Innovation, Sciences et Développement économique Canada
Office de la Propriété Intellectuelle du Canada

Innovation, Science and Economic Development Canada
Canadian Intellectual Property Office

CA 2957774 C 2023/08/08

(11)(21) 2 957 774

(12) BREVET CANADIEN
CANADIAN PATENT

(13) C

(22) Date de dépôt/Filing Date: 2017/02/10

(41) Mise à la disp. pub./Open to Public Insp.: 2017/08/11

(45) Date de délivrance/Issue Date: 2023/08/08

(30) Priorité/Priority: 2016/02/11 (FR16/51105)

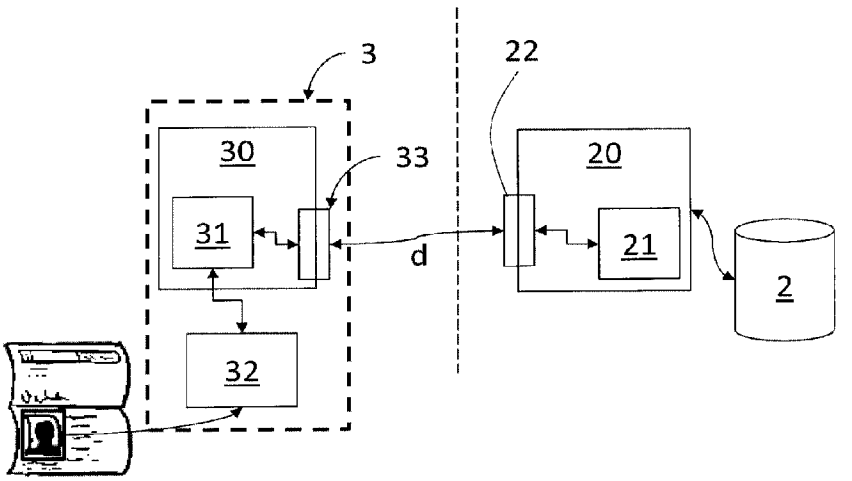
(51) Cl.Int./Int.Cl. *B42D 25/00* (2014.01), *B42D 25/305* (2014.01), *G07D 7/12* (2016.01)

(72) Inventeurs/Inventors:
CHABANNE, HERVE, FR;
FONDEUR, JEAN-CHRISTOPHE, FR;
GENTRIC, STEPHANE, FR;
VAN DIJK, ERIK, FR

(73) Propriétaire/Owner:
IDEMIA IDENTITY & SECURITY FRANCE, FR

(74) Agent: NORTON ROSE FULBRIGHT CANADA LLP/S.E.N.C.R.L., S.R.L.

(54) Titre : PROCEDE DE SECURISATION ET DE VERIFICATION D'UN DOCUMENT
(54) Title: PROCESS FOR SECURING AND VERIFYING A DOCUMENT



(57) Abrégé/Abstract:
L'invention concerne un procédé de sécurisation d'un document comportant un élément visuel, mis en oeuvre par une unité de traitement comprenant des moyens de traitement, le procédé comprenant la génération, à partir de l'élément visuel, d'une donnée de sécurité de référence, et la mémorisation de la donnée de sécurité de référence,
dans lequel la donnée de sécurité de référence est générée au moyen d'un algorithme configuré de manière à générer :
- pour toute image acquise de l'élément visuel, une donnée de sécurité dont les différences par rapport à la donnée de sécurité de référence sont inférieures à un seuil déterminé, et
- pour toute image acquise sur un élément visuel différent, une donnée de sécurité dont les différences par rapport à la donnée de sécurité de référence sont supérieures audit seuil.

PROCEDE DE SECURISATION ET DE VERIFICATION D'UN DOCUMENT

ABREGE

L'invention concerne un procédé de sécurisation d'un document comportant un élément visuel, mis en œuvre par une unité de traitement comprenant des moyens de traitement, le procédé comprenant la génération, à partir de l'élément visuel, d'une donnée de sécurité de référence, et la mémorisation de la donnée de sécurité de référence,

dans lequel la donnée de sécurité de référence est générée au moyen d'un algorithme configuré de manière à générer :

- pour toute image acquise de l'élément visuel, une donnée de sécurité dont les différences par rapport à la donnée de sécurité de référence sont inférieures à un seuil déterminé, et
- pour toute image acquise sur un élément visuel différent, une donnée de sécurité dont les différences par rapport à la donnée de sécurité de référence sont supérieures audit seuil.

PROCEDE DE SECURISATION ET DE VERIFICATION D'UN DOCUMENT

DOMAINE DE L'INVENTION

L'invention concerne le domaine de la sécurisation de documents comprenant au moins un élément visuel. Les documents peuvent notamment être des documents d'identité de type par exemple carte d'identité, permis de conduire, acte de naissance ou passeport ou bien encore tout « document électronique » (type documents personnels et/ou d'identité) pouvant être hébergé sur un smartphone ou autre dispositif portable disposant de moyens d'affichage. L'invention concerne également la vérification de l'intégrité de tels documents une fois sécurisés.

ETAT DE LA TECHNIQUE

Des services de sécurité nationaux ont découvert des fraudes menées sur des documents d'identité, dans lesquelles un document authentique pourvu d'une photographie d'identité originale a été falsifié, en remplaçant la photographie par la photographie d'une personne différente. De ce fait l'utilisateur du document falsifié peut usurper l'identité de la personne à qui le document d'identité a été délivré initialement.

Dans un contexte plus général, les exigences imposées en termes de sûreté aux organismes concevant et délivrant des documents d'identité sont de plus en plus strictes.

PRESENTATION DE L'INVENTION

Un but de l'invention est de proposer un procédé de sécurisation d'un document, notamment d'un document d'identité, permettant de garantir notamment l'intégrité d'éléments visuels du document tels que des photographies.

Un autre but de l'invention est de proposer un procédé de vérification de l'intégrité d'un document sécurisé par le procédé proposé.

Un autre but de l'invention est d'assurer que le procédé de vérification de l'intégrité du document soit robuste aux variations subies par le document liées à son utilisation, ses conditions d'utilisation, etc.

partir de l'élément visuel, d'une donnée de sécurité de référence, et la mémorisation de la donnée de sécurité de référence,

dans lequel la donnée de sécurité de référence est générée au moyen d'un algorithme configuré de manière à générer :

- pour toute image acquise de l'élément visuel, une donnée de sécurité dont les différences par rapport à la donnée de sécurité de référence sont inférieures à un seuil déterminé, et
- pour toute image acquise sur un élément visuel différent, une donnée de sécurité dont les différences par rapport à la donnée de sécurité de référence sont supérieures audit seuil.

Préférablement, l'algorithme est paramétré à partir d'un entraînement sur une base de données d'apprentissage.

Avantageusement, mais facultativement, le procédé selon l'invention peut en outre comprendre au moins l'une des caractéristiques suivantes :

- la génération de la donnée de sécurité de référence est mise en œuvre lors de la création du document.
- la donnée de sécurité de référence est mémorisée dans le document, par enregistrement de la donnée dans une puce électronique stockée dans le document ou affichage, par exemple impression, de la donnée sur le document.
- la donnée de sécurité de référence est mémorisée en étant enregistrée dans une base de données.
- la donnée de sécurité de référence est signée par l'unité de traitement, au moyen d'un algorithme de signature à clé publique, ou enregistrée avec un certificat d'authenticité obtenu par l'application d'un algorithme de codage basé sur l'utilisation d'un code correcteur d'erreur, dit secure sketch.
- la donnée de sécurité de référence est mémorisée dans le document par affichage, par exemple impression, de la donnée sur le document et dans lequel l'élément visuel est lui aussi affiché, par exemple imprimé, sur le document.
- le document est un document électronique comprenant des moyens d'affichage, par exemple un écran.
- l'algorithme est choisi de sorte que la reconstitution de l'élément visuel à partir de la donnée de sécurité correspondante soit impossible.

- l'algorithme est un algorithme à descripteur, de type BRIEF, ou de type SIFT, ou de type SURF ou de type GLOH, ou de type ORB, ou de type BRISK ou de type FREAK ou de type LATCH.
- l'algorithme est du type comprenant l'utilisation d'histogrammes de gradients orientés sur l'élément visuel, ou de réseaux de neurones convolutionels, ou bien encore de type BRIEF, ou de type SIFT, ou de type SURF ou de type GLOH, ou de type ORB, ou de type BRISK ou de type FREAK ou de type LATCH.
- pour l'entrainement de l'algorithme, l'algorithme est exécuté
  sur un grand nombre de paires d'images, et des indications lui sont fournies sur celles qui doivent résulter en des données de sécurité sensiblement identiques, (typiquement la même image capturée à des instants et/ou dans des conditions différentes, par exemple lorsque l'image est détériorée par le temps, les frottements, le jaunissement et/ou que lors de l'acquisition,la luminosité, l'angle, etc. ne sont pas les mêmes), et
  sur d'autres paires d'images qui doivent résulter en des données de sécurité sensiblement différentes, (typiquement lorsque la paire comporte deux images différentes soit d'individus différents, soit d'un même individu, par exemple dans le cas où l'autre image a été prise à des moments différents et/ou avec des conditions différentes).
- l'élément visuel est une image du visage d'un individu, et l'algorithme est entrainé de manière à générer :
  - pour toute image acquise de l'image du visage de l'individu figurant sur le document, une donnée de sécurité dont les différences par rapport à la donnée de sécurité de référence sont inférieures à un seuil déterminé, et
  - pour toute image acquise d'une image représentant un autre individu, ou le même individu dans des conditions d'acquisition d'image différentes, une donnée de sécurité dont les différences par rapport à la donnée de sécurité de référence sont supérieures audit seuil.

L'invention a également pour objet un procédé de sécurisation d'un document comportant un élément visuel, mis en œuvre par une unité de traitement comprenant des moyens de traitement, le procédé comprenant la génération, à

partir de l'élément visuel, d'une donnée de sécurité de référence, et la mémorisation de la donnée de sécurité de référence,

dans lequel la donnée de sécurité de référence est générée au moyen d'un algorithme paramétré à partir d'un entraînement sur une base de données d'apprentissage,

dans lequel, pour l'entrainement de l'algorithme, l'algorithme est exécuté

sur un grand nombre de paires d'images, et des indications lui sont fournies sur celles qui doivent résulter en des données de sécurité sensiblement identiques,

sur d'autres paires d'images qui doivent résulter en des données de sécurité sensiblement différentes.

En particulier, l'algorithme est préférablement configuré de manière à générer :

- pour toute image acquise de l'élément visuel, une donnée de sécurité dont les différences par rapport à la donnée de sécurité de référence sont inférieures à un seuil déterminé, et
- pour toute image acquise sur un élément visuel différent, une donnée de sécurité dont les différences par rapport à la donnée de sécurité de référence sont supérieures audit seuil.

Les caractéristiques additionnelles décrites précédemment s'appliquent également pour cet objet.

L'invention a également pour objet un produit programme d'ordinateur, comprenant des instructions de code pour la mise en œuvre d'un procédé selon la description qui précède, quand il est exécuté par des moyens de traitement d'une unité de traitement.

L'invention a également pour objet un document sécurisé pouvant être obtenu par la mise en œuvre d'un procédé selon la description qui précède.

L'invention a également pour objet un procédé de vérification de l'intégrité d'un document sécurisé par la mise en œuvre du procédé selon la description qui précède, le procédé comprenant les étapes consistant à :

- acquérir une image de l'élément visuel du document,

- générer, à partir de l'image, une donnée de sécurité par le même algorithme que celui ayant permis de générer la donnée de sécurité de référence,
- comparer la donnée de sécurité obtenue à la donnée de sécurité de référence, et
- si les différences entre la donnée de sécurité et la donnée de sécurité de référence sont inférieures au seuil déterminé, déterminer que l'élément visuel est intègre, sinon déterminer que l'élément visuel est frauduleux.

Avantageusement, mais facultativement, le procédé de vérification comprend en outre, avant l'étape de comparaison, une étape de vérification de l'intégrité de la donnée de sécurité de référence.

L'invention a enfin pour objet un système de vérification d'un document, comprenant :

- un capteur d'image,
- une unité de traitement, comprenant des moyens de traitement adaptés pour mettre en œuvre, sur une image acquise par le capteur, un algorithme de classification, et une interface de communication avec une base de données,

le système de vérification étant configuré pour mettre en œuvre le procédé de vérification selon la description qui précède.

Le procédé proposé permet de garantir l'intégrité d'un élément visuel d'un document tel qu'une photographie, ou encore une chaîne de caractères, une signature, etc. En effet, à chaque élément visuel est attribuée une donnée de sécurité de référence, qui est obtenue par un algorithme configuré pour que la donnée obtenue soit globalement la même pour toutes les images d'un même élément visuel, quelles que soient les conditions d'acquisition des images ou l'usure de l'élément, et qui soit différente pour des images d'un élément visuel différent.

Pour cela, l'algorithme est entrainé sur une base de données d'apprentissage.

Pour renforcer encore la sécurité du document, l'intégrité de la donnée de sécurité de référence peut être garantie au moyen d'un algorithme de signature à clé publique ou d'un algorithme de codage dit secure sketch. Ainsi, la donnée de sécurité ne peut pas être falsifiée par l'individu porteur du document.

DESCRIPTION DES FIGURES

D'autres caractéristiques, buts et avantages de la présente invention apparaîtront à la lecture de la description détaillée qui va suivre, au regard des figures annexées, données à titre d'exemples non limitatifs et sur lesquelles :

- Les figures 1a et 1b représentent schématiquement un système de traitement pour sécuriser un document et un système pour vérifier l'intégrité d'un document.
- La figure 2 représente schématiquement les principales étapes d'un procédé de sécurisation d'un document,
- La figue 3 représente schématiquement les principales étapes d'un procédé de vérification de l'intégrité d'un document.

DESCRIPTION DETAILLEE D'AU MOINS UN MODE DE REALISATION DE L'INVENTION

Sécurisation d'un document

En référence à la figure 1a, on a représenté un système de traitement permettant de sécuriser un document, par exemple un document d'identité tel qu'un passeport, une carte d'identité, etc. Le type de document n'est pas limité à un document d'identité, mais pourrait également concerner des documents pour jouer, par exemple une carte à puce personnelle pour jouer au casino, etc. Le document peut être tout « document électronique » (type documents personnels et/ou d'identité) pouvant être hébergé sur un smartphone ou autre dispositifs portables, et comprenant des moyens d'affichage, par exemple un écran.

Ce système comprend une unité de traitement 10, par exemple un ordinateur ou un serveur, disposant de moyens de traitement 11 adapté pour exécuter un algorithme qui sera décrit plus en détails ci-après. Les moyens de traitement 11 peuvent par exemple être un calculateur de type processeur, microprocesseur, microcontrôleur, etc.

L'unité de traitement 10 peut également être adaptée pour mettre en œuvre des algorithmes cryptographiques, par exemple de type algorithme de signature à clé publique ou de type « secure sketch » évoqué plus en détails ci-après.

L'unité de traitement 10 et les moyens de traitement 11 sont opérés par une entité considérée non frauduleuse, typiquement un gouvernement dans le cas où le document est un document d'identité.

Avantageusement, le système peut également comprendre une base de données 2, ainsi qu'une unité de traitement 20 gestionnaire de la base de données. L'unité de traitement peut également être un ordinateur ou un serveur, disposant de moyens de traitement 21, par exemple un calculateur de type processeur, microprocesseur, microntrôleur, etc., permettant à l'unité de traitement d'accéder à la base de données en lecture et en écriture.

Les deux unités de traitement 10, 20 comprennent avantageusement des interfaces de communication 12, 22 à distance pour l'envoi et la réception de données, par exemple par Internet sans fil, signal radiofréquence, etc.

En référence à la figure 2, un procédé 100 de sécurisation d'un document comprend la sécurisation d'un élément visuel figurant sur le document.

Cet élément visuel est une image comprenant des données pertinentes lors de l'utilisation du document. Dans le cas d'un document d'identité, l'élément visuel est une image comporte des données liées à l'individu à qui est délivré le document d'identité. Avantageusement, il s'agit une photographie d'identité, c'est-à-dire une photographie représentant un signe distinctif de l'individu à qui le document a été délivré, typiquement son visage. Alternativement, l'élément visuel peut également être une image d'un autre signe distinctif de l'individu, par exemple une signature manuscrite.

L'élément visuel peut aussi être la représentation sur le document d'un ensemble de signes liés à l'identité de l'individu, par exemple une chaîne de caractères (nom, prénom, date de naissance, etc.).

Selon une autre variante, l'élément visuel peut être le document tout entier, par exemple dans le cas où le document utilisé est électronique et qu'il est affiché sur un écran de dispositif électronique tel qu'une tablette ou un téléphone mobile.

La sécurisation de l'élément visuel est de préférence mise en œuvre lors de la création du document, afin de garantir que l'élément visuel est authentique.

La sécurisation de l'élément visuel comprend la génération 110, par l'unité de traitement 10, à partir de l'élément visuel, d'une donnée de sécurité dite de référence d_r. Cette donnée prend avantageusement la forme d'une séquence de bits, d'une longueur de quelques octets à quelques dizaines d'octets.

Si l'élément visuel est une image numérique insérée dans le document lors de sa fabrication, l'étape 110 est mise en œuvre directement sur l'élément. Alternativement, l'étape 110 peut être mise en œuvre sur une image de l'élément visuel capturée sur le document à l'aide d'un capteur numérique d'image approprié (non représenté).

L'élément visuel peut être traité avant de générer la donnée de sécurité de référence. Il peut être avantageusement recalé par rapport à un référentiel, soit en réalisant un alignement, soit en cherchant à faire correspondre des points particuliers, par exemple en utilisant la méthode SIFT. Puis l'élément visuel peut être normalisé par exemple par la méthode d'égalisation d'histogrammes.

La donnée de sécurité de référence d_r est obtenue, à partir de l'élément visuel, par l'exécution d'un algorithme qui est configuré pour obtenir des propriétés recherchées pour la donnée de sécurité de référence.

Une première propriété est la suivante :

- Des images acquises d'un même élément visuel, quelles que soient les conditions d'acquisition, doivent conduire à l'obtention, par l'algorithme, de données de sécurité sensiblement identiques.

Dans toute la suite, on entend par « données de sécurité sensiblement identiques » des données de sécurité présentant entre elles des différences inférieures à un seuil déterminé. La quantité de différences entre deux données de sécurité peut être évaluée de manière connue en utilisant une métrique adaptée, par exemple en calculant une distance entre les données, comme par exemple la distance euclidienne ou la distance de Hamming. La valeur du seuil dépend de la nature de la fonction calculée.

Les conditions d'acquisition de l'image de l'élément visuel regroupent à la fois :

- des aléas liés aux conditions de l'acquisition elle-même avec un capteur d'image, par exemple les conditions d'éclairage, les paramètres du capteur d'image, la distance de l'élément visuel par rapport au capteur, etc., ainsi que :

- des aléas liés à l'apparence de l'élément visuel, comme par exemple une variation d'aspect du document provenant de son vieillissement, un jaunissement d'une photographie, l'apparition de rayures ou de marques, ou encore une variation d'aspect lié à des ajouts apportés pour accroître la sécurité du document : présence sur une partie de l'élément d'un tampon, d'un hologramme, etc.

En particulier, une donnée de sécurité obtenue à partir d'une image du même élément visuel que celui à partir duquel est obtenue la donnée de sécurité de référence doit être sensiblement identique à cette dernière.

Une autre propriété est la suivante :

- Des images acquises d'éléments visuels différents doivent conduire à l'obtention, par l'algorithme, de données de sécurité sensiblement différentes.

Dans toute la suite, on entend par « données de sécurité sensiblement différentes », des données de sécurité présentant entre elles des différences supérieures au seuil précédemment évoqué.

En particulier, une donnée de sécurité obtenue à partir d'une image d'un élément visuel différent de celui à partir duquel est obtenue la donnée de sécurité de référence d_r, doit être sensiblement différente à la donnée de sécurité de référence.

En outre, dans le cas où l'élément visuel du document est une photographie d'un individu, la donnée de sécurité doit être sensiblement la même que la donnée de sécurité de référence d_r (c'est-à-dire présenter des différences inférieures à un certain seuil) pour toutes les images prises de la même photographie du même individu.

En revanche, une donnée de sécurité doit être sensiblement différente de la donnée de sécurité de référence d_r si elle est obtenue à partir de toute autre photographie du même individu, ou de toute photographie d'un autre individu.

Pour obtenir ces propriétés, l'algorithme est entrainé, c'est-à-dire paramétré sur une base de données d'apprentissage (non représentée) contenant un ensemble d'images. Lors de cet entrainement, l'algorithme est exécuté sur un grand

nombre de paires d'images, et des indications lui sont fournies sur celles qui doivent résulter en des données de sécurité sensiblement identiques (typiquement la même image capturée à des instants et/ou dans des conditions différentes, par exemple lorsque l'image est détériorée par le temps, les frottements, le jaunissement et/ou que lors de l'acquisition, la luminosité, l'angle, etc. ne sont pas les mêmes), et sur d'autres paires d'images qui doivent résulter en des données de sécurité sensiblement différentes (typiquement lorsque la paire comporte deux images différentes d'un même objet ou d'objets différents mais de même nature, plus particulièrement lorsque la paire comporte deux images différentes soit d'individus différents (ou autre objets), soit d'un même individu (ou objet), par exemple dans le cas où l'autre image a été prise à des moments différents et/ou dans des conditions différentes).

La valeur du seuil permettant d'établir une classification entre des données sensiblement identiques et des données sensiblement différentes est déterminée par l'algorithme à l'issue de son apprentissage.

Avantageusement, la base de données d'apprentissage comporte le plus d'images possibles, par exemple au moins 10000 images, et de préférence au moins un million, car plus la base de données comporte d'images et plus l'apprentissage sur cette base de données augmente la fiabilité de l'algorithme.

L'algorithme de classification choisi pour générer la donnée de sécurité à partir d'une image est avantageusement un algorithme de classification du type employant un réseau de neurones convolutionnel également connu sous l'acronyme CNN (pour l'anglais Convolutional Neural Network).

De manière connue de l'Homme du métier, un réseau de neurones convolutionnel comporte une structure formée par une succession d'opérations mises en œuvre sur une donnée d'entrée (en l'occurrence une image), les opérations comprenant des opérations linéaires de type convolution, dont le résultat est pondéré par un facteur de pondération, ainsi que des opérations non linéaires, par exemple seuillage, etc.

L'ajustement de l'algorithme lors de l'apprentissage revient à ajuster les valeurs des facteurs de pondération.

Un exemple de structure de réseau de neurones convolutionnel applicable à la génération d'une donnée de sécurité à partir d'une image est celle qui est

détaillée pour le réseau F1 du document de Y. Sun et al., « *Deep Convolutional Network Cascade for Facial Point Detection* », *Proceedings of IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2013.

Le mode d'apprentissages des paramètres de l'algorithme CNN, de sorte qu'il génère deux données de sécurité différentes à partir d'images différentes d'une même personne, ainsi que la présence d'opérations non linéaires dans la génération de la donnée à partir de l'élément visuel, empêche la reconstitution de l'image à partir de la donnée de sécurité et préserve ainsi la confidentialité des données contenues dans l'image sur l'individu.

Alternativement, l'algorithme peut être du type BRIEF (pour « Binary robest Independant Elementary Feature »), tel que décrit dans la publication éponyme de Fua et al (« Brief : Binary Robust Independant Elementary Features ; Calonder, Lepetit, Strecha, Fua ; CvLab, EPFL). Toutefois, à l'inverse de cette publication où l'algorithme BRIEF est utilisé est extraire des caractéristiques (« features ») des images, l'algorithme est ici utilisé pour détecter les altérations de l'élément visuel. Ainsi, à la place des pondérations (« weight factors ») de BRIEF, une étape d'apprentissage (« machine learning ») est utilisée pour générer le pattern de paires de points le plus adéquat (« point pair pattern »), fondé sur une faible distance de Hamming entre l'élément visuel original, typiquement la photographie du visage, et l'élément visuel du document (l'original qui a subi des altérations), et sur une forte distance de Hamming entre l'élément visuel original et un élément visuel frauduleux Le pattern est généré par sélection parmi un grand nombre de paires de points tirées au hasard..

Alternativement, un autre descripteur binaire, type SIFT, SURF, GLOH, ORB, BRISK, FREAK, LATCH... ou même un descripteur type HOG peut être utilisé (voir ci-dessous). Ces descripteurs ont été introduits pour capturer des éléments caractéristiques des images. Ici, ils sont construits pour satisfaire aussi les propriétés précédentes : permettre la reconnaissance d'une même image tout empêchant la reconstruction de l'élément visuel à partir d'une donnée de sécurité correspondante.

Alternativement, l'algorithme peut être du type employant un descripteur HOG, c'est-à-dire à histogramme de gradient orienté.

Un tel algorithme est appliqué à une image répartie en zones. Pour chaque zone, des gradients sont calculés pour un ensemble de points de la zone, indépendamment de leur position dans la zone, et un histogramme des directions des gradients est agrégé pour l'ensemble des gradients calculés sur la zone.

L'algorithme comprend ensuite la concaténation de l'ensemble des histogrammes de gradients orientés pour toutes les zones, et la réduction du vecteur obtenu par une méthode de réduction d'espace de type par exemple analyse en composantes principales ou analyse discriminante linéaire.

Cet algorithme peut également comprendre une étape préliminaire de traitement des images pour normaliser les couleurs des images et le facteur de contraste.

On pourra se référer à la publication de N. Dalal et al., « *Histograms of Oriented Gradients for Human Detection », Conference on Computer Vision and Pattern Recognition,* 2005, pour plus de détails et un exemple d'implémentation d'un algorithme basé sur un descripteur HOG.

Dans ce mode de réalisation, le paramétrage de l'algorithme sur la base de données d'apprentissage pour satisfaire les deux propriétés détaillées ci-avant sur les conditions de similarité et de dissimilarité des données de sécurié, comprend l'ajustement des paramètres liés aux prétraitements, à la taille des zones choisies, au nombre de gradient par zone, au type de filtres utilisés pour calculer les gradients, à la nature de la réduction d'espace choisie, etc.

L'utilisation d'un tel algorithme, qui élimine la localisation des informations sur l'image, permet également de garantir la confidentialité des éléments visuels en empêchant de reconstituer un élément visuel à partir d'une donnée de sécurité correspondante.

Préférablement, dans le cas d'un élément visuel comprenant une information biométrique (telle qu'une photographie), les algorithmes précités ne cherchent pas à reconnaitre la personne présente sur l'élément visuel, comme cela est souvent recherché en identification biométrique, mais uniquement à savoir si l'élément visuel est authentique. Par conséquent, cela signifie que leur mise en œuvre n'implique pas l'identification de la personne possédant le document. C'est pourquoi un

document comprenant un autre élément visuel représentant la personne présente sur l'élément visuel de référence (typiquement une autre photographie représentant la même personne que celle présente sur la photographie de référence) sera considéré comme frauduleux après vérification, alors qu'elle conduirait à une authentification ou en identification biométrique.

Une fois la donnée de sécurité de référence d_r obtenue pour l'élément visuel du document, cette donnée est mémorisée lors d'une étape 120.

Elle peut être mémorisée dans le document lui-même. Par exemple, elle peut être stockée en mémoire dans une puce électronique intégrée dans le document.

Alternativement, elle peut être imprimée sur le document, de manière visible ou non, c'est-à-dire par exemple en filigrane, sous la forme d'un code-barres, etc.

Alternativement, elle peut être collée, déposée ou gravée sur le document, de sorte qu'il y ait un affichage physique.

Dans les deux alternatives précédentes, la donnée de référence peut alors être visible ou invisible (à l'instar des « digital watermark » connues).

On parle plus généralement d'affichage.

Cependant, la donnée de sécurité de référence d_r est de préférence mémorisée dans une base de données 2 gérée par une unité de traitement 20 gestionnaire, qui peut ainsi être fiable, par exemple dépendante d'un organisme étatique. Ceci limite les possibilités d'accès, par un individu malveillant ou par le détenteur du document lui-même à la donnée stockée dans le document.

Dans ce cas, l'unité de traitement 10 communique la donnée de sécurité de référence à l'unité de traitement 20 qui la stocke dans la base. Cette communication peut être mise en œuvre sur un canal sécurisé et/ou au moyen d'un protocole cryptographique pour assurer la confidentialité de la donnée.

En outre, et quel que soit le support de stockage de la donnée de sécurité, l'intégrité de cette donnée de sécurité est de préférence elle-même garantie.

Par exemple, la donnée de sécurité peut être signée par l'unité de traitement 10 qui a généré la donnée de sécurité, par exemple au moyen d'un algorithme de signature à clé publique, utilisant classiquement une clé privée qui est détenue par l'unité 20, et une clé publique.

En variante, l'intégrité de la donnée de sécurité peut être garantie au moyen d'un algorithme de type secure sketch, c'est-à-dire un algorithme de codage basé sur l'utilisation d'un code correcteur d'erreur, qui comprend la mise en œuvre, par l'unité de traitement 10, des étapes consistant à :

- Binariser le cas échéant la donnée de sécurité pour obtenir une donnée b,
- A partir d'un mot c d'un code correcteur d'erreur, obtenir à partir de la référence un résultat tel que r = [c XOR b, h(c)], où XOR est la fonction « ou exclusif », et h est une fonction de hashage cryptographique, par exemple de type SHA-256, et enregistrer le résultat r avec la donnée de sécurité, soit dans le document, soit dans la base de données 2.

Vérification de l'intégrité d'un document

En référence à la figure 1b, on a représenté un système de vérification 3 de l'intégrité d'un document. La vérification peut avoir lieu par exemple lors d'un contrôle du document, ou d'un contrôle de l'identité d'un individu dans le cas où le document est un document d'identité de l'individu.

Le système de vérification 3 comprend avantageusement une unité de traitement 30, comprenant des moyens de traitement 31 comme un calculateur, par exemple de type processeur, microprocesseur, microcontrôleur, etc.

Les moyens de traitement 31 sont adaptés pour exécuter un algorithme identique à celui qui a déjà été décrit ci-avant pour obtenir, à partir d'une image, une donnée de sécurité.

Le système de vérification comporte également un capteur d'images 32, typiquement un appareil photographique numérique. Il peut s'agir d'un appareil photographique intégré dans un téléphone mobile (smartphone) ou une tablette numérique.

Le système de vérification 3 est avantageusement intégré dans un boitier portatif de manière à pouvoir être déployé facilement lors d'un contrôle ; par exemple le système de vérification peut être intégré à un téléphone mobile, une tablette numérique, etc.

Le cas échéant, si la donnée de sécurité de référence est enregistrée dans la base de données 2, le système de vérification 3 comprend enfin une interface de communication 33 adaptée pour communiquer à distance avec l'unité de traitement

gestionnaire 20 de la base de données 2, par exemple par Internet sans fil, signal radiofréquence, etc.

En référence à la figure 3, un procédé de vérification 200 de l'intégrité d'un document comprend une première étape 210 d'acquisition, avec le capteur d'images 32, d'une image de l'élément visuel du document dont on souhaite vérifier l'intégrité.

Puis, l'unité de traitement 30 exécute 220, à partir de cette image, le même algorithme que celui qui a été exécuté lors du procédé de sécurisation pour obtenir la donnée de sécurité de référence d_r, et elle obtient une nouvelle donnée de sécurité d.

Avantageusement, l'image acquise lors de l'étape 210 peut être traitée de la même manière que l'élément visuel avant de générer la nouvelle donnée de sécurité pour estomper les variations liées à la prise d'image. Ainsi l'image peut aussi être recalée et normalisée.

L'unité de traitement 30 récupère ensuite, auprès de la base de données 2 ou du document, la donnée de sécurité de référence d_r correspondant à l'élément visuel à vérifier.

Avantageusement, le procédé de vérification 200 comporte une étape 230 de vérification de l'intégrité de la donnée de sécurité de référence.

Si la donnée de sécurité de référence d_r a été signée par l'unité de traitement 10, l'unité de traitement 30 du système de vérification 3 vérifie au cours d'une étape 230 que la signature est valide en utilisant la clé publique associée à la clé privée utilisée lors de la signature.

Si la donnée de sécurité de référence est enregistrée avec un résultat r de l'application d'un algorithme secure sketch, l'intégrité de la donnée de référence est vérifiée lors d'une même étape 230 par l'unité de traitement 30. Pour ce faire l'unité de traitement 30 binarise la nouvelle donnée de sécurité d pour obtenir une donnée binarisée b'.

Elle calcule ensuite c XOR b XOR b' à partir de la donnée r. Si b et b' sont suffisamment proche alors cette opération fournit le mot de code c utilisé initialement par l'unité 10, grâce à la capacité correctrice du code correcteur et garantit donc l'intégrité de la donnée de sécurité de référence.

Si le résultat de l'étape 230 de vérification indique que la donnée de sécurité de référence n'est pas intègre, alors l'unité de traitement 30 détermine que le document est frauduleux.

Si le résultat de l'étape 230 de vérification indique que la donnée de sécurité de référence est intègre, alors l'unité de traitement 30 compare lors d'une étape 240 la nouvelle donnée de sécurité d à la donnée de sécurité de référence d_r, par le calcul entre ces données d'une fonction appropriée telle qu'une distance euclidienne, une distance de Hamming, etc, et compare le résultat à un seuil déterminé, qui correspond au seuil introduit ci-avant, et discriminant des images sensiblement identiques et des images sensiblement différentes.

Le procédé 200 comprend enfin une étape de détermination 250, en fonction du résultat de la comparaison, du caractère frauduleux ou non du document. Si les différences entre les deux données sont inférieures au seuil, le document est considéré intègre. Sinon, le document est considéré falsifié.

REVENDICATIONS

1. Procédé de sécurisation (100) d'un document comportant un élément visuel, mis en œuvre par une unité de traitement (10) comprenant des moyens de traitement (11), le procédé comprenant la génération (110), à partir de l'élément visuel, d'une donnée de sécurité de référence (d_r), et la mémorisation (120) de la donnée de sécurité de référence,

dans lequel la donnée de sécurité de référence (d_r) est générée au moyen d'un algorithme paramétré à partir d'un entraînement sur une base de données d'apprentissage,

dans lequel, pour l'entrainement de l'algorithme, l'algorithme est exécuté

sur un grand nombre de paires d'images, et des indications lui sont fournies sur celles qui doivent résulter en des données de sécurité sensiblement identiques,

sur d'autres paires d'images qui doivent résulter en des données de sécurité sensiblement différentes.

2. Procédé de sécurisation (100) d'un document selon la revendication 1, dans lequel la génération (110) de la donnée de sécurité de référence (d_r) est mise en œuvre lors de la création du document.

3. Procédé de sécurisation (100) d'un document selon l'une des revendications 1 ou 2, dans lequel la donnée de sécurité de référence est mémorisée (120) dans le document, par affichage, par exemple impression, de la donnée sur le document ou par enregistrement de la donnée dans une puce électronique stockée dans le document.

4. Procédé de sécurisation (100) d'un document selon l'une des revendications 1 ou 2, dans lequel la donnée de sécurité de référence (d_r) est mémorisée (120) en étant enregistrée dans une base de données (2).

5. Procédé de sécurisation (100) d'un document selon l'une quelconque des revendications 1 à 4, dans lequel la donnée de sécurité de référence (d_r) est mémorisée (120) dans le document par affichage, par exemple impression, de la

Date Reçue/Date Received 2022-02-08

donnée sur le document et dans lequel l'élément visuel est lui aussi affiché, par exemple imprimé sur le document.

6. Procédé de sécurisation (100) d'un document selon l'une quelconque des revendications 1 à 5, dans lequel le document est un document électronique comprenant préférablement des moyens d'affichage.

7. Procédé de sécurisation (100) d'un document selon l'une quelconque des revendications 3 à 6, dans lequel la donnée de sécurité de référence (d_r) est signée par l'unité de traitement (10), au moyen d'un algorithme de signature à clé publique, ou enregistrée avec un certificat d'authenticité obtenu par l'application d'un algorithme de codage basé sur l'utilisation d'un code correcteur d'erreur, dit secure sketch.

8. Procédé de sécurisation (100) d'un document selon l'une quelconque des revendications 1 à 7, dans lequel l'algorithme est choisi de sorte que la reconstitution de l'élément visuel à partir de la donnée de sécurité correspondante soit impossible.

9. Procédé de sécurisation (100) d'un document selon l'une quelconque des revendications 1 à 8, dans lequel l'algorithme est du type comprenant l'utilisation d'histogrammes de gradients orientés sur l'élément visuel, ou de réseaux de neurones convolutionels, ou de type algorithme à descripteur.

10. Procédé de sécurisation (100) d'un document selon l'une quelconque des revendications 1 à 9, dans lequel l'algorithme est à descripteur de type BRIEF, ou de type SIFT, ou de type SURF ou de type GLOH, ou de type ORB, ou de type BRISK ou de type FREAK ou de type LATCH.

11. Procédé de sécurisation (100) d'un document selon l'une quelconque des revendications 1 à 10, dans lequel ledit algorithme étant entrainé de manière à générer :

Date Reçue/Date Received 2022-02-08

- pour toute image acquise de l'élément visuel, une donnée de sécurité dont les différences par rapport à la donnée de sécurité de référence sont inférieures à un seuil déterminé, et
- pour toute image acquise sur un élément visuel différent, une donnée de sécurité dont les différences par rapport à la donnée de sécurité de référence sont supérieures audit seuil.

12. Procédé de sécurisation (100) d'un document selon l'une quelconque des revendications 1 à 11, dans lequel l'élément visuel est une image du visage d'un individu, et l'algorithme est entrainé de manière à générer :

- pour toute image acquise de l'image du visage de l'individu figurant sur le document, une donnée de sécurité dont les différences par rapport à la donnée de sécurité de référence sont inférieures à un seuil déterminé, et
- pour toute image acquise d'une image représentant un autre individu, ou le même individu dans des conditions d'acquisition d'image différentes, une donnée de sécurité dont les différences par rapport à la donnée de sécurité de référence sont supérieures audit seuil.

13. Procédé de sécurisation (100) d'un document comportant un élément visuel, mis en œuvre par une unité de traitement (10) comprenant des moyens de traitement (11), le procédé comprenant la génération (110), à partir de l'élément visuel, d'une donnée de sécurité de référence (d_r), et la mémorisation (120) de la donnée de sécurité de référence,

dans lequel la donnée de sécurité de référence (d_r) est générée au moyen d'un algorithme paramétré à partir d'un entraînement sur une base de données d'apprentissage, ledit algorithme étant entrainé de manière à générer :

- pour toute image acquise de l'élément visuel, une donnée de sécurité dont les différences par rapport à la donnée de sécurité de référence sont inférieures à un seuil déterminé, et
- pour toute image acquise sur un élément visuel différent, une donnée de sécurité dont les différences par rapport à la donnée de sécurité de référence sont supérieures audit seuil.

Date Reçue/Date Received 2022-02-08

14. Produit programme d'ordinateur, comprenant des instructions de code pour la mise en œuvre d'un procédé selon l'une quelconque des revendications 1 à 13, quand il est exécuté par des moyens de traitement (11) d'une unité de traitement (10).

15. Document sécurisé pouvant être obtenu par la mise en œuvre d'un procédé selon l'une quelconque des revendications 1 à 13.

16. Procédé de vérification (200) de l'intégrité d'un document sécurisé par la mise en œuvre du procédé selon l'une quelconque des revendications 1 à 13, le procédé comprenant les étapes consistant à :

- acquérir une image (210) de l'élément visuel du document,
- générer (220), à partir de l'image, une donnée de sécurité (d) par le même algorithme que celui ayant permis de générer la donnée de sécurité de référence (d_r),
- comparer (240) la donnée de sécurité (d) obtenue à la donnée de sécurité de référence (d_r), et
- si les différences entre la donnée de sécurité (d) et la donnée de sécurité de référence (d_r) sont inférieures au seuil déterminé, déterminer (250) que l'élément visuel est intègre, sinon déterminer (250) que l'élément visuel est frauduleux.

17. Procédé de vérification (200) selon la revendication 16, dans lequel le procédé comprend en outre, avant l'étape de comparaison, une étape de vérification (230) de l'intégrité de la donnée de sécurité de référence (d_r).

18. Système (3) de vérification d'un document, comprenant :

- un capteur d'image (32),
- une unité de traitement (30), comprenant des moyens de traitement (30) adaptés pour mettre en œuvre, sur une image acquise par le capteur, un algorithme de classification, et une interface de communication (33) avec une base de données (2),

le système de vérification étant configuré pour mettre en œuvre le procédé selon l'une des revendications 16 ou 17.

Date Reçue/Date Received 2022-02-08

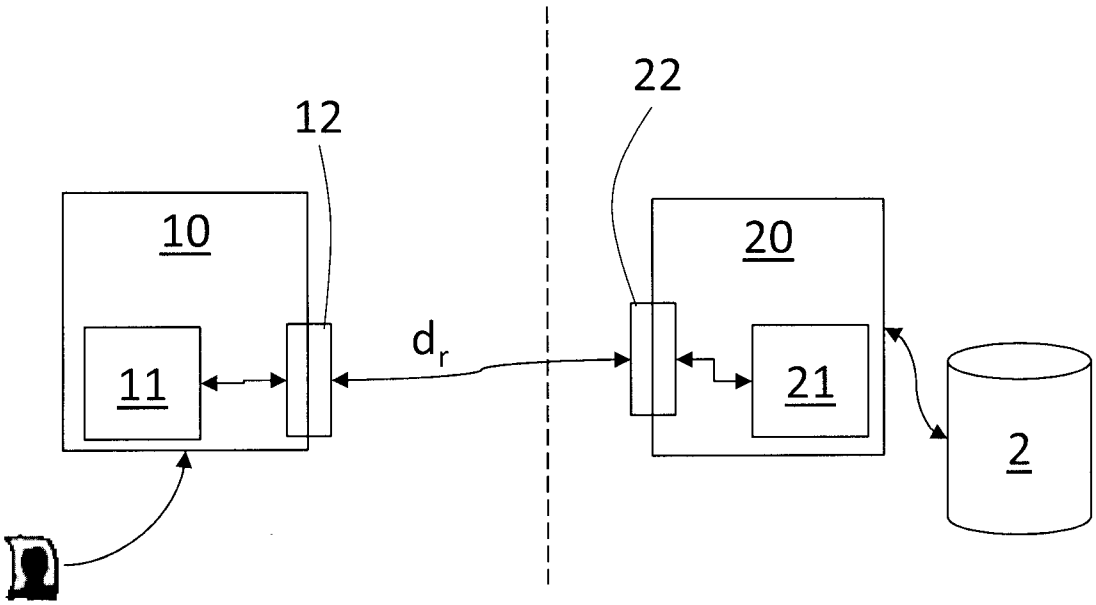


FIG. 1a

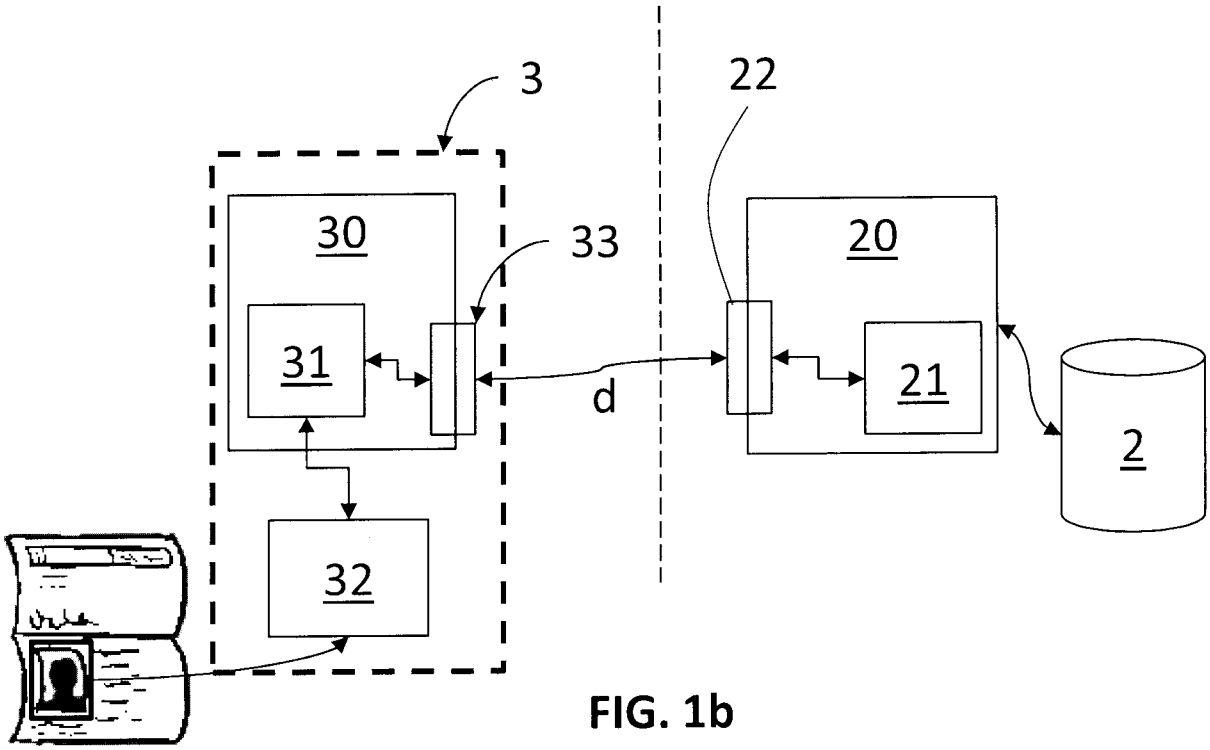


FIG. 1b

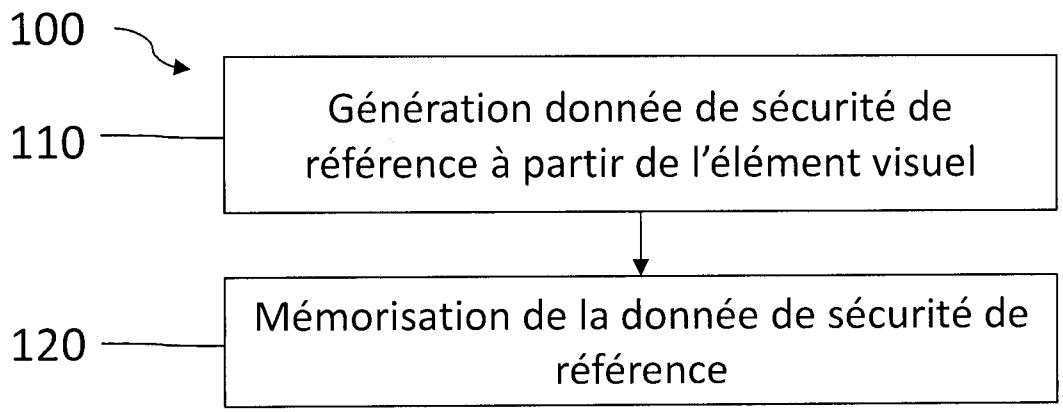

100
110
Génération donnée de sécurité de référence à partir de l'élément visuel
120
Mémorisation de la donnée de sécurité de référence

FIG. 2

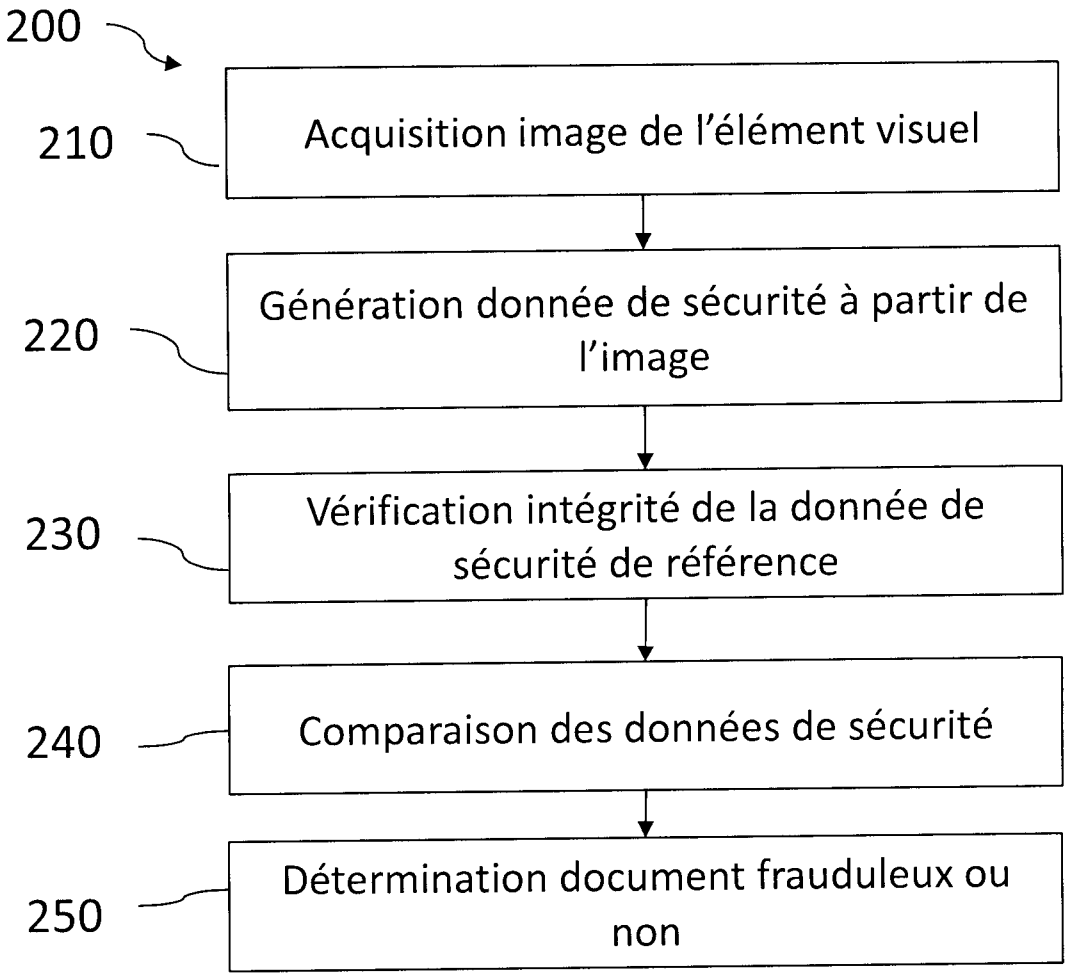
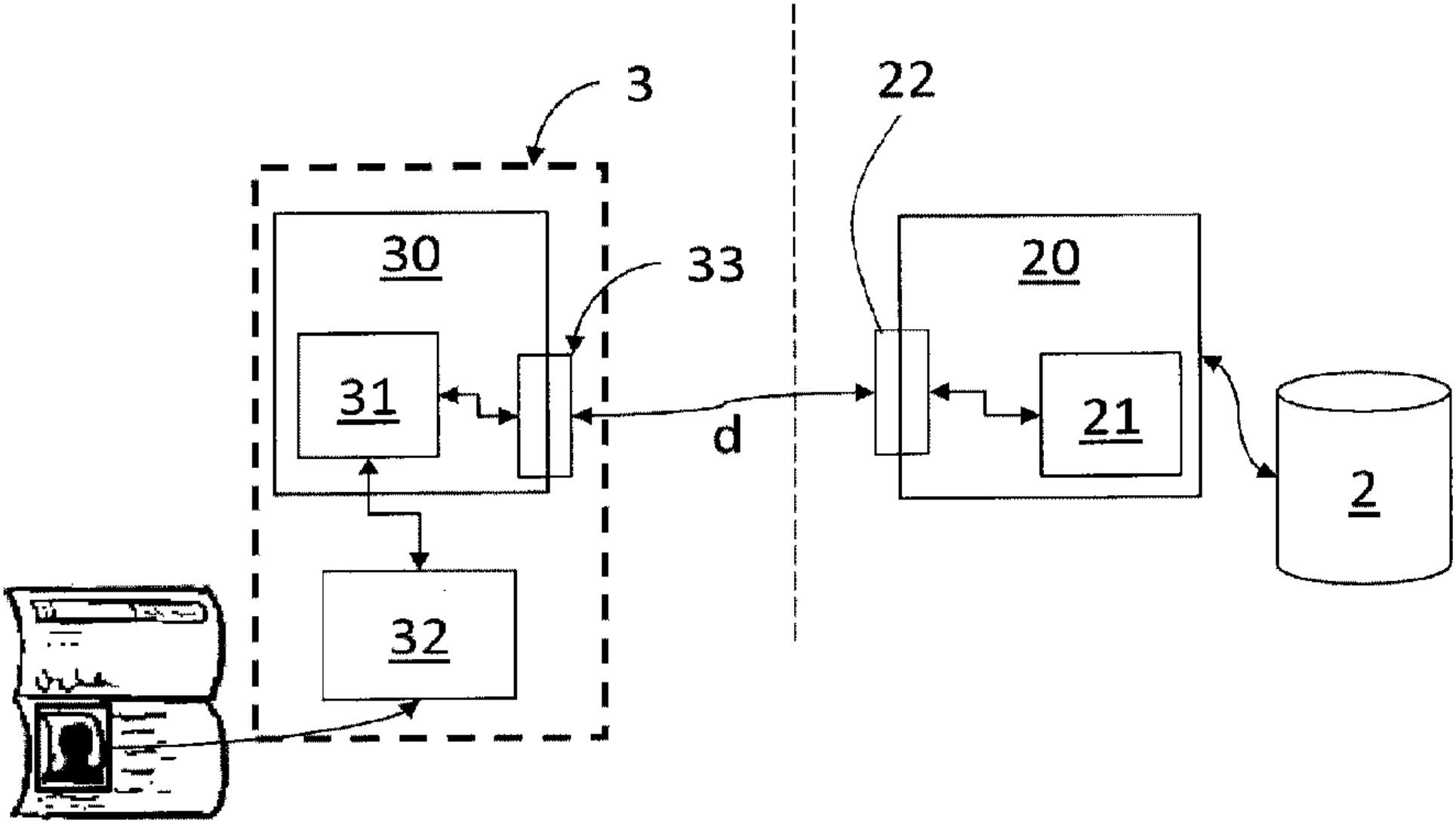

200
210
Acquisition image de l'élément visuel
220
Génération donnée de sécurité à partir de l'image
230
Vérification intégrité de la donnée de sécurité de référence
240
Comparaison des données de sécurité
250
Détermination document frauduleux ou non

FIG. 3


3
22
30
33
20
31
21
d
2
32