

12

DEMANDE DE BREVET D'INVENTION

A1

22 Date de dépôt : 27.06.00.

30 Priorité :

43 Date de mise à la disposition du public de la
demande : 28.12.01 Bulletin 01/52.

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) : HUARD DE VERNEUIL FRANCOIS
— FR.

72 Inventeur(s) : HUARD DE VERNEUIL FRANCOIS.

73 Titulaire(s) :

74 Mandataire(s) : ARMENGAUD AINE.

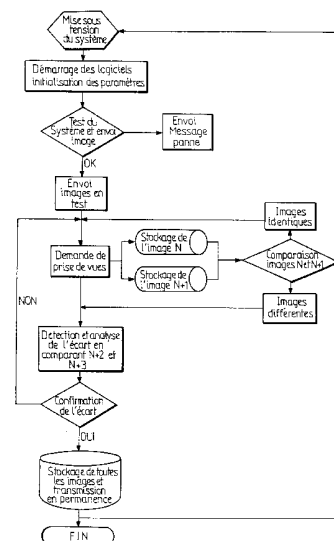
54 PROCEDE PERMETTANT DE DETECTER UNE PRESENCE DANS UNE ENCEINTE PROTEGEE.

57 Procédé permettant de détecter une présence dans
une enceinte protégée, caractérisé en ce qu'il comporte les
étapes suivantes:

- dans une première étape, on réalise des images vidéo
de ladite enceinte protégée à l'aide d'au moins une caméra,
de préférence numérique, disposée à un ou plusieurs en-
droits stratégiques de ladite enceinte, lesdites images étant
transformées en fichiers informatiques, à un format stan-
dard ; - dans une deuxième étape, on stocke lesdits fichiers
informatiques dans une mémoire d'une unité centrale, les-
dits fichiers correspondant aux images réalisées aux ins-
tants N et N + 1, N étant un nombre entier supérieur ou égal
à zéro;

- dans une troisième étape, on compare lesdits fichiers
correspondant aux images réalisées aux instants N et N + 1
à l'aide d'un logiciel commandé par ladite unité centrale, le-
dit logiciel superposant lesdits fichiers de façon à détecter
un éventuel écart entre lesdites images;

- si un écart est détecté à la troisième étape, on transmet
au cours d'une quatrième étape lesdits fichiers à un centre
de contrôle à l'aide d'un modem piloté par ladite unité cen-
trale, ledit centre de contrôle pouvant alors contacter les for-
ces de l'ordre et/ ou une société spécialisée en vue
d'effectuer une intervention.



La présente invention est relative à un procédé permettant de détecter une présence dans une enceinte protégée.

Elle vise plus particulièrement un procédé qui permet
5 de détecter un intrus dès son entrée dans une enceinte protégée, de prendre sa photographie et de la transmettre à un centre de contrôle pour permettre une intervention rapide des forces de l'ordre.

En France, on recense plus de 400 000 cambriolages
10 chaque année, la grande majorité de ces effractions étant réalisée chez des particuliers. L'isolement de certaines demeures favorisent notamment la recrudescence de tels actes dans les zones rurales ce qui a pour conséquence d'augmenter le temps nécessaire aux forces de l'ordre
15 (police, gendarmerie, etc...) pour intervenir, ajouté à la difficulté naturelle de surveiller des zones géographiques plus étendues.

Par ailleurs, le temps d'intervention au plan national est en moyenne supérieur à 20 minutes ce qui laisse
20 généralement le temps aux malfaiteurs de s'enfuir des lieux protégés.

Enfin, les forces de l'ordre n'interviennent pour un cambriolage que si une levée de doute a été effectuée afin d'éviter tout déplacement pour une fausse alerte.

25 La présente invention vise donc à pallier de tels inconvénients en proposant un procédé de détection d'intrusion qui permet à la fois d'alerter sans délai les forces de l'ordre, et d'effectuer une levée de doute nécessaire à leur intervention tout en gardant de façon
30 sûre une trace de cette intrusion.

A cet effet, le procédé permettant de détecter une présence dans une enceinte protégée selon l'invention, se caractérise en ce qu'il comporte les étapes suivantes :

- dans une première étape, on réalise des images vidéo de ladite enceinte protégée à l'aide d'au moins une caméra, de préférence numérique, disposée à un ou plusieurs endroits stratégiques de ladite enceinte, lesdites images étant transformées en fichiers informatiques, à un format standard ;
- dans une deuxième étape, on stocke lesdits fichiers informatiques dans une mémoire d'une unité centrale, lesdits fichiers correspondant aux images réalisées aux instants N et $N + 1$, N étant un nombre entier supérieur ou égal à zéro ;
- dans une troisième étape, on compare lesdits fichiers correspondant aux images réalisées aux instants N et $N + 1$ à l'aide d'un logiciel commandé par ladite unité centrale, ledit logiciel superposant lesdits fichiers de façon à détecter un éventuel écart entre lesdites images ;
- si un écart est détecté à la troisième étape, on transmet au cours d'une quatrième étape lesdits fichiers à un centre de contrôle à l'aide d'un modem piloté par ladite unité centrale, ledit centre de contrôle pouvant alors contacter les forces de l'ordre et/ou une société spécialisée en vue d'effectuer une intervention.

D'autres caractéristiques et avantages de la présente invention ressortiront de la description faite ci-après, en référence au dessin annexé qui en illustre un exemple de réalisation dépourvu de tout caractère limitatif.

Le procédé selon l'invention permettant de détecter une présence dans une enceinte protégée comporte essentiellement les quatre étapes suivantes (cf. figure) :

Une première étape consiste à réaliser des images vidéo de l'enceinte protégée. Pour ce faire, on utilise au moins une caméra vidéo, de préférence numérique, qui permet de capturer une image de ladite enceinte et de la transformer en fichier informatique, à un format standard.

Ces caméras sont installées à l'intérieur de ladite enceinte protégée, à plusieurs endroits stratégiques (par exemple, devant un coffre ou un meuble de valeur, dans un couloir, etc...) et à une distance de prise de vue
5 convenable pour permettre l'identification d'un individu (par exemple, cette distance de prise de vue pourra être comprise entre 1 et 10 mètres).

Par ailleurs, ces caméras vidéo sont reliées à une unité centrale qui transmet les ordres de prises de vue, et
10 éventuellement de déplacement de ces caméras. Celles-ci transmettent alors les images des prises de vue transformées en fichiers informatiques à ladite unité centrale.

Cette unité centrale présentent donc des
15 caractéristiques standards lui permettant de réaliser les fonctions suivantes :

- commander et piloter les caméras vidéos ;
- stocker momentanément dans une mémoire les fichiers images transmis par lesdites caméras ;
- 20 - analyser et comparer entre elles lesdites images à l'aide d'un logiciel informatique décrit ultérieurement ; et
- commander et piloter un modem permettant de transmettre des données à un centre de contrôle.

Bien entendu, avant de réaliser cette première étape,
25 on pourra prévoir une étape supplémentaire qui consiste, par exemple, à mettre sous tension le système (caméras et unité centrale), démarrer et initialiser le logiciel de comparaison, tester ledit système et envoyer à l'aide du modem piloté par l'unité centrale un message signalant une
30 éventuelle panne au centre de contrôle.

Une deuxième étape du procédé selon l'invention a pour objet le stockage dans une mémoire de l'unité centrale des fichiers informatiques correspondant aux images des prises de vue à l'instant N et à l'instant N + 1 (avec N, nombre

entier supérieur ou égal à zéro). A titre d'exemple, et en fonction de la distance de prise de vue des caméras et de la taille de la mémoire de ladite unité centrale, on pourra stocker des fichiers images correspondant à des prises de vue espacées de 2 ou 3 secondes les unes des autres.

La troisième étape consiste à comparer les fichiers images N et N + 1 ainsi stockés dans la mémoire de l'unité centrale afin de détecter une éventuelle intrusion. Cette comparaison est réalisée à l'aide d'un logiciel informatique commandé par ladite unité centrale. Ce logiciel permet ainsi de détecter une éventuelle différence d'image entre le fichier image N et le fichier image N + 1.

En effet, ce logiciel de comparaison superpose les fichiers images N et N + 1 et analyse les différences qui se présentent alors sous la forme d'une surface de l'image différente entre les images N et N + 1.

En outre, ledit logiciel de comparaison permet d'évaluer la pertinence de cet écart enregistré entre les deux images. Cette analyse porte principalement sur un calcul du pourcentage de cette surface différente par rapport à la surface totale de l'image prise à l'instant N.

Deux cas se présentent alors :

- si ce pourcentage dépasse un seuil fonction des différents paramètres de la caméra (distance de prise de vue, espacement entre deux prises de vue successives, ...), une quatrième étape du procédé selon l'invention a pour objet de transmettre à un centre de contrôle et d'intervention ces fichiers informatiques correspondants aux images sur lesquelles l'intrus a été détecté. A titre d'exemple, ledit seuil est de l'ordre de 2% pour une distance de prise de vue de la caméra de 10 mètres environ.
- si ce pourcentage est inférieur audit seuil, et ce compte-tenu des différents paramètres de la caméra, cet écart entre les images N et N + 1 n'est pas prise en compte

par le logiciel de comparaison qui considère donc que ces images sont identiques. Ce dernier va alors comparer de nouvelles images réalisées au cours de la première étape du procédé.

5 Le logiciel de comparaison permet donc de discerner si l'on a affaire à un intrus ou si l'on est en présence d'un incident mineur, comme par exemple un simple mouvement de rideaux. Cette caractéristique essentielle du logiciel a donc pour avantage d'éviter aux forces de l'ordre de se
10 déplacer pour une effraction qui n'en est pas une en éliminant les incidents mineurs.

 Selon une caractéristique avantageuse de l'invention, si on est en présence d'un écart significatif entre les images aux instants N et $N + 1$ (pourcentage au-dessus dudit
15 seuil), le procédé comporte une étape supplémentaire qui consiste à analyser les fichiers informatiques correspondant aux images réalisées aux instants $N + 2$ et $N + 3$ de façon à confirmer l'écart précédemment analysé entre les images N et $N + 1$.

20 Cette nouvelle analyse est effectuée de manière identique à la précédente à l'aide du même logiciel informatique contenu dans l'unité centrale. Elle présente l'avantage de vérifier et de contrôler la présence détectée entre les images N et $N + 1$ et donc de faire, une fois de
25 plus, la différence entre un simple incident, qui peut par exemple être dû à un mouvement d'oscillation d'un rideau, et une réelle intrusion.

 La transmission de fichiers entre l'unité centrale et le centre de contrôle est effectuée à l'aide d'un modem
30 standard installé dans l'unité centrale et commandé par celle-ci. Ce modem permet donc d'appeler le numéro de téléphone d'un opérateur d'accès à internet et de gérer le flux de données échangées entre l'unité centrale et le site internet appelé.

Selon une autre caractéristique avantageuse de l'invention, ce modem est couplé à une ligne de téléphone répondant aux normes GPRS ou UMTS de manière à éviter un risque de coupure de ligne malveillant ou inopportun.

5 Ainsi, l'envoi par le modem des fichiers images représentant une ou plusieurs photos de l'intrusion se fait à un centre de contrôle et d'intervention qui pourra déclencher, selon la pertinence de cette intrusion, une intervention appropriée en faisant appel aux forces de
10 l'ordre et/ou à une société spécialisée.

Bien entendu, parallèlement à cette alerte, on peut également envisager une transmission de ces mêmes données entre l'unité centrale et le propriétaire de l'enceinte protégée afin de prévenir celui-ci de l'intrusion. Par
15 exemple, cette transmission peut être réalisée par un simple appel téléphonique ou par envoi d'un message électronique, etc...

Le centre de contrôle et d'intervention possède un site internet qui a pour fonction de réceptionner des
20 fichiers images en provenance de différentes enceintes à surveiller, de stocker ces images reçues dans une mémoire et si besoin, de contacter les forces de l'ordre ou une société de gardiennage privée. Par ailleurs, l'envoi des fichiers images s'effectuera de préférence par tout mode
25 sécurisé de transmission de données informatiques sur internet.

Enfin, on peut également envisager différentes fonctions remplies par le site internet du centre de contrôle, comme par exemple d'informer les clients des
30 interventions effectuées, des nouveautés de ce système de surveillance, ou de contrôler à distance le bon fonctionnement de ces systèmes, etc...

La présente invention telle que décrite précédemment offre de multiples avantages ; notamment, elle propose un

procédé permettant de détecter sans délai toute présence imprévue dans une enceinte protégée, de capturer une ou plusieurs images de cette intrusion et de les envoyer directement à un centre de contrôle afin de procéder à une
5 intervention rapide des forces de l'ordre. Cette intervention sera d'autant plus rapide que la levée de doute est immédiatement effectuée par l'envoi des fichiers images au centre de contrôle. En outre, les forces de l'ordre peuvent garder une trace sûre de cette intrusion.

10 Il demeure bien entendu que la présente invention n'est pas limitée aux exemples de réalisation décrits et représentés ci-dessus, mais qu'elle en englobe toutes les variantes.

REVENDEICATIONS

1 - Procédé permettant de détecter une présence dans une enceinte protégée, caractérisé en ce qu'il comporte les
5 étapes suivantes :

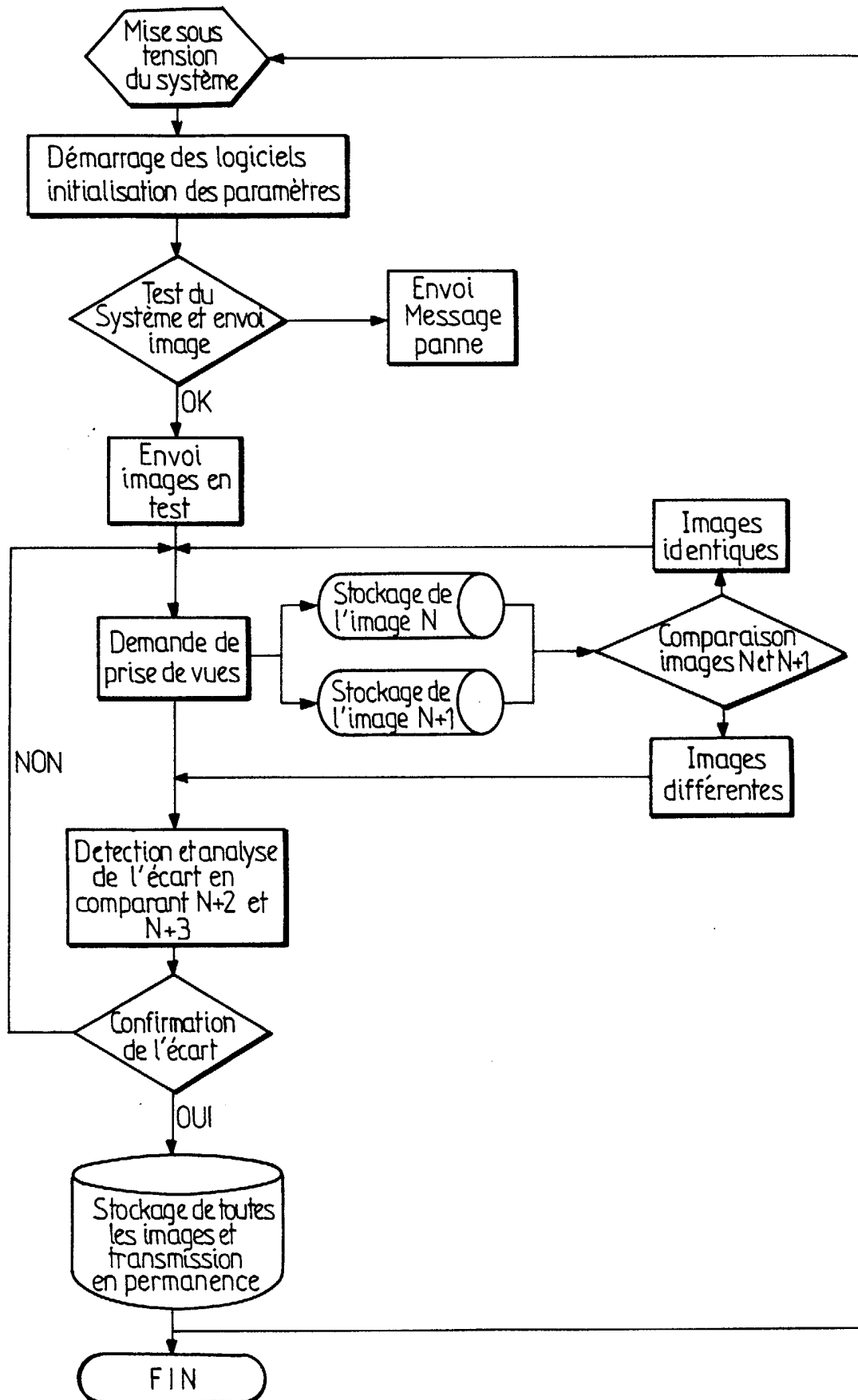
- dans une première étape, on réalise des images vidéo de ladite enceinte protégée à l'aide d'au moins une caméra, de préférence numérique, disposée à un ou plusieurs endroits stratégiques de ladite enceinte, lesdites images étant
10 transformées en fichiers informatiques, à un format standard ;
- dans une deuxième étape, on stocke lesdits fichiers informatiques dans une mémoire d'une unité centrale, lesdits fichiers correspondant aux images réalisées aux
15 instants N et $N + 1$, N étant un nombre entier supérieur ou égal à zéro ;
- dans une troisième étape, on compare lesdits fichiers correspondant aux images réalisées aux instants N et $N + 1$ à l'aide d'un logiciel commandé par ladite unité centrale,
20 ledit logiciel superposant lesdits fichiers de façon à détecter un éventuel écart entre lesdites images ;
- si un écart est détecté à la troisième étape, on transmet au cours d'une quatrième étape lesdits fichiers à un centre de contrôle à l'aide d'un modem piloté par ladite unité
25 centrale, ledit centre de contrôle pouvant alors contacter les forces de l'ordre et/ou une société spécialisée en vue d'effectuer une intervention.

2 - Procédé selon la revendication 1, caractérisé en ce qu'il comporte une étape supplémentaire permettant de
30 confirmer l'écart détecté à la troisième étape en comparant les fichiers correspondant aux images réalisées aux instants $N + 2$ et $N + 3$.

3 - Procédé selon l'une des revendications 1 ou 2, caractérisé en ce que la transmission desdits fichiers

audit centre de contrôle s'effectue à l'aide d'un modem couplé à une ligne de téléphone répondant aux normes GPRS ou UMTS de manière à éviter un risque de coupure de ligne malveillant ou inopportun.

1/1



**RAPPORT DE RECHERCHE
PRÉLIMINAIRE**

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

2810775

N° d'enregistrement
national

FA 590096

FR 0008261

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	EP 0 805 426 A (KELLY SIMON ; TRUEFITT GORDON (GB)) 5 novembre 1997 (1997-11-05) * abrégé *	1-3	G08B25/00
X	DE 38 27 928 A (STANDARD ELEKTRIK LORENZ AG) 22 février 1990 (1990-02-22) * abrégé *	1-3	
X	US 4 777 526 A (SAITOH MITSUMASA ET AL) 11 octobre 1988 (1988-10-11) * abrégé *	1-3	
X	EP 0 529 196 A (PIONEER ELECTRONIC CORP) 3 mars 1993 (1993-03-03) * abrégé *	1-3	
			DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7)
			G08B
Date d'achèvement de la recherche		Examineur	
26 février 2001		Sgura, S	
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			