(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
16 janvier 2025 (16.01.2025)

WIPO | PCT

(10) Numéro de publication internationale
WO 2025/012147 A1

(51) Classification internationale des brevets :
G06T 1/00 (2006.01)

(21) Numéro de la demande internationale :
PCT/EP2024/069075

(22) Date de dépôt international :
05 juillet 2024 (05.07.2024)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
FR2307578 13 juillet 2023 (13.07.2023) FR

(71) Déposant : **THALES** [FR/FR] ; 4 RUE DE LA VERRERIE, 92190 MEUDON (FR).

(72) Inventeurs : **TROYA-GALVIS, Andres** ; Thales Alenia Space, 26 avenue Jean-François Champollion, 31100 TOULOUSE (FR). **NAUD, Caroline** ; Thales Alenia Space, 26 avenue Jean-François Champollion, 31100 TOULOUSE (FR). **SEMLAL, Reda** ; Thales Alenia Space, 26 avenue Jean-François Champollion, 31100 TOULOUSE (FR). **PALLUEL, Luis** ; AKKA Technologies, 7 Boulevard Henri Ziegler, 31700 BLAGNAC (FR). **HUGUES, Romain** ; Thales Alenia Space, 26 avenue Jean-François Champollion, TOULOUSE 31100 (FR). **RAINJONNEAU, Serge** ; Thales Alenia Space, 26 avenue Jean-François Champollion, 31100 TOULOUSE (FR).

(74) Mandataire : **ATOUT PI LAPLACE** ; Immeuble UP ON, 25 Boulevard Romain Rolland, CS 40072, 75685 PARIS CEDEX 14 (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH,

WO 2025/012147 A1

(54) **Title:** METHOD FOR DIGITALLY WATERMARKING AN IMAGE, METHOD FOR EXTRACTING A DIGITAL WATERMARK AND METHOD FOR DETECTING FALSIFICATION OF A WATERMARKED IMAGE

(54) **Titre :** MÉTHODE DE TATOUAGE NUMÉRIQUE D'UNE IMAGE, MÉTHODE D'EXTRACTION D'UN TATOUAGE NUMÉRIQUE ET MÉTHODE DE DÉTECTION DE FALSIFICATION D'UNE IMAGE TATOUÉE

[Fig. 2]

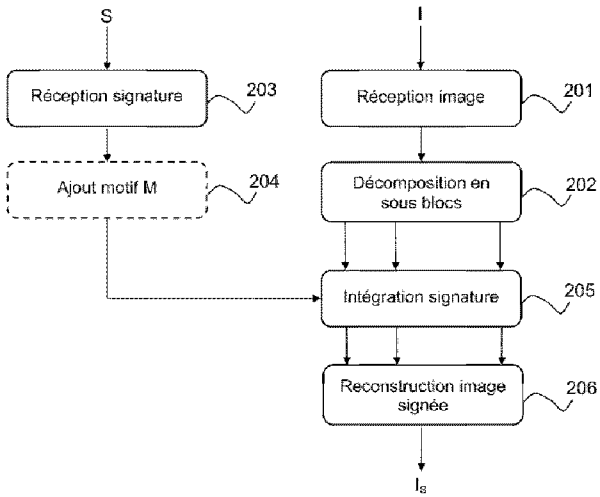


FIG.2

201 Receiving the image
202 Decomposing the image into sub-blocks
203 Receiving the signature
204 Adding the pattern M
205 Integrating the signature
206 Reconstructing the signed image

(57) **Abstract:** The invention relates to a computer-implemented method for digitally watermarking an image, the method comprising the steps of: - receiving (201) a digital image; - decomposing (202) the digital image into a plurality of sub-blocks having the same predefined dimensions; - generating (203) a digital binary signature; - for each sub-block; i transforming the sub-block into an intermediate space via a predetermined transform; ii. combining the signature with the sub-block in the intermediate space to obtain a signed sub-block in the intermediate space; iii. applying an inverse transform, which is the inverse of the predetermined transform, to the signed sub-block; - concatenating (206) the set of signed sub-blocks to form a signed image.

(57) **Abrégé :** Méthode, mise en œuvre par ordinateur, de tatouage numérique d'une image comprenant les étapes de : - Recevoir (201) une image numérique, - Décomposer (202) l'image numérique en une pluralité de sous-blocs de mêmes dimensions prédéfinies, - Générer (203) une signature binaire numérique, - Pour chaque sous-bloc, i. Transformer le sous-bloc dans un espace intermédiaire via une transformée prédéterminée, ii. Combiner la signature avec le sous-bloc dans l'espace intermédiaire pour obtenir un sous-bloc signé dans l'espace intermédiaire, iii. Appliquer au sous-bloc signé une transformée inverse à la transformée prédéterminée, - Concaténer (206) l'ensemble des sous-blocs signés pour former une image signée.

[Suite sur la page suivante]

TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) **États désignés** *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Publiée:

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

DESCRIPTION

Titre de l'invention : Méthode de tatouage numérique d'une image, méthode d'extraction d'un tatouage numérique et méthode de détection de falsification d'une image tatouée

[0001] L'invention concerne le domaine du suivi d'intégrité d'images numériques, en particulier d'images acquises par un satellite d'observation de la Terre.

[0002] L'invention porte plus précisément sur une méthode de tatouage numérique d'une image, une méthode d'extraction d'un tatouage et une méthode de détection de falsification d'une image tatouée.

[0003] Dans le contexte de l'accroissement des quantités de données, en particulier d'images, transmises via des systèmes de transmission numérique, il existe un besoin général pour détecter les atteintes volontaires ou non à l'intégrité des images reçues.

[0004] En particulier, dans le domaine des transmissions d'images acquises par un satellite d'observation de la Terre, ce besoin est particulièrement présent car les images acquises peuvent transiter par différents équipements, réseaux de communications et plateformes de transmission.

[0005] Dans ce contexte, les possibilités d'atteinte à l'intégrité des images augmentent et il est impératif pour un utilisateur de pouvoir vérifier cette intégrité avant l'utilisation finale des images.

[0006] Un problème plus spécifique concerne la localisation, dans l'image, d'une falsification de l'image, c'est-à-dire la capacité à identifier quelle zone d'une image a été falsifiée.

[0007] Un autre problème spécifique concerne la robustesse d'une méthode de tatouage numérique à certaines transformations dites classiques telles que les transformations de découpage ou recadrage d'une image.

[0008] Différentes solutions existent dans l'état de l'art pour adresser le sujet de l'intégrité des images.

[0009] Une première solution connue consiste à calculer, au moment de la production ou de la livraison de l'image une clé unique de longueur fixe représentant

précisément un objet d'origine et ses caractéristiques. Cette clé peut être recalculée au moment de la vérification d'intégrité de l'image et comparée à la clé d'origine pour en déduire si une modification a eu lieu sur l'image. Cette première méthode présente l'avantage d'une faible complexité cependant elle a plusieurs inconvénients. Tout d'abord, elle n'est robuste à aucune transformation opérée sur l'image. La moindre modification de l'image telle qu'un découpage ou un miroir entraine une clé différente et donc conduit à détecter une falsification de l'image alors que celle-ci a uniquement subi une transformation acceptable.

[0010] Un autre inconvénient est que cette méthode implique un calcul sur l'image entière ce qui ne permet pas de localiser les zones de l'image affectées par une falsification.

[0011] Une deuxième solution connue consiste à appliquer un tatouage numérique sur une image entière. En cas de modification de l'image, le tatouage est altéré de façon visible et permet de détecter les falsifications. L'inconvénient principal de cette méthode est qu'elle altère visuellement et fonctionnellement l'utilisabilité de l'image. Un autre inconvénient est que cette méthode ne permet pas de localiser une falsification dans une zone locale de l'image.

[0012] Une troisième solution connue consiste à analyser le contenu de l'image reçue et à comparer à un attendu statistique pour évaluer la probabilité d'authenticité de l'information contenue dans l'image. Cette solution ne s'applique pas à tous les domaines techniques car elle suppose des a priori forts sur le contenu des images traitées et les falsifications éventuellement appliquées à l'image.

[0013] L'invention consiste en une nouvelle méthode de tatouage numérique qui consiste en l'intégration d'un tatouage sur chaque sous-bloc d'une grille appliquée à l'image de manière à permettre une localisation de falsification dans l'image.

[0014] L'invention porte également sur une méthode d'extraction du tatouage numérique ainsi qu'une méthode de localisation de falsification qui ne nécessite pas de tatouage de référence.

[0015] Avantageusement, l'invention s'appuie sur un moteur d'intelligence artificielle pour réaliser l'apprentissage des fonctions de tatouage et d'extraction de tatouage.

[0016] La méthode proposée présente notamment l'avantage d'être robuste aux opérations de découpage ou recadrage d'une image.

[0017] L'invention s'applique avantageusement à la vérification d'intégrité d'images satellites d'observations de la Terre.

[0018] L'invention a pour objet une méthode, mise en œuvre par ordinateur, de tatouage numérique d'une image comprenant les étapes de :

- Recevoir une image numérique,
- Décomposer l'image numérique en une pluralité de sous-blocs de mêmes dimensions prédéfinies,
- Générer une signature binaire numérique,
- Pour chaque sous-bloc,
    i. Transformer le sous-bloc dans un espace intermédiaire via une transformée prédéterminée,
    ii. Combiner la signature avec le sous-bloc dans l'espace intermédiaire pour obtenir un sous-bloc signé dans l'espace intermédiaire,
    iii. Appliquer au sous-bloc signé une transformée inverse à la transformée prédéterminée,
- Concaténer l'ensemble des sous-blocs signés pour former une image signée.

[0019] Dans une variante de réalisation, la méthode de tatouage numérique selon l'invention comprend en outre les étapes de :

- Ajouter à la signature binaire numérique un motif binaire,
- Transformer la signature binaire en une matrice de dimensions inférieures aux dimensions d'un sous-bloc,
- Le motif binaire étant inséré dans la signature binaire de sorte à être positionné sur des positions prédéfinies de la matrice identiques pour chaque sous-bloc

[0020] Selon un aspect particulier de l'invention, le motif binaire est positionné sur au moins trois zones de la matrice correspondant à trois coins d'un carré, par exemple trois coins de la matrice.

[0021] Selon un aspect particulier de l'invention, l'étape de combiner la signature avec un sous-bloc est réalisée au moyen d'un premier moteur d'intelligence artificielle entrainé pour minimiser l'impact visuel d'une signature sur une image signée.

[0022] L'invention a aussi pour objet une méthode, mise en œuvre par ordinateur, d'extraction d'un tatouage numérique comprenant les étapes de :

- Recevoir une image numérique signée au moyen de la méthode de tatouage numérique selon l'invention,
- Décomposer l'image numérique en une pluralité de sous-blocs de mêmes dimensions utilisées pour générer l'image numérique signée,
- Pour chaque sous-bloc,
    i. Extraire la signature binaire tatouée dans le sous-bloc

[0023] Selon un aspect particulier de l'invention, l'étape d'extraire la signature binaire d'un sous bloc est réalisée au moyen d'un second moteur d'intelligence artificielle entrainé pour minimiser un écart entre la signature binaire générée à l'origine et la signature binaire extraite d'un sous bloc.

[0024] Selon un aspect particulier de l'invention, le premier moteur d'intelligence artificielle et le second moteur d'intelligence artificielle sont entrainés conjointement.

[0025] Dans une variante de réalisation, la méthode d'extraction d'un tatouage numérique selon l'invention comprend en outre les étapes de :

- Détecter, pour au moins un sous-bloc, un motif binaire inséré dans la signature extraite,
- Comparer les positions du motif binaire détecté à un ensemble de positions attendues et si elles diffèrent des positions attendues, en déduire que l'image numérique reçue a subi une opération de découpage,
- Reconstruire la signature binaire associée à l'image avant opération de découpage à partir des positions du motif binaire en appliquant à la signature numérique une opération inverse à l'opération de découpage

[0026] L'invention a encore pour objet une méthode, mise en œuvre par ordinateur, de détection de falsification d'une image tatouée numériquement au moyen de la méthode de tatouage numérique selon l'invention, la méthode comprenant les étapes de:

- Exécuter la méthode d'extraction d'un tatouage numérique pour une image reçue selon l'invention,
- Rechercher, pour l'ensemble des sous-blocs de l'image, la signature extraite majoritaire parmi cet ensemble,
- pour chaque sous-bloc,
    i. comparer la signature extraite pour le sous-bloc à la signature majoritaire et,
    ii. en déduire si le sous-bloc de l'image a été falsifié ou non

[0027] Selon un aspect particulier de l'invention, l'image numérique est une image acquise par un satellite.

[0028] L'invention a aussi pour objet un programme d'ordinateur comportant des instructions pour l'exécution de la méthode selon l'invention, lorsque le programme est exécuté par un processeur.

[0029] L'invention a aussi pour objet un support d'enregistrement lisible par un processeur sur lequel est enregistré un programme comportant des instructions pour l'exécution de la méthode selon l'invention, lorsque le programme est exécuté par un processeur.

[0030] D'autres caractéristiques et avantages de la présente invention apparaîtront mieux à la lecture de la description qui suit en relation aux dessins annexés suivants.

[0031] [Fig. 1] représente un schéma de principe général d'une méthode de tatouage numérique selon l'art antérieur,

[0032] [Fig. 2] représente un schéma d'une méthode de tatouage numérique selon un mode de réalisation de l'invention,

[0033] [Fig. 3] représente un schéma d'une méthode d'extraction d'un tatouage numérique selon un mode de réalisation de l'invention,

[0034] [Fig. 4] représente un schéma d'un moteur d'intelligence artificielle entrainé pour réaliser une première fonction de tatouage numérique et une seconde fonction d'extraction de tatouage numérique selon un mode de réalisation de l'invention,

[0035] [Fig. 5] représente un exemple de modèle d'intelligence artificielle entrainé pour réaliser la première fonction de tatouage numérique,

[0036] [Fig. 6] représente un exemple de modèle d'intelligence artificielle entrainé pour réaliser la seconde fonction d'extraction de tatouage numérique,

[0037] [Fig. 7] représente un organigramme détaillant les étapes de mise en œuvre d'une méthode de détection de falsification selon un mode de réalisation de l'invention,

[0038] [Fig. 8a] représente pour le même exemple, le tatouage numérique extrait si aucun découpage de l'image n'a eu lieu,

[0039] [Fig. 8b] représente un exemple de tatouage numérique extrait suite à une opération de découpage d'une image,

[0040] [Fig. 9a] représente un premier exemple de motif combiné à un tatouage numérique selon un mode de réalisation de l'invention,

[0041] [Fig. 9b] représente un second exemple de motif combiné à un tatouage numérique selon un mode de réalisation de l'invention,

[0042] La figure 1 illustre un schéma de principe d'une méthode de tatouage numérique d'une image pour vérifier l'intégrité de l'image.

[0043] Le principe du tatouage numérique ou « watermarking » en anglais est d'intégrer dans une image I un tatouage ou signature binaire qui soit non visible au sens où elle n'altère pas le contenu de l'image mais qui est modifiée lorsqu'une falsification de l'image est réalisée au cours de la chaine de transmission.

[0044] Sur la figure 1, on a représenté une image I qui est projetée dans un espace particulier au moyen d'une transformation donnée, par exemple une transformée de Fourier, une transformée DCT ou autre pour obtenir une image transformée I'.

[0045] Un tatouage ou signature binaire W est ensuite combiné à l'image transformée I' pour obtenir une image tatouée I'_t. L'image tatouée I'_t dans l'espace de transformation est ensuite convertie dans l'espace initial via une transformation inverse pour obtenir l'image signée I_t.

[0046] Pour extraire la signature W de l'image tatouée I_t, les opérations inverses sont appliquées, c'est à dire qu'on transforme l'image tatouée dans l'espace de transformation puis on applique l'opération inverse à l'opération de combinaison pour récupérer la signature.

[0047] Il est ensuite possible de comparer la signature extraite à la signature d'origine pour détecter une falsification de l'image.

[0048] L'opération de combinaison peut prendre différentes formes mais doit être robuste à certaines opérations de traitement d'image, par exemple les opérations de découpage ou « cropping » en anglais. Autrement dit, une opération de découpage de l'image tatouée I_t ne doit pas altérer la signature enfouie dans l'image.

[0049] L'invention concerne une méthode particulière de tatouage numérique qui permet notamment la localisation dans l'image d'une falsification.

[0050] La figure 2 représente un organigramme détaillant les étapes d'une méthode de tatouage numérique selon un mode de réalisation de l'invention.

[0051] La méthode débute à l'étape 201 par la réception d'une image numérique qui est, par exemple, une image d'observation de la Terre acquise par un satellite. La méthode de tatouage peut être appliquée par exemple dans une station sol appartenant à un segment sol d'un système de communications par satellite ou dans un serveur déporté.

[0052] L'image peut être une image à un seul canal ou une image multi-spectrales comprenant plusieurs canaux à différentes longueurs d'ondes.

[0053] A l'étape 202, on applique une décomposition de l'image en sous-blocs de dimensions identiques selon une grille de découpage de l'image prédéterminée. Les dimensions des sous-blocs sont choisies a priori en fonction de contraintes liées au stockage des données et à la complexité des traitements mais aussi

selon le niveau de granularité souhaité pour localiser l'impact d'une falsification de l'image.

[0054] A l'étape 203, on reçoit une signature binaire S ou tatouage qui contient par exemple des informations utiles. Cette signature est ensuite intégrée à chaque sous- bloc à l'étape 205 selon un processus de tatouage numérique tel que décrit à la figure 1. Une différence notable est que l'opération de tatouage n'est pas appliquée à l'image I entière mais à chaque sous-bloc dans lequel est intégrée la même signature.

[0055] Ensuite à l'étape 206, on reconstruit l'image signée en agrégeant tous les sous-blocs tatoués selon la même grille de décomposition utilisée à l'étape 202.

[0056] La figure 3 représente un organigramme détaillant les étapes d'une méthode d'extraction de signatures d'une image tatouée numériquement, selon un mode de réalisation de l'invention.

[0057] La méthode de la figure 3 débute avec la réception 301 d'une image I_t qui a été tatouée au moyen de la méthode de tatouage de la figure 2. A l'étape 302, l'image est décomposée en sous-blocs selon la même grille de découpage utilisée pour tatouer l'image. Ensuite, à l'étape 303, une signature est extraite de chaque sous-bloc au moyen d'une procédure d'extraction de signature qui met en œuvre des opérations inverses à celles utilisées pour tatouer l'image.

[0058] On obtient in fine un nombre N de signatures, où N est le nombre de blocs de l'image.

[0059] Une étape 304 de détection de falsification peut ensuite être appliquée en comparant ces signatures entre elles puisque ces signatures sont censées être toutes identiques si l'image n'a pas été falsifiée.

[0060] La figure 4 divulgue un exemple particulier de mise en œuvre des étapes d'intégration d'une signature dans un sous bloc (étape 205) et d'extraction des signatures d'un sous bloc (étape 303).

[0061] Dans un mode de réalisation particulier de l'invention, la technique de tatouage numérique est basée sur l'emploi de deux moteurs d'intelligence artificielle. Le premier moteur d'intelligence artificielle est entrainé pour apprendre à réaliser une fonction d'intégration d'une signature binaire dans une image de

manière à minimiser l'impact visuel de la signature sur l'image. Le second moteur d'intelligence artificielle est entrainé pour apprendre à réaliser une fonction d'extraction d'une signature d'une image tatouée de manière à reconstruire au mieux la signature initiale.

[0062] Un exemple d'un ensemble de deux moteurs d'intelligence artificielle entrainés conjointement est décrit à la figure 4.

[0063] Une image I est reçue en entrée puis décomposée en sous blocs B_i. Chaque sous-bloc est produit en entrée d'un premier réseau R1 de type encodeur chargé de transformer chaque sous bloc dans un espace latent.

[0064] Une signature S binaire est reçue en entrée, elle est transformée en une matrice W de taille au plus égale à celle d'un sous bloc. La signature matricielle W est ensuite concaténée, via une opération de concaténation C, au vecteur de sortie du premier réseau encodeur R1, puis l'ensemble est fourni à un second réseau R2 de type décodeur qui décode les informations de l'espace latent pour obtenir un sous bloc signé Bs_i. Une fonction de cout F1 est utilisée pour l'apprentissage du réseau auto-encodeur constitué de R1 et R2. Cette fonction de cout est, par exemple, définie par une minimisation d'une erreur entre un sous bloc signé Bs_i et un sous bloc d'origine B_i.

[0065] Un troisième réseau R3 est entrainé pour extraire une signature d'un bloc signé Bs_i pour retrouver une signature extraite Se.

[0066] Dans une variante de réalisation, le troisième réseau R3 est entrainé en appliquant certaines perturbations aux blocs en entrée afin d'encourager un apprentissage robuste. Les perturbations correspondent à des altérations de l'image qui pourraient être réalisées par un tiers. Par exemple, il peut s'agir de l'ajout de différents types de bruit, d'un changement d'intensité ou de contraste dans l'image, d'une compression de l'image ou encore d'une transformation géométrique telle qu'une rotation ou une mise à l'échelle.

[0067] Une seconde fonction de cout F2 est utilisée pour l'entrainement du troisième réseau R3, par exemple définie par une erreur entre la signature extraite Se et la signature d'origine S.

[0068] Avantageusement l'entrainement des trois réseaux R1,R2,R3 est réalisé conjointement à partir d'une base de données d'images, par exemple des images

satellites, en produisant en entrée du premier réseau R1 des sous blocs choisis aléatoirement dans chaque image.

[0069] Un objectif de l'apprentissage de ces réseaux est notamment une robustesse à certaines transformations de l'image, telles que par exemple une transformation miroir, une invisibilité de la signature enfouie dans l'image, une absence d'impact fonctionnel sur l'utilisabilité de l'image mais aussi une capacité minimum des quantités de données pouvant être inclues dans la signature.

[0070] Différents algorithmes d'intelligence artificielle peuvent être utilisés pour réaliser les réseaux R1,R2,R3. Un exemple de modèles d'intelligence artificielle compatible du système décrit à la figure 4 est présenté aux figures 5 et 6. Il est basé sur le modèle décrit dans la référence [1].

[0071] Le schéma de la figure 5 représente un exemple de réseau de neurones artificiels auto-encodeur pour réaliser les réseaux R1 et R2 de la figure 4.

[0072] Il est composé d'une première couche de convolution 501 à paramètres fixes pour transformer un bloc d'une image dans un espace latent, une opération de concaténation C pour concaténer une signature S à l'image transformée, un réseau de neurones artificiels 502 et une seconde couche de convolution 503 à paramètres fixes pour transformer le résultat obtenu vers l'espace image.

[0073] Le réseau 502 est entrainé pour apprendre à intégrer la signature dans l'image sans impact visuel. Il est par exemple composé de plusieurs couches de convolutions successives.

[0074] La figure 6 décrit un exemple de réseau de neurones artificiels pour réaliser le réseau R3 de la figure 4.

[0075] Il est composé d'une première couche de convolution 601 à paramètres fixes puis un ensemble de couches de convolution 602 dont les paramètres sont appris pour extraire une signature Se d'un bloc signé Bs.

[0076] Sans sortir du cadre de l'invention, tout autre modèle d'intelligence artificielle entrainable pour apprendre à réaliser les deux fonctions précitées peut être utilisé en remplacement des réseaux de neurones décrits aux figures 5 et 6.

[0077] La figure 7 représente, sur un organigramme, les étapes de mise en œuvre d'une méthode de détection et localisation de falsification dans une image selon

un mode de réalisation de l'invention. Cette méthode correspond à un exemple de réalisation de l'étape 304 de la méthode de la figure 3.

[0078] La méthode de la figure 7 débute à l'étape 701 avec l'extraction de N signatures correspondants à N sous-blocs d'une image telle que décrite à la figure 3.

[0079] A l'étape 702, on recherche la signature dominante parmi les N signatures extraites. La signature dominante ou majoritaire est la signature la plus présente parmi les N signatures extraites. Pour réaliser l'étape 702, on compare les N signatures entre elles et on les regroupe par groupes de signatures identiques. Le groupe contenant le plus grand nombre de signatures identiques correspond au groupe majoritaire.

[0080] Les étapes suivantes 703 à 707 sont exécutées pour chaque sous-bloc de l'image.

[0081] A l'étape 703 on compare la signature extraite du sous-bloc d'indice i à la signature dominante. Si ces deux signatures sont identiques, on en déduit à l'étape 704 que le sous-bloc d'indice i n'a pas été falsifié. Dans le cas contraire, on calcule, à l'étape 705, la différence entre les deux signatures puis on compare, à l'étape 706, cette différence à un seuil de détection prédéfini. Si la différence est inférieure ou égale au seuil, on retourne à l'étape 704 pour conclure que le sous-bloc d'indice i n'a pas été falsifié. Dans le cas contraire, on passe à l'étape 707 pour signaler le sous-bloc d'indice i comme un sous-bloc falsifié.

[0082] Les étapes 703 à 707 sont itérées pour tous les sous-blocs de l'image.

[0083] Une étape 708 optionnelle permet de générer une carte de falsification indiquant quels sous blocs de l'image ont été falsifiés.

[0084] Ainsi, la méthode de la figure 7 permet de localiser précisément les zones de l'image qui ont été falsifiées à la différence des méthodes globales qui intègrent une seule signature dans une image.

[0085] On décrit à présent un mode de réalisation particulier de l'invention qui permet de rendre la technique proposée robuste aux opérations de découpage ou « cropping » en anglais sur une image.

[0086] La figure 8a illustre un exemple de signature ou tatouage représenté sous la forme d'une matrice. Selon l'invention, ce tatouage est intégré à chaque bloc d'une image décomposée en N blocs.

[0087] Lorsque l'image subit, au cours de sa transmission, une opération de découpage ou recadrage, l'extraction des signatures pour chaque bloc est faussée comme cela est illustré à la figure 8b qui représente une signature extraite pour un bloc d'une image après que celle-ci ait subi un recadrage. On voit que la signature extraite ne correspond alors plus à la signature intégrée dans un bloc car le découpage n'est plus cohérent avec la grille de définition initiale des blocs.

[0088] Afin de pallier cet inconvénient, il est proposé d'ajouter à une signature un motif identifiable avant de l'intégrer dans un bloc.

[0089] Un exemple d'un tel motif est donné à la figure 9a, il s'agit de placer des bits à 1 dans au moins 3 zones 901,902,903,904 correspondant à des coins de la matrice. Les motifs ainsi créés dans les coins de la matrice doivent être identiques.

[0090] En référence à la figure 2, avant l'intégration 205 de la signature dans un bloc de l'image, le motif décrit à la figure 9a est ajouté à la signature reçue à l'étape 203, l'ensemble étant représenté sous une forme matricielle. La taille de la matrice est inférieure ou égale à celle d'un bloc de l'image et est telle que le ratio entre la taille d'un bloc et la taille de la matrice est fixe.

[0091] Lors de l'extraction des signatures, une étape supplémentaire 305 (en référence à la figure 3) est exécutée pour recombiner les signatures extraites à l'aide du motif M pour compenser l'opération de découpage de l'image.

[0092] Pour cela, les éléments du motif M sont détectés dans la signature extraite (par exemple elle de la figure 8b), puis on en déduit le décalage entre la position initiale du motif M lors de son intégration dans un bloc et la position de ce motif dans la signature extraite. Un décalage vertical et un décalage horizontal peuvent être estimés. Ensuite ces décalages sont appliqués aux pixels de la signature matricielle pour obtenir la signature décodée.

[0093] La figure 9b montre un autre exemple de motif M possible constitué de quatre éléments de même forme géométrique (par exemple des croix) situés aux quatre coins d'un carré.

[0094] De façon générale, le motif M est constitué d'au moins trois éléments disposés en trois positions fixes, par exemple trois coins d'un carré inscrit dans la matrice de la signature. Les éléments du motif sont constitués de valeurs à 1. Avantageusement ils sont placés sur les bords ou les coins de la matrice de manière à éviter des zones où sont situés les bits utiles de la signature.

[0095] Les étapes de l'invention peuvent être mises en œuvre en tant que programme d'ordinateur comportant des instructions pour son exécution. Le programme d'ordinateur peut être enregistré sur un support d'enregistrement lisible par un processeur.

[0096] La référence à un programme d'ordinateur qui, lorsqu'il est exécuté, effectue l'une quelconque des fonctions décrites précédemment, ne se limite pas à un programme d'application s'exécutant sur un ordinateur hôte unique. Au contraire, les termes programme d'ordinateur et logiciel sont utilisés ici dans un sens général pour faire référence à tout type de code informatique (par exemple, un logiciel d'application, un micro logiciel, un microcode, ou toute autre forme d'instruction d'ordinateur) qui peut être utilisé pour programmer un ou plusieurs processeurs pour mettre en œuvre des aspects des techniques décrites ici. Les moyens ou ressources informatiques peuvent notamment être distribués ("*Cloud computing*"), éventuellement selon des technologies de pair-à-pair. Le code logiciel peut être exécuté sur n'importe quel processeur approprié (par exemple, un microprocesseur) ou cœur de processeur ou un ensemble de processeurs, qu'ils soient prévus dans un dispositif de calcul unique ou répartis entre plusieurs dispositifs de calcul (par exemple tels qu'éventuellement accessibles dans l'environnement du dispositif). Le code exécutable de chaque programme permettant au dispositif programmable de mettre en œuvre les processus selon l'invention, peut être stocké, par exemple, dans le disque dur ou en mémoire morte. De manière générale, le ou les programmes pourront être chargés dans un des moyens de stockage du dispositif avant d'être exécutés. L'unité centrale peut commander et diriger l'exécution des instructions ou portions de code logiciel du ou des programmes selon l'invention, instructions qui sont stockées dans le

disque dur ou dans la mémoire morte ou bien dans les autres éléments de stockage précités.

[0097] Références

[0098] [1] « ReDMark : Framework for Residual Diffusion Watermarking based on Deep Networks", M Ahmadi et al

REVENDICATIONS

1. Méthode, mise en œuvre par ordinateur, de tatouage numérique d'une image comprenant les étapes de :

- Recevoir (201) une image numérique,
- Décomposer (202) l'image numérique en une pluralité de sous-blocs de mêmes dimensions prédéfinies,
- Générer (203) une signature binaire numérique,
- Pour chaque sous-bloc,
    i. Transformer le sous-bloc dans un espace intermédiaire via une transformée prédéterminée,
    ii. Combiner la signature avec le sous-bloc dans l'espace intermédiaire pour obtenir un sous-bloc signé dans l'espace intermédiaire,
    iii. Appliquer au sous-bloc signé une transformée inverse à la transformée prédéterminée,
- Concaténer (206) l'ensemble des sous-blocs signés pour former une image signée.

2. Méthode de tatouage numérique selon la revendication 1 comprenant en outre les étapes de :

- Ajouter (204) à la signature binaire numérique un motif binaire,
- Transformer la signature binaire en une matrice de dimensions inférieures aux dimensions d'un sous-bloc,
- Le motif binaire étant inséré dans la signature binaire de sorte à être positionné sur des positions prédéfinies de la matrice identiques pour chaque sous-bloc

3. Méthode de tatouage numérique selon la revendication 2 dans laquelle le motif binaire est positionné sur au moins trois zones de la matrice correspondant à trois coins d'un carré, par exemple trois coins de la matrice.

4. Méthode de tatouage numérique selon l'une quelconque des revendications précédentes dans laquelle l'étape de combiner la signature avec un sous-bloc est réalisée au moyen d'un premier moteur d'intelligence artificielle entrainé pour minimiser l'impact visuel d'une signature sur une image signée.

5. Méthode, mise en œuvre par ordinateur, d'extraction d'un tatouage numérique comprenant les étapes de :

- Recevoir (301) une image numérique signée au moyen de la méthode de tatouage numérique selon la revendication 1,
- Décomposer (302) l'image numérique en une pluralité de sous-blocs de mêmes dimensions utilisées pour générer l'image numérique signée,
- Pour chaque sous-bloc,
    i. Extraire (303) la signature binaire tatouée dans le sous-bloc

6. Méthode d'extraction d'un tatouage numérique selon la revendication 5 dans laquelle l'étape d'extraire la signature binaire d'un sous bloc est réalisée au moyen d'un second moteur d'intelligence artificielle entrainé pour minimiser un écart entre la signature binaire générée à l'origine et la signature binaire extraite d'un sous bloc.

7. Méthode d'extraction d'un tatouage numérique selon la revendication 6 dans laquelle :

- l'étape de combiner la signature avec un sous-bloc de la méthode de tatouage numérique est réalisée au moyen d'un premier moteur d'intelligence artificielle entrainé pour minimiser l'impact visuel d'une signature sur une image signée,
- le premier moteur d'intelligence artificielle et le second moteur d'intelligence artificielle sont entrainés conjointement.

8. Méthode d'extraction d'un tatouage numérique selon l'une quelconque des revendications 5 à 7 comprenant en outre les étapes de :

- Détecter (305), pour au moins un sous-bloc, un motif binaire inséré dans la signature extraite,

- Comparer (305) les positions du motif binaire détecté à un ensemble de positions attendues et si elles diffèrent des positions attendues, en déduire que l'image numérique reçue a subi une opération de découpage,
- Reconstruire (305) la signature binaire associée à l'image avant opération de découpage à partir des positions du motif binaire en appliquant à la signature numérique une opération inverse à l'opération de découpage

9. Méthode, mise en œuvre par ordinateur, de détection de falsification d'une image tatouée numériquement, la méthode comprenant les étapes de:

- Exécuter (701) la méthode d'extraction d'un tatouage numérique pour une image reçue selon l'une quelconque des revendications 5 à 8,
- Rechercher (702), pour l'ensemble des sous-blocs de l'image, la signature extraite majoritaire parmi cet ensemble,
- pour chaque sous-bloc,
    i. comparer (703) la signature extraite pour le sous-bloc à la signature majoritaire et,
    ii. en déduire si le sous-bloc de l'image a été falsifié ou non

10. Méthode selon l'une quelconque des revendications précédentes dans laquelle l'image numérique est une image acquise par un satellite.

11. Programme d'ordinateur comportant des instructions pour l'exécution de la méthode selon l'une quelconque des revendications 1 à 10, lorsque le programme est exécuté par un processeur.

12. Support d'enregistrement lisible par un processeur sur lequel est enregistré un programme comportant des instructions pour l'exécution de la méthode selon l'une quelconque des revendications 1 à 10, lorsque le programme est exécuté par un processeur.

[Fig. 1]

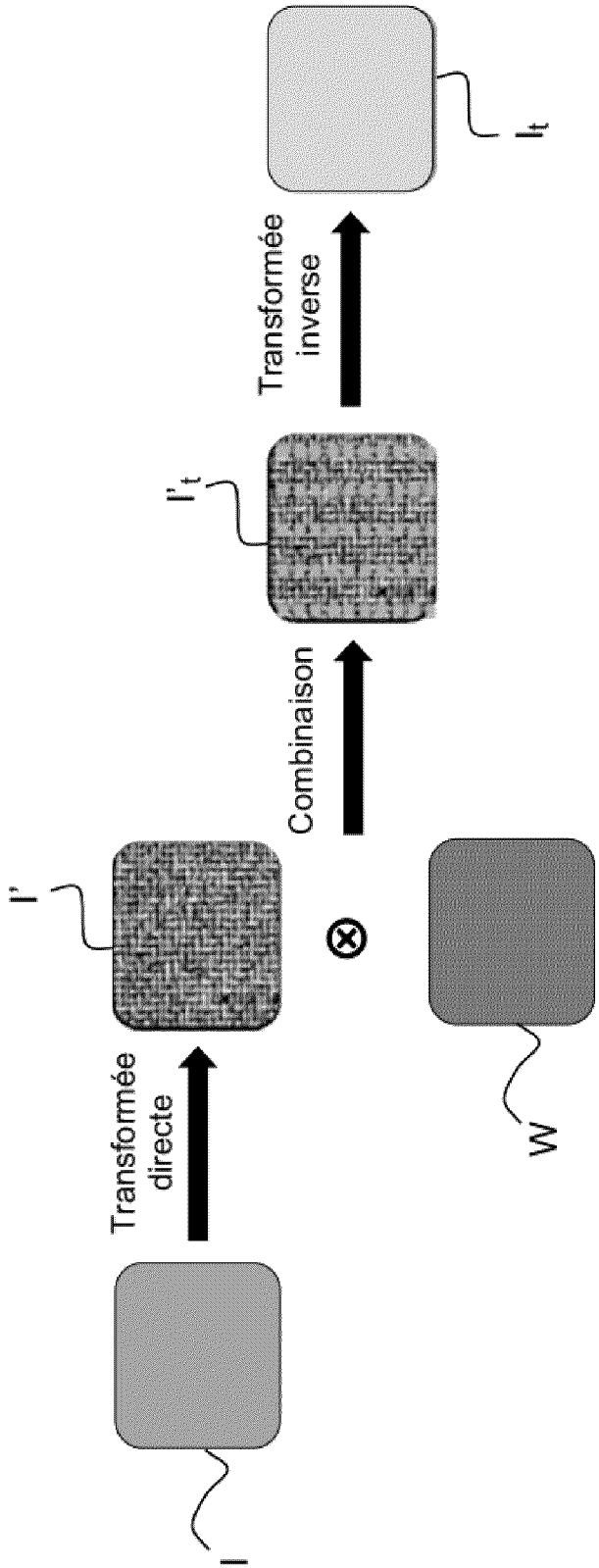

I
Transformée directe
I'
⊗
W
Combinaison
I't
Transformée inverse
It

FIG.1

[Fig. 2]

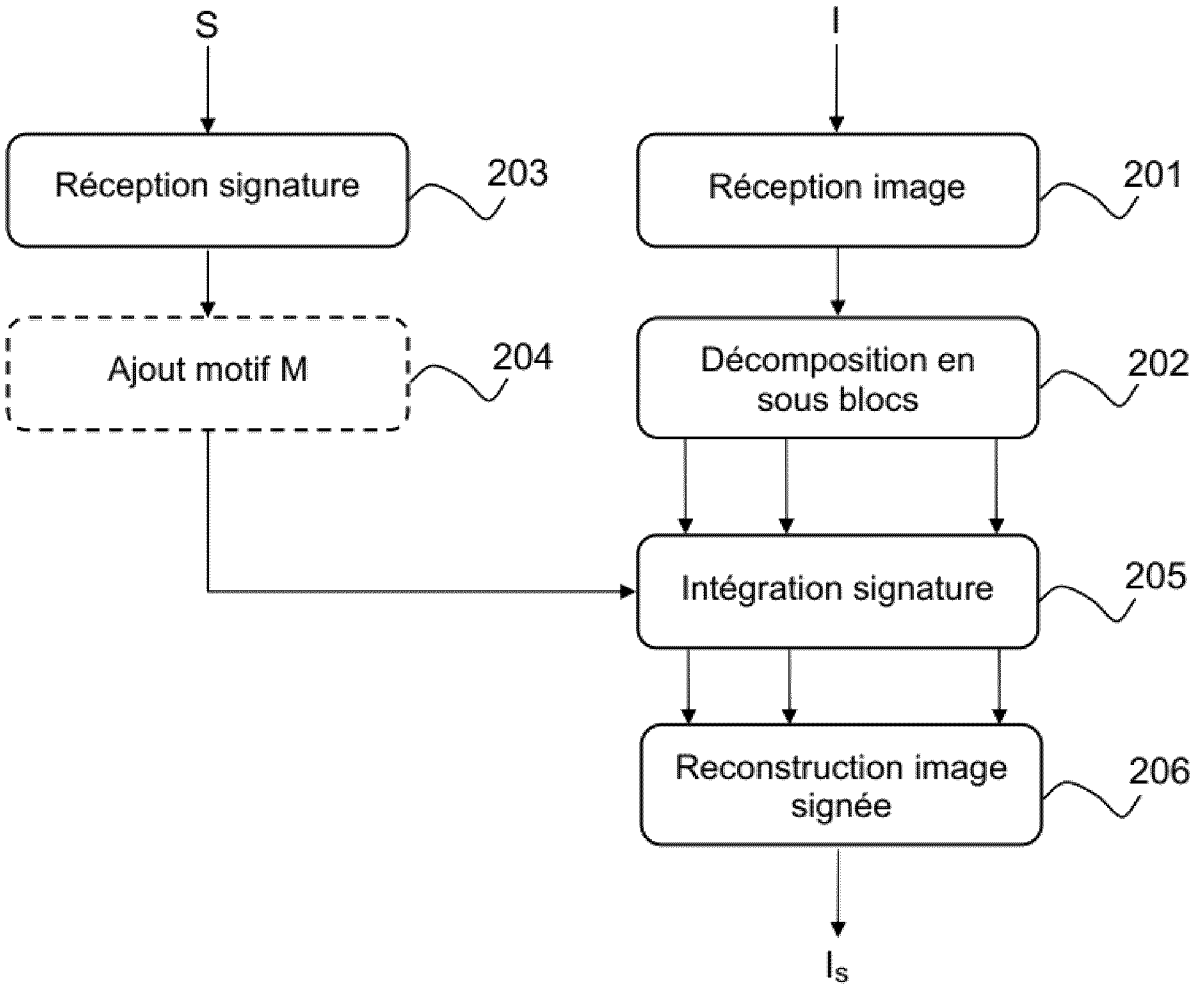

S
I
Réception signature
203
Réception image
201
Ajout motif M
204
Décomposition en sous blocs
202
Intégration signature
205
Reconstruction image signée
206
I_S

FIG.2

[Fig. 3]

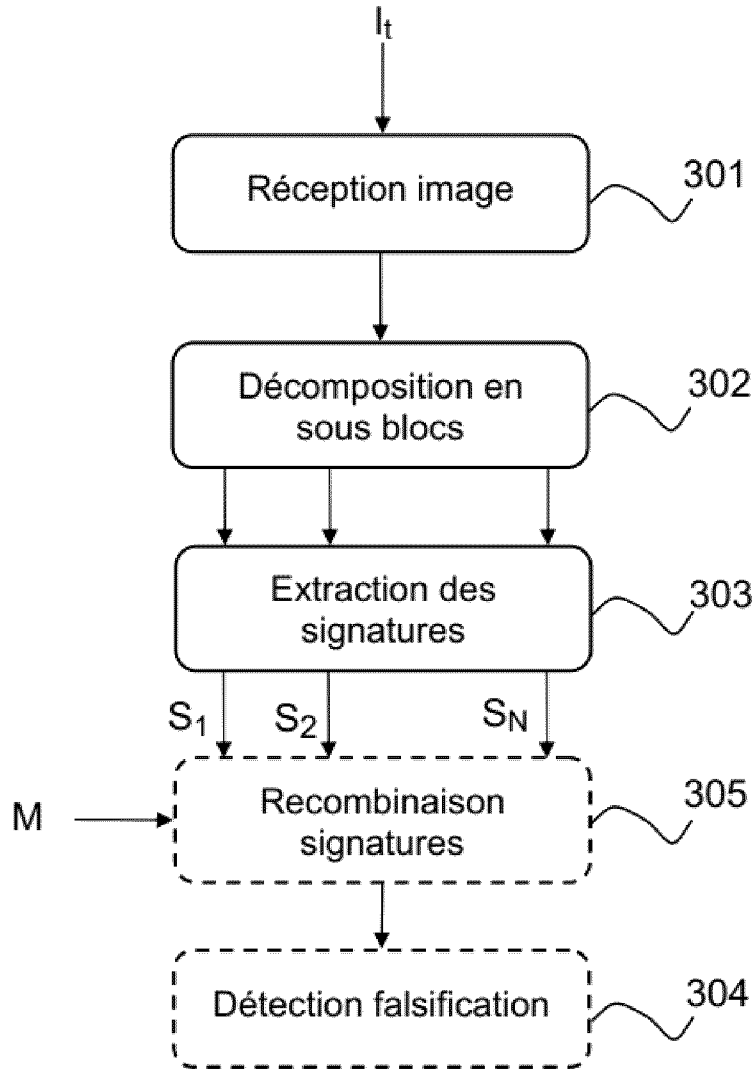

I_t
Réception image
301
Décomposition en sous blocs
302
Extraction des signatures
303
S_1
S_2
S_N
M
Recombinaison signatures
305
Détection falsification
304

FIG.3

[Fig. 4]

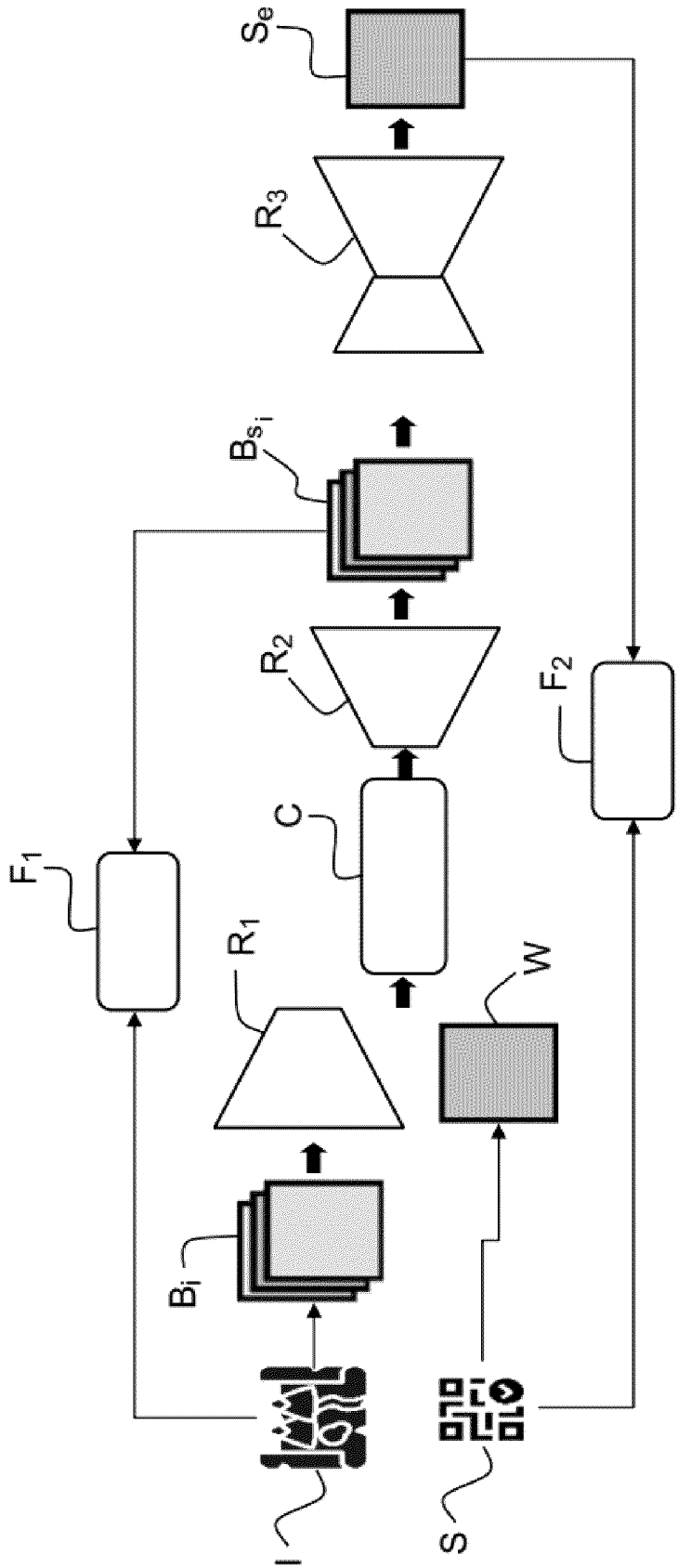


FIG.4

[Fig. 5]

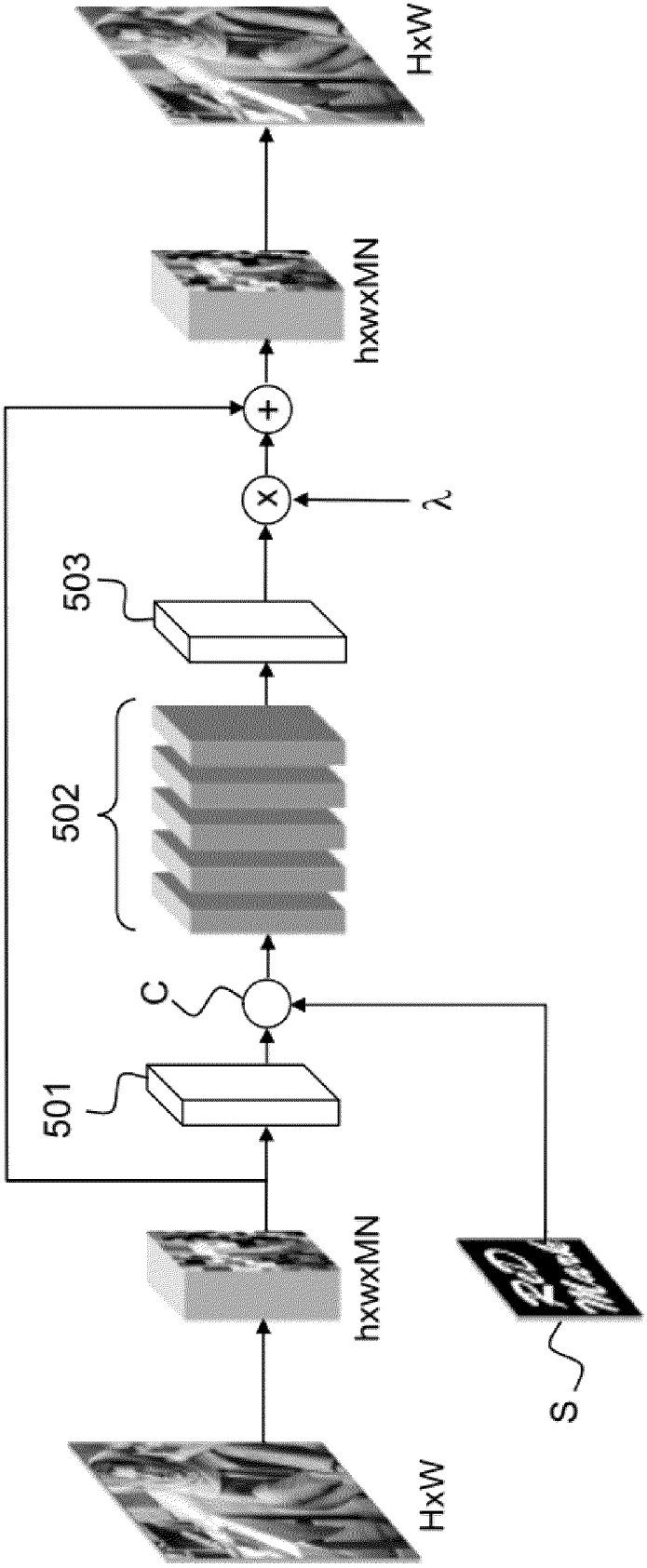


FIG.5

[Fig. 6]

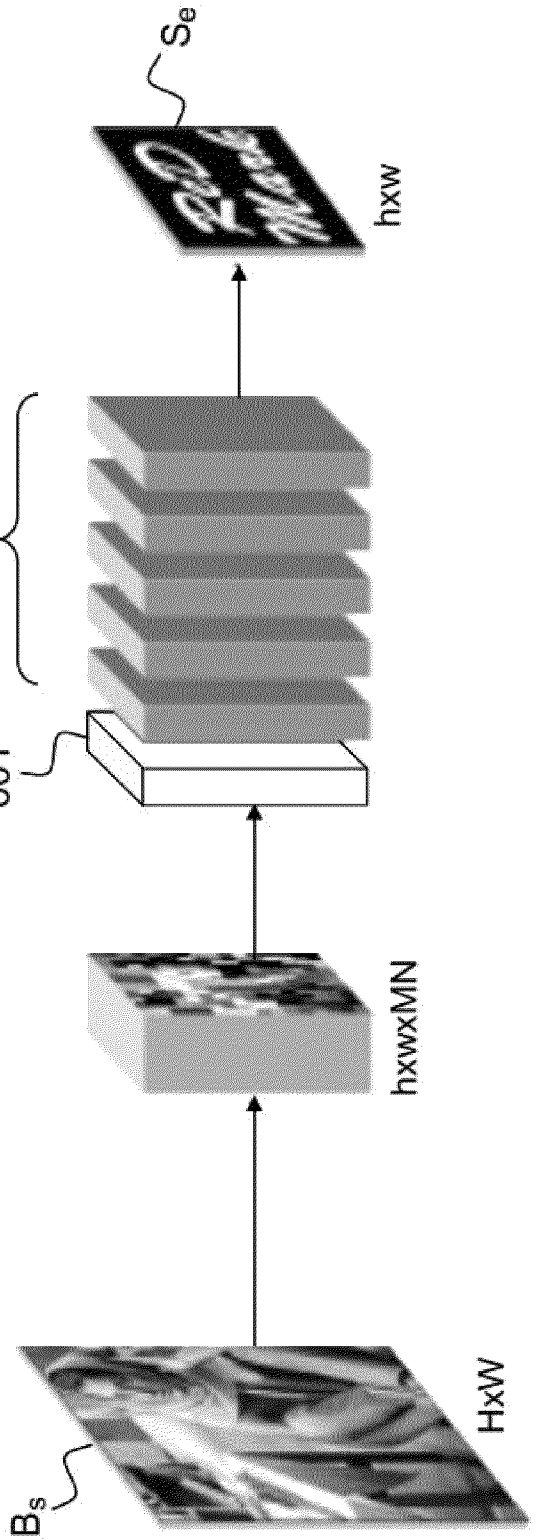


FIG.6

[Fig. 7]

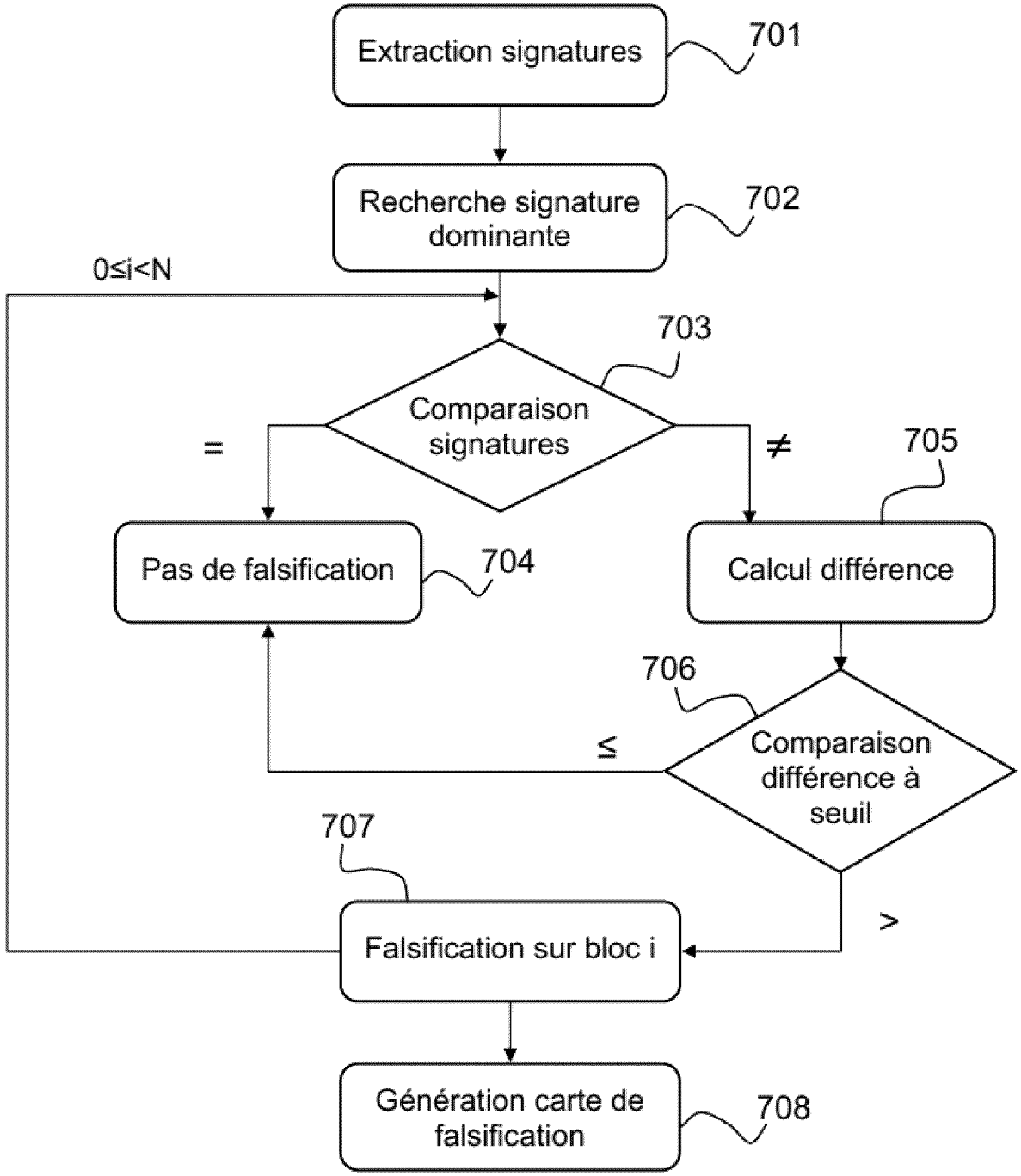

Extraction signatures
701
Recherche signature dominante
702
0≤i<N
703
Comparaison signatures
=
≠
705
Pas de falsification
704
Calcul différence
706
Comparaison différence à seuil
≤
>
707
Falsification sur bloc i
Génération carte de falsification
708

FIG.7

[Fig. 8a]

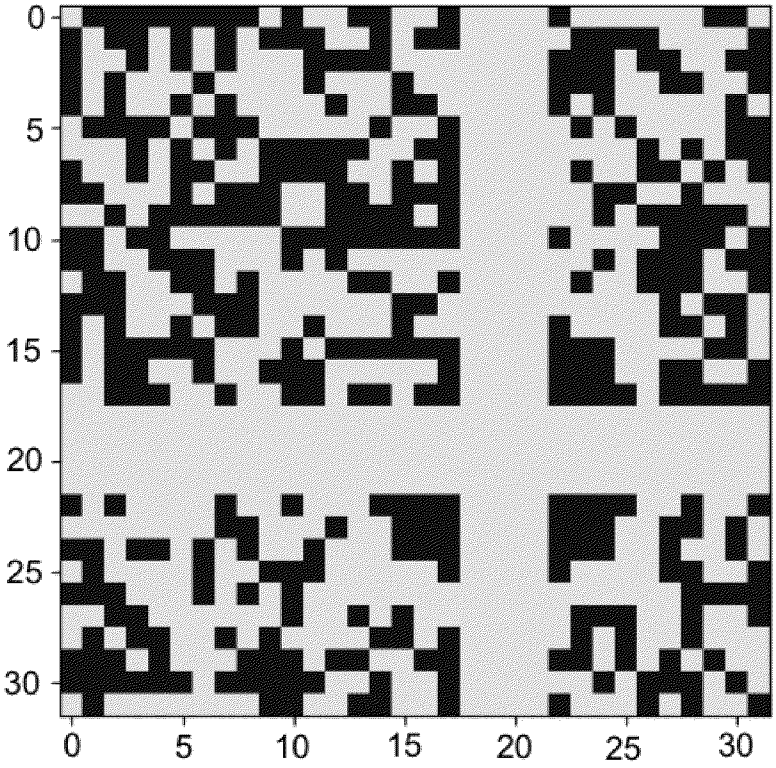


FIG.8a

[Fig. 8b]

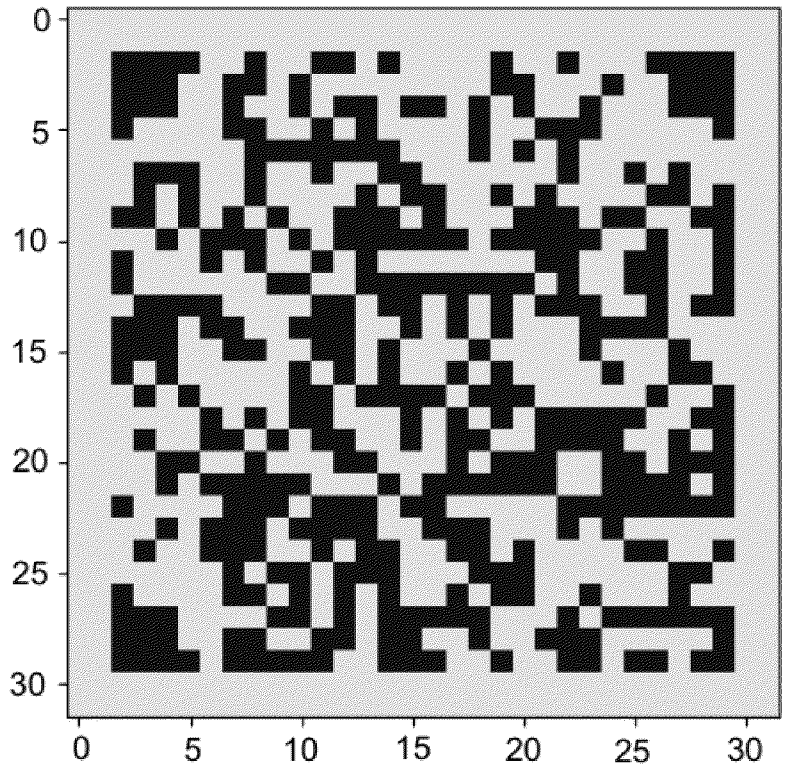


FIG.8b

[Fig. 9a]

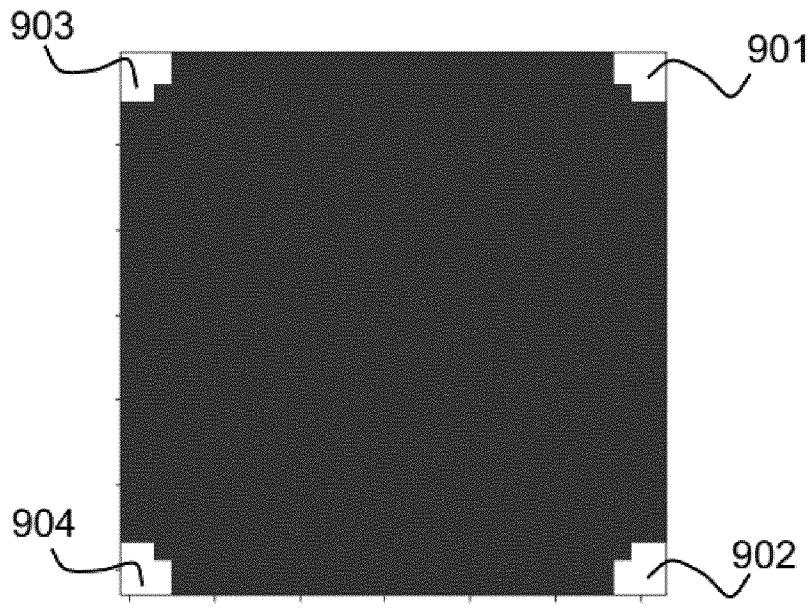


FIG.9a

[Fig. 9b]

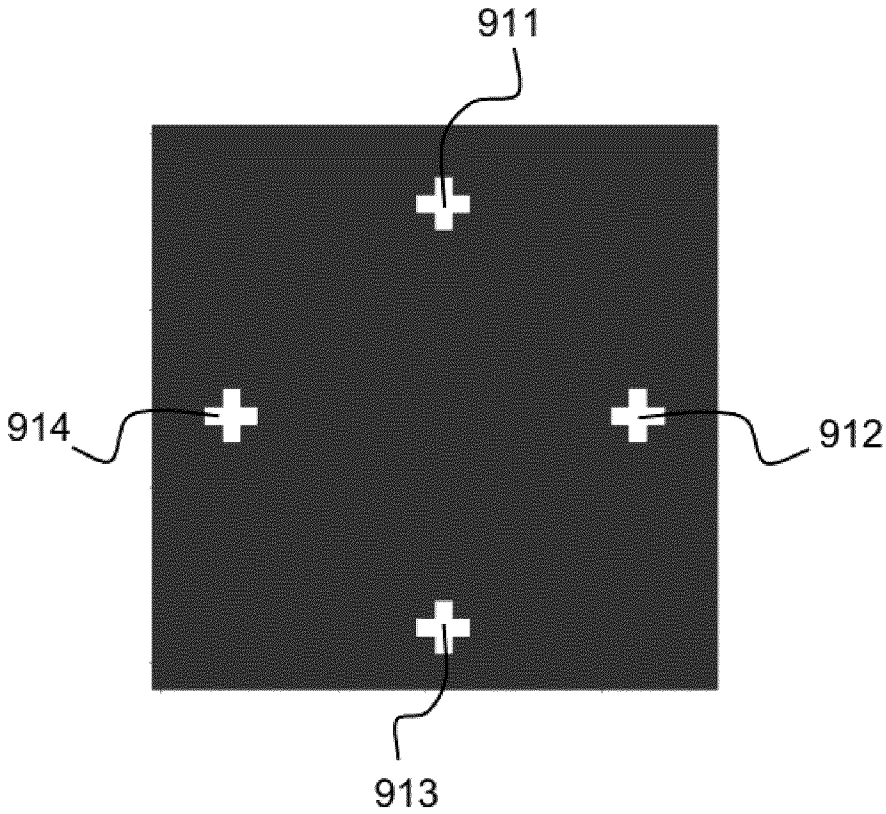


FIG.9b

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2024/069075

A. CLASSIFICATION OF SUBJECT MATTER

G06T 1/00(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06T

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	BEGUM MAHBUBA ET AL. "Digital Image Watermarking Techniques: A Review" *INFORMATION,* Vol. 11, No. 2, 01 January 2020 (2020-01-01), page 110 DOI: 10.3390/info11020110 ISSN: 2078-2489, XP093067196	1,4-7,10-12
Y	abstract page 7 - page 8 page 17 figure 12 page 10	9
Y	SEUNG-MIN MUN ET AL. "A Robust Blind Watermarking Using Convolutional Neural Network" *ARXIV.ORG, CORNELL UNIVERSITY LIBRARY, 201 OLIN LIBRARY CORNELL UNIVERSITY ITHACA, NY 14853,* 11 April 2017 (2017-04-11), XP080762209 abstract page 2	9

☑ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 August 2024	**18 September 2024**
Name and mailing address of the ISA/EP **European Patent Office** **p.b. 5818, Patentlaan 2, 2280 HV Rijswijk** **Netherlands (Kingdom of the)** Telephone No. **(+31-70)340-2040** Facsimile No. **(+31-70)340-3016**	Authorized officer **Luca, Mihai Bogdan** Telephone No.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JAIN SHIPRA ET AL. "VGG16Unet: effective passive model for image splicing forgery localization" *JOURNAL OF ELECTRONIC IMAGING, S P I E - INTERNATIONAL SOCIETY FOR OPTICAL ENGINEERING, US,* Vol. 32, No. 4, 01 July 2023 (2023-07-01), page 43015, [retrieved on 2023-07-17] DOI: 10.1117/1.JEI.32.4.043015 ISSN: 1017-9909, XP060186842 the whole document	1-12
A	HUSSAIN SHEHZEEN ET AL. "FastStamp: Accelerating Neural Steganography and Digital Watermarking of Images on FPGAs" *2022 IEEE/ACM INTERNATIONAL CONFERENCE ON COMPUTER AIDED DESIGN (ICCAD), ACM,* 29 October 2022 (2022-10-29), pages 1-9 DOI: 10.1145/3508352.3549357 XP034312740 the whole document	1-12

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/EP2024/069075

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. G06T1/00
ADD.

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
G06T

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)
EPO-Internal

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	BEGUM MAHBUBA ET AL: "Digital Image Watermarking Techniques: A Review", INFORMATION, vol. 11, no. 2, 1 janvier 2020 (2020-01-01), page 110, XP093067196, ISSN: 2078-2489, DOI: 10.3390/info11020110	1,4-7, 10-12
Y	abrégé page 7 - page 8 page 17 figure 12 page 10	9

-/--

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

[ ] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
"E" document antérieur, mais publié à la date de dépôt international ou après cette date
"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée
"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
"X" document particulièrement pertinent;; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
"Y" document particulièrement pertinent;; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
26 août 2024	18/09/2024

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

1

Formulaire PCT/ISA/210 (deuxième feuille) (avril 2005)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/EP2024/069075

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	SEUNG-MIN MUN ET AL: "A Robust Blind Watermarking Using Convolutional Neural Network", ARXIV.ORG, CORNELL UNIVERSITY LIBRARY, 201 OLIN LIBRARY CORNELL UNIVERSITY ITHACA, NY 14853, 11 avril 2017 (2017-04-11), XP080762209, abrégé page 2	9

A	JAIN SHIPRA ET AL: "VGG16Unet: effective passive model for image splicing forgery localization", JOURNAL OF ELECTRONIC IMAGING, S P I E - INTERNATIONAL SOCIETY FOR OPTICAL ENGINEERING, US, vol. 32, no. 4, 1 juillet 2023 (2023-07-01), page 43015, XP060186842, ISSN: 1017-9909, DOI: 10.1117/1.JEI.32.4.043015 [extrait le 2023-07-17] le document en entier	1-12

A	HUSSAIN SHEHZEEN ET AL: "FastStamp: Accelerating Neural Steganography and Digital Watermarking of Images on FPGAs", 2022 IEEE/ACM INTERNATIONAL CONFERENCE ON COMPUTER AIDED DESIGN (ICCAD), ACM, 29 octobre 2022 (2022-10-29), pages 1-9, XP034312740, DOI: 10.1145/3508352.3549357 le document en entier	1-12

1