(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** ***3 070 086***

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

(21) **N° d'enregistrement national :** **17 57585**

(51) Int Cl[8] : ***G 07 C 9/00*** *(2018.01), G 01 G 19/44*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 08.08.17.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 15.02.19 Bulletin 19/07.

(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) :** *SAFRAN IDENTITY & SECURITY* *Société par actions simplifiée* — FR.

(72) **Inventeur(s) :** BEAUDET JEAN, RIEUL FRANCOIS, FOURRE JOEL-YANN et CHASTEL PIERRE.

(73) **Titulaire(s) :** SAFRAN IDENTITY & SECURITY Société par actions simplifiée.

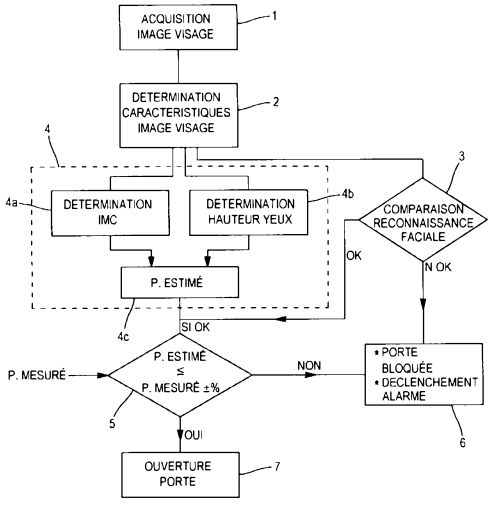
(74) **Mandataire(s) :** REGIMBEAU.

(54) DETECTION DE FRAUDE POUR CONTROLE D'ACCES PAR RECONNAISSANCE FACIALE.

(57) L'invention concerne un procédé de détection de fraude pour contrôle d'accès par reconnaissance faciale, dans lequel on met en œuvre au niveau d'une zone où le contrôle d'accès est vérifié pour un individu se présentant au niveau de ladite zone :

- une mesure du poids de l'individu, au moins un capteur de poids étant prévu au sol à cet effet ;
- une estimation du poids de l'individu par traitement par une unité de calcul d'une image acquise du visage d'un individu se présentant au contrôle d'accès ;
- une comparaison par ladite unité de calcul entre le poids estimé et le poids mesuré ;

et dans lequel ladite unité de calcul déclenche ou non l'émission d'un signal de détection de fraude en fonction du résultat de cette comparaison.



FR 3 070 086 - A1

DETECTION DE FRAUDE POUR CONTROLE D'ACCES PAR RECONNAISSANCE FACIALE

DOMAINE TECHNIQUE GÉNÉRAL ET ART ANTÉRIEUR

La présente invention concerne le contrôle d'accès par reconnaissance faciale.

Plus particulièrement, l'invention propose un procédé et un système de détection de fraude pour les systèmes de contrôle d'accès de ce type.

La reconnaissance faciale est classiquement connue et couramment utilisée par des systèmes de contrôle d'accès, notamment pour le contrôle aux frontières (aéroports ou autres).

Elle consiste à acquérir au moins une image d'un individu se présentant au système de contrôle (sas ou couloir de contrôle muni d'une ou plusieurs caméras, par exemple), à l'analyser pour en déduire un certain nombre de caractéristiques du visage (par exemple, écartement des yeux, des arêtes du nez, des commissures des lèvres, des oreilles, du menton, etc.) et à comparer ces caractéristiques à des jeux de caractéristiques stockés dans une base de données existante afin d'identifier une personne ou de vérifier son identité.

L'une des fraudes possibles avec ce type de système consiste pour un individu à essayer de passer juste derrière une autre personne en se faufilant de façon à être occulté par rapport aux caméras.

Plusieurs techniques ont déjà été envisagées pour permettre de détecter ce type de fraude.

Une première solution consiste à détecter sur les images l'existence de plusieurs visages.

Une autre technique possible consiste à utiliser une caméra en temps de vol (« time of fly » selon la terminologie anglo-saxonne) que l'on positionne en surplomb par rapport à la zone où les personnes se présentent et circulent.

Une autre solution encore consiste à utiliser un tapis d'unicité, c'est-à-dire un tapis permettant l'acquisition de mesures de pression liées à la marche d'une personne sur celui-ci et à mettre sur ces mesures un traitement destiné à détecter le fait que deux personnes avancent sur le tapis.

Un exemple en ce sens est par exemple décrit dans la demande de brevet français FR2871602.

Cette solution s'avère toutefois insuffisante pour véritablement permettre d'éviter toute fraude.

Toutes ces solutions sont complémentaires et aucune ne se suffit à elle-même.

Il persiste donc toujours un besoin pour de nouvelles solutions de détection de fraude, simples, peu onéreuses, fiables et potentiellement complémentaires aux solutions existantes.

PRÉSENTATION GÉNÉRALE DE L'INVENTION

Un but général de l'invention est de proposer une solution de détection de fraude pour système de contrôle d'accès par reconnaissance faciale qui soit efficace, simple à mettre en œuvre et peu onéreuse.

A cet effet, l'invention propose un procédé de détection de fraude pour contrôle d'accès par reconnaissance faciale, dans lequel on met en œuvre au niveau d'une zone où le contrôle d'accès est vérifié pour un individu se présentant au niveau de ladite zone :

- une mesure du poids de l'individu, au moins un capteur de poids étant prévu au sol à cet effet ;
- une estimation du poids de l'individu par traitement par une unité de calcul d'une image acquise du visage d'un individu se présentant au contrôle d'accès ;
- une comparaison par ladite unité de calcul entre le poids estimé et le poids mesuré ;

et dans lequel ladite unité de calcul déclenche ou non l'émission d'un signal de détection de fraude en fonction du résultat de cette comparaison.

Ce procédé est avantageusement complété par les différentes caractéristiques suivantes prises seules ou en combinaison :

- l'estimation du poids de l'individu met en œuvre une estimation de l'indice de masse corporelle de la personne par traitement d'une image du visage par l'unité de calcul ;

- l'estimation du poids de l'individu met en œuvre une estimation de la hauteur de celui-ci par traitement d'au moins une image du visage par l'unité de calcul ;

- l'estimation de la hauteur de l'individu met en œuvre une détermination de la hauteur des yeux de celui-ci ;

- lors de la comparaison par l'unité de calcul entre le poids estimé et le poids mesuré, ladite unité de calcul vérifie si le poids mesuré est plus élevé que le poids estimé, à une marge d'erreur donnée, et déclenche un signal de détection de fraude lorsque c'est le cas ;

- la marge d'erreur donnée est de l'ordre de 20 kg ;

- la marge d'erreur donnée est comprise entre 7 et 15 kg.

L'invention propose en outre un procédé de contrôle d'accès dans lequel :

- on acquiert au moins une image du visage d'un individu se présentant dans une zone où le contrôle d'accès est vérifié,

- on détermine sur cette image des caractéristiques biométriques du visage,

- on compare ces caractéristiques biométriques du visage de l'individu à des caractéristiques biométriques stockées dans un document de référence ou dans une base de données,

- on autorise ou non l'accès en fonction du résultat de cette comparaison,

caractérisé en ce que l'on met on met en outre en œuvre une détection de fraude du type exposé ci-dessus.

L'invention propose par ailleurs un système de détection de fraude et un système de contrôle d'accès.

PRÉSENTATION DES FIGURES

D'autres caractéristiques et avantages de l'invention ressortiront encore de la description qui suit, laquelle est purement illustrative et non limitative, et doit être lue en regard des figures annexées sur lesquelles :

- la figure 1 est une représentation schématique d'un système de contrôle d'accès conforme à un mode de réalisation possible de l'invention ;

- la figure 2 illustre différentes étapes d'un traitement de contrôle d'accès et de détection de fraude conforme à un mode de mise en œuvre possible de l'invention.

DESCRIPTION D'UN OU PLUSIEURS MODES DE MISE EN ŒUVRE ET DE RÉALISATION

On a représenté sur la figure 1 un système de contrôle d'accès S par reconnaissance faciale.

Ce système comporte une ou plusieurs caméra(s) C disposée(s) dans un sas de contrôle d'accès à une hauteur et avec une orientation permettant l'acquisition d'une image du visage d'un individu I se déplaçant dans un couloir menant à une porte d'accès PA.

La ou les caméra(s) C sont connectées à une unité de traitement U (ordinateur, serveur de calcul, etc.) à laquelle les images sont envoyées.

Cette unité de traitement U est apte à traiter la ou les image(s) reçue(s) pour en déduire des caractéristiques de biométrie faciale.

Elle est en outre apte à échanger avec un lecteur L de documents portant des informations biométriques (lecteur de puce de passeport biométrique par exemple) ou encore avec une base de données BdD dans laquelle sont stockées les caractéristiques biométriques des individus auxquels on souhaite permettre de donner l'accès à une zone réservée au-delà de la porte PA (ou encore des individus que l'on souhaite détecter lorsqu'il se présente à la porte PA par exemple).

L'unité que constitue l'ordinateur U commande l'ouverture ou le blocage de la porte PA en fonction des résultats des comparaisons menées sur les caractéristiques des images.

Cette ouverture est en outre fonction du résultat d'une comparaison entre un poids estimé pour l'individu I se déplaçant dans le couloir du sas et son poids mesuré alors qu'il passe dans le sas.

A cet effet, le couloir peut présenter un tapis de mesure de poids qui permet de mesurer le poids de l'individu se déplaçant sur celui-ci.

Notamment, il peut être prévu dans le couloir d'accès une zone Z spécifique au niveau de laquelle on demande à l'individu I de s'arrêter pour permettre la mesure de poids et l'acquisition des images de son visage.

Cette zone Z est par exemple matérialisée au sol par de simples traits ou est de préférence une zone fermée de type sas.

Le tapis sur lequel l'individu I se déplace est équipé de capteurs de poids CP, notamment au niveau de cette zone Z d'arrêt.

Les mesures de poids ainsi obtenues sont transmises à l'unité de traitement U pour mise en œuvre d'une comparaison entre le poids ainsi mesuré et le poids estimé déterminé à partir des caractéristiques de l'image du visage de l'individu I.

Plus particulièrement, le traitement d'une image de visage et le contrôle d'accès peuvent se faire ainsi qu'illustré sur la figure 2.

Après acquisition de l'image (étape 1), l'unité de traitement détermine les caractéristiques biométriques du visage (écartement des yeux, des arêtes du nez, des commissures des lèvres, des oreilles, du menton, etc.) (étape 2).

Ces caractéristiques biométriques de l'individu sont ensuite utilisées d'une part pour mettre en œuvre la reconnaissance faciale (étape 3) et d'autre part pour déterminer le poids estimé (étape 4).

La reconnaissance faciale 3 se fait en interrogeant la base de données BdD ou en comparant les caractéristiques de l'image acquise à des caractéristiques fournies par un document officiel tel qu'un passeport biométrique à puce.

Selon le résultat de la comparaison, l'unité U peut être amenée à déclencher une alarme en maintenant la porte d'accès PA bloquée (étape 6 - cas résultat NOK) ou au contraire à considérer que l'une des conditions pour l'ouverture de la porte est satisfaite (cas OK).

L'estimation du poids (étape 4) s'effectue en traitant les caractéristiques biométriques de l'image pour estimer l'indice de masse corporelle de la personne (étape 4a), ainsi qu'en déterminant la hauteur des yeux de l'individu (étape 4b).

L'estimation de l'IMC se fait par exemple de la façon proposée dans l'article *Wen, L., & Guo, G. (2013), A Computational Approach To Body Mass Index Prediction From Face Images, Image and Vision Computing, 31(5), 392-400*.

Des traitements à base d'algorithmes d'intelligence artificielle (machine learning) sont également possibles.

En parallèle à cette étape 4a, le traitement met en œuvre une détermination de la hauteur des yeux de l'individu I (étape 4b). Cette détermination est fonction de l'orientation de la caméra et se fait par exemple en déterminant la position des yeux sur l'image acquise lorsque l'individu marque un temps d'arrêt au niveau de la zone Z.

Elle peut également se faire par analyse de plusieurs images successives acquises alors que l'individu I se déplace dans le couloir qui mène à la porte d'accès PA.

La hauteur des yeux ainsi déterminée permet une approximation de la hauteur de la personne.

La double estimation de l'indice de masse corporelle d'une part et de la hauteur des yeux de l'individu d'autre part permet ainsi une estimation de la masse de la personne (étape 4c) :

$$\text{poids estimé} = \text{IMC} \times (\text{hauteur de l'individu})^2$$

Le poids « P estimé » est ensuite comparé au poids « P mesuré » (étape 5) avec une marge d'erreur donnée.

Lorsque le poids mesuré est nettement plus élevé que le poids estimé, la porte d'accès PA est bloquée et une alarme est déclenchée (étape 6).

Par contre, lorsque le poids estimé et le poids mesuré correspondent sensiblement, l'ouverture de la porte est commandée (étape 7).

L'ordre de grandeur de l'erreur entre le poids estimé et le poids mesuré est par exemple d'une dizaine de kilos (par exemple de l'ordre de 20 kg, ou entre 7 et 15 kg). Cet ordre de grandeur tient compte de la marge d'erreur sur l'estimation du poids ainsi que des éventuels bagages à main que l'individu peut avoir avec lui au moment où il franchit le contrôle.

Ainsi, le traitement proposé permet une détection de fraude en détectant non pas le fraudeur lui-même mais une incohérence entre la personne qui se montre à la caméra et le poids mesuré.

REVENDICATIONS

1. Procédé de détection de fraude pour contrôle d'accès par reconnaissance faciale, dans lequel on met en œuvre au niveau d'une zone où le contrôle d'accès est vérifié pour un individu se présentant au niveau de ladite zone :

- une mesure du poids de l'individu, au moins un capteur de poids étant prévu au sol à cet effet ;
- une estimation du poids de l'individu par traitement par une unité de calcul d'une image acquise du visage d'un individu se présentant au contrôle d'accès ;
- une comparaison par ladite unité de calcul entre le poids estimé et le poids mesuré ;

et dans lequel ladite unité de calcul déclenche ou non l'émission d'un signal de détection de fraude en fonction du résultat de cette comparaison.

2. Procédé selon la revendication 1, dans lequel l'estimation du poids de l'individu met en œuvre une estimation de l'indice de masse corporelle de la personne par traitement d'une image du visage par l'unité de calcul.

3. Procédé selon la revendication 2, dans lequel l'estimation du poids de l'individu met en œuvre une estimation de la hauteur de celui-ci par traitement d'au moins une image du visage par l'unité de calcul.

4. Procédé selon la revendication 3, dans lequel l'estimation de la hauteur de l'individu met en œuvre une détermination de la hauteur des yeux de celui-ci.

5. Procédé selon l'une des revendications précédentes, dans lequel, lors de la comparaison par l'unité de calcul entre le poids estimé et le poids mesuré, ladite unité de calcul vérifie si le poids mesuré est plus élevé que

le poids estimé, à une marge d'erreur donnée, et déclenche un signal de détection de fraude lorsque c'est le cas.

6. Procédé selon la revendication 5, dans lequel la marge d'erreur donnée est de l'ordre de 20 kg.

7. Procédé selon la revendication 5, dans lequel la marge d'erreur donnée est comprise entre 7 et 15 kg.

8. Procédé de contrôle d'accès dans lequel :

- on acquiert au moins une image du visage d'un individu se présentant dans une zone où le contrôle d'accès est vérifié,

- on détermine sur cette image des caractéristiques biométriques du visage,

- on compare ces caractéristiques biométriques du visage de l'individu à des caractéristiques biométriques stockées dans un document de référence ou dans une base de données,

- on autorise ou non l'accès en fonction du résultat de cette comparaison,

caractérisé en ce que l'on met on met en outre en œuvre une détection de fraude selon l'une des revendications précédentes.

9. Système de détection de fraude pour contrôle d'accès par reconnaissance faciale, comportant, dans une zone où le contrôle d'accès est vérifié pour un individu se présentant au niveau de ladite zone :

- au moins un capteur de poids au sol pour la mesure du poids d'une individu se présentant dans ladite zone ;

- une unité de calcul adaptée pour la mise en œuvre d'une estimation du poids d'un individu sur une image acquise du visage d'un individu se présentant au contrôle d'accès ;

- ladite unité de calcul étant en outre adaptée pour la mise en œuvre d'une comparaison entre le poids estimé et le poids mesuré et pour le

déclenchement ou non de l'émission d'un signal de détection de fraude en fonction du résultat de cette comparaison.

10. Système de contrôle d'accès comportant :

- au moins une caméra pour l'acquisition d'au moins une image du visage d'un individu se présentant dans une zone où le contrôle d'accès est vérifié,

- une unité de traitement adaptée à la détermination sur cette image des caractéristiques biométriques du visage de l'individu, ladite unité de calcul étant en outre adaptée à la comparaison de ces caractéristiques biométriques du visage de l'individu à des caractéristiques biométriques stockées dans un document de référence ou dans une base de données et autorisant ou non l'accès à la zone réservée en fonction du résultat de cette comparaison,

caractérisé en ce qu'il comporte en outre un système de détection de fraude selon la revendication 9.

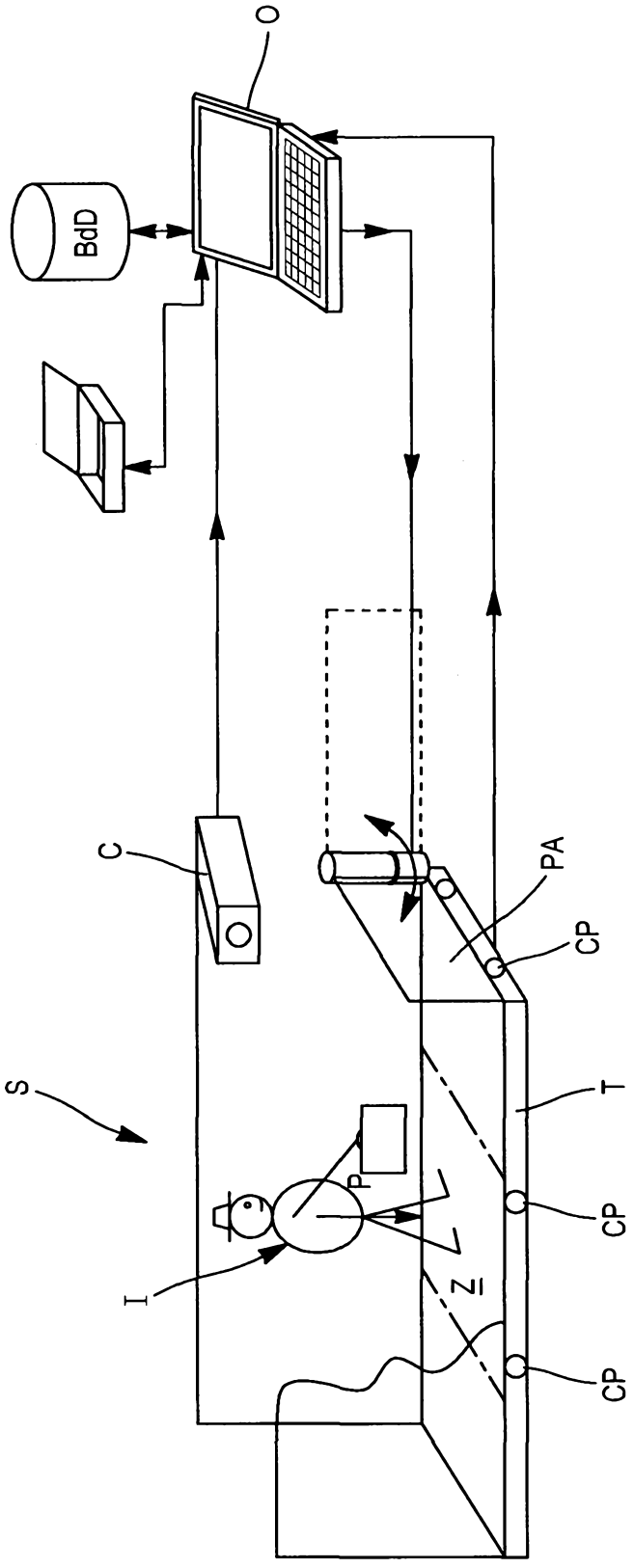


FIG. 1

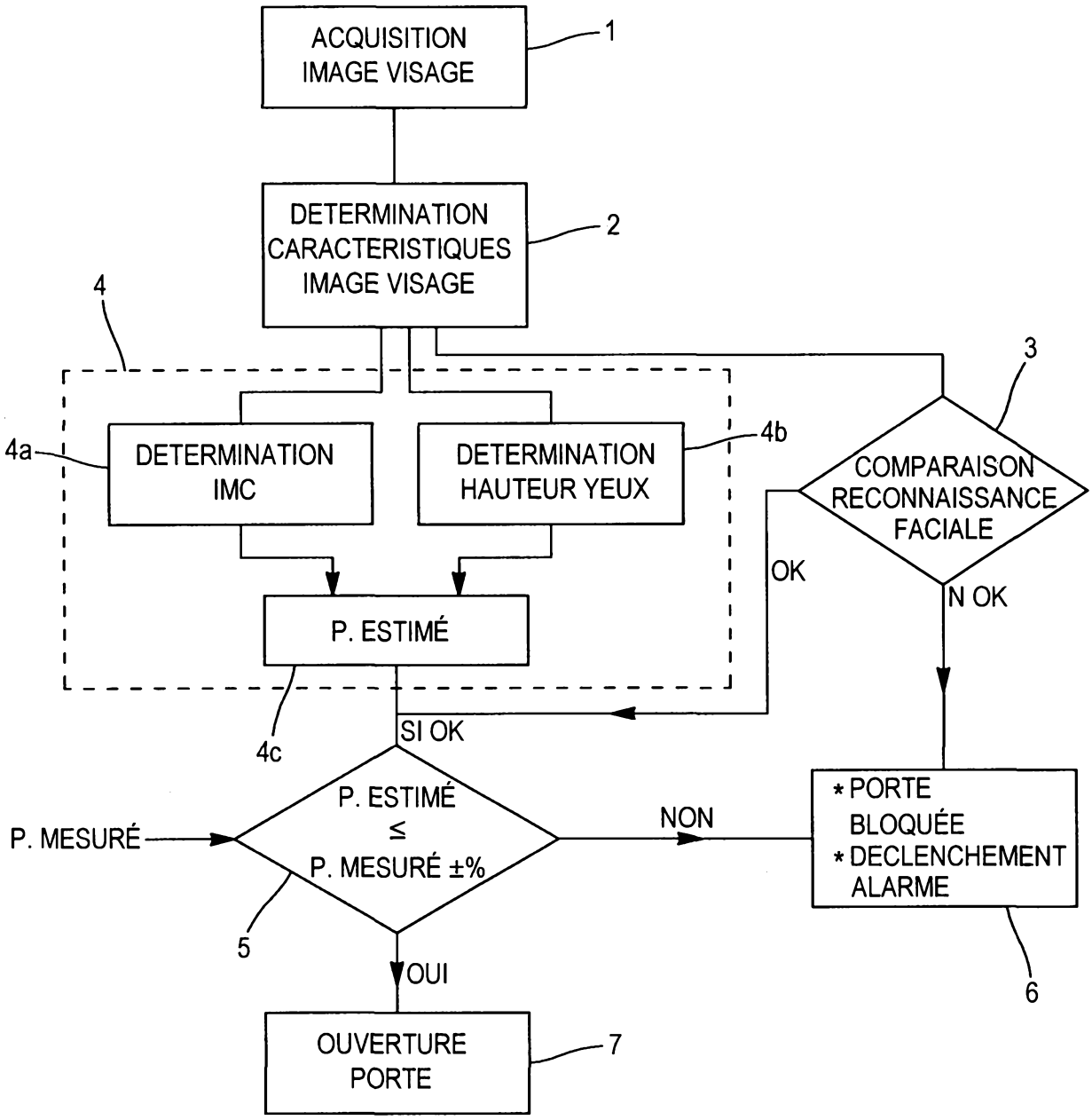

ACQUISITION IMAGE VISAGE
1
DETERMINATION CARACTERISTIQUES IMAGE VISAGE
2
4
3
4a
DETERMINATION IMC
DETERMINATION HAUTEUR YEUX
4b
COMPARAISON RECONNAISSANCE FACIALE
OK
N OK
P. ESTIMÉ
4c
SI OK
P. MESURÉ
P. ESTIMÉ ≤ P. MESURÉ ±%
NON
* PORTE BLOQUÉE
* DECLENCHEMENT ALARME
5
6
OUI
OUVERTURE PORTE
7

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 846063
FR 1757585

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		
Y	CN 101 246 608 A (SHANGHAI ISVISION INTELLIGENT [CN]) 20 août 2008 (2008-08-20) * abrégé * * figure 1 * * alinéa [0006] - alinéa [0016] * -----	1-10	G07C9/00 G01G19/44
Y	US 2016/063314 A1 (SAMET SHAI [US]) 3 mars 2016 (2016-03-03) * abrégé; figure 15 * * alinéa [0006] - alinéa [0007] * * alinéas [0055], [0086] * * alinéa [0158] - alinéa [0161] * * alinéa [0187] - alinéas [0191], [0248] * -----	1-10	
A	US 2016/091359 A1 (ALAM MAQSOOD [US] ET AL) 31 mars 2016 (2016-03-31) * abrégé; figures 1, 2 * -----	1-10	
A	US 2016/109281 A1 (HERRING DEAN FREDERICK [US] ET AL) 21 avril 2016 (2016-04-21) * abrégé; figure 1 * -----	1-10	DOMAINES TECHNIQUES RECHERCHÉS (IPC) G07C G01G H04W G06K
A	JP 2017 041218 A (ISHIZAKI JINICHI) 23 février 2017 (2017-02-23) * abrégé; figure 7 * -----	1-10	
A	LINGYUN WEN ET AL: "A computational approach to body mass index prediction from face images", IMAGE AND VISION COMPUTING, vol. 31, no. 5, 2 avril 2013 (2013-04-02), pages 392-400, XP055476402, GUILDFORD, GB ISSN: 0262-8856, DOI: 10.1016/j.imavis.2013.03.001 * abrégé * -----	1-10	

Date d'achèvement de la recherche	Examinateur
23 mai 2018	Saraceni, Alessandro

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 1757585 FA 846063

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 23-05-2018
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
CN 101246608 A	20-08-2008	AUCUN	
US 2016063314 A1	03-03-2016	US 2016063314 A1	03-03-2016
		US 2016307030 A1	20-10-2016
US 2016091359 A1	31-03-2016	AUCUN	
US 2016109281 A1	21-04-2016	US 2016109281 A1	21-04-2016
		US 2016110622 A1	21-04-2016
		US 2016110700 A1	21-04-2016
		US 2016110701 A1	21-04-2016
		US 2016110702 A1	21-04-2016
		US 2016110703 A1	21-04-2016
		US 2016110751 A1	21-04-2016
		US 2016110760 A1	21-04-2016
		US 2016110772 A1	21-04-2016
		US 2016110786 A1	21-04-2016
		US 2016110791 A1	21-04-2016
		US 2016110793 A1	21-04-2016
		US 2016110797 A1	21-04-2016
		US 2016110799 A1	21-04-2016
		US 2016110902 A1	21-04-2016
		US 2018108074 A1	19-04-2018
JP 2017041218 A	23-02-2017	AUCUN	

EPO FORM P0465