(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** **3 073 301**

(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **17 71186**

(51) Int Cl[8] : ***G 06 F 21/32*** *(2018.01), G 06 K 9/20*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 09.11.17.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 10.05.19 Bulletin 19/19.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

( ) **Demande(s) d'extension :**

(71) **Demandeur(s) :** *ICARE TECHNOLOGIES Société par actions simplifiée* — FR.

(72) **Inventeur(s) :** NEYROU JEREMY, RAIOLA FABIEN et BERTOLOZZI SEBASTIEN.

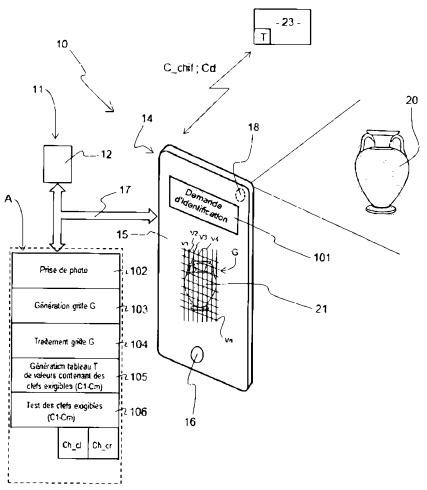
(73) **Titulaire(s) :** ICARE TECHNOLOGIES Société par actions simplifiée.

(74) **Mandataire(s) :** MARCONNET Sébastien.

(54) PROCEDE D'IDENTIFICATION PAR ANALYSE STANDARDISEE DE DONNEES PHYSIQUES.

(57) L'invention porte principalement sur un procédé d'identification d'un utilisateur par analyse d'une image numérique représentant un objet physique (20) pour accéder à un service, caractérisé en ce qu'il comporte les étapes suivantes:

- une étape (101) d'émission d'une demande d'identification émise notamment par une application (A),
- une étape (102) de prise d'une photographie numérique d'au moins un objet physique (20), au moyen d'un appareil (10) muni d'une caméra (18) par exemple de type téléphone mobile ou tablette numérique, pour obtenir une image numérique (21) représentant l'objet (20),
- une étape de chiffrement (103, 104, 105) d'un champ connu (Ch_cl, Ch_cr) à partir de données issues de l'image numérique (21), et
- une étape de déchiffrement du champ connu de sorte qu'en cas de déchiffrement correct du champ connu, l'identification de l'utilisateur est validée et l'opération est autorisée, et en cas de déchiffrement incorrect du champ connu (Ch_cl, Ch_cr), l'identification de l'utilisateur est invalidée et l'opération n'est pas autorisée.



FR 3 073 301 - A1

PROCÉDÉ D'IDENTIFICATION PAR ANALYSE STANDARDISÉE DE DONNÉES PHYSIQUES

[0001] La présente invention porte sur un procédé d'identification par analyse standardisée de données physiques. L'invention trouve une application particulièrement avantageuse, mais non exclusive, pour l'accès à un compte utilisateur d'une application mobile ou la récupération d'un mot de passe. L'invention pourra également être mise en œuvre pour le contrôle d'une identité, l'accès à un lieu, à des services, ou bien encore le chiffrement des données en utilisant un objet comme clef de chiffrement accès à des services, l'accès ou le démarrage d'un véhicule, la réalisation directe ou indirecte d'un ou plusieurs achats, éventuellement à distance par Internet. L'invention pourra être mise en œuvre dans tout système informatique visant à protéger les données personnelles d'un utilisateur.

[0002] Les protocoles classiques de récupération de mots de passe nécessitent généralement l'envoi d'un message électronique, d'un sms, l'émission d'un appel ou autre. Généralement, le téléphone mobile du propriétaire reçoit des notifications pour permettre l'identification du porteur.

[0003] Ces systèmes conventionnels présentent une importante faille de sécurité, dans la mesure où ils font appel soit à un canal de communication dérivé, soit à une connaissance particulière de l'utilisateur (nom de jeune fille de sa mère, nom du premier animal de compagnie, etc...).

[0004] Ces questions de sécurité obligent l'utilisateur à entrer une information considérée comme “personnelle" qui reste toutefois accessible du fait de l'étalement de la vie privée sur Internet, ou à entrer une information aucunement liée à la question. Dans la grande majorité des cas, l'utilisateur ayant oublié son mot de passe a également oublié la réponse à la question secrète.

[0005] Le principe de changement de canal est relativement efficace, mais repose sur le téléphone mobile, de sorte que si celui-ci venait à être dérobé, une grande partie des données sensibles et des comptes deviendrait accessibles. En effet, dans ce cas, l'usurpateur recevrait tous les appels, sms

ou mails de récupération de mot de passe sur le téléphone, ce qui lui donnerait la possibilité de prendre le contrôle des comptes de l'utilisateur.

[0006] L'invention vise à remédier efficacement à ces inconvénients en proposant un procédé d'identification d'un utilisateur par analyse d'une image numérique représentant un objet physique pour autoriser une opération, caractérisé en ce que ledit procédé comporte:
- une étape d'émission d'une demande d'identification émise notamment par une application,
- une étape de prise d'une photographie numérique d'au moins un objet physique, au moyen d'un appareil muni d'une caméra par exemple un appareil de type téléphone mobile ou tablette numérique, pour obtenir une image numérique représentant l'objet,
- une étape de chiffrement d'un champ connu à partir de données issues de l'image numérique, et
- une étape de déchiffrement du champ connu de sorte qu'en cas de déchiffrement correct du champ connu, l'identification de l'utilisateur est validée et l'opération est autorisée, et en cas de déchiffrement incorrect du champ connu, l'identification de l'utilisateur est invalidée et l'opération n'est pas autorisée.

[0007] Selon une mise en œuvre, ledit procédé comporte:
- une étape de création d'une grille de valeurs correspondant à l'image numérique échantillonnée,
- une étape de traitement de la grille de valeurs pour obtenir une grille de valeurs modifiées.

[0008] Selon une mise en œuvre, ledit procédé comporte:
- une étape de génération d'un tableau de valeurs contenant des clefs éligibles à partir des valeurs modifiées de la grille, et
- une étape de test des clefs éligibles pour déchiffrer le champ connu.

[0009] L'étape de test peut être réalisée via l'application d'un algorithme de reconnaissance qui teste successivement les clés éligibles pour déchiffrer le champ connu ou selon toute autre méthode de détrompage permettant de déterminer la bonne clef, notamment à l'aide de variable de somme de contrôle, dite de type "checksum".

[0010] Selon une mise en œuvre, le champ connu est stocké crypté et en clair.

[0011] Selon une mise en œuvre, le champ connu est défini de façon aléatoire ou non lors d'une création de compte de l'utilisateur. Ce champ connu pourra par exemple être une chaîne de caractères générée lors de la création du comte de l'utilisateur. La génération de cette chaîne de caractères pourra être transparente pour l'utilisateur.

[0012] Selon une mise en œuvre, l'étape de traitement des valeurs de la grille pour obtenir une grille de valeurs modifiées est basée sur:
- l'application de filtres de traitement sur la grille de valeurs pour réduire un nombre de valeurs de la grille, et/ou
- l'application de filtres, dits de compréhension, effectuant une analyse et une pondération de la grille de valeurs en fonction de densités de valeurs.

[0013] A aucun moment la valeur des clefs n'est comparée à une valeur stockée en local ou à distance.

[0014] Selon une mise en œuvre, au moins une partie des étapes peut être effectuée à distance ou en local sur l'appareil.

[0015] Selon une mise en œuvre, une corrélation est effectuée avec d'autres capteurs de manière à générer des valeurs supplémentaires et/ou complémentaires.

[0016] Selon une mise en œuvre, dans le cas où certaines étapes sont réalisées à distance, un mécanisme de chiffrement des communications, par exemple lors de la transmission des clefs éligibles vers un serveur (23), est mis en œuvre afin de sécuriser des échanges d'informations.

[0017] Selon une mise en œuvre, les étapes suivantes sont mises en œuvre préalablement à l'étape de test des clefs éligibles:
- une étape d'application d'un algorithme de création d'une chaîne chiffrée par concaténation des valeurs pour obtenir une clef chiffrée, ladite clef chiffrée contenant un ensemble de clefs éligibles issues du tableau de valeurs,
- une étape de décryptage de la clef chiffrée par le serveur pour régénérer l'ensemble du tableau de valeurs,

- une étape d'application d'un algorithme, dit de lutte contre la fraude, testant une concordance des valeurs du tableau régénéré et la faisabilité réelle d'un tel enchaînement pour se prémunir d'un piratage par brute force, et
- dans le cas où l'algorithme valide le tableau de valeurs, le procédé met en œuvre l'étape de test des clefs éligibles.

[0018] Selon une mise en œuvre, l'étape de prise de la photographie numérique est effectuée dans des conditions de prises de vue standardisées.

[0019] Selon une mise en œuvre, les conditions de prise de vue standardisées sont choisies parmi les suivantes: fond blanc, jusqu'à trois objets visibles, objets non superposés, objets visibles en intégralité, et conditions d'éclairage standardisées sans ombre.

[0020] Selon une mise en œuvre, une intelligence artificielle est configurée pour améliorer une détection de l'objet dans des conditions réelles d'éclairage et/ou traiter des objets incomplets sur l'image numérique et/ou superposés quel qu'en soit le fond.

[0021] Selon une mise en œuvre, ledit procédé comporte une étape de traitement combinée à une reconnaissance infrarouge pour s'affranchir de conditions d'éclairage et/ou d'ombre.

[0022] Selon une mise en œuvre, ledit procédé est mis en œuvre sur plusieurs photographies numériques, notamment en prenant des photographies de plusieurs objets dans un ordre spécifique, par exemple trois objets successifs, ou un objet sous plusieurs angles différents, par exemple sous trois angles différents.

[0023] Selon une mise en œuvre, ledit procédé comporte en outre une étape d'analyse de sons et/ou de vidéos pour corroborer l'identification effectuée via la photographie numérique.

[0024] Selon une mise en œuvre, ledit procédé comporte en outre une étape d'analyse de code, tel qu'un code barre en deux dimensions, associé à ou aux objets (20) pris en photo pour corroborer l'identification.

[0025] Selon une mise en œuvre, l'opération autorisée ou non est choisi parmi: récupération d'un mot de passe, connexion à un compte utilisateur, contrôle d'identité, accès à un lieu, accès à des applications, ou déchiffrement de données, accès à des services, accès ou démarrage d'un véhicule, réalisation directe ou indirecte d'un ou plusieurs achats, éventuellement à distance par Internet.

[0026] Selon une mise en œuvre, ledit procédé est mis en œuvre dans les cas d'utilisation d'un casque de réalité augmentée ou de réalité virtuelle.

[0027] Selon une mise en œuvre, ledit procédé comporte une étape de reconnaissance biométrique dans laquelle une partie du corps est contrôlée de manière à réaliser une identification forte.

[0028] Selon une mise en œuvre, à la fin de l'étape de traitement de la grille de valeurs, des points restants représentent une structure de l'objet ou d'une partie du corps de l'utilisateur.

[0029] Selon une mise en œuvre, une analyse est pratiquée sur autre chose qu'une photographie, notamment un son, une image 2D, 3D, créée à partir d'un ou de capteurs ultrasons, thermiques, tactiles, ou autre.

[0030] Selon une mise en œuvre, ledit procédé est mis en œuvre sur une série d'images numériques ou sur une vidéo numérique. On peut ainsi analyser en direct, sur une vidéo, les images utilisées pour réaliser l'identification de l'utilisateur.

[0031] Selon une mise en œuvre, ledit procédé comporte une étape de détection d'une partie du corps d'un utilisateur, notamment un tour de doigt, basé sur la réalisation d'une étape de détermination d'une donnée relative à une dimension de la zone cible en fonction d'un écart entre des repères de mesure et pourra, le cas échéant, faire intervenir des modèles 2D ou 3D de la partie du corps, ainsi que des données biométriques ou non pour effectuer une identification du porteur. On pourra se référer à la demande de brevet français déposée sous le numéro FR1771088 pour plus de détails sur ce procédé.

[0032] Selon une mise en œuvre, ledit procédé comporte une étape d'analyse conventionnelle d'identification avant de réaliser une analyse d'une image d'un

objet ou d'une partie du corps de l'utilisateur. Ainsi, lorsqu'un appareil de type montre ou bague est connectée via une liaison radio, par exemple de type Bluetooth (marque déposée) à un téléphone mobile via lequel a été effectuée une identification, on considère par persistance que l'utilisateur reste le même et identifié, un objet utilisé comme clef de chiffrement étant présenté pour finaliser une authentification forte.

[0033] Selon une mise en œuvre, ledit procédé comporte une étape de combinaison de plusieurs mesures et/ou plusieurs capteurs, notamment au moins deux capteurs pour créer une image en trois dimensions.

[0034] Selon une mise en œuvre, une caméra disposée sous une vitre est configurée pour réaliser des étapes de traitement d'image d'une partie de l'objet ou d'une partie du corps posé sur ladite vitre.

[0035] Selon une mise en œuvre, une caméra ou un détecteur ultrason ou un détecteur infrarouge déporté du dispositif filme une zone colorée ou calibrée, de sorte que lorsque l'utilisateur place un objet ou une partie de son corps dans cette zone calibrée, un examen aisé peut être réalisé.

[0036] Selon une mise en œuvre, ledit procédé comporte une étape de prélèvement d'une ou plusieurs informations propres à un environnement et/ou à une partie du corps de l'utilisateur issues de capteurs biométriques avant, pendant ou après une phase d'identification, notamment par combinaison et avec d'autres capteurs, de type température, poids, humidité, densité graisseuse, lecture de veines, de pouls, lecteur d'iris, d'impédance, réflectivité, ADN, pigmentation de la peau, empreinte digitale, gerçures ou aspérités de la peau, ou autres données biométriques.

[0037] Selon une mise en œuvre, ledit procédé comporte une étape de prélèvement ou d'échange d'une ou plusieurs informations d'un ou plusieurs des objets portés par une partie du corps de l'utilisateur avant, pendant ou après l'identification (par combinaison et avec d'autres capteurs), via un réseau radiofréquence, notamment de type NFC (pour Near Field Communication en anglais), Bluetooth (marque déposée), lora (marque déposée), Sigfox (marque déposée), GSM, et/ou téléphonique de tout type,

code barre à une ou plusieurs dimensions, couleur, forme, modèle d'un objet, plusieurs informations pouvant être corrélées entre elles.

[0038] Selon une mise en œuvre, ledit procédé comporte une étape de reconnaissance et d'analyse d'un ou plusieurs tatouages, de grains de beauté, de cicatrice ou autres imperfections de la peau.

[0039] Selon une mise en œuvre, ledit procédé comporte une étape de reconnaissance d'objets portés ou non par l'utilisateur, tel qu'une bague, un bracelet, un collier, une montre, un vêtement, des chaussures, un chapeau, une casquette, des lunettes, ou autre. Cela permet de détecter la présence ou non de ces objets sur l'utilisateur ainsi que leurs dimensions.

[0040] L'invention sera mieux comprise à la lecture de la description qui suit et à l'examen des figures qui l'accompagnent. Ces figures ne sont données qu'à titre illustratif mais nullement limitatif de l'invention.

[0041] La figure 1 est une représentation schématique d'un appareil portatif de type téléphone mobile ou tablette apte à mettre en œuvre le procédé selon l'invention d'identification d'un utilisateur par la prise de photographie d'un objet de son choix;

[0042] La figure 2 est une représentation schématique des différentes étapes du procédé selon la présente invention.

[0043] Il est à noter que le procédé d'identification selon l'invention peut être mis en œuvre avec une très large diversité de périphériques. Dans la pratique, il peut être mise en œuvre avec tous les périphériques réalisant une identification directement ou indirectement comme les lecteurs, les caméras ou lecteurs de reconnaissance biométrique, les claviers à code, les smartphones (caméra(s) avant et/ou arrière), les ordinateurs, les consoles de jeu, portes, sas de contrôle. La description qui suit faisant intervenir un appareil portatif n'est donc aucunement limitative.

[0044] La figure 1 montre un appareil portatif 10 de type téléphone mobile ou tablette numérique comportant un microcontrôleur 11 intégrant un microprocesseur 12 et une mémoire 13, ainsi qu'une interface homme-machine 14 comprenant par exemple un écran tactile 15.

[0045] Suivant un exemple de réalisation particulier, l'appareil portatif 10 peut comporter également un bouton central de commande 16 ainsi que d'autres boutons de commande physiques, tels que des boutons de réglage du volume sonore. Toutefois, cela n'est pas obligatoire, l'appareil 10 pouvant comporter uniquement des boutons de commande numériques s'affichant sur l'écran 15. Les éléments fonctionnels 12, 13, 15 communiquent entre eux via un bus de communication standard 17. En variante, l'écran 15 n'est pas tactile et l'interface homme-machine 14 prend la forme d'un clavier physique.

[0046] Une caméra 18 pourra être implantée à l'avant et/ou à l'arrière de l'appareil 10. Cette caméra 18 permet la prise de photographie numérique.

[0047] L'appareil portatif 10 peut comporter également d'autres composants nécessaires à son fonctionnement (module de communication, microphone, haut-parleur, etc…) qui ne sont pas représentés sur la figure afin de faciliter la compréhension de l'invention. Ces composants élémentaires sont bien connus de l'homme du métier.

[0048] La mémoire 13 stocke des instructions logicielles gérées par une application pour la mise en œuvre du procédé d'identification décrit ci-après. Ces instructions logicielles sont gérées par une application A. Il est à noter que les clefs éligibles C1-Cm sont stockées uniquement dans la mémoire vive lors de leur utilisation et sont donc effacées après chaque utilisation.

[0049] La principale différence de l'invention par rapport à un système d'identification biométrique conventionnel de type analyse de visage ou d'empreinte digitale est qu'il n'est pas nécessaire que le procédé selon l'invention détienne (directement ou indirectement) une copie (totale ou partielle) de l'objet 20, de la photographie, de la couleur, des dimensions, de la structure ni d'aucune de ses caractéristiques physiques qui seraient recherchées pour l'identification. Cela procure un haut niveau de sécurisation au système.

[0050] En effet, contrairement à un algorithme de reconnaissance faciale ou de lecture d'un code barre à deux dimensions (QR code), le système n'utilise aucune référence pour ensuite effectuer une identification ou identifier des points de référence. Le système ne nécessite pas de connaître l'objet qu'il

recherche sur l'image et doit se comporter d'une manière identique, quel que soit l'objet 20 physique utilisé pour l'identification. L'ensemble des clefs éligibles C1-Cm générées peut être limité de manière à ce qu'une brute force (piratage par tentatives successives) ne puisse pas être utilisée. La limitation peut être effectuée en termes de quantité et/ou de temporalité et/ou d'écart de concordance entre deux clefs.

[0051] Les clefs générées C1-Cm issues de la combinaison des valeurs du tableau T sont testées par un module qui ne fournit en retour qu'un vrai ou faux. Un lien peut être effectué d'une clef à l'autre pour permettre la création d'une chaîne de valeurs, notamment de type chaîne de bloc ou "blockchain" en anglais. Ainsi, dans un exemple de réalisation, la clef N+2 peut contenir le résultat d'un traitement particulier des valeurs pondérées et être concaténée avec la clef N+1 (qui elle-même pourrait contenir la même structure accompagnée de la clef N+0).

[0052] La reconnaissance peut être effectuée à partir de n'importe laquelle des caractéristiques physiques de l'objet 20 physique ou du corps et selon certaines réalisations la corrélation entre plusieurs caractéristiques physiques est aussi possible (couleur/ratios dimensionnels).

[0053] On décrit ci-après, en référence avec les figures 1 et 2, un exemple de mise en œuvre détaillé du procédé d'identification d'un utilisateur par analyse standardisée d'une image numérique 21 représentant un objet 20 physique pour accéder à un service. Ce service pourra être la récupération d'un mot de passe, la connexion à un compte utilisateur, un contrôle d'identité, l'accès à un lieu, des applications, ou un chiffrement de données utilisant l'objet 20 comme clef de chiffrement. accès à des services, accès ou démarrage d'un véhicule, la réalisation directe ou indirecte d'un ou plusieurs achats, éventuellement à distance par Internet.

[0054] Dans une étape 101, l'application A émet une demande d'identification.

[0055] Dans une étape 102, l'utilisateur prend une photographie numérique d'un objet 20 physique, notamment un objet inerte, au moyen de l'appareil 10 muni de sa caméra, pour obtenir une image numérique 21 représentant l'objet

20. L'objet 20 choisi est propre à l'utilisateur et seul l'utilisateur en a connaissance. Cet objet 20 pourra avoir un usage non exclusif pour cette application.

[0056] L'application A génère, dans une étape 103, une grille G de valeurs V1-Vn pondérées par des couleurs correspondant à l'image numérique 21 échantillonnée.

[0057] La grille G de valeurs V1-Vn est traitée dans une étape 104 pour obtenir une grille de valeurs modifiées. Cette étape de traitement des valeurs de la grille pour obtenir une grille de valeurs G modifiées est basée sur l'application de filtres de traitement sur la grille de valeurs G pour réduire un nombre de valeurs de la grille, et/ou l'application de filtres, dits de compréhension, effectuant une analyse et une pondération de la grille de valeurs G en fonction de densités de valeurs. A la fin de l'étape de traitement de la grille de valeurs G, des points restants peuvent représenter une structure de l'objet ou d'une partie du corps de l'utilisateur. Autrement dit, on obtient à la fin du traitement une empreinte identifiable de l'image numérique 21.

[0058] L'application génère, dans une étape 105, un tableau de valeurs T contenant des clefs éligibles C1-Cm à partir d'une combinaison des valeurs modifiées de la grille G.

[0059] Dans une étape 106, les clefs éligibles C1-Cm sont testées pour déchiffrer un champ connu. Ce champ connu est stocké crypté (Ch_cr) et en clair (Ch_cl). Le champ connu Ch_cl est défini aléatoirement à la création d'un compte de l'utilisateur. Ce champ connu pourra par exemple être une chaîne de caractères générée lors de la création du comte de l'utilisateur. La génération de cette chaîne de caractères est transparente pour l'utilisateur.

[0060] En cas de déchiffrement correct du champ connu Ch_cr à l'aide des clefs éligibles C1-Cm, l'identification de l'utilisateur est validée et l'accès au service est autorisé. En cas de déchiffrement incorrect du champ connu Ch_cr, l'identification de l'utilisateur est invalidée et l'accès au service n'est pas autorisé.

[0061] L'étape de test 106 peut être réalisée via l'application d'un algorithme de reconnaissance qui teste successivement les clés éligibles C1-Cm pour déchiffrer le champ connu ou selon toute autre méthode de détrompage permettant de déterminer la bonne clef, notamment à l'aide d'une variable de somme de contrôle, dite variable "checksum" en anglais associée aux différentes clefs pour faciliter le test de leur authenticité.

[0062] Il est à noter qu'à aucun moment la valeur des clefs C1-Cm n'est comparée à une valeur correspondant de clefs stockée en local ou à distance.

[0063] Par ailleurs, au moins une partie des étapes 101-106 peut être effectuée à distance ou en local sur l'appareil portatif 10. Dans le cas où certaines étapes sont réalisées à distance, un mécanisme de chiffrement des communications, par exemple lors de la transmission des clefs éligibles C1-Cm vers un serveur 23, est mis en œuvre afin de sécuriser des échanges d'informations.

[0064] Plus précisément, préalablement à l'étape de test 106 des clefs éligibles C1-Cm, on applique, dans une étape 201, un algorithme de création d'une chaîne chiffrée par concaténation des valeurs pour obtenir une clef chiffrée C_chif, ladite clef chiffrée C_chif contenant un ensemble de clefs éligibles C1-Cm issues du tableau de valeurs T. La clef chiffrée C_chif et une clef de décodage Cd détenue ou générée aléatoirement par l'application A sont transmises au serveur 23 dans une étape 202.

Le serveur 23 décrypte ensuite la clef chiffrée C_chif pour régénérer l'ensemble du tableau de valeurs T dans une étape 203. Un algorithme, dit de lutte contre la fraude, est appliqué, dans une étape 204, pour tester une concordance des valeurs du tableau T régénéré et la faisabilité réelle d'un tel enchaînement pour se prémunir d'un piratage par brute force. Dans le cas où l'algorithme valide le tableau de valeurs T, le procédé met en œuvre l'étape de test 106 précitée des clefs éligibles C1-Cm.

[0065] Une corrélation des résultats du test des clefs C1-Cm pourra être effectuée avec d'autres capteurs de manière à générer des valeurs supplémentaires et/ou complémentaires.

[0066] Suivant certaines mises en œuvre, la prise de la photographie numérique est effectuée dans des conditions de prises de vue standardisées. Les conditions de prise de vue standardisées sont choisies parmi les suivantes: fond blanc, jusqu'à trois objets 20 visibles, objets 20 non superposés, objets 20 visibles en intégralité, et conditions d'éclairage standardisées sans ombre.

[0067] Une intelligence artificielle est configurée pour améliorer une détection de l'objet 20 dans des conditions réelles d'éclairage et/ou traiter des objets 20 incomplets sur l'image 21 et/ou superposés quel qu'en soit le fond.

[0068] Il est également possible de prévoir une étape de traitement combinée à une reconnaissance infrarouge pour s'affranchir de conditions d'éclairage et/ou d'ombre.

[0069] Le procédé d'identification peut également être mis en œuvre sur plusieurs photographies numériques, notamment en prenant des photographies de plusieurs objets 20 dans un ordre spécifique, par exemple trois objets 20 successifs, ou un objet 20 sous plusieurs angles différents, par exemple sous trois angles différents.

[0070] Le procédé peut être mis en œuvre sur une série d'images numériques ou sur une vidéo numérique. On peut ainsi analyser en direct, sur une vidéo, les images utilisées pour réaliser l'identification de l'utilisateur.

[0071] Il est également possible d'effectuer une analyse de sons et/ou de vidéos pour corroborer l'identification effectuée via la photographie numérique, ainsi qu'une analyse de code, tel qu'un QR code associé à ou aux objets 20 pris en photo pour corroborer l'identification.

[0072] Selon certaines réalisations l'analyse peut être pratiquée sur autre chose qu'une photographie, sur un son, une image 2D, 3D, crée à partir d'un ou de capteurs ultrasons, thermiques, tactiles. Il est possible de combiner plusieurs mesures et/ou plusieurs capteurs, notamment au moins deux capteurs pour créer une image en trois dimensions.

[0073] Un objet 20 et/ou une partie du corps peut donc efficacement être contrôlé de manière à réaliser une authentification/identification forte, dans la

mesure où la personne possède l'objet 20 d'identification, et la personne est la seule à connaître l'objet 20 qui est nécessaire à son authentification. Dans certains cas, notamment dans le domaine de la reconnaissance biométrique, la personne peut constituer l'objet 20.

[0074] Une caméra pourra être disposée sous une vitre est configurée pour réaliser des étapes de traitement d'image d'une partie de l'objet ou d'une partie du corps de l'utilisateur posée sur ladite vitre.

[0075] Une caméra ou un détecteur ultrason ou un détecteur infrarouge déporté du dispositif peut filmer une zone colorée ou calibrée, de sorte que lorsque l'utilisateur place un objet ou une partie de son corps dans cette zone calibrée, un examen aisé peut être réalisé.

[0076] Il est également possible de prévoir une étape de reconnaissance et d'analyse d'un ou plusieurs tatouages, de grains de beauté, de cicatrice ou autres imperfections de la peau.

[0077] Il est également possible de reconnaitre les objets portés ou non par l'utilisateur, tel qu'une bague, un bracelet, un collier, une montre, un vêtement, des chaussures, un chapeau, une casquette, des lunettes, ou autre. Cela permet de détecter la présence ou non de ces objets sur l'utilisateur ainsi que leurs dimensions.

[0078] On pourra prélever une ou plusieurs informations propres à un environnement et/ou à une partie du corps de l'utilisateur issues de capteurs biométriques avant, pendant ou après une phase d'identification, notamment par combinaison et avec d'autres capteurs, de type température, poids, humidité, densité graisseuse, lecture de veines, de pouls, lecteur d'iris, d'impédance, réflectivité, ADN, pigmentation de la peau, empreinte digitale, gerçures ou aspérités de la peau, ou autres données biométriques.

[0079] Il est également possible de prélever ou d'échanger une ou plusieurs informations d'un ou plusieurs des objets portés par une partie du corps de l'utilisateur avant, pendant ou après l'identification (par combinaison et avec d'autres capteurs), via un réseau radiofréquence, notamment de type NFC (pour Near Field Communication en anglais), Bluetooth (marque déposée),

lora (marque déposée), Sigfox (marque déposée), GSM, et/ou téléphonique de tout type, code barre à une ou plusieurs dimensions, couleur, forme, modèle d'un objet, plusieurs informations pouvant être corrélées entre elles.

[0080] Il est également possible d'assurer une détection d'une partie du corps d'un utilisateur, notamment un tour de doigt, basé sur la réalisation d'une étape de détermination d'une donnée relative à une dimension de la zone cible en fonction d'un écart entre des repères de mesure et pourra, le cas échéant, faire intervenir des modèles 2D ou 3D de la partie du corps, ainsi que des données biométriques ou non pour effectuer une identification du porteur. On pourra se référer à la demande de brevet français déposée sous le numéro FR1771088 pour plus de détails sur ce procédé.

[0081] Une analyse conventionnelle d'identification pourra être réalisée avant l'analyse d'image d'un objet ou d'une partie du corps de l'utilisateur. Ainsi, lorsqu'un appareil de type montre ou bague est connectée via une liaison radio, par exemple de type Bluetooth (marque déposée) à un téléphone mobile via lequel a été effectuée une identification, on considère par persistance que l'utilisateur reste le même et identifié, un objet utilisé comme clef de chiffrement étant présenté pour finaliser une authentification forte.

[0082] Le procédé selon l'invention peut avantageusement être mis en œuvre dans les cas d'utilisation d'un casque de réalité augmentée ou de réalité virtuelle afin d'identifier l'utilisateur.

[0083] Il est à noter que la description qui précède a été donnée à titre d'exemple uniquement et ne limite pas le domaine de l'invention dont on ne sortirait pas en remplaçant les différents éléments ou étapes par tous autres équivalents.

[0084] En outre, les différentes caractéristiques, variantes, et/ou formes de réalisation de la présente invention peuvent être associées les unes avec les autres selon diverses combinaisons, dans la mesure où elles ne sont pas incompatibles ou exclusives les unes des autres.

REVENDICATIONS

1. Procédé d'identification d'un utilisateur par analyse d'une image numérique représentant un objet physique (20) pour autoriser une opération, caractérisé en ce que ledit procédé comporte:
- une étape (101) d'émission d'une demande d'identification émise notamment par une application (A),
- une étape (102) de prise d'une photographie numérique d'au moins un objet physique (20), au moyen d'un appareil (10) muni d'une caméra (18) par exemple un appareil de type téléphone mobile ou tablette numérique, pour obtenir une image numérique (21) représentant l'objet (20),
- une étape de chiffrement (103, 104, 105) d'un champ connu (Ch_cl, Ch_cr) à partir de données issues de l'image numérique (21), et
- une étape de déchiffrement du champ connu de sorte qu'en cas de déchiffrement correct du champ connu, l'identification de l'utilisateur est validée et l'opération est autorisée, et en cas de déchiffrement incorrect du champ connu (Ch_cl, Ch_cr), l'identification de l'utilisateur est invalidée et l'opération n'est pas autorisée.

2. Procédé selon la revendication 1, caractérisé en ce qu'il comporte:
- une étape (103) de création d'une grille de valeurs (V1-Vn) correspondant à l'image numérique (21) échantillonnée,
- une étape (104) de traitement de la grille de valeurs (V1-Vn) pour obtenir une grille (G) de valeurs modifiées.

3. Procédé selon la revendication 2, caractérisé en ce qu'il comporte:
- une étape (105) de génération d'un tableau de valeurs (T) contenant des clefs éligibles (C1-Cm) à partir des valeurs modifiées de la grille (G), et
- une étape (106) de test des clefs éligibles (C1-Cm) pour déchiffrer le champ connu (Ch_cl, Ch_cr).

4. Procédé selon l'une quelconque des revendications 1 à 3, caractérisé en ce que le champ connu (Ch_cl, Ch_cr) est stocké crypté et en clair.

5. Procédé selon l'une quelconque des revendications 1 à 4, caractérisé en ce que le champ connu (Ch_cl, Ch_cr) est défini de façon aléatoire ou non lors d'une création de compte de l'utilisateur.

6. Procédé selon la revendication 2, caractérisé en ce que l'étape (104) de traitement des valeurs de la grille (G) pour obtenir une grille de valeurs modifiées est basée sur:
- l'application de filtres de traitement sur la grille de valeurs (G) pour réduire un nombre de valeurs de la grille, et/ou
- l'application de filtres, dits de compréhension, effectuant une analyse et une pondération de la grille de valeurs en fonction de densités de valeurs.

7. Procédé selon l'une quelconque des revendications 1 à 6, caractérisé en ce qu'au moins une partie des étapes (101-106) peut être effectuée à distance ou en local sur l'appareil (10).

8. Procédé selon l'une quelconque des revendications 1 à 7, caractérisé en ce qu'une corrélation est effectuée avec d'autres capteurs de manière à générer des valeurs supplémentaires et/ou complémentaires.

9. Procédé selon la revendication 3, caractérisé en ce que dans le cas où certaines étapes (101-106) sont réalisées à distance, un mécanisme de chiffrement des communications, par exemple lors de la transmission des clefs éligibles (C1-Cm) vers un serveur (23), est mis en œuvre afin de sécuriser des échanges d'informations.

10. Procédé selon la revendication 9, caractérisé en ce que les étapes suivantes sont mises en œuvre préalablement à l'étape de test des clefs éligibles (C1-Cm):
- une étape (201) d'application d'un algorithme de création d'une chaîne chiffrée par concaténation des valeurs pour obtenir une clef chiffrée (C_chif), ladite clef chiffrée (C_chif) contenant un ensemble de clefs éligibles (C1-Cm) issues du tableau de valeurs (T),
- une étape (203) de décryptage de la clef chiffrée par le serveur (23) pour régénérer l'ensemble du tableau de valeurs (T),
- une étape (204) d'application d'un algorithme, dit de lutte contre la fraude, testant une concordance des valeurs du tableau régénéré et la faisabilité réelle d'un tel enchaînement pour se prémunir d'un piratage par brute force, et
- dans le cas où l'algorithme valide le tableau de valeurs (T), le procédé met en œuvre l'étape (106) de test des clefs éligibles C1-Cm.

11. Procédé selon l'une quelconque des revendications 1 à 10, caractérisé en ce que l'étape (102) de prise de la photographie numérique est effectuée dans des conditions de prises de vue standardisées.

12. Procédé selon la revendication 11, caractérisé en ce que les conditions de prise de vue standardisées sont choisies parmi les suivantes:
- fond blanc,
- jusqu'à trois objets (20) visibles,
- objets (20) non superposés,
- objets (20) visibles en intégralité, et
- conditions d'éclairage standardisées sans ombre.

13. Procédé selon l'une quelconque des revendications 1 à 12, caractérisé en ce qu'une intelligence artificielle est configurée pour améliorer une détection de l'objet (20) dans des conditions réelles d'éclairage et/ou traiter des objets (20) incomplets sur l'image numérique (21) et/ou superposés quel qu'en soit le fond.

14. Procédé selon l'une quelconque des revendications 1 à 13, caractérisé en ce qu'il comporte une étape de traitement combinée à une reconnaissance infrarouge pour s'affranchir de conditions d'éclairage et/ou d'ombre.

15. Procédé selon l'une quelconque des revendications 1 à 14, caractérisé en ce qu'il est mis en œuvre sur plusieurs photographies numériques, notamment en prenant des photographies de plusieurs objets (20) dans un ordre spécifique, par exemple trois objets (20) successifs, ou un objet (20) sous plusieurs angles différents, par exemple sous trois angles différents.

16. Procédé selon l'une quelconque des revendications 1 à 15, caractérisé en ce qu'il comporte en outre une étape d'analyse de sons et/ou de vidéos pour corroborer l'identification effectuée via la photographie numérique.

17. Procédé selon l'une quelconque des revendications 1 à 16, caractérisé en ce qu'il comporte en outre une étape d'analyse de code, tel qu'un code barre en deux dimensions, associé à ou aux objets (20) pris en photo pour corroborer l'identification.

18. Procédé selon l'une quelconque des revendications 1 à 17, caractérisé en ce que l'opération autorisée ou non est choisi parmi: récupération d'un mot de passe, connexion à un compte utilisateur, contrôle d'identité, accès à un lieu, accès à des applications, ou déchiffrement de données, accès à des services, accès ou démarrage d'un véhicule, réalisation directe ou indirecte d'un ou plusieurs achats, éventuellement à distance par Internet.

19. Procédé selon l'une quelconque des revendications 1 à 18, caractérisé en ce qu'il est mis en œuvre dans les cas d'utilisation d'un casque de réalité augmentée ou de réalité virtuelle.

20. Procédé selon l'une quelconque de revendications 1 à 19, caractérisé en ce qu'il comporte une étape de reconnaissance biométrique dans laquelle une partie du corps de l'utilisateur est contrôlée de manière à réaliser une identification forte.

21. Procédé selon la revendication 2, caractérisé en ce qu'à la fin de l'étape de traitement de la grille de valeurs (G), des points restants de l'image numérique (21) représentent une structure de l'objet ou d'une partie du corps de l'utilisateur.

22. Procédé selon l'une quelconque des revendications 1 à 21, caractérisé en ce qu'une analyse est pratiquée sur autre chose qu'une photographie, notamment un son, une image 2D, 3D, créée à partir d'un ou de capteurs ultrasons, thermiques, tactiles, ou autre.

23. Procédé selon l'une quelconque des revendications 1 à 22, caractérisé en ce qu'il est mis en œuvre sur une série d'images numériques ou sur une vidéo numérique.

24. Procédé selon l'une quelconque des revendications 1 à 23, caractérisé en ce qu'il comporte une étape de détection d'une partie du corps d'un utilisateur, notamment un tour de doigt, basé sur la réalisation d'une étape de détermination d'une donnée relative à une dimension de la zone cible en fonction d'un écart entre des repères de mesure et pourra, le cas échéant, faire intervenir des modèles 2D ou 3D de la partie du corps, ainsi que des données biométriques ou non pour effectuer une identification de l'utilisateur.

25. Procédé selon l'une quelconque des revendications 1 à 24, caractérisé en ce qu'il comporte une étape d'analyse conventionnelle d'identification avant de réaliser une analyse d'une image d'un objet ou d'une partie du corps de l'utilisateur pour finaliser une authentification forte.

26. Procédé selon l'une quelconque des revendications 1 à 25, caractérisé en ce qu'il comporte une étape de combinaison de plusieurs mesures et/ou plusieurs capteurs, notamment au moins deux capteurs pour créer une image en trois dimensions.

27. Procédé selon l'une quelconque des revendications 1 à 26, caractérisé en ce qu'une caméra disposée sous une vitre est configurée pour réaliser des étapes de traitement d'image d'une partie de l'objet ou d'une partie du corps de l'utilisateur posée sur ladite vitre.

28. Procédé selon l'une quelconque des revendications 1 à 27, caractérisé en ce qu'une caméra ou un détecteur ultrason ou un détecteur infrarouge déporté du dispositif filme une zone colorée ou calibrée, de sorte que lorsque l'utilisateur place un objet ou une partie de son corps dans cette zone calibrée, un examen aisé peut être réalisé.

29. Procédé selon l'une quelconque des revendications 1 à 28, caractérisé en ce qu'il comporte une étape de prélèvement d'une ou plusieurs informations propres à un environnement et/ou à une partie du corps de l'utilisateur issues de capteurs biométriques avant, pendant ou après une phase d'identification, notamment par combinaison et avec d'autres capteurs, de type température, poids, humidité, densité graisseuse, lecture de veines, de pouls, lecteur d'iris, d'impédance, réflectivité, ADN, pigmentation de la peau, empreinte digitale, gerçures ou aspérités de la peau, ou autres données biométriques.

30. Procédé selon l'une quelconque des revendications 1 à 29, caractérisé en ce qu'il comporte une étape de prélèvement ou d'échange d'une ou plusieurs informations d'un ou plusieurs des objets portés par une partie du corps de l'utilisateur avant, pendant ou après l'identification via un réseau radiofréquence et/ou téléphonique de tout type, code barre à une ou plusieurs dimensions, couleur, forme, modèle d'un objet, plusieurs informations pouvant être corrélées entre elles.

31. Procédé selon l'une quelconque des revendications 1 à 30, caractérisé en ce qu'il comporte une étape de reconnaissance et d'analyse d'un ou plusieurs tatouages, de grains de beauté, de cicatrice ou autres imperfections de la peau.

32. Procédé selon l'une quelconque des revendications 1 à 31, caractérisé en ce qu'il comporte une étape de reconnaissance d'objets portés ou non par l'utilisateur, tel qu'une bague, un bracelet, un collier, une montre, un vêtement, des chaussures, un chapeau, une casquette, des lunettes ou autre.

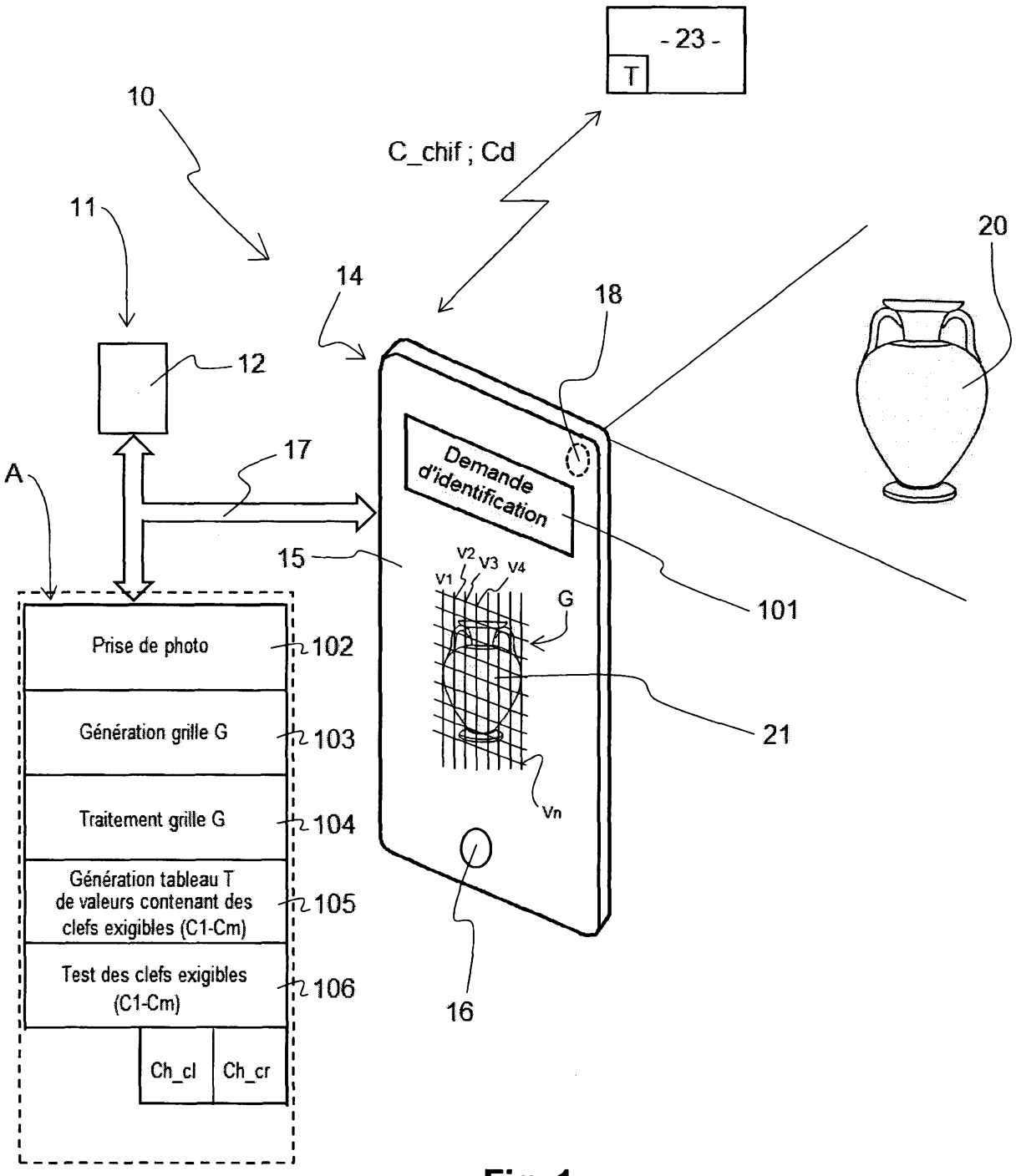

- 23 -
T
10
C_chif ; Cd
11
20
14
18
12
17
A
Demande d'identification
15
V1
V2
V3
V4
G
101
Prise de photo
102
Génération grille G
103
21
Traitement grille G
104
Génération tableau T de valeurs contenant des clefs exigibles (C1-Cm)
105
Vn
Test des clefs exigibles (C1-Cm)
106
16
Ch_cl
Ch_cr

Fig. 1

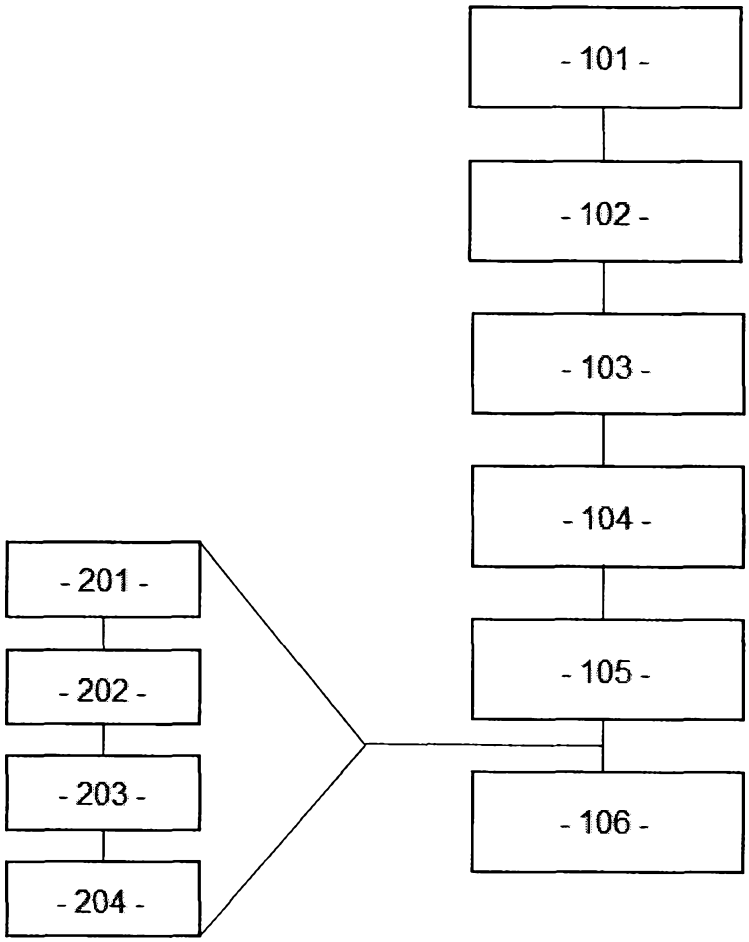


Fig. 2

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 848888
FR 1771186

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	US 2013/269013 A1 (PARRY BEAU ROBERTSON [US] ET AL) 10 octobre 2013 (2013-10-10) * figures 1-6, 7-10, 12, 22 * * alinéas [0003] - [0007] * * alinéas [0037] - [0040] * * alinéas [0049] - [0084] * * alinéas [0086] - [0103] * * alinéas [0124] - [0125] * * revendications 1-14 * -----	1-32	G06F21/32 G06K9/20
A	US 2014/372754 A1 (AISSI SELIM [US] ET AL) 18 décembre 2014 (2014-12-18) * figures 2-9, 11 * * alinéas [0002] - [0006] * * alinéas [0020] - [0039] * * alinéas [0070] - [0098] * * alinéas [0104] - [0107] * * revendications 1-9 * -----	1-32	
A	US 2008/031446 A1 (SUGA YUJI [JP]) 7 février 2008 (2008-02-07) * figures 4-6, 9 * * alinéas [0004] - [0027] * * alinéas [0044] - [0085] * * alinéas [0127] - [0135] * * revendications 1-16 * -----	1-32	DOMAINES TECHNIQUES RECHERCHÉS (IPC) G06F H04L H04W
A	US 9 811 653 B1 (MARESH MARK E [US] ET AL) 7 novembre 2017 (2017-11-07) * figures 1-5, 7-9 * * colonnes 1-4 * * colonnes 7-9 * * revendications 1-18 * -----	1-32	

Date d'achèvement de la recherche	Examinateur
25 avril 2018	Erdene-Ochir, O

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 1771186 FA 848888

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 25-04-2018
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2013269013 A1	10-10-2013	US 2013269013 A1	10-10-2013
		US 2014289534 A1	25-09-2014
		US 2015379256 A1	31-12-2015
		US 2017193215 A1	06-07-2017
		US 2018018454 A1	18-01-2018
		WO 2013154936 A1	17-10-2013
US 2014372754 A1	18-12-2014	AU 2014311784 A1	21-01-2016
		AU 2018200611 A1	08-02-2018
		CN 105453483 A	30-03-2016
		EP 3008854 A2	20-04-2016
		RU 2016100178 A	18-07-2017
		US 2014372754 A1	18-12-2014
		US 2017078267 A1	16-03-2017
		US 2017346806 A1	30-11-2017
		WO 2015030903 A2	05-03-2015
US 2008031446 A1	07-02-2008	CN 101118586 A	06-02-2008
		JP 2008059561 A	13-03-2008
		US 2008031446 A1	07-02-2008
US 9811653 B1	07-11-2017	AUCUN	

EPO FORM P0465