(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 895 122**

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

(21) **N° d'enregistrement national :** **05 12857**

(51) Int Cl[8] : **G 07 C 9/00** (2006.01), H 04 L 9/32, H 04 N 5/225

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 16.12.05.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 22.06.07 Bulletin 07/25.

(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 :**

(71) **Demandeur(s) :** *SAGEM DEFENSE SECURITE Société anonyme* — FR.

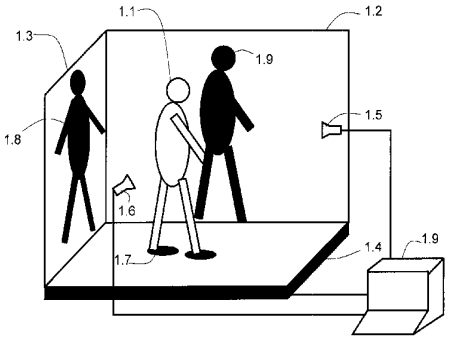
(72) **Inventeur(s) :** BERNARD EMMANUEL, FONDEUR JEAN CHRISTOPHE et LAMBERT LAURENT.

(73) **Titulaire(s) :**

(74) **Mandataire(s) :** CABINET LE GUEN ET MAILLET.

(54) PROCEDE DE SECURISATION D'UN ACCES PHYSIQUE ET DISPOSITF D'ACCES IMPLEMENTANT LE PROCEDE.

(57) L'invention vise à améliorer le taux de détection des tentatives de fraude lors du passage d'une personne dans un espace contrôlé. Elle est basée sur l'utilisation de différents jeux de paramètres issus d'au moins deux systèmes de capteurs différents, certains de ces jeux de paramètres étant basés sur des corrélations de mesures issues de ces différents systèmes de capteurs. Un apprentissage est fait de façon à caractériser différents types de fraude pour ensuite permettre l'identification d'une tentative de fraude par corrélation entre les mesures obtenues et les caractérisations de chaque type de fraude pour chaque jeu de paramètres.



FR 2 895 122 - A1

Domaine technique

L'invention se situe dans le domaine du contrôle d'accès physique aux issues d'une zone sensible et plus particulièrement du contrôle de l'unicité d'une personne franchissant un passage contrôlé. Ce domaine regroupe deux types de problématiques, une première consistant à authentifier une personne se présentant, le second consistant à s'assurer que seule la personne authentifiée franchit le passage contrôlé de façon à se prémunir d'une fraude où une personne non autorisée profite du passage d'une personne autorisée pour se faufiler (« tailgating » en anglais).

Art antérieur

Il est connu de par le document EP 1 100 050 A1 des systèmes de comptage de personnes empruntant une entrée par traitement d'images vidéo. Dans ce document, un seul type de capteur est utilisé. Il est également connu de par le document US 2002/0067259 A1 d'utiliser plusieurs types de capteurs pour déterminer la présence d'une personne et son unicité. Dans ce document, il est décrit de corréler les données de plusieurs capteurs, une configuration de coupure de faisceaux et un détecteur de chaleur, pour détecter un objet non humain de façon à discriminer une personne avec bagage d'une intrusion. Le document US 2004/0188185, quant à lui, décrit de corréler les informations d'une image de chaleur et d'une image optique pour compter le nombre de personnes présentes dans un espace. Dans le document EP 1 308 905 A1 est décrit l'utilisation d'un tapis sensible à la pression pour détecter la présence de personnes, leur sens de déplacement, et effectuer un comptage à partir des données du tapis et de leur évolution dans le temps.

Ces méthodes ne sont toutefois pas suffisantes pour détecter avec fiabilité les tentatives de fraude d'une personne déterminée.

Exposé de l'invention

L'invention vise à améliorer le taux de détection des tentatives de fraude lors du passage d'une personne dans un espace contrôlé. Elle est basée sur l'utilisation de différents jeux de paramètres issus d'au moins deux systèmes de capteurs différents, certains de ces jeux de paramètres étant basés sur des corrélations de mesures issues de ces différents systèmes de capteurs. Un apprentissage est fait de façon à caractériser différents types de fraudes pour ensuite permettre l'identification d'une

tentative de fraude par corrélation entre les mesures obtenues et les caractérisations de chaque type de fraude pour chaque jeu de paramètres.

L'invention concerne un procédé de sécurisation d'un accès physique disposant d'une pluralité de systèmes de capteurs (1.4, 1.5, 1.6), ledit procédé visant à discriminer un accès valide d'une tentative d'accès en fraude, comprenant les étapes suivantes :

dans une phase préliminaire :

- détermination d'au moins un jeu de paramètres issus des systèmes de capteurs dont au moins un jeu de paramètres issus d'au moins deux systèmes de capteurs différents (6.1) ;
- détermination par apprentissage, pour chaque jeu de paramètres et pour chaque type de fraude envisagé, d'une classe de valeurs des paramètres du jeu correspondant à ce type de fraude pour ce jeu de paramètres (6.2) ;

lors d'un accès :

- détermination de jeux de valeurs formés des valeurs prises par chaque paramètre de chaque jeu de paramètres pour cet accès (6.3) ;
- détermination d'une probabilité de fraude associée à chaque type de fraude pour chaque jeu de paramètres, en fonction du jeu de valeurs déterminé lors de cet accès et de la classe correspondant au type de fraude pour ce jeu de paramètres (6.4) ;
- détermination d'une probabilité de fraude globale associée à l'accès en fonction des probabilités de fraude obtenues pour chaque jeu de paramètres et pour chaque type de fraude (6.5).

Selon un mode particulier de l'invention la probabilité de fraude associée à chaque type de fraude pour chaque jeu de paramètres est estimée par calcul d'une distance entre le jeu de valeurs déterminé lors de cet accès et la classe correspondant au type de fraude pour ce jeu de paramètres.

Selon un mode particulier de l'invention, cette distance est une distance algébrique entre le jeu de valeurs déterminé et le barycentre de la classe.

Selon un mode particulier de l'invention la probabilité de fraude associée à chaque type de fraude pour chaque jeu de paramètres est estimée par un réseau neuromimétique et où l'étape de détermination par apprentissage des classes comprend une étape d'entraînement de ce réseau neuromimétique.

Selon un mode particulier de l'invention les systèmes de capteurs comprennent un système de caméras (1.5, 1.6) fournissant des images de profil (1.8, 1.9, Fig. 3).

Selon un mode particulier de l'invention les systèmes de capteurs comprennent un système de tapis de pression au sol (1.4) fournissant des images de pression (1.7, Fig. 4).

L'invention concerne également un dispositif de sécurisation d'un accès physique comprenant :

- un espace de contrôle ;
- une pluralité de systèmes de capteurs dans cet espace de contrôle (1.4, 1.5, 1.6) ;
- des moyens d'analyse des informations issues des systèmes de capteurs (1.9) ;

et sachant qu'est déterminé au moins un jeu de paramètres issus des systèmes de capteurs dont au moins un jeu de paramètres issus d'au moins deux systèmes de capteurs différents, étant déterminée par apprentissage, pour chaque jeu de paramètres et pour chaque type de fraude envisagé, une classe d'espace de valeurs des paramètres du jeu correspondant à ce type de fraude pour ce jeu de paramètres, les moyens d'analyse comprennent :

- des moyens de détermination de jeux de valeurs formés des valeurs prises par chaque paramètre de chaque jeu de paramètres pour cet accès ;
- des moyens de détermination d'une probabilité de fraude associée à chaque type de fraude et pour chaque jeu de paramètres, en fonction du jeu de valeurs déterminé lors de cet accès et de la classe correspondant au type de fraude pour ce jeu de paramètres ;
- des moyens de détermination d'une probabilité de fraude globale associée à l'accès en fonction des probabilités de fraude obtenues pour chaque jeu de paramètres et pour chaque type de fraude.

Brève description des dessins

Les caractéristiques de l'invention mentionnées ci-dessus, ainsi que d'autres, apparaîtront plus clairement à la lecture de la description suivante d'un exemple de réalisation, ladite description étant faite en relation avec les dessins joints, parmi lesquels :

La Fig. 1 représente un schéma d'ensemble d'un mode de réalisation de l'invention.

La Fig. 2 représente graphiquement une classe de caractérisation d'un type de fraude dans l'espace d'un jeu de paramètres selon un mode de réalisation de l'invention.

La Fig. 3 représente un exemple d'image de profil obtenue par une caméra.

La Fig. 4 représente un exemple d'image de pression obtenue par un tapis de pression.

La Fig. 5 représente un exemple d'image de pression correspondant à un passage suivi, dos à dos en « collant les pieds ».

La Fig. 6 représente un organigramme de la méthode.

Exposé détaillé de l'invention

Dans le cadre du contrôle et de la sécurisation d'accès physiques, il est souvent crucial de vérifier qu'une personne est bien la seule à avoir franchi une porte, un couloir, un sas de sécurité, etc. On peut alors parler de détection d'unicité. Le « tourniquet » du métro ou le sas sécurisé d'un aéroport sont des exemples de mise en œuvre de la détection d'unicité. Les moyens de mesure mis en œuvre peuvent être de tous horizons : capteur de pression, de température, moyens optiques (caméra, faisceaux laser...). De même l'analyse des mesures peut être plus ou moins consolidée (utilisation combinée ou indépendante des données), interprétée (prise en compte de facteurs dynamiques ou statiques), etc.

Le système décrit ici, est basé sur un système de détection d'unicité utilisant un tapis de pression au sol. L'intérêt d'un système de ce type est d'observer les contacts aux sols et leur évolution au cours du temps afin de pouvoir déduire le nombre de

personnes présentes selon les traces présentes au sol et leur évolution. Néanmoins, il existe des moyens très simples de frauder un tel système en réduisant les contacts au sol. Par exemple, deux personnes peuvent passer simultanément si elles sont suffisamment proches l'une de l'autre.

L'objet de l'invention est de consolider la détection d'unicité existante en utilisant une association de capteurs de pression au sol et de caméras et/ou détection de profil, et de traiter les tentatives de fraude avec un algorithme de fusion de données et d'analyse comportementale des objets détectés. Ainsi l'algorithme permet de classifier le passage selon le type d'attaques possibles en comparant les mesures faites et les différentes classes associées à des types de fraude envisagés, la décision de fraude ou non est alors prise selon la classe.

Dans l'exemple de réalisation décrit, l'invention est réalisée au sein d'un sas contrôlant un accès. Ce sas est représenté schématiquement Fig. 1. Une personne 1.1 franchit le sas de gauche à droite. Le sas est équipé d'un certain nombre de systèmes de capteurs. Nous appelons système de capteurs, un système permettant l'acquisition d'informations et basé sur une pluralité de capteurs du même type. Le sas est équipé au niveau du sol d'un premier système de capteurs constitué d'un tapis sensible à la pression 1.4. Ce tapis fournit une image de pression 1.7 en deux dimensions fournissant en chacun de ses points la valeur de la pression exercée. Un exemple de ces images de pression est représenté Fig. 4. Ces images permettent de déterminer les contacts entre une personne ou un objet présent dans le sas et le sol ainsi que de calculer son poids et d'avoir une idée de la répartition de ce poids dans le plan. D'autre part, le tapis de pression est capable d'acquérir des images de pression de façon périodique ce qui permet également d'étudier le comportement dynamique de ces objets et d'en déduire, par exemple, une vitesse moyenne de déplacement, une direction ainsi que les déplacements relatifs entre objets. Le sas est également pourvu d'un second système de capteurs constitué des caméras vidéo 1.5 et 1.6. Ces caméras sont au nombre de deux dans l'exemple de réalisation, mais leur nombre peut être plus ou moins élevé en fonction de la quantité d'information que l'on souhaite obtenir. On peut, en particulier, ajouter une caméra sur le dessus. Ces caméras fournissent des images de profil 1.2, 1.3 permettant de déterminer des profils 1.8, 1.9 associés aux personnes ou objets présents dans le sas. Le sol et les parois du sas peuvent être de

couleurs saturées afin de limiter les problèmes induits par les ombres portées par les personnes ou objets présents dans le sas. Un exemple d'image de profil est représenté Fig. 3.

Ce dispositif peut être complété par d'autres systèmes de capteurs comme des barrières infrarouges, des diodes, des lasers ou autres permettant de détecter l'arrivée d'une personne ou d'un objet dans le sas, de mesurer la chaleur émise par une personne ainsi que tout autre paramètre utile. Le sas se voit, de plus, généralement, muni de moyens d'authentification non représentés comme un lecteur de badge ou des moyens d'identification biométriques comme un lecteur d'iris de l'œil ou d'empreintes digitales.

Le sas est typiquement connecté à des moyens d'acquisition des données produites par les systèmes de capteurs, des moyens d'analyse de ces données, de prise de décision ainsi que de contrôle. Ces moyens peuvent être constitués d'un ordinateur 1.9 qui est doté d'un disque dur permettant le stockage des images reçues, tant de pression que de profils, ainsi que des programmes nécessaires pour traiter ces images et en extraire les paramètres qui sont utilisés pour déterminer si le passage est validé ou non. Dans le cas d'un passage valide, cet ordinateur peut, par exemple, autoriser l'ouverture d'une porte située à l'extrémité du sas. Dans le cas contraire, la porte reste fermée et une alarme peut être émise en direction d'un poste de surveillance ou autre.

Une personne désireuse de frauder et donc d'entrer sans autorisation, tente généralement de profiter du passage d'une personne autorisée pour se faufiler par la porte via le sas. Cette tentative peut se faire à l'insu de la personne autorisée qui supposera, par exemple, que la personne la suivant est également autorisée. Cette tentative peut également se faire avec la complicité de la personne autorisée ou encore par coercition. Il s'agit donc pour le fraudeur de tenter de tromper les systèmes de capteurs en essayant de dissimuler son passage. Pour ce faire, il peut tenter de se coller à la première personne, par exemple dos à dos, pour tromper les caméras et de coller ses pieds à ceux de la première personne pour que le système ne distingue que deux « grandes » empreintes de pas, voir par exemple l'image de pression Fig. 6. Nous appellerons ce type de fraude « fraude collé ». Le fraudeur peut également tenter de passer accroupi, ou encore en restant exactement sur le côté de la personne

autorisée. Certains cas particuliers peuvent également poser des problèmes de reconnaissance d'un enfant au côté d'un adulte ou même d'un bébé dans les bras de sa mère. Ces tentatives de fraude ne représentant que des exemples des types de fraude possibles. L'enjeu du système est donc de réussir à discriminer les passages valides d'une seule personne et ceci quels que soient la taille, la corpulence, la tenue ou les bagages de cette personne d'une tentative de fraude comme celles que nous venons de décrire.

En fonction de ces types de fraude que l'on doit détecter, il faut choisir un certain nombre de paramètres issus des systèmes de capteurs. Ces paramètres peuvent être des données directement issues des capteurs ou des paramètres calculés à partir des informations fournies.

Pour le système de caméras, il est possible d'obtenir à partir des images prises, des images dites de profil. Ces images sont obtenues par discrimination du sujet par rapport au fond. Les techniques de traitement d'images numériques nécessaires sont connues. Une fois ces images de profils obtenues, il est possible d'en extraire des paramètres comme illustré par la Fig. 3. On obtient facilement l'emplacement du centre de gravité 3.3 de l'objet 3.2, sa hauteur 3.6, sa largeur 3.5. Par une analyse des images au cours du temps, il est également possible d'extraire la vitesse moyenne 3.4 du centre de gravité. Il est aussi possible d'appliquer un algorithme permettant de compter les têtes, en fait un algorithme qui va compter les excroissances du profil 5.1 dans sa partie haute. Par croisement des profils issus de plusieurs caméras, il est encore possible de calculer le volume de l'objet, ainsi que la répartition de ce volume en fonction de la hauteur de l'objet. On peut, par exemple, choisir de diviser la hauteur en trois parties égales et déterminer le pourcentage du volume situé dans la partie basse, la partie médiane et la partie haute de l'objet. Ces paramètres ne représentent que des exemples des paramètres envisageables issus du système de caméras.

De manière analogue, des paramètres sont extraits du système de capteurs constitué par le tapis de pression. Les images de pression, telles que celles illustrées Fig. 4, permettent ici aussi d'obtenir pour chaque objet 4.2, sa hauteur 4.6, sa largeur 4.5 et le centre de gravité global des objets détectés 4.3. Une étude de l'évolution au cours du temps des objets permet de calculer la vitesse de déplacement 4.4 moyenne

de ce centre de gravité ainsi que la moyenne au cours du temps des valeurs précédentes. Il est également possible de calculer une hauteur et une largeur globales. Une intégration des valeurs de pression permet une estimation du poids total des objets présents dans le sas.

On peut faire de même avec tous les systèmes de capteurs que l'on choisit d'utiliser. Chacun d'eux est susceptible de fournir des paramètres pouvant être utiles pour la discrimination des différents types de fraude possibles dans le sas.

Outre ces paramètres issus de chaque système de capteurs, le fait d'utiliser au moins deux systèmes de capteurs rend possible le calcul de paramètres supplémentaires issus de la corrélation d'informations fournies par chacun des systèmes de capteurs. Il est par exemple possible d'établir un ratio volume/poids des objets présents dans le sas, ou encore la différence de vitesse de déplacement entre les objets détectés par les caméras et les objets détectés par le tapis de pression. Il est aussi possible de comparer les positions et le nombre de contacts au sol avec les objets détectés par les caméras.

Un choix est fait parmi tous ces paramètres possibles. On définit ainsi un certain nombre de jeu de paramètres comme illustré Fig. 6, étape 6.1. On fait correspondre les paramètres choisis issus d'un système de capteurs à un jeu de paramètres. Les paramètres issus de la corrélation entre deux systèmes de capteurs vont également fournir un jeu de paramètres. On obtient donc ainsi un jeu de paramètres par système de capteurs et un jeu de paramètres par corrélation faite entre deux systèmes de capteurs. Pour chaque accès par le sas, le système est donc capable de calculer un ensemble de jeux de valeurs pour chaque jeu de paramètres correspondant à cet accès.

Pour pouvoir déterminer la validité d'un accès, c'est-à-dire répondre à la question de savoir si ce passage correspond au passage d'une seule personne ou pas, il faut donc déterminer si un ensemble de jeux de paramètres calculés lors de cet accès correspond au passage d'une seule personne ou à une tentative de fraude.

Pour ce faire, il est possible de procéder à une phase d'apprentissage. Les valeurs des différents jeux de paramètres définis plus haut vont être enregistrées.

Chaque jeu de paramètres peut être vu comme un espace multidimensionnel où chaque dimension correspond à un paramètre. Lors d'un passage déterminé, les valeurs calculées pour chaque paramètre définissent un vecteur dans cet espace représentant le jeu de valeurs. Ceci est illustré Fig. 2. Sur cette figure, est représenté un espace de dimension trois correspondant à un jeu de trois paramètres. Chacune des dimensions 2.1, 2.2, 2.3 correspond donc à un paramètre du jeu. Le vecteur 2.3 correspond aux valeurs mesurées ou calculées lors d'un passage donné. Les mesures successives de différents passages donnent une collection de vecteurs définissant une classe de valeurs correspondant à ces passages. Une telle classe 2.5 est représentée Fig. 2. Pour chaque jeu de paramètres on définit ainsi une classe correspondant aux mesures effectuées lors d'une série de passages. Si l'on effectue de telles séries de mesures pour des passages valides, puis pour des passages correspondant à des tentatives de fraude on établit pour chaque jeu de paramètres des classes correspondant à un passage valide et des classes correspondant aux types de fraude envisagés. On obtient ainsi, comme illustré Fig. 6, étape 6.2, et pour chaque jeu de paramètres, une classe correspondant aux différentes tentatives de fraude.

Lorsque l'on cherche à classifier un passage ou accès on commence donc par acquérir les informations de chaque système de capteurs. Ces informations sont ensuite utilisées pour calculer les paramètres correspondant à chaque jeu de paramètres. On obtient donc les jeux de valeurs correspondant à chaque jeu de paramètres, comme illustré Fig. 6, étape 6.3. Il est donc possible de calculer une mesure de distance entre les valeurs de paramètres mesurées et/ou calculées d'un jeu de paramètres et les différentes classes correspondant aux différents types de passages. Cette mesure de distance peut être une simple distance algébrique entre le vecteur mesuré et le barycentre des vecteurs de la classe ou toute autre mesure de distance dans l'espace. On déduit de cette distance une probabilité que le passage appartienne à la classe considérée, comme illustré Fig. 6, étape 6.4. Chaque jeu de paramètres est ainsi classifié et une probabilité est associée à cette classification. La classification du passage s'effectue par consolidation des classifications obtenues pour chaque jeu de paramètres, comme illustré Fig. 6, étape 6.5.

Alternativement, les étapes de classification d'un jeu de paramètres peuvent être effectuées par un réseau de neurones formels, autrement appelé réseau

neuromimétique. Ces réseaux fonctionnent sur le modèle d'une interconnexion de neurones formels, chacun de ses neurones formels effectuant une somme pondérée de ses entrées et appliquant à cette somme une fonction de sortie non linéaire qui peut être un simple seuil ou une fonction plus sophistiquée comme la fonction sigmoïde. La connaissance ou l'information stockée dans le réseau correspond aux poids synaptiques de chaque neurone, ces poids étant calculés par apprentissage. Cet apprentissage se fait à l'aide d'un algorithme « d'entraînement » qui consiste à modifier les poids synaptiques en fonction d'un jeu de données présentées en entrée du réseau. Le but de cet entraînement est de permettre au réseau de neurones « d'apprendre » à partir des exemples. Si l'entraînement est correctement réalisé, le réseau est capable de fournir des réponses en sortie très proches des valeurs d'origines du jeu de données d'entraînement. Mais tout l'intérêt des réseaux de neurones réside dans leur capacité à généraliser à partir du jeu de test. Un tel réseau de neurones entraîné sur les passages constituant les classes lors d'une phase d'apprentissage est donc à même de réaliser avec fiabilité une classification des passages et de donner pour chaque passage une probabilité associée à chaque jeu de paramètres et à chaque passage ou accès.

La pertinence du choix des paramètres constituant le jeu de paramètres pour chaque système de capteurs, l'utilisation de jeux de paramètres supplémentaires impliquant dans leur calculs plusieurs systèmes de capteurs ainsi que la caractérisation dans l'espace de chaque jeu de paramètres des types de fraude par apprentissage sont autant de facteurs contribuant chacun à la robustesse et à la fiabilité de la classification.

L'homme du métier comprendra que l'invention, bien que décrivant l'utilisation d'un tapis de pression et de caméra, peut inclure de la même façon différents systèmes de capteurs comme des barrières infrarouges ou laser, des caméras infrarouges, des systèmes de diodes ou tout autre moyen d'obtenir des informations sur les objets ou corps présent dans un espace de contrôle. De même, l'invention décrite vise à discriminer l'unicité de présence d'une personne, mais elle pourrait tout aussi facilement s'appliquer à d'autres critères, comme l'unicité d'un véhicule ou autres.

REVENDICATIONS

1/ Procédé de sécurisation d'un accès physique disposant d'une pluralité de systèmes de capteurs (1.4, 1.5, 1.6), ledit procédé visant à discriminer un accès valide d'une tentative d'accès en fraude, caractérisé en ce qu'il comprend les étapes suivantes :

dans une phase préliminaire :

- détermination d'au moins un jeu de paramètres issus des systèmes de capteurs dont au moins un jeu de paramètres issus d'au moins deux systèmes de capteurs différents (6.1) ;
- détermination par apprentissage, pour chaque jeu de paramètres et pour chaque type de fraude envisagé, d'une classe de valeurs des paramètres du jeu correspondant à ce type de fraude pour ce jeu de paramètres (6.2) ;

lors d'un accès :

- détermination de jeux de valeurs formés des valeurs prises par chaque paramètre de chaque jeu de paramètres pour cet accès (6.3) ;
- détermination d'une probabilité de fraude associée à chaque type de fraude pour chaque jeu de paramètres, en fonction du jeu de valeurs déterminé lors de cet accès et de la classe correspondant au type de fraude pour ce jeu de paramètres (6.4) ;
- détermination d'une probabilité de fraude globale associée à l'accès en fonction des probabilités de fraude obtenues pour chaque jeu de paramètres et pour chaque type de fraude (6.5).

2/ Procédé selon la revendication 1 où la probabilité de fraude associée à chaque type de fraude pour chaque jeu de paramètres est estimée par calcul d'une distance entre le jeu de valeurs déterminé lors de cet accès et la classe correspondant au type de fraude pour ce jeu de paramètres.

3/ Procédé selon la revendication 2 où cette distance est une distance algébrique entre le jeu de valeurs déterminé et le barycentre de la classe.

4/ Procédé selon la revendication 1 où la probabilité de fraude associée à chaque type de fraude pour chaque jeu de paramètres est estimée par un réseau neuromimétique et où l'étape de détermination par apprentissage des classes comprend une étape d'entraînement de ce réseau neuromimétique.

5/ Procédé selon l'une quelconque des revendications précédentes où les systèmes de capteurs comprennent un système de caméras (1.5, 1.6) fournissant des images de profil (1.8, 1.9, Fig. 3).

6/ Procédé selon l'une quelconque des revendications précédentes où les systèmes de capteurs comprennent un système de tapis de pression au sol (1.4) fournissant des images de pression (1.7, Fig. 4).

7/ Dispositif de sécurisation d'un accès physique comprenant :

- un espace de contrôle ;
- une pluralité de systèmes de capteurs dans cet espace de contrôle (1.4, 1.5, 1.6) ;
- des moyens d'analyse des informations issues des systèmes de capteurs (1.9) ;

caractérisé en ce que, étant déterminé au moins un jeu de paramètres issus des systèmes de capteurs dont au moins un jeu de paramètres issus d'au moins deux systèmes de capteurs différents, étant déterminée par apprentissage, pour chaque jeu de paramètres et pour chaque type de fraude envisagé, une classe d'espace de valeurs des paramètres du jeu correspondant à ce type de fraude pour ce jeu de paramètres, les moyens d'analyse comprennent :

- des moyens de détermination de jeux de valeurs formés des valeurs prises par chaque paramètre de chaque jeu de paramètres pour cet accès ;
- des moyens de détermination d'une probabilité de fraude associée à chaque type de fraude et pour chaque jeu de paramètres, en fonction du jeu de valeurs déterminé lors de cet accès et de la classe correspondant au type de fraude pour ce jeu de paramètres ;
- des moyens de détermination d'une probabilité de fraude globale associée à l'accès en fonction des probabilités de fraude obtenues pour chaque jeu de paramètres et pour chaque type de fraude.

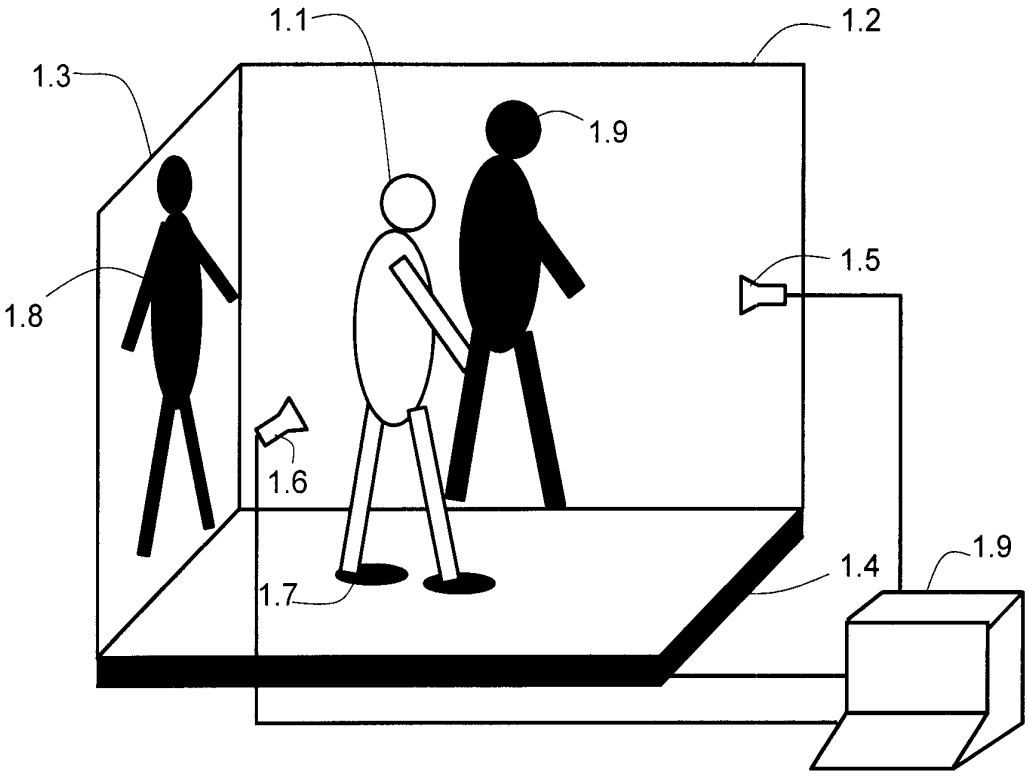


Fig. 1

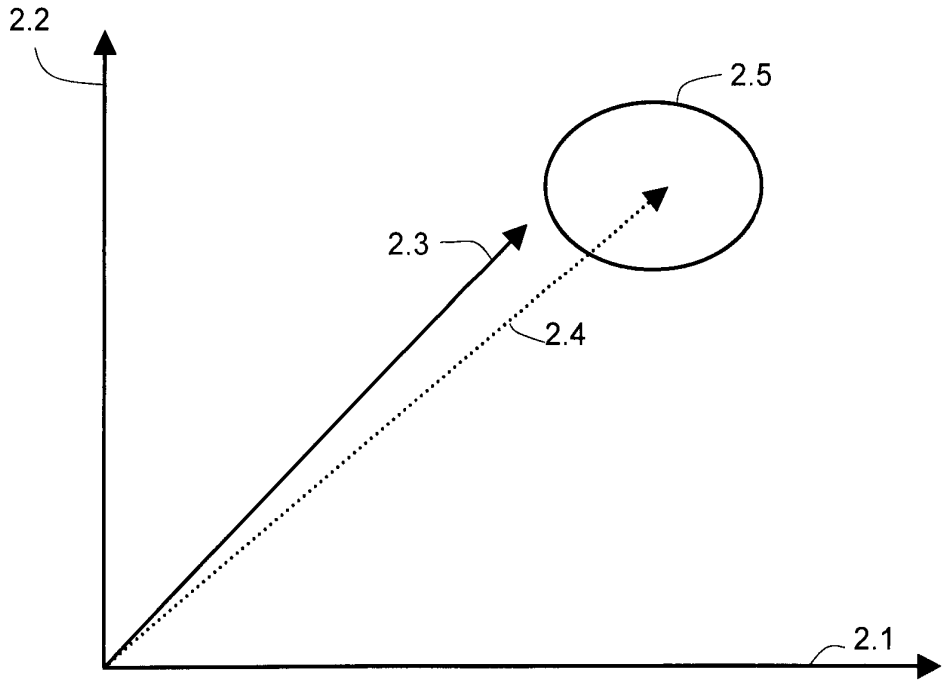


Fig. 2

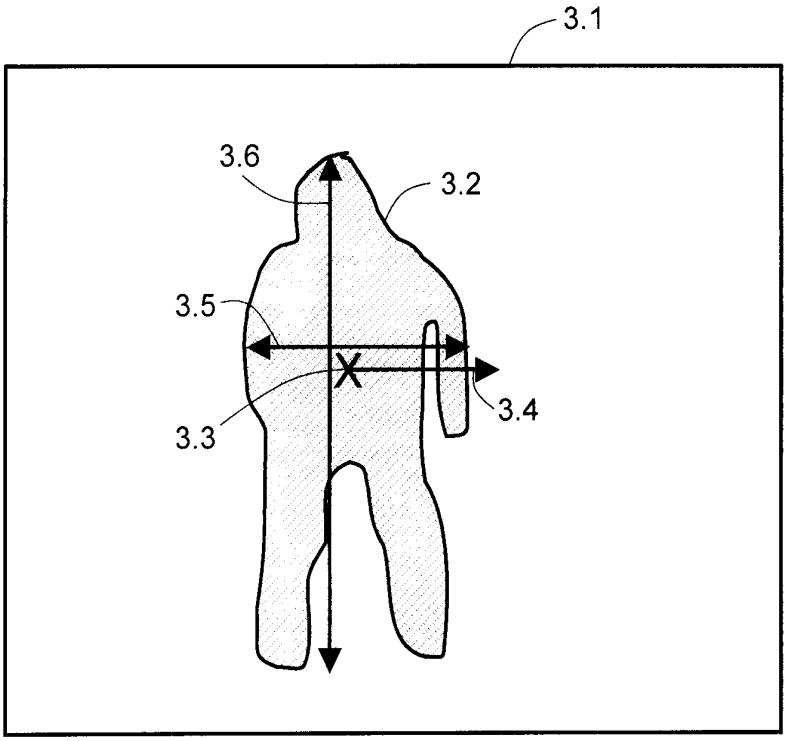


Fig. 3

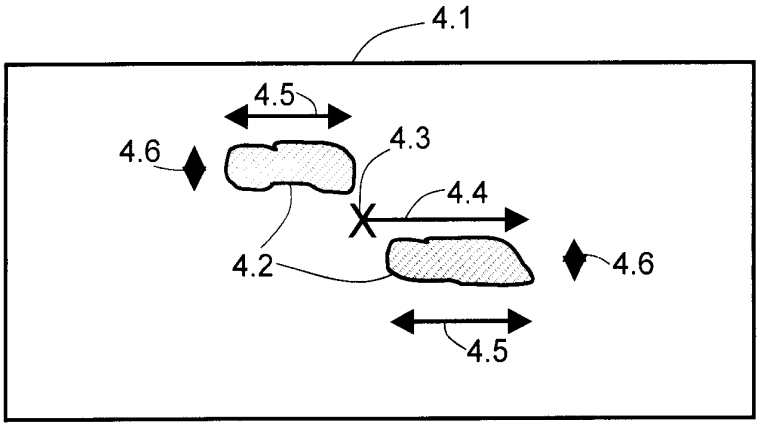


Fig. 4

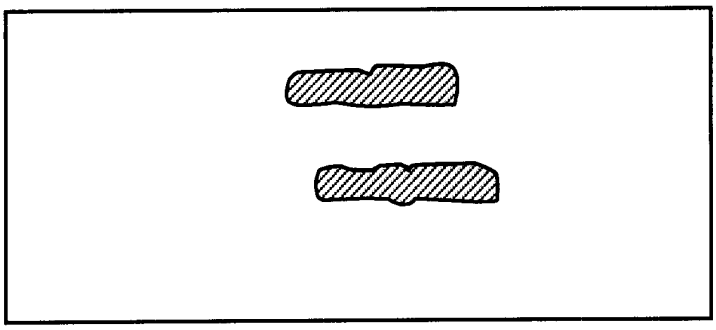


Fig. 5

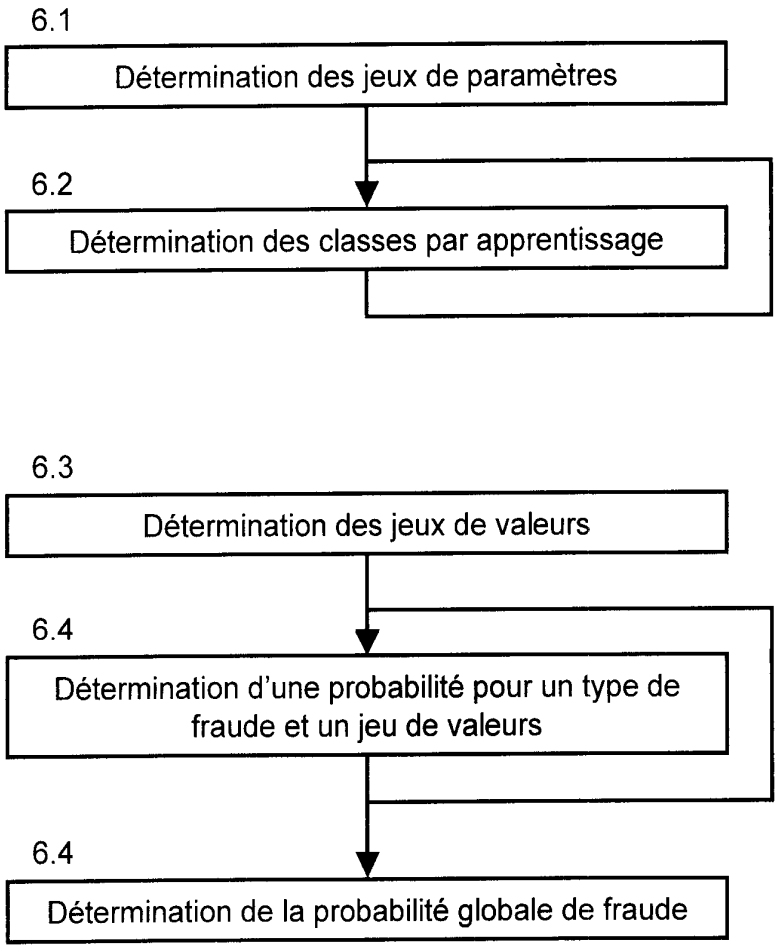

6.1
Détermination des jeux de paramètres
6.2
Détermination des classes par apprentissage
6.3
Détermination des jeux de valeurs
6.4
Détermination d'une probabilité pour un type de fraude et un jeu de valeurs
6.4
Détermination de la probabilité globale de fraude

Fig. 6

RÉPUBLIQUE FRANÇAISE

2895122

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement national

FA 674396
FR 0512857

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 Y	EP 0 706 062 A (SAT ; SAGEM SA) 10 avril 1996 (1996-04-10) * colonne 2, ligne 35 - colonne 3, ligne 44 * * colonne 5, ligne 33 - colonne 6, ligne 32 * * figures 1-4,7-10 *	1-3,7 4	G07C9/00 H04L9/32 H04N5/225
Y	US 2002/097145 A1 (TUMEY DAVID M ET AL) 25 juillet 2002 (2002-07-25) * alinéa [0038] - alinéa [0039] * * alinéa [0048] - alinéa [0058] * * figures 2-6 *	4	
X	WO 03/088157 A (NEWTON SECURITY INC; BRAMBLET, JOHN, WESTLEY; WITTY, CARL, ROGER; LAFO) 23 octobre 2003 (2003-10-23) * page 11, ligne 31 - page 14, ligne 27 * * page 20, ligne 28 - page 21, ligne 7 * * figures 1,2,4c-4f *	1-3,5,7	
X	FR 2 713 805 A (ALKAN SA; PARIENTI RAOUL; CAMUT YVES) 16 juin 1995 (1995-06-16) * page 2, ligne 21 - page 4, ligne 5 * * figures *	1-3,6,7	DOMAINES TECHNIQUES RECHERCHÉS (IPC) G07C
E	FR 2 871 602 A (THEPAULT YVES) 16 décembre 2005 (2005-12-16) * page 2, ligne 7 - ligne 21 * * page 3, ligne 8 - ligne 25 * * page 4, ligne 3 - ligne 19 * * page 5, ligne 13 - ligne 25 * * figures *	1-3,6,7	

Date d'achèvement de la recherche	Examinateur
7 septembre 2006	Paraf, Edouard

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 0512857 FA 674396

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 07-09-2006
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
EP 0706062	A	10-04-1996	DE	69521003 D1	28-06-2001
			FR	2725278 A1	05-04-1996
US 2002097145	A1	25-07-2002	AUCUN		
WO 03088157	A	23-10-2003	AU	2003221893 A1	27-10-2003
			CA	2481250 A1	23-10-2003
			EP	1493130 A1	05-01-2005
FR 2713805	A	16-06-1995	AUCUN		
FR 2871602	A	16-12-2005	AUCUN		

EPO FORM P0465