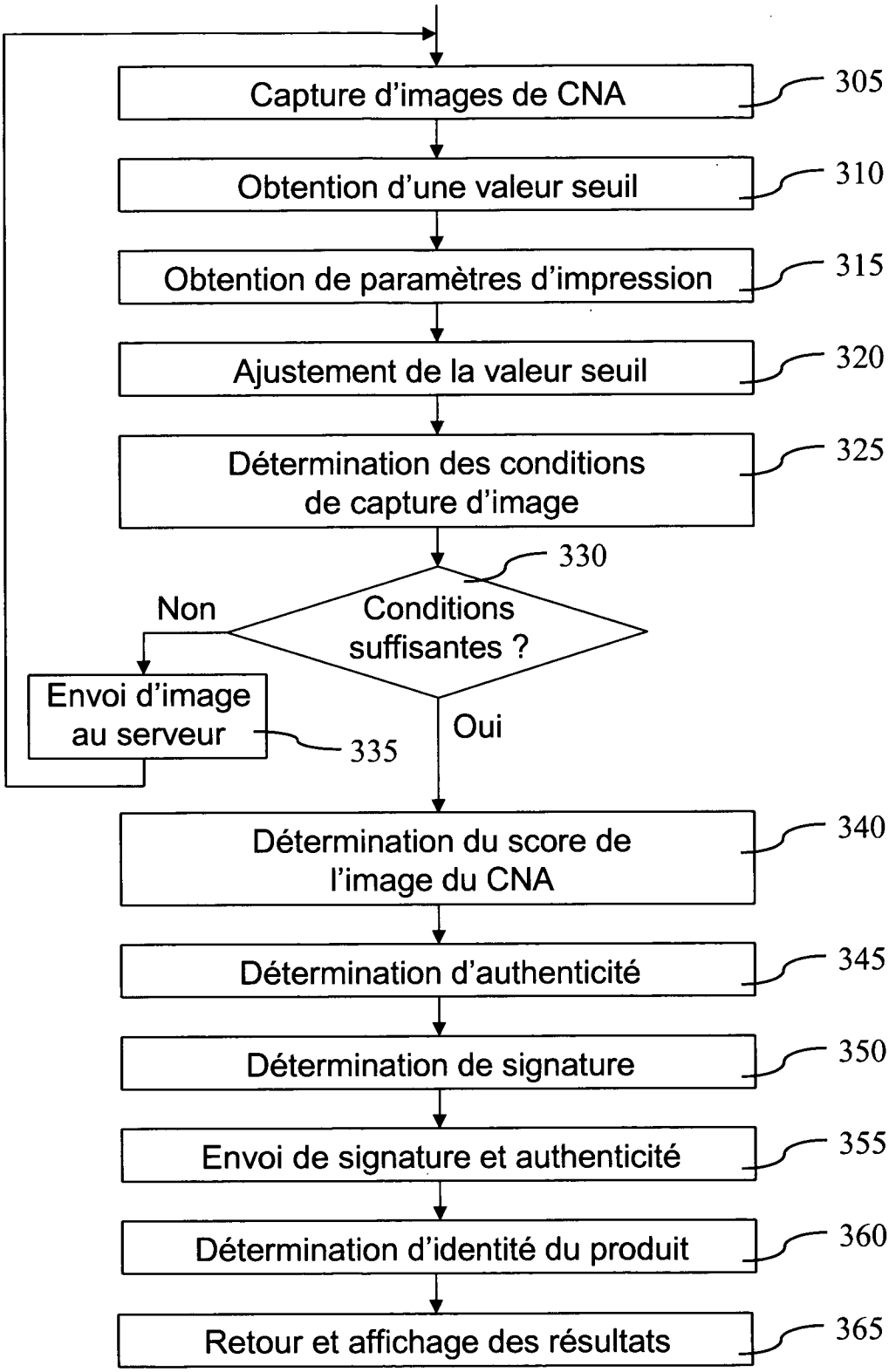
Capture d'images de CNA
305
Obtention d'une valeur seuil
310
Obtention de paramètres d'impression
315
Ajustement de la valeur seuil
320
Détermination des conditions de capture d'image
325
330
Conditions suffisantes ?
Non
Oui
Envoi d'image au serveur
335
Détermination du score de l'image du CNA
340
Détermination d'authenticité
345
Détermination de signature
350
Envoi de signature et authenticité
355
Détermination d'identité du produit
360
Retour et affichage des résultats
365

Figure 3A

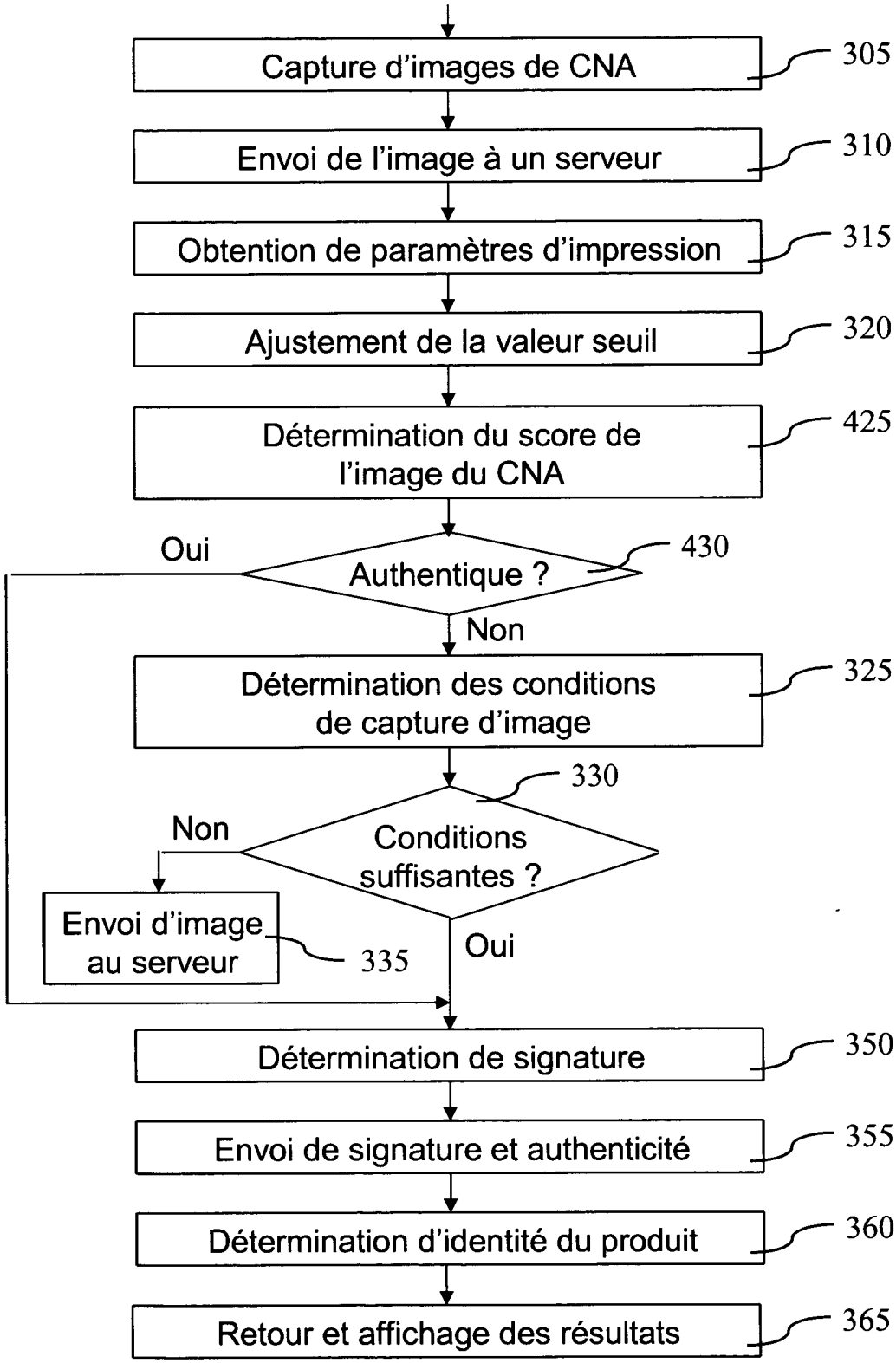
Capture d'images de CNA
305
Envoi de l'image à un serveur
310
Obtention de paramètres d'impression
315
Ajustement de la valeur seuil
320
Détermination du score de l'image du CNA
425
Oui
Authentique ?
430
Non
Détermination des conditions de capture d'image
325
330
Non
Conditions suffisantes ?
Envoi d'image au serveur
335
Oui
Détermination de signature
350
Envoi de signature et authenticité
355
Détermination d'identité du produit
360
Retour et affichage des résultats
365

Figure 3B

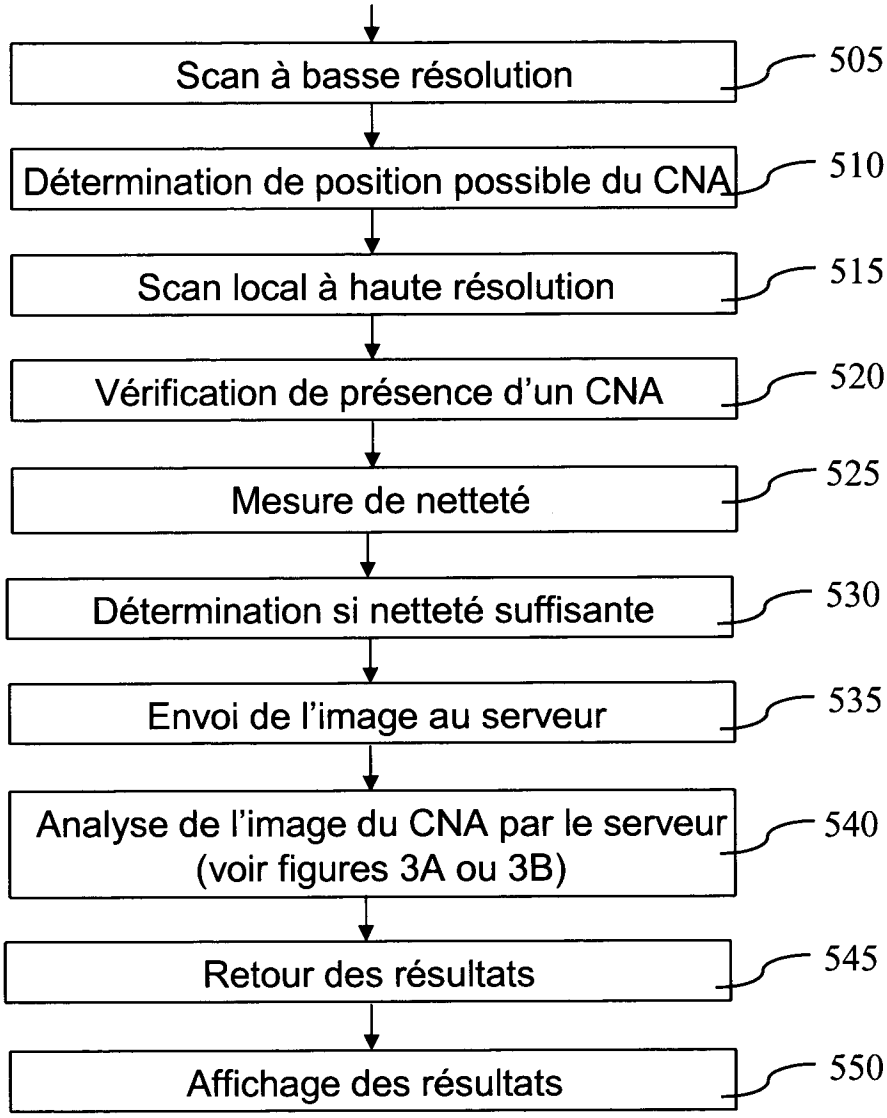
Scan à basse résolution
505
Détermination de position possible du CNA
510
Scan local à haute résolution
515
Vérification de présence d'un CNA
520
Mesure de netteté
525
Détermination si netteté suffisante
530
Envoi de l'image au serveur
535
Analyse de l'image du CNA par le serveur (voir figures 3A ou 3B)
540
Retour des résultats
545
Affichage des résultats
550

Figure 3C

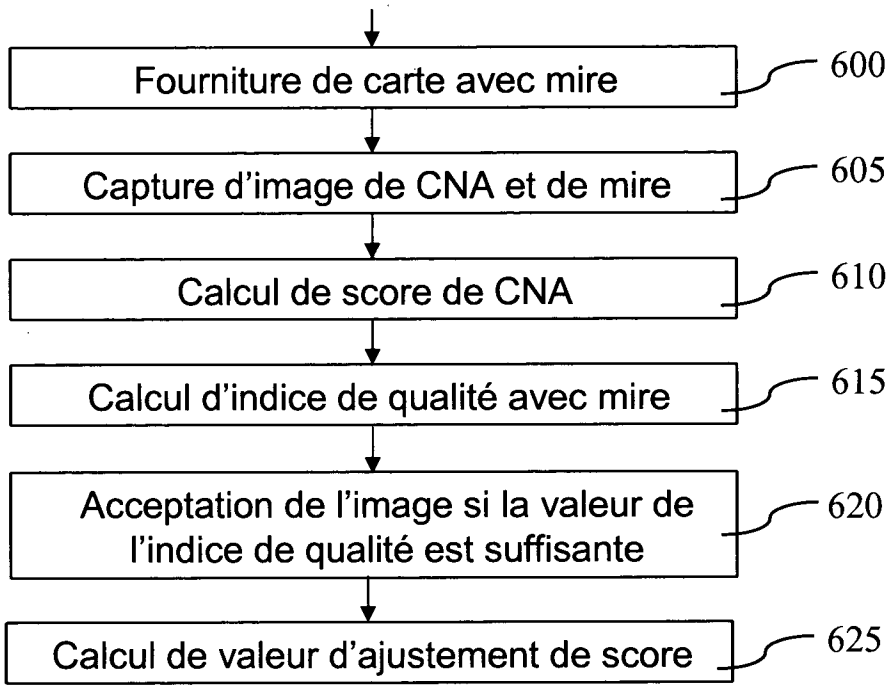
Fourniture de carte avec mire
600
Capture d'image de CNA et de mire
605
Calcul de score de CNA
610
Calcul d'indice de qualité avec mire
615
Acceptation de l'image si la valeur de l'indice de qualité est suffisante
620
Calcul de valeur d'ajustement de score
625

Figure 3D

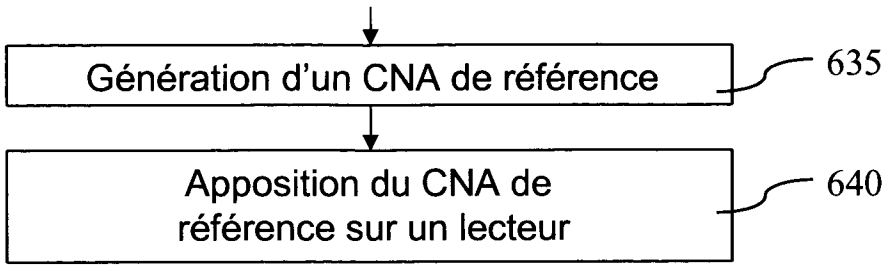

Figure 3E

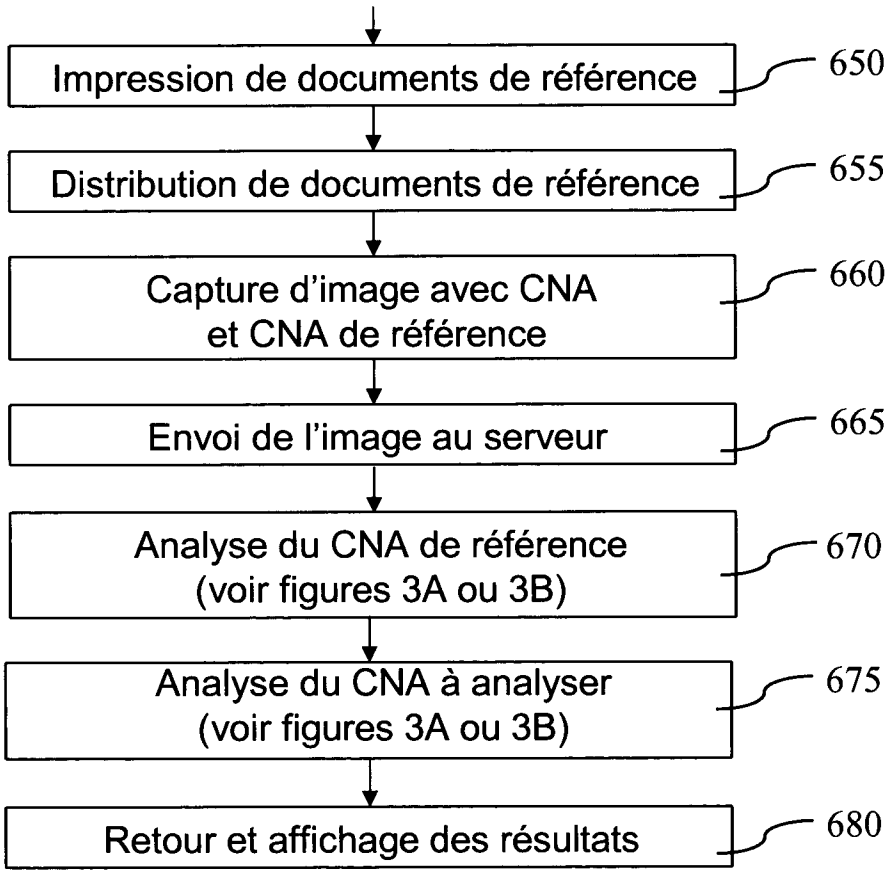

Figure 3F

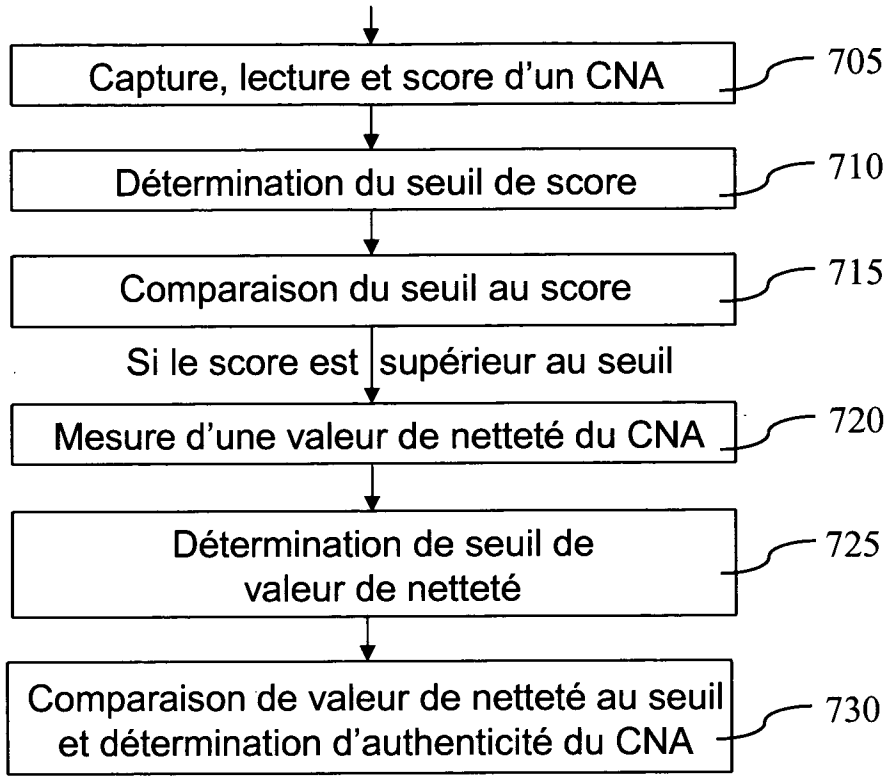

Figure 3G

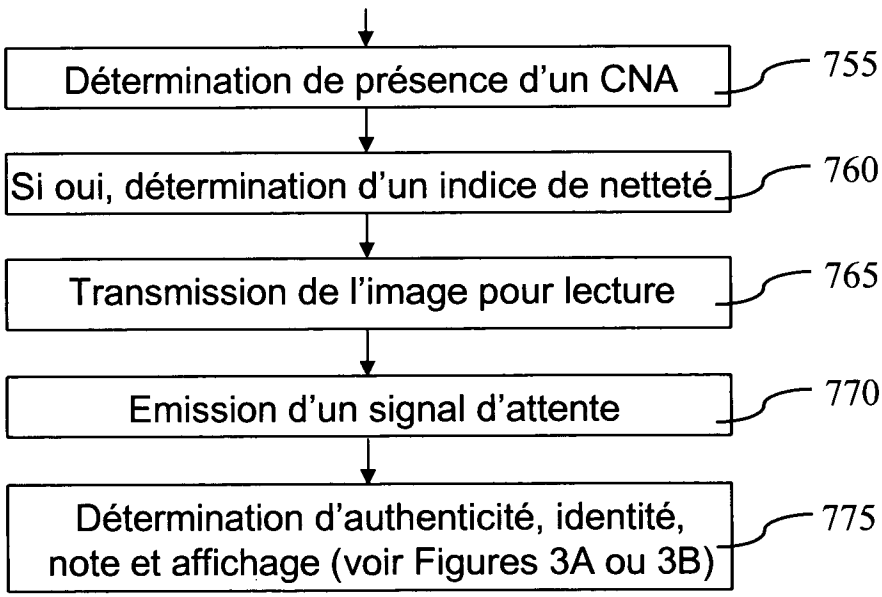

Figure 3H

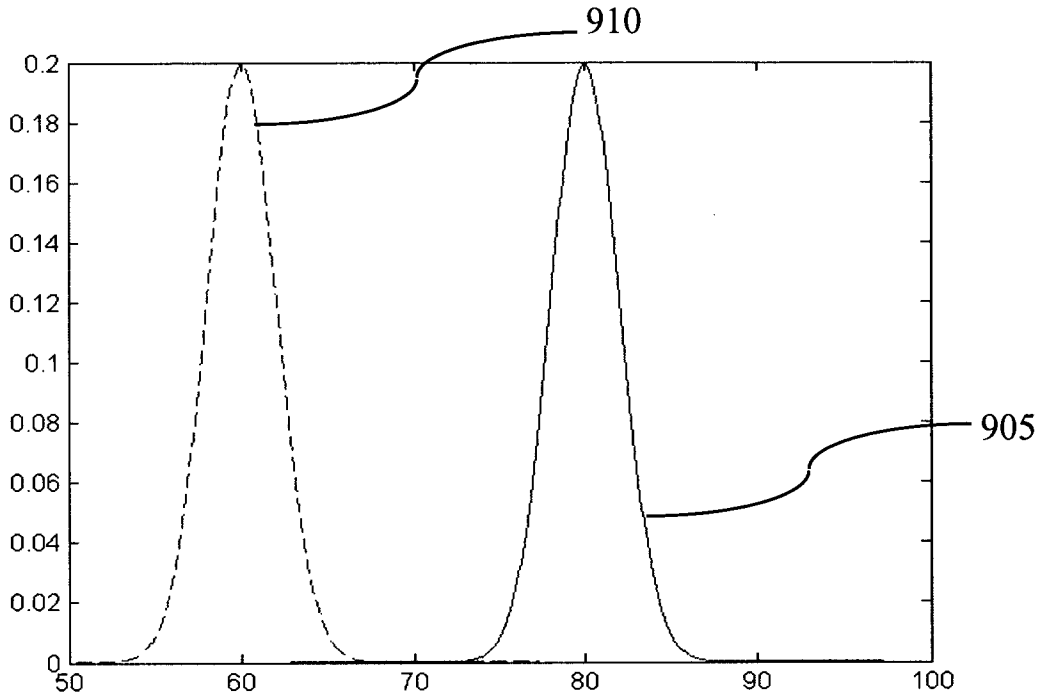

Figure 4

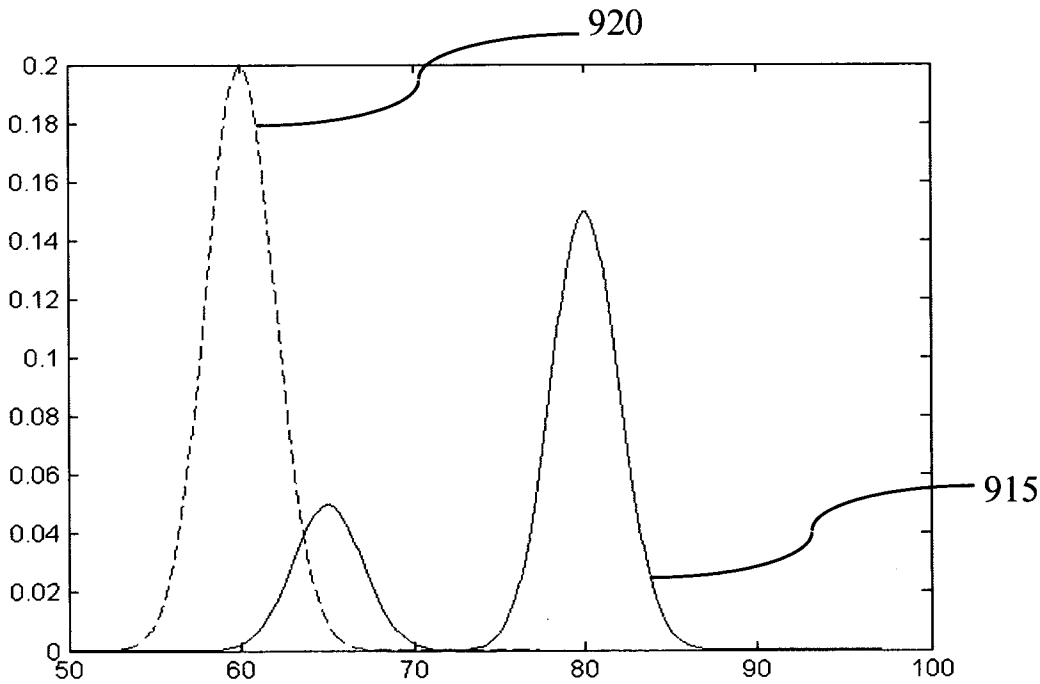

Figure 5

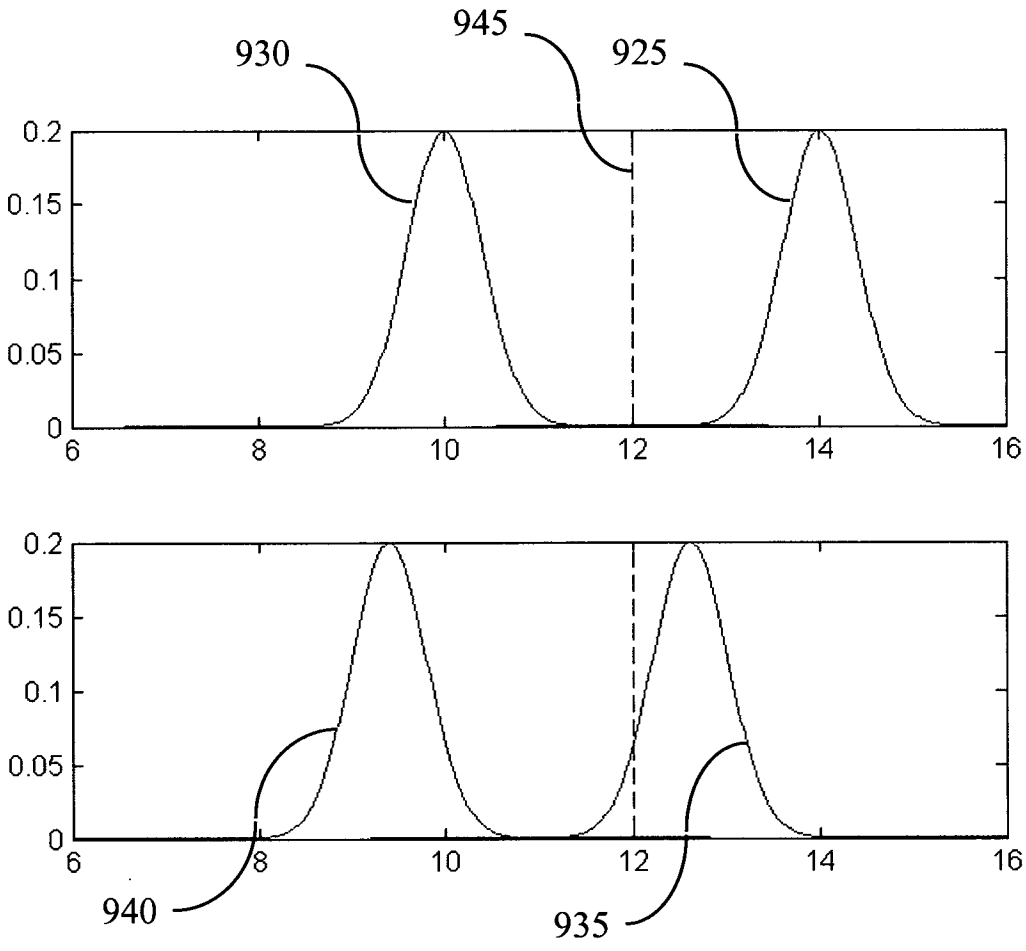

Figure 6

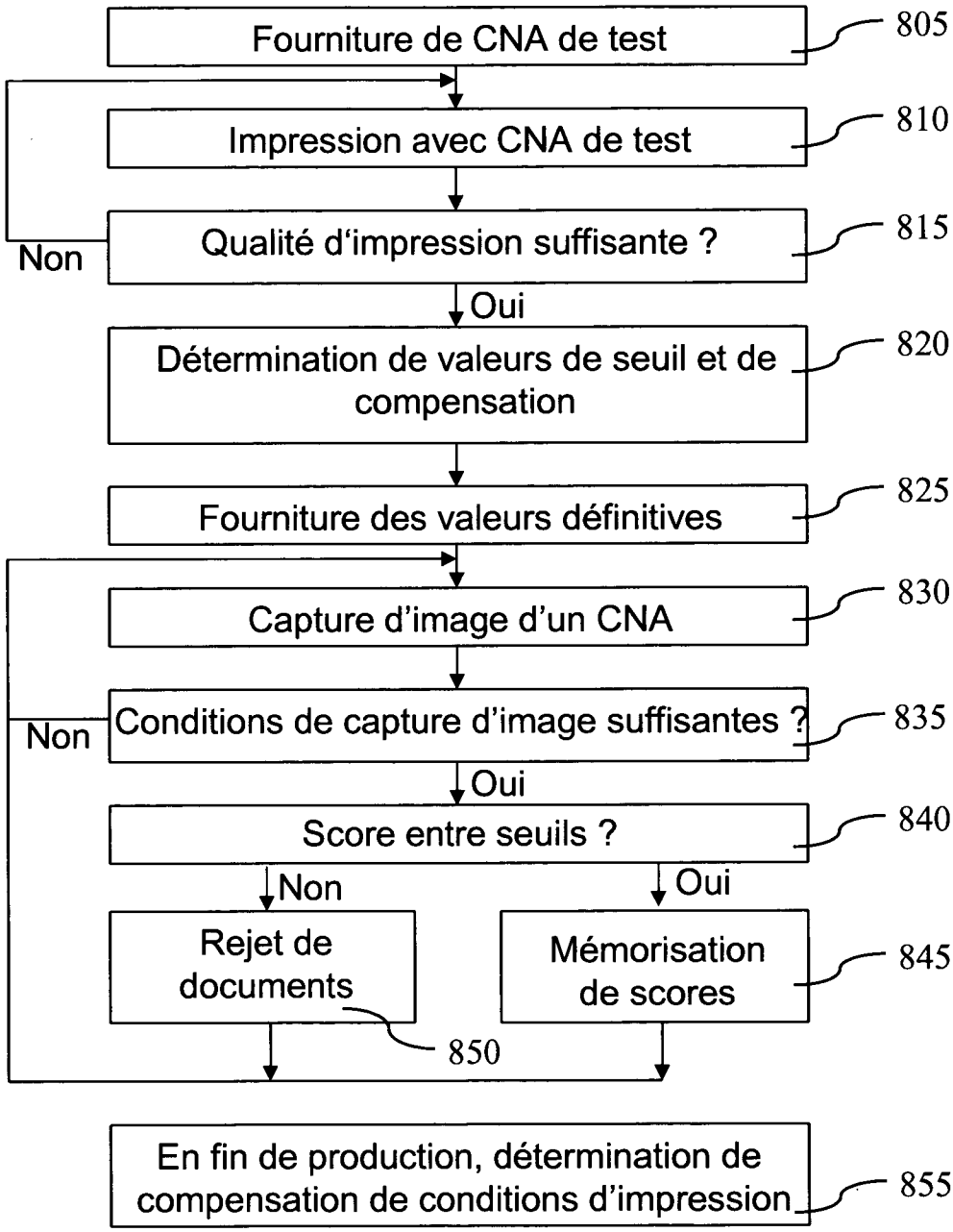
Fourniture de CNA de test
805
Impression avec CNA de test
810
Qualité d'impression suffisante ?
815
Non
Oui
Détermination de valeurs de seuil et de compensation
820
Fourniture des valeurs définitives
825
Capture d'image d'un CNA
830
Conditions de capture d'image suffisantes ?
835
Non
Oui
Score entre seuils ?
840
Non
Oui
Rejet de documents
Mémorisation de scores
845
850
En fin de production, détermination de compensation de conditions d'impression
855

Figure 7A

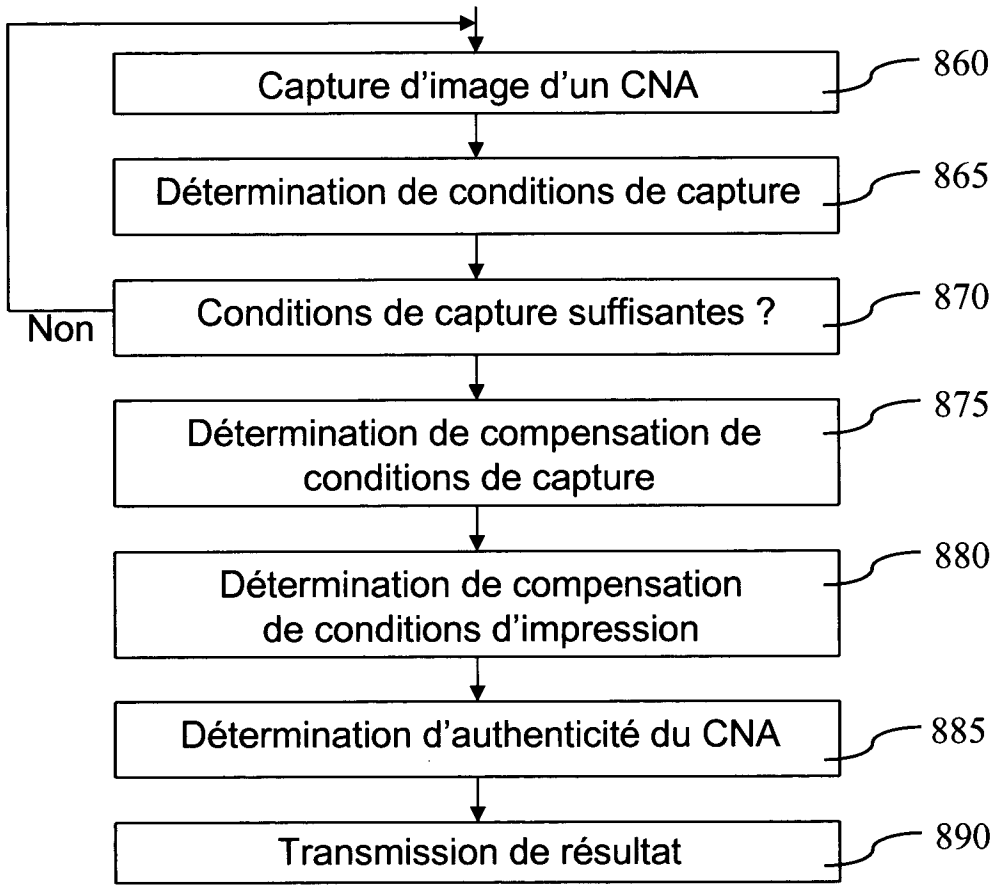
Capture d'image d'un CNA
860
Détermination de conditions de capture
865
Conditions de capture suffisantes ?
870
Non
Détermination de compensation de conditions de capture
875
Détermination de compensation de conditions d'impression
880
Détermination d'authenticité du CNA
885
Transmission de résultat
890

Figure 7B

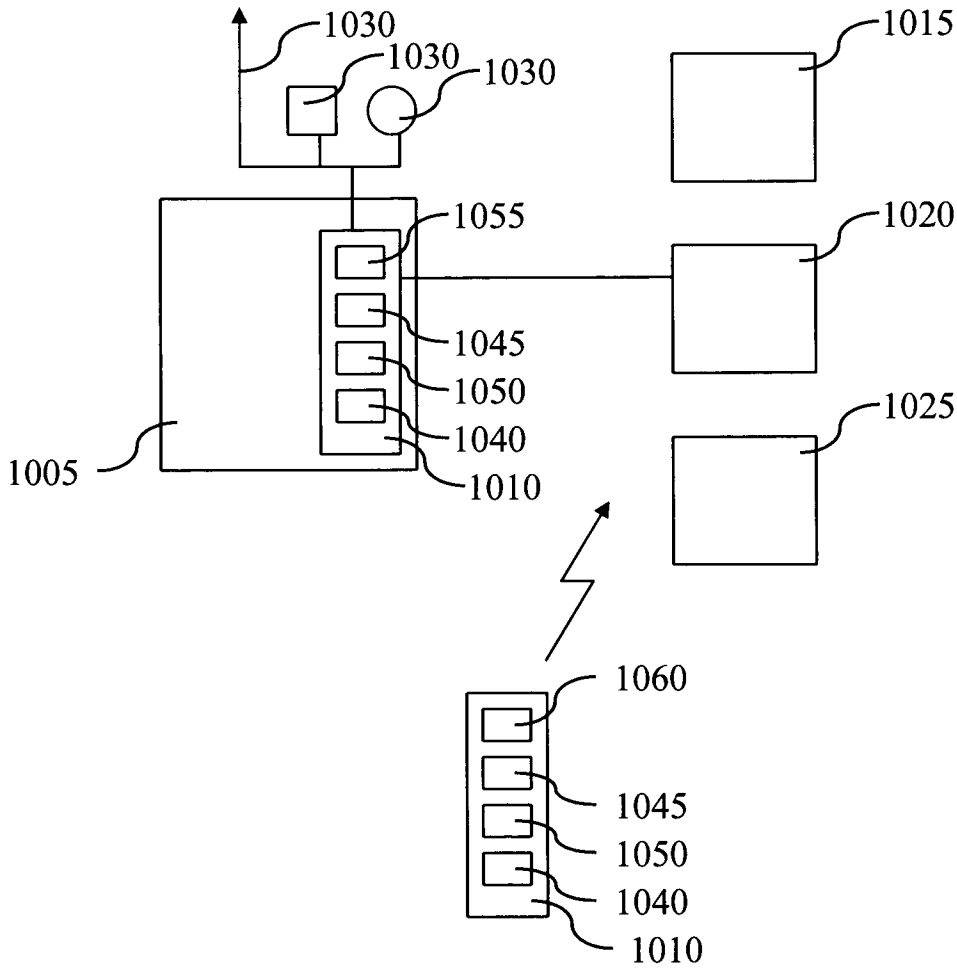
1030
1030
1030
1015
1055
1020
1045
1050
1040
1010
1005
1025
1060
1045
1050
1040
1010

Figure 8

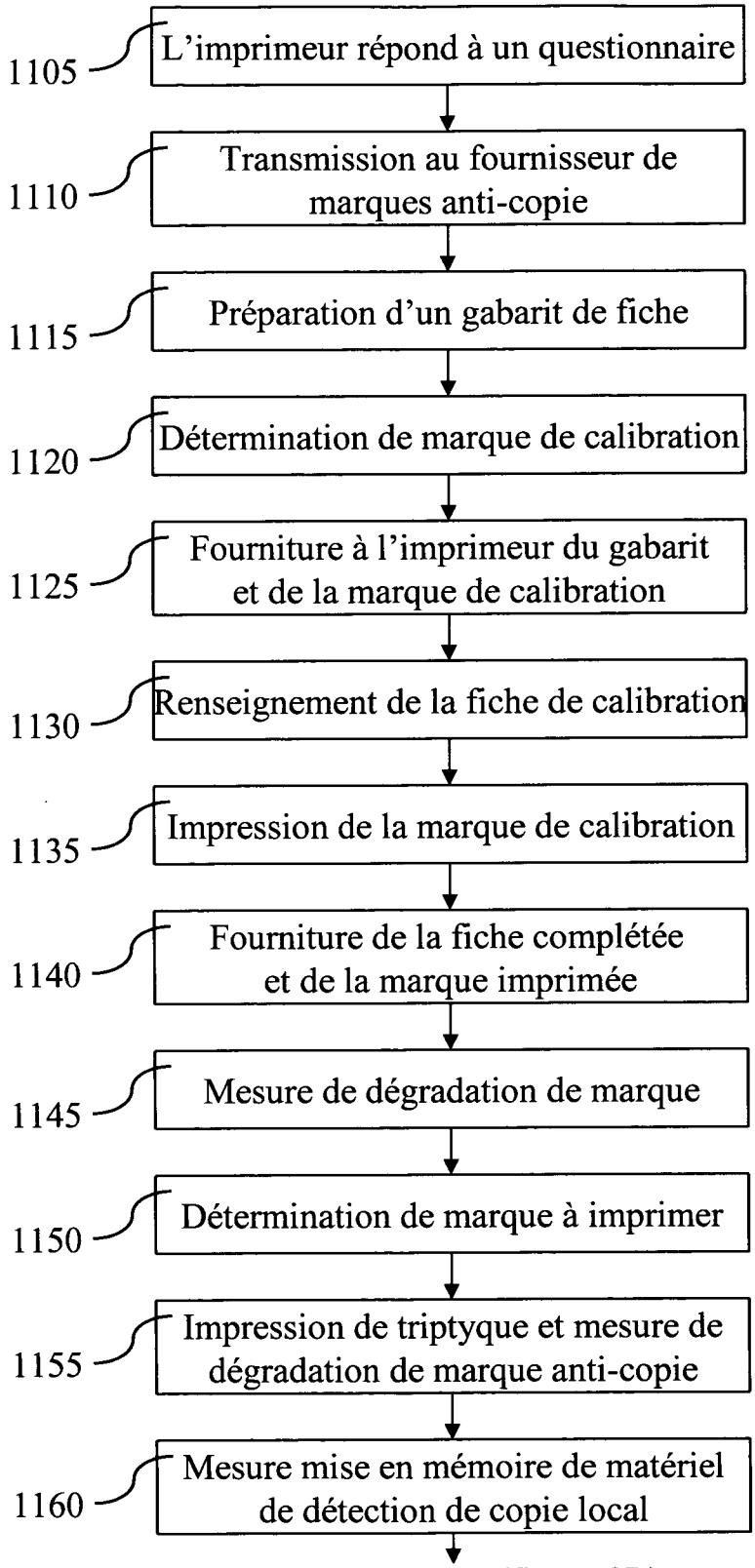
1105
L'imprimeur répond à un questionnaire
1110
Transmission au fournisseur de marques anti-copie
1115
Préparation d'un gabarit de fiche
1120
Détermination de marque de calibration
1125
Fourniture à l'imprimeur du gabarit et de la marque de calibration
1130
Renseignement de la fiche de calibration
1135
Impression de la marque de calibration
1140
Fourniture de la fiche complétée et de la marque imprimée
1145
Mesure de dégradation de marque
1150
Détermination de marque à imprimer
1155
Impression de triptyque et mesure de dégradation de marque anti-copie
1160
Mesure mise en mémoire de matériel de détection de copie local
Vers étape 1165 (figure 9B)

Figure 9A

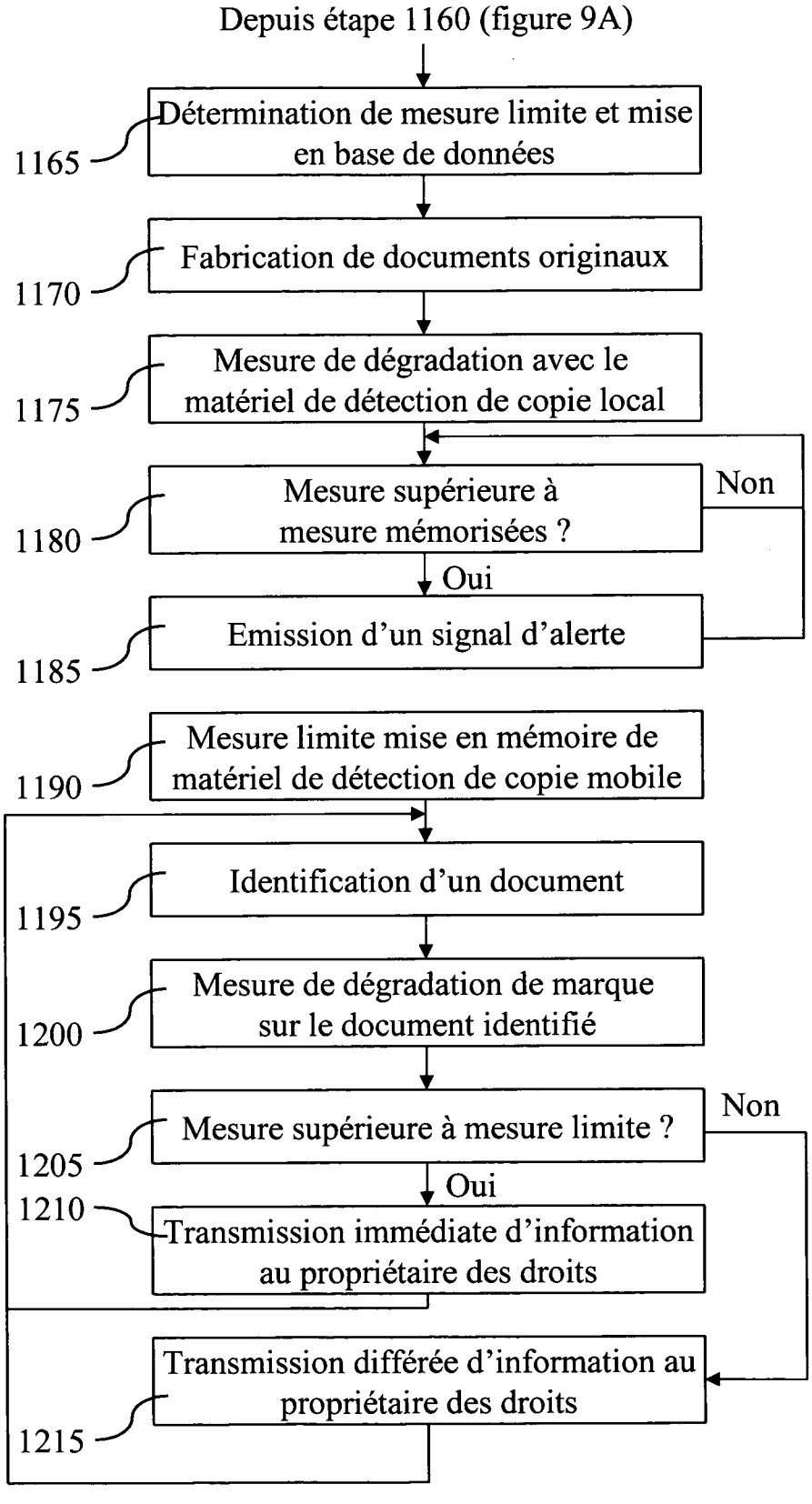
Depuis étape 1160 (figure 9A)
1165
Détermination de mesure limite et mise en base de données
1170
Fabrication de documents originaux
1175
Mesure de dégradation avec le matériel de détection de copie local
1180
Mesure supérieure à mesure mémorisées ?
Non
Oui
1185
Emission d'un signal d'alerte
1190
Mesure limite mise en mémoire de matériel de détection de copie mobile
1195
Identification d'un document
1200
Mesure de dégradation de marque sur le document identifié
1205
Mesure supérieure à mesure limite ?
Non
Oui
1210
Transmission immédiate d'information au propriétaire des droits
1215
Transmission différée d'information au propriétaire des droits

Figure 9B