(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 3 716 239 A1**

(12) **DEMANDE DE BREVET EUROPEEN**

(43) Date de publication:
30.09.2020 Bulletin 2020/40

(51) Int Cl.:
G08B 13/196 *(2006.01)*

(21) Numéro de dépôt: **19305379.0**

(22) Date de dépôt: **26.03.2019**

(84) Etats contractants désignés:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Etats d'extension désignés:
BA ME
Etats de validation désignés:
KH MA MD TN

(71) Demandeur: **Alcom Technologies**
10600 Barberey St Sulpice (FR)

(72) Inventeur: **GAUTIER, Fabrice**
33000 BORDEAUX (FR)

(74) Mandataire: **Ipside**
7-9 Allées Haussmann
33300 Bordeaux Cedex (FR)

(54) **DISPOSITIF DE DÉTECTION D'INTRUSION PAR VISION INFRAROUGE ET PROCÉDÉ DE SÉCURISATION**

(57) Dispositif de détection d'intrusion (100), pour sécuriser une zone déterminée, comportant une unité de surveillance (10), comprenant au moins un capteur d'image (11) et un moyen d'éclairage (12), un support (20), un boitier électronique (30), comportant un module de communication sans-fil (33), un dispositif d'alimentation électrique (41), et une antenne (50), ledit au moins un capteur d'image étant une caméra infrarouge, et le module de communication sans-fil étant apte à communiquer sur un réseau de téléphonie mobile.

L'invention porte également sur un procédé de sécurisation mettant en oeuvre un tel dispositif et permettant d'envoyer des images à un serveur (300) sécurisé par une blockchain, de traiter les images avec une intelligence artificielle dans un calculateur (400), et d'alerter un utilisateur sur son téléphone mobile par exemple.

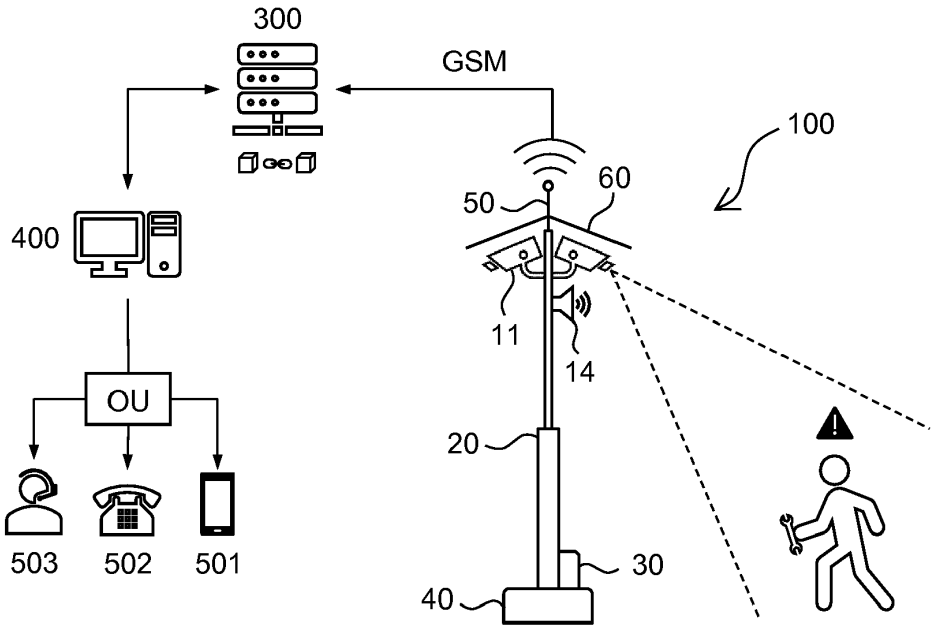


Fig. 5

EP 3 716 239 A1

Description

DOMAINE TECHNIQUE

[0001] La présente invention appartient au domaine général des systèmes de sécurité, notamment des dispositifs de surveillance et de sécurisation des terrains agricoles ou des chantiers isolés, et concerne plus particulièrement un dispositif de détection d'intrusion par vision et imagerie infrarouges ainsi qu'un procédé de sécurisation, optimisé par une intelligence artificielle, pour sécuriser des terrains agricoles, tels que des vignes, des plantations ou des serres, des chantiers non gardiennés, et assimilés.

ÉTAT DE L'ART

[0002] La sécurisation des terrains isolés tels que les vastes champs agricoles ou les chantiers est une problématique bien connue. En effet, la surveillance de ces terrains nécessite le déploiement d'importants moyens et ressources, qui, souvent, s'avèrent rédhibitoires pour les propriétaires, ces derniers optant ainsi pour une sécurité très limitée, voire inexistante. De ce fait, ces terrains représentent des cibles « faciles » pour les malfrats qui y trouvent une occasion pour dérober du matériel de valeur, de la matière première telle que du carburant, etc.

[0003] L'importance des caméras pour la surveillance des biens et la protection des personnes est bien connue. La miniaturisation des caméras, les capacités de calcul des outils embarqués et les performances des algorithmes actuels permettent d'entrevoir de nouvelles applications pour les technologies basées sur la détection d'intrusions. Il est nécessaire d'avoir des informations fiables sur la présence d'une personne suspecte dans l'endroit surveillé.

[0004] Les dispositifs d'alarme ne dissuadent plus les intrus décidés à commettre un vol sur un terrain agricole ou un chantier car ces intrus sont conscients du temps d'intervention du propriétaire qui leur permet généralement de commettre leur vol et d'échapper sans le moindre souci.

[0005] L'utilisation des caméras de vidéosurveillance ne permet pas au propriétaire du terrain surveillé, lorsqu'il n'est pas devant son écran de surveillance, d'être informé d'une intrusion en temps réel ou très sensiblement différé. Dans ce cas, le propriétaire ayant repéré des indices de l'intrusion et/ou du vol (en remarquant un manque au niveau du matériel, une infraction, etc.) doit chercher dans l'enregistrement des caméras la scène d'intrusion, l'analyser de façon très approximative, et en faire part aux autorités concernées. Généralement, il est très difficile, voir impossible, d'identifier des informations utiles sur les images obtenues.

[0006] Il existe des solutions basées sur l'utilisation de la vision infrarouge et la transmission en temps réel des images captées.

[0007] Le document US 2017/0116836 A1 décrit un système de détection d'intrusion installé dans une zone de surveillance comprenant un dispositif à rayonnement thermique pour mesurer le rayonnement infrarouge généré par les intrus pénétrant dans la zone afin de déterminer un évènement d'intrusion et de générer un signal d'alarme pour indiquer l'occurrence de l'intrusion. Le signal d'alarme est ensuite transmis à un contrôleur par liaison radio avant que celui-ci ne le transmette à un serveur via un réseau internet. Le signal est in fine transmis à un terminal mobile, toujours par internet, pour que le propriétaire en prenne connaissance. Ce signal contient par défaut trois images de la scène : une image de référence et deux images avec l'intrus rendant compte d'un éventuel mouvement de l'intrus.

[0008] Ce système présente des inconvénients majeurs qui rendent son efficacité très limitée : les images envoyées sont des images thermiques et ne permettent aucune identification des visages des intrus ou d'autres éléments informatifs, le système utilise un biais qui est le contrôleur, celui-ci transmet le signal d'alarme sur un réseau internet et ne peut donc pas être adapté aux champs agricoles ou chantiers isolés sans couverture internet, le serveur n'est pas sécurisé, aucun traitement des images thermiques n'est effectué.

PRÉSENTATION DE L'INVENTION

[0009] La présente invention a pour but principal de pallier les limitations de l'art antérieur en proposant un dispositif, un système et un procédé de détection d'intrusion pour sécuriser des terrains isolés, à distance et avec une efficacité améliorée de sorte à limiter au maximum les failles rencontrées avec les dispositifs de l'art antérieur.

[0010] À cet effet, la présente invention concerne un dispositif de détection d'intrusion, pour sécuriser une zone déterminée, comportant une unité de surveillance, comprenant au moins un capteur d'image et un moyen d'éclairage, un support, un boitier électronique, comportant un module de communication sans-fil, un dispositif d'alimentation électrique, et une antenne. Ce dispositif est remarquable en ce que le capteur d'image est une caméra infrarouge pourvue de moyens de détection de présence commandant ses prises d'images, et en ce que le module de communication sans-fil est apte à communiquer sur un réseau de téléphonie mobile. Par exemple, les moyens de détection de présence mettent en oeuvre des algorithmes de reconnaissance de corps (humains, véhicules, etc.) par analyse du rayonnement thermique, et plus particulièrement de la puissance rayonnée, limitant ainsi tout déclenchement intempestif du dispositif, qui peut être causé par la présence d'un animal par exemple.

[0011] Grâce aux moyens de détection de présence de la caméra, celle-ci n'enregistre pas la scène observée en permanence et n'enclenche la prise de photos que lorsqu'une présence a été détectée.

[0012] Avantageusement, le dispositif de détection

d'intrusion comporte trois caméras infrarouges disposées en triangle équilatéral de sorte que leurs axes forment deux à deux un angle de 120°, et le moyen d'éclairage comprend un flash photographique pour chaque caméra infrarouge.

[0013] Plus particulièrement, le moyen d'éclairage comprend un flash photographique à base de diodes électroluminescentes.

[0014] De façon avantageuse, le boitier électronique comprend une unité centrale de traitement et une mémoire informatique.

[0015] Selon un mode de réalisation particulièrement avantageux, le module de communication sans-fil est un module GSM.

[0016] Le dispositif d'alimentation électrique est une batterie électrique rechargeable fixe ou amovible, placée à l'intérieur d'une base du dispositif de détection d'intrusion.

[0017] Selon un mode de réalisation, l'unité de surveillance comprend en outre au moins un détecteur de mouvement.

[0018] Avantageusement, le dispositif de détection d'intrusion comporte un haut-parleur pour diffuser un message vocal préenregistré.

[0019] Selon un mode de réalisation particulièrement avantageux, le dispositif de détection d'intrusion comporte des organes de déplacement, comme des roues ou des roulettes permettant le déplacement dudit dispositif, et des moyens de préhension facilitant le transport dudit dispositif.

[0020] L'invention concerne également un procédé de sécurisation d'une zone déterminée mettant en oeuvre un dispositif de détection d'intrusion tel que décrit, et comprenant :

- une étape de détection d'une présence humaine dans ladite zone par l'unité de surveillance ;
- une étape de prise de photos de la scène par l'unité de surveillance ;
- une étape d'envoi des photos prises à un serveur sécurisé par une chaîne de blocs (blockchain) via un réseau de téléphonie mobile ;
- une étape de transmission des photos reçues à un calculateur ;
- une étape de traitement et d'analyse des photos transmises par des algorithmes d'intelligence artificielle implémentés sur le calculateur ; et
- une étape d'envoi d'une alerte à un utilisateur.

[0021] De façon avantageuse, l'étape de traitement et d'analyse des photos par intelligence artificielle comprend une opération ou une combinaison d'opérations parmi :

- une analyse automatique de formes dans les photos, pour une prédiction des menaces ;
- une recherche automatique de situations à partir de classificateurs normés spécifiques ; et
- une détection automatique d'éléments informatifs sur les photos.

[0022] Plus particulièrement, les opérations de l'étape de traitement et d'analyse des photos par intelligence artificielle sont basées sur des classificateurs normés spécifiques de l'intelligence artificielle.

[0023] L'étape de détection d'une présence humaine comprend une sous-étape de mesure par une caméra infrarouge d'une puissance rayonnée par un objet capté et de comparaison de la puissance rayonnée mesurée avec des valeurs connues représentatives de la puissance rayonnée par un corps humain.

[0024] Selon un mode de réalisation particulièrement avantageux, le procédé comprend une étape d'horodatage par le serveur des photos reçues et une étape de stockage desdites photos, chacune étant associée à un certificat d'horodatage.

[0025] L'invention concerne également un système de détection d'intrusion pour la sécurisation d'une zone déterminée selon le procédé décrit, comportant un dispositif de détection d'intrusion tel que décrit, un serveur sécurisé par une blockchain et un calculateur implémentant au moins un algorithme d'intelligence artificielle.

[0026] Les concepts fondamentaux de l'invention venant d'être exposés ci-dessus dans leur forme la plus élémentaire, d'autres détails et caractéristiques ressortiront plus clairement à la lecture de la description qui suit et en regard des dessins annexés, donnant à titre d'exemple non limitatif des modes de réalisations d'un dispositif de détection d'intrusion et de son procédé de mise en oeuvre conformes aux principes de l'invention.

BRÈVE DESCRIPTION DES FIGURES

[0027] Les figures ainsi que les éléments d'une même figure ne sont pas nécessairement à la même échelle. Sur l'ensemble des figures, les éléments identiques portent la même référence numérique.

[0028] Il est ainsi illustré en :

- Figure 1 : une vue en perspective d'un dispositif de détection d'intrusion selon un mode de réalisation de l'invention ;
- Figure 2 : un diagramme bloc schématique des composants électroniques du dispositif de détection d'intrusion ;
- Figure 3 : un exemple d'agencement d'un ensemble de détection selon l'invention ;
- Figure 4 : une modélisation du champ de vision résultant de l'association de trois capteurs d'image ;
- Figure 5 : un schéma synoptique d'un exemple de sécurisation mettant en oeuvre le dispositif de détection d'intrusion ;
- Figure 6 : les principales étapes du procédé de sécurisation selon l'invention ;
- Figure 7 : un schéma des étapes de détection de présence humaine et de prise des photos selon

l'invention ;

- Figure 8 : un schéma d'un tri de photos selon leur netteté par intelligence artificielle ;
- Figure 9 : les étapes du procédé de sécurisation selon un mode de réalisation de l'invention ;
- Figure 10 : une vue en perspective d'un dispositif de détection d'intrusion portable selon un mode de réalisation de l'invention ;
- Figure 11 : un exemple d'interface graphique de réception d'alerte selon l'invention.

DESCRIPTION DÉTAILLÉE DE MODES DE RÉALISATION

[0029] La terminologie employée dans la présente description ne doit en aucun cas être interprétée de manière limitative ou restrictive. Elle est simplement employée en conjonction avec une description détaillée de certains modes de réalisation de l'invention.

[0030] Dans le mode de réalisation décrit ci-après, on fait référence à un dispositif de détection d'intrusion destiné principalement à une utilisation dans un terrain agricole, tel qu'un champ, ou dans un chantier isolé pour surveiller, dans les deux cas, du matériel et/ou de la matière première susceptibles d'être dérobés. Cet exemple non limitatif est donné pour une meilleure compréhension de l'invention et n'exclut pas une utilisation de celle-ci sur un site industriel, un lieu professionnel, une propriété privée ou tout autre endroit vaste dans lequel du matériel peut être entreposé ou stocké.

[0031] Dans la suite de la description, l'expression « dispositif anti-intrusion » est employée pour désigner un dispositif de détection d'intrusion, et les éléments du dispositif anti-intrusion sont physiquement décrits avant que leurs fonctions ne soient détaillées en description du procédé mettant en oeuvre ledit dispositif.

[0032] La figure 1 représente un dispositif anti-intrusion 100 selon l'invention, comportant principalement une unité de surveillance 10, un support 20, un boitier électronique 30, une base 40 contenant un dispositif d'alimentation en énergie électrique 41, une antenne 50 et un moyen de protection 60 contre les intempéries.

[0033] Selon un mode de réalisation «fixe », le dispositif anti-intrusion 100 présente une forme allongée en poteau et doit être installé au milieu de la zone à sécuriser, en étant dressé au-dessus du sol, par tout mode d'installation possible selon la nature du sol. Par exemple, dans un champ agricole, le dispositif anti-intrusion 100 peut être planté en terre, de préférence, avec son boitier électronique 30 et sa base 40 placés dans un caisson donnant accès, via des trappes par exemple, auxdits boitier et base, ledit caisson étant placé dans une excavation de dimensions adaptées.

[0034] Selon un mode de réalisation « mobile » illustré sur la figure 10, le dispositif anti-intrusion 100 est pourvu, au niveau de sa base 40, de roues 42 pour être facilement déplacé à proximité immédiate du matériel à surveiller, ainsi que de moyens de préhension 43, tels que des poignées, pour être tiré, soulevé et transporté.

[0035] L'unité de surveillance 10, positionnée au niveau du sommet du dispositif anti-intrusion 100, comporte des capteurs d'image 11, des moyens d'éclairage 12 et un haut-parleur 14. Selon l'exemple de la figure 1, l'unité de surveillance 10 présente une partie cylindrique à base circulaire surmontée d'une partie hémisphérique en forme de dôme. Cette forme de réalisation particulière de l'unité de surveillance 10 offre une compacité et une discrétion avantageuses, et permet par exemple l'intégration d'une visière panoramique à 360° derrière laquelle sont positionnés les capteurs d'image 11, d'anneaux lumineux 12 de part et d'autre de ladite visière, et de sorties haut-parleur 14 ménagées de façon périphérique dans une partie inférieure de ladite unité de surveillance. De plus, la partie hémisphérique de l'unité de surveillance 10 peut, à l'image d'un radôme, servir à abriter différents capteurs et composants, et notamment des composants de radiocommunication, et à les protéger des intempéries en l'absence du moyen de protection 60 ou en supplément de ce dernier. La partie hémisphérique peut également être raccordée à la partie cylindrique par vissage ou au moyen d'une articulation et être ainsi amovible pour permettre un accès aux composants embarqués de l'unité de surveillance 10 en vue d'une réparation ou d'une maintenance par exemple.

[0036] Les capteurs d'image 11 sont de préférence des caméras infrarouges aptes à capturer des images dans des conditions de faible éclairage, voire d'obscurité totale, et qui sont donc adaptées à un fonctionnement diurne, en permettant une prise d'image aussi bien en conditions nocturnes qu'avec un éclairage suffisant en lumière du jour par exemple. Chaque caméra infrarouge dispose éventuellement de ses propres moyens d'éclairage qui peuvent être des diodes électroluminescentes LED infrarouges.

[0037] En outre, les caméras infrarouges 11 comprennent tous les moyens nécessaires à leur fonctionnement tels que des unités de traitement et de calcul, des mémoires de stockage et des unités de traitement numérique du signal.

[0038] Selon un mode de réalisation alternatif, les capteurs d'image 11 sont des caméras multispectrales couvrant au moins un domaine spectral de l'infrarouge.

[0039] Les moyens d'éclairage 12 sont de préférence des flashs photographiques tels que des flashs électroniques à LED. En plus de produire une lumière intense pendant un laps de temps très court, les flashs photographiques 12 produisent, le cas échéant, un éclairage prolongé de la scène à la manière d'un projecteur.

[0040] Le haut-parleur 14 est agencé axialement à l'intérieur de l'unité de surveillance 10 de sorte qu'il soit orienté vers le bas de ladite unité de surveillance, sensiblement au-dessus des sorties haut-parleur.

[0041] Toutefois, l'unité de surveillance 10 peut également comporter plusieurs haut-parleurs synchronisés disposés différemment.

[0042] Le support 20 est disposé verticalement et per-

met de tenir l'unité de surveillance 10 à une certaine hauteur du sol en fonction du champ de vision et de la couverture souhaités. De préférence, le support 20 est de hauteur réglable.

[0043] Selon l'exemple de réalisation illustré, le support 20 est télescopique et comprend un tronçon fixe et au moins un tronçon coulissant de plus faible diamètre qui coulisse à l'intérieur dudit tronçon fixe comme illustré par la flèche à double sens sur la figure 1. Le verrouillage de la hauteur du support 20 peut être réalisé par tout moyen de verrouillage adapté connu de l'homme du métier.

[0044] Le support 20 assure également une jonction électrique entre l'unité de surveillance 10 et les parties inférieures du dispositif anti-intrusion 100, à savoir le boitier électronique 30 et la base 40 contenant le dispositif d'alimentation électrique 41, comme représenté sur la figure 2.

[0045] Le boitier électronique 30, en référence à la figure 2, comporte principalement une unité centrale de traitement 31, qui se présente sous forme d'un processeur ou d'un contrôleur permettant la gestion et le contrôle des différents composants électroniques du dispositif anti-intrusion 100, une mémoire informatique 32, de type mémoire vive pour l'exécution de programmes dans ladite unité centrale, et un module de communication sans-fil 33, de préférence, un module de communication sur un réseau de téléphonie mobile selon la norme GSM.

[0046] Le réseau GSM permet une couverture géographique, la plus large possible, adaptée aux territoires agricoles et aux chantiers isolés auxquels le dispositif anti-intrusion 100 est principalement destiné.

[0047] La base 40 du dispositif anti-intrusion 100 constitue un élément structural stabilisant et permet audit dispositif de résister à des perturbations et contraintes latérales en l'ancrant dans sa position verticale. À cet effet, la base 40 présente une surface élargie par rapport au reste du dispositif anti-intrusion et définit ainsi un volume intérieur suffisant pour recevoir le dispositif d'alimentation en énergie électrique 41, la taille dudit dispositif d'alimentation dépendant directement de l'autonomie qu'il procure.

[0048] La base 40 peut également contenir le boitier électronique 30 tel que représenté sur la figure 10.

[0049] Le dispositif d'alimentation en énergie électrique 41 permet de fournir l'énergie électrique nécessaire au fonctionnement de chaque équipement et composant du dispositif anti-intrusion 100, et se présente par exemple sous forme d'une batterie électrique rechargeable fixe ou amovible.

[0050] Le dispositif d'alimentation 41 comprend en outre tous les éléments et moyens nécessaires à son fonctionnement tels qu'une prise de chargement et/ou de branchement sur secteur, avec éventuellement un cordon enroulé, et un circuit intégré de gestion de l'alimentation (PMIC).

[0051] Les différents équipements et composants du dispositif anti-intrusion 100 sont reliés et branchés entre eux, selon une conception électronique et une architecture interne bien déterminées, au moyen de câbles 21 de liaison électrique dont seule la partie traversant le support 20 est représentée pour ne pas alourdir le schéma de la figure 2.

[0052] L'antenne 50 est une antenne d'émission couplée au module de communication sans-fil 33 et permet la transmission de données sur un réseau tel que le réseau GSM. L'antenne 50 peut être une antenne d'émission et de réception pour permettre, en plus de l'envoi de données, l'établissement d'une liaison téléphonique de sorte qu'un utilisateur distant puisse par exemple transmettre un message vocal en temps réel qui sera diffusé par le haut-parleur.

[0053] Selon l'exemple de réalisation illustré, l'antenne 50 est en saillie par rapport au sommet de l'unité de surveillance 10 et peut être logée à l'intérieur d'un mât tubulaire supportant le dispositif de protection 60. L'antenne 50 peut être escamotable pour être dissimulée à l'intérieur de l'unité de surveillance 10 en vue de sa protection, à condition que son émissivité et/ou sa réceptivité ne s'en trouvent pas notablement atténuées.

[0054] Le dispositif de protection 60 contre les intempéries, selon l'exemple de réalisation illustré, est un abri conique en forme de « chapeau chinois », pour une meilleure évacuation des gouttes de pluie et une gêne minimale des caméras infrarouges 11, et comporte préférablement une toile rigide opaque ou transparente fabriquée dans un matériau résistant aux effets de la pluie et du soleil, tel qu'un polychlorure de vinyle (PVC), et pouvant éventuellement être traité au Teflon pour faciliter l'écoulement des gouttes de pluie.

[0055] Au vu de son exposition prolongée à la lumière du soleil, le dispositif de protection 60 peut être équipé de cellules photovoltaïques permettant d'emmagasiner une quantité d'énergie dans une batterie électrique auxiliaire ou de recharger la batterie électrique 41 principale du dispositif anti-intrusion 100.

[0056] Selon le mode de réalisation décrit, les caméras infrarouges 11 constituent l'organe de détection primordial du dispositif anti-intrusion 100 et doivent observer constamment la scène pour détecter une présence humaine comme il sera décrit plus loin dans la description.

[0057] Néanmoins, l'unité de surveillance 10 peut être équipée de détecteurs de mouvement 13, à raison d'un détecteur de mouvement par caméra infrarouge pointant vers la même direction que ladite caméra, déterminant le moment propice au déclenchement de la prise de vue par la caméra infrarouge. En effet, chaque caméra infrarouge peut être mise en veille et ne s'activer que lorsque le détecteur de mouvement qui lui est associé détecte un mouvement. Ainsi, l'autonomie de la batterie du dispositif anti-intrusion est prolongée en raison de la consommation énergétique des détecteurs de mouvement considérablement inférieure à celle des caméras infrarouges.

[0058] Préférablement, les caméras infrarouges 11 et les détecteurs de mouvement 13, lorsqu'ils sont réunis,

fonctionnent simultanément pour une détection plus fiable et plus robuste.

[0059] La figure 3 illustre un agencement possible d'une caméra infrarouge 11, d'un flash 12 et d'un détecteur de mouvement 13, formant un ensemble autonome de détection de présence et de capture d'images. Pour une couverture panoramique à 360°, un tel ensemble pris seul ne saurait suffire et l'unité de surveillance doit disposer d'au moins trois ensembles similaires en raison du champ de vision des caméras infrarouges limité angulairement.

[0060] La figure 4 schématise un exemple de disposition permettant une couverture à 360°. Seules les caméras infrarouges 11 sont représentées pour une meilleure lisibilité de la figure, mais il faut comprendre qu'un ensemble tel que celui de la figure 3 est prévu à l'emplacement de chaque caméra infrarouge 11.

[0061] Les caméras 11 peuvent être caractérisées par leur angle de champ a, celui-ci permet de déterminer le nombre de caméras nécessaires pour établir un champ de vision à 360°. Pour obtenir un tel champ de vision, il faut au moins trois caméras disposées en triangle équilatéral de sorte que leurs axes forment un angle de 120° deux à deux. Cette disposition laisse subsister une zone morte DZ, en pointillés sur la figure 4, qui peut être confinée ou non dans le volume intérieur de l'unité de surveillance 10 suivant le diamètre de ladite unité de surveillance et la distance mutuelle entre les caméras.

[0062] Par exemple, l'unité de surveillance 10, dont le contour est en trait continu, présente un diamètre suffisant pour que la zone morte reste totalement confinée à l'intérieur. Par contre, l'unité de surveillance 10', dont le contour est en trait interrompu, ne permet pas un confinement de la zone morte, ladite zone morte dépassant sur des zones extérieures DZ_e qui peuvent s'avérer problématiques si leur étendue est importante.

[0063] La figure 5 illustre un scénario de mise en oeuvre du dispositif anti-intrusion 100 dans le cadre d'un procédé de sécurisation selon l'invention.

[0064] Le dispositif anti-intrusion 100 est par exemple installé au milieu d'un terrain agricole pour protéger un matériel se trouvant à proximité. Un intrus pénètre dans le champ de vision d'une des caméras infrarouges 11 du dispositif anti-intrusion, ledit intrus voulant par exemple dérober ou saboter un matériel et disposant éventuellement d'outils suspects et/ou d'armes. La détection d'une présence humaine étant confirmée par la caméra infrarouge 11, un flash en lumière visible est allumé et la caméra prend des photos de la scène en mode rafale. En parallèle, le haut-parleur 14 diffuse un message vocal d'avertissement pour intimider et dissuader l'intrus. Ces photos sont ensuite envoyées sur un serveur 300 sécurisé via un réseau GSM, avec un service de messagerie multimédia (MMS) par exemple. Le serveur 300 est sécurisé par une blockchain pour assurer un stockage d'information immuable et irréversible et pour permettre éventuellement de générer des certificats horodatés pour attester de l'authenticité des photos prises à une date donnée. Le serveur 300 est connecté à un calculateur 400 et lui transmet les photos de l'intrusion enregistrée. Le calculateur 400 effectue alors une analyse et un traitement desdites photos au moyen d'une intelligence artificielle avant d'envoyer une alerte, accompagnée ou non de photos, au propriétaire ou à la personne responsable de la sécurité du terrain agricole franchi, que ce soit sur un terminal mobile 501, de type smartphone, sur un poste fixe 502 ou par le biais d'un téléconseiller 503 au sein d'un centre de sécurité mandaté par le propriétaire du terrain.

[0065] De façon générale, le procédé de sécurisation, tel que représenté sur la figure 6, se décompose principalement en :

- une étape 110 de détection d'une présence humaine par une caméra 11 du dispositif anti-intrusion 100 ;
- une étape 120 d'allumage du flash 12 ;
- une étape 130 de prise de photos de la scène en mode rafale ;
- une étape 140 de diffusion d'un message vocal d'avertissement par le haut-parleur 14 ;
- une étape 150 d'envoi des photos prises au serveur sécurisé 300 ;
- une étape 310 de stockage et de transmission des photos au calculateur 400 ;
- une étape 410 de traitement et d'analyse des photos par des algorithmes d'intelligence artificielle exécutés par ledit calculateur ;
- une étape 420 d'envoi d'une alerte en temps réel à un utilisateur du dispositif anti-intrusion 100.

[0066] L'étape 110 de détection d'une présence humaine permet au dispositif anti-intrusion d'éviter les fausses alertes et de ne s'enclencher que lorsqu'un humain est détecté, et comprend dans l'ordre les sous-étapes suivantes, schématisées sur la figure 7 :

- une observation permanente de la scène par les caméras et/ou une surveillance permanente du périmètre par les détecteurs de mouvement ;
- une détection d'anomalie par une caméra et/ou un détecteur de mouvement, ladite anomalie pouvant être un gradient thermique, qui correspond à une augmentation du rayonnement reçu par la caméra due à la présence d'un objet dont la température est supérieure à l'environnement par exemple, ou un mouvement d'un objet mobile pénétrant dans le périmètre de sécurité ;
- une vision infrarouge active permettant de capter une image thermique brute de la scène ;
- une segmentation de l'avant-plan pour isoler l'objet en mouvement et/ou dont la température induit un gradient thermique local dans l'image brute ;
- une reconnaissance d'un corps humain par un calcul de puissance rayonnée, obtenue par intégration de la densité de flux radiatif.

[0067] La segmentation de l'avant-plan est un traitement avantageux qui permet de simplifier au maximum l'image brute, sans altérer ses informations, pour ne laisser aux étapes suivantes que quelques régions d'intérêt (régions de l'image où il y a une forte probabilité de présence d'un corps humain). Différents algorithmes de segmentation de l'avant-plan, connus de l'homme du métier, peuvent être implémentés dans les caméras infrarouges.

[0068] Le calcul de la puissance rayonnée $\Phi°(T)$ du corps isolé par la segmentation de l'avant-plan permet de savoir si ledit corps correspond à un corps humain ou non. En effet, la segmentation de l'avant-plan peut parfaitement se déclencher en présence d'un corps animal, car seuls un gradient thermique et un mouvement conditionnent cette étape. Ainsi, les détections d'animaux sont écartées par un test sur la puissance rayonnée mesurée.

[0069] Dans le cas où un animal présente une puissance rayonnée proche de celle d'un humain, le procédé se poursuit et les photos de la scène arrivent au calculateur 400. Cependant, les algorithmes d'intelligence artificielle permettent de reconnaitre l'animal, ou de constater une absence d'humain sur les photos, et aucune alerte n'est envoyée.

[0070] La reconnaissance d'un corps humain est à priori suffisante pour prévenir un vol ou un sabotage du matériel sécurisé. Car un malfaiteur qui, par exemple, s'introduirait avec un véhicule est obligé de descendre de son véhicule pour accomplir son acte. Toutefois, pour une meilleure sécurité, l'étape de reconnaissance peut être généralisée à la reconnaissance de véhicules grâce à des classificateurs normés spécifiques de l'intelligence artificielle.

[0071] Lorsque la reconnaissance d'un corps humain et/ou d'un véhicule est confirmée, la caméra procède à la prise de photos de la scène.

[0072] L'étape 120 d'allumage du flash permet, outre l'éclairage de la scène pour la prise de photos, de déstabiliser l'intrus avec un effet de surprise qui peut s'avérer dissuasif, l'intrus prenant conscience qu'il va être photographié et/ou repéré.

[0073] L'étape 130 de prise de photos s'accompagne d'une mise au point et d'un réglage optiques automatiques effectués par la caméra, qui présente à cet effet une grande profondeur de champ, et nécessaires à l'amélioration de la qualité des photos.

[0074] L'étape 140 permet la diffusion en boucle d'un message vocal préenregistré dans une mémoire intégrée du haut-parleur par exemple, et contenant un avertissement, une mise en garde et/ou une sommation du type « Vous avez été identifié, vous êtes illégalement entré sur une propriété privée, vous êtes priés de quitter immédiatement les lieux ... ».

[0075] Les photos prises sont ensuite envoyées lors de l'étape 150 au serveur 300, sécurisé par une blockchain, où elles sont stockées accompagnées, le cas échéant, d'un certificat horodaté.

[0076] Le serveur sécurisé 300 transmet à son tour les photos au calculateur 400, qui peut être un ordinateur, qui se charge d'effectuer une analyse et un traitement desdites photos par des algorithmes d'intelligence artificielle.

[0077] Une analyse initiale peut par exemple consister en un tri des photos selon leurs nettetés et plus particulièrement selon la netteté de l'intrus sur les photos.

[0078] La figure 8 donne un schéma simplifié d'une telle analyse, dans lequel parmi une photo 001 entièrement nette, une photo 002 entièrement floue, une photo 003 dont l'arrière-plan est net et l'avant-plan est flou, et une photo 004 dont l'arrière-plan est flou et l'avant-plan est net, seules les photos 001 et 004 sont retenue car représentent une image nette de l'intrus pouvant être exploitée pour identifier ledit intrus ou répertorier son visage et/ou sa physionomie.

[0079] Le traitement et l'analyse basés sur une intelligence artificielle et effectués par le calculateur 400 lors de l'étape 410 comprennent par exemple :

Une analyse automatique des formes sur les photos pour caractériser la menace réelle. Par exemple, les formes d'un bras levé en haut et d'un corps qui se baisse de façon répétée sur les photos peuvent correspondre à une action de destruction d'un verrou par des coups de hache ;

Une recherche automatique de situations, potentiellement critiques ou dangereuses, au moyen de classificateurs normés spécifiques tels que la présence d'arme, de cagoule, de bidons etc. ;

Une détection automatique d'éléments informatifs tels que des inscriptions alphanumériques (plaque minéralogique ou autre) ou des signes distinctifs divers sur les vêtements ou le véhicule grâce à des classificateurs normés spécifiques de l'intelligence artificielle ;

Une détermination de similitudes par un calcul des occurrences géographiques et une interrogation d'anciens cas d'intrusions, cette opération peut être effectuée à l'ouverture d'une enquête judiciaire par exemple.

[0080] Selon un mode de réalisation préféré, représenté sur la figure 9, le procédé de sécurisation comprend les étapes suivantes :

- une étape 105 d'observation de la scène ;
- une étape 106 de détection d'un gradient thermique et/ou une étape 107 de détection d'un mouvement ;
- une étape 108 de segmentation de l'avant-plan ;
- une étape 109 de reconnaissance d'un corps humain par un calcul de puissance rayonnée ;
- une étape 120 d'allumage du flash ;
- une étape 130 de prise de photos en mode rafale, en parallèle d'une étape 140 de diffusion d'un message vocal en boucle ;
- une étape 150 d'envoi des photos sur le serveur 300 sécurisé par une blockchain ;

- une étape 308 d'horodatage des photos reçues ;
- une étape 309 de stockage des photos et de certificats d'horodatage sur le serveur 300 ;
- une étape 310 de transmission de données au calculateur 400 ;
- une étape 410 d'exécution d'algorithmes d'intelligence artificielle ;
- une étape optionnelle 415 de demande de photos supplémentaires ;
- une étape 420 d'envoi d'une alerte avec les informations nécessaires.

[0081] Cette dernière étape d'envoi d'une alerte consiste par exemple à avertir un utilisateur par le biais d'un appareil mobile tel qu'une tablette ou un smartphone en lui communiquant les éléments essentiels de l'intrusion détectée. La figure 11 illustre par exemple un exemple de photos pouvant être transmises à la personne concernée afin de lui permettre de prendre la décision adéquate.

[0082] Ainsi, le dispositif anti-intrusion 100 permet de repérer des activités anormales ou suspectes sur le terrain surveillé, et d'avoir une connaissance sur les tentatives d'intrusions réussies comme échouées.

[0083] Pour ne pas être détecté par son propre dispositif anti-intrusion, l'utilisateur doit pouvoir désactiver ledit dispositif avant la pénétration sur le terrain surveillé ou le désamorcer en cas de besoin. Le dispositif anti-intrusion peut par exemple être désactivé à distance par une application dédiée installée sur le téléphone mobile de l'utilisateur, ou programmé pour effectuer une reconnaissance faciale de l'utilisateur qui se présente devant une caméra du dispositif.

[0084] Ainsi, le dispositif anti-intrusion 100 permet de repérer des activités anormales ou suspectes sur le terrain surveillé, et d'avoir une connaissance sur les tentatives d'intrusions réussies comme échouées.

Revendications

1. Dispositif de détection d'intrusion (100), pour sécuriser une zone déterminée, comportant une unité de surveillance (10), comprenant au moins un capteur d'image (11) et un moyen d'éclairage (12), un support (20), un boitier électronique (30), comportant un module de communication sans-fil (33), un dispositif d'alimentation électrique (41), et une antenne (50), **caractérisé en ce que** ledit au moins un capteur d'image est une caméra infrarouge pourvue de moyens de détection de présence commandant ses prises d'images, et **en ce que** le module de communication sans-fil est apte à communiquer sur un réseau de téléphonie mobile.

2. Dispositif de détection d'intrusion selon la revendication 1, **caractérisé en ce qu'**il comporte trois caméras infrarouges (11) disposées en triangle équilatéral de sorte que leurs axes forment deux à deux un angle de 120°, et **en ce que** le moyen d'éclairage (12) comprend un flash photographique pour chaque caméra infrarouge.

3. Dispositif de détection d'intrusion selon la revendication 1 ou la revendication 2, dans lequel le moyen d'éclairage (12) comprend un flash photographique à base de diodes électroluminescentes.

4. Dispositif de détection d'intrusion selon l'une quelconque des revendications précédentes, dans lequel le boitier électronique (30) comprend une unité centrale de traitement (31) et une mémoire informatique (32).

5. Dispositif de détection d'intrusion selon l'une quelconque des revendications précédentes, dans lequel le module de communication sans-fil (33) est un module GSM.

6. Dispositif de détection d'intrusion selon l'une quelconque des revendications précédentes, dans lequel le dispositif d'alimentation électrique (41) est une batterie électrique rechargeable fixe ou amovible, ladite batterie étant placée à l'intérieur d'une base (40) dudit dispositif de détection d'intrusion.

7. Dispositif de détection d'intrusion selon l'une quelconque des revendications précédentes, dans lequel l'unité de surveillance (10) comprend en outre au moins un détecteur de mouvement (13).

8. Dispositif de détection d'intrusion selon l'une quelconque des revendications précédentes, comportant en outre un haut-parleur (14) pour diffuser un message vocal préenregistré.

9. Dispositif de détection d'intrusion selon l'une quelconque des revendications précédentes, **caractérisé en ce qu'**il comporte des organes de déplacement (42), comme des roues ou des roulettes permettant le déplacement dudit dispositif, et des moyens de préhension (43) facilitant le transport dudit dispositif.

10. Procédé de sécurisation d'une zone déterminée **caractérisé en ce qu'**il met en oeuvre un dispositif de détection d'intrusion (100) selon l'une des revendications précédentes, et **en ce qu'**il comprend :

    - une étape (110) de détection d'une présence humaine dans ladite zone par l'unité de surveillance (10) ;
    - une étape (130) de prise de photos de la scène par l'unité de surveillance (10) ;
    - une étape (150) d'envoi des photos prises à un serveur (300) sécurisé par une chaîne de

blocs (blockchain) via un réseau de téléphonie mobile ;
- une étape (310) de transmission des photos reçues à un calculateur (400) ;
- une étape (410) de traitement et d'analyse des photos transmises par des algorithmes d'intelligence artificielle implémentés sur le calculateur ; et
- une étape (420) d'envoi d'une alerte à un utilisateur.

11. Procédé de sécurisation selon la revendication 10, dans lequel l'étape (410) de traitement et d'analyse des photos par intelligence artificielle comprend une opération ou une combinaison d'opérations parmi :

- une analyse automatique de formes dans les photos, pour une prédiction des menaces ;
- une recherche automatique de situations à partir de classificateurs normés spécifiques ; et
- une détection automatique d'éléments informatifs sur les photos.

12. Procédé de sécurisation selon la revendication 11, dans lequel les opérations de l'étape (410) de traitement et d'analyse des photos par intelligence artificielle sont basées sur des classificateurs normés spécifiques.

13. Procédé de sécurisation selon la revendication 10 ou la revendication 11, dans lequel l'étape (110) de détection d'une présence humaine comprend une sous-étape de mesure par une caméra infrarouge (11) d'une puissance rayonnée par un objet capté et de comparaison de la puissance rayonnée mesurée avec des valeurs connues représentatives de la puissance rayonnée par un corps humain.

14. Procédé de sécurisation selon l'une quelconque des revendications 10 à 12, comprenant en outre une étape (308) d'horodatage par le serveur (300) des photos reçues et une étape (309) de stockage desdites photos, chacune étant associée à un certificat d'horodatage.

15. Système de détection d'intrusion pour la sécurisation d'une zone déterminée selon le procédé d'une des revendications 10 à 13, **caractérisé en ce qu'**il comporte un dispositif de détection d'intrusion (100) selon l'une des revendications 1 à 9, un serveur (300) sécurisé par une blockchain et un calculateur (400) implémentant au moins un algorithme d'intelligence artificielle.

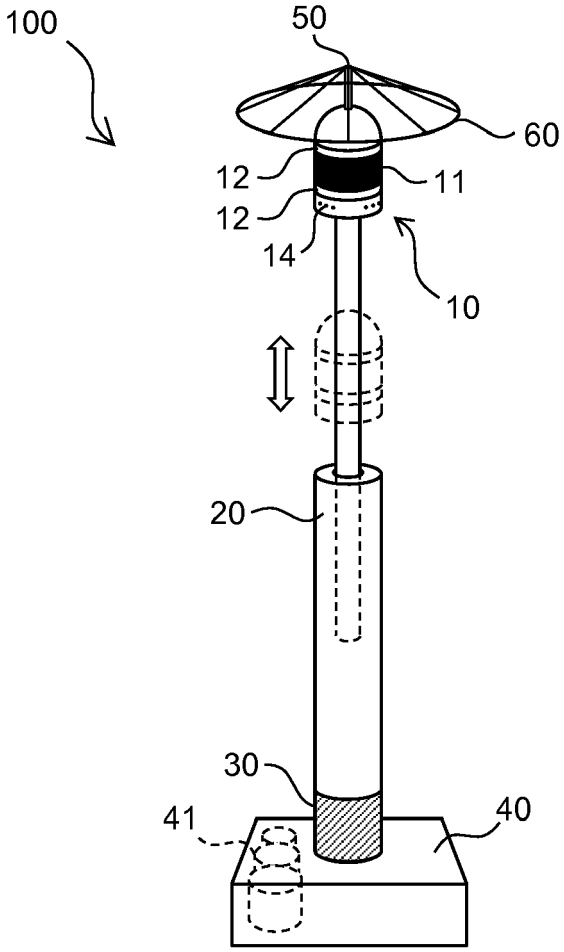


Fig. 1

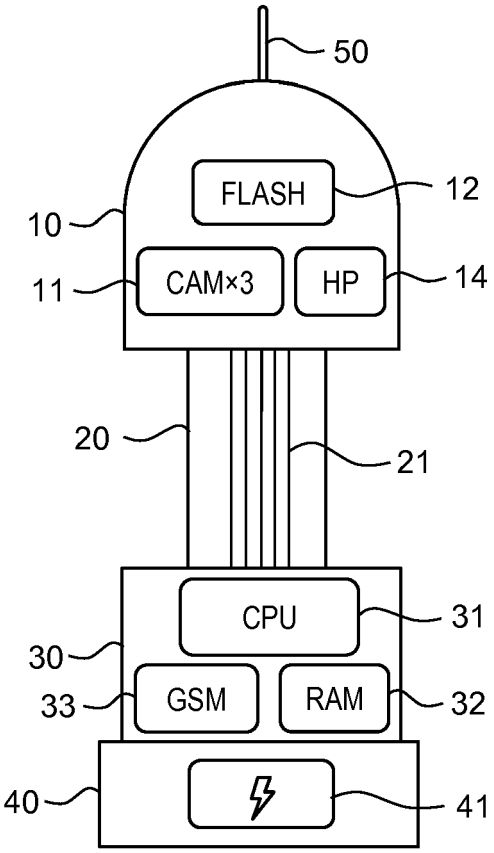


Fig. 2

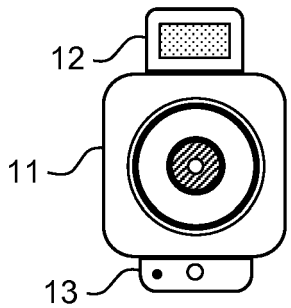


Fig. 3

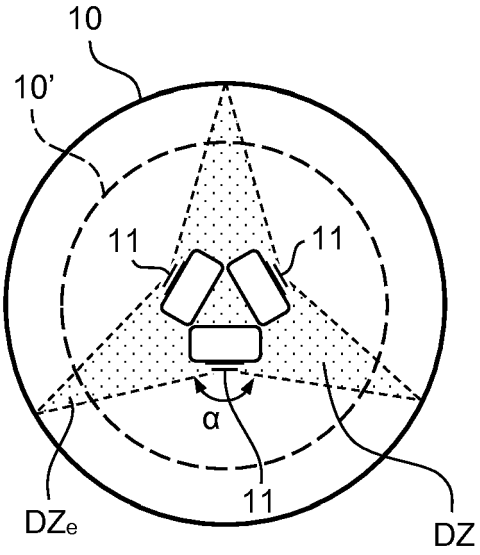


Fig. 4

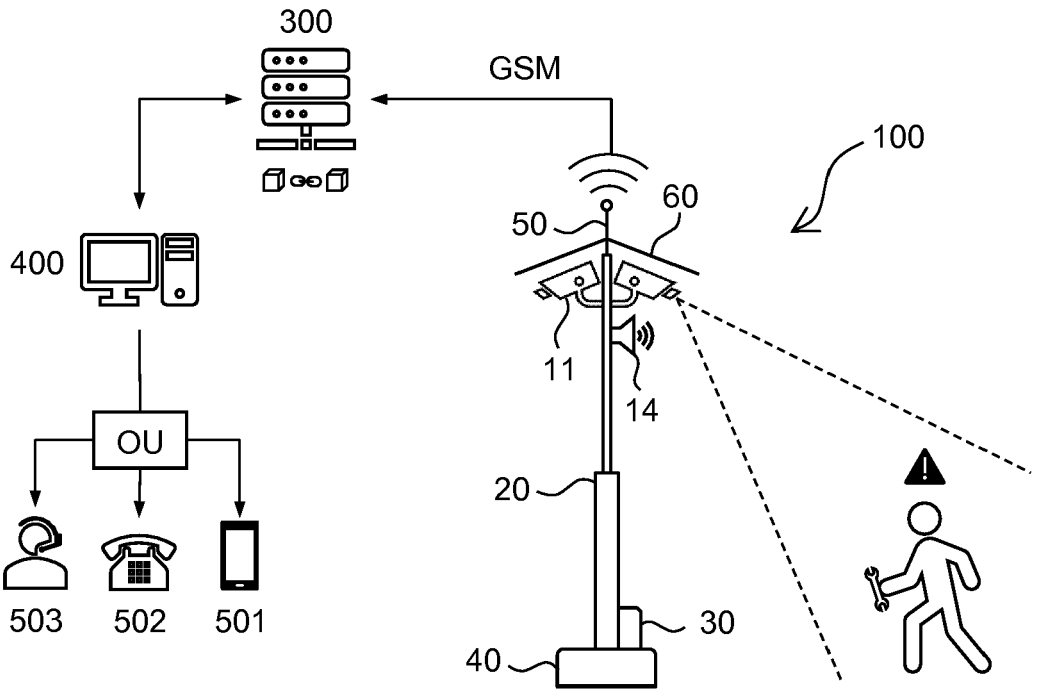

300
GSM
100
60
50
400
11
14
OU
20
503
502
501
30
40

Fig. 5

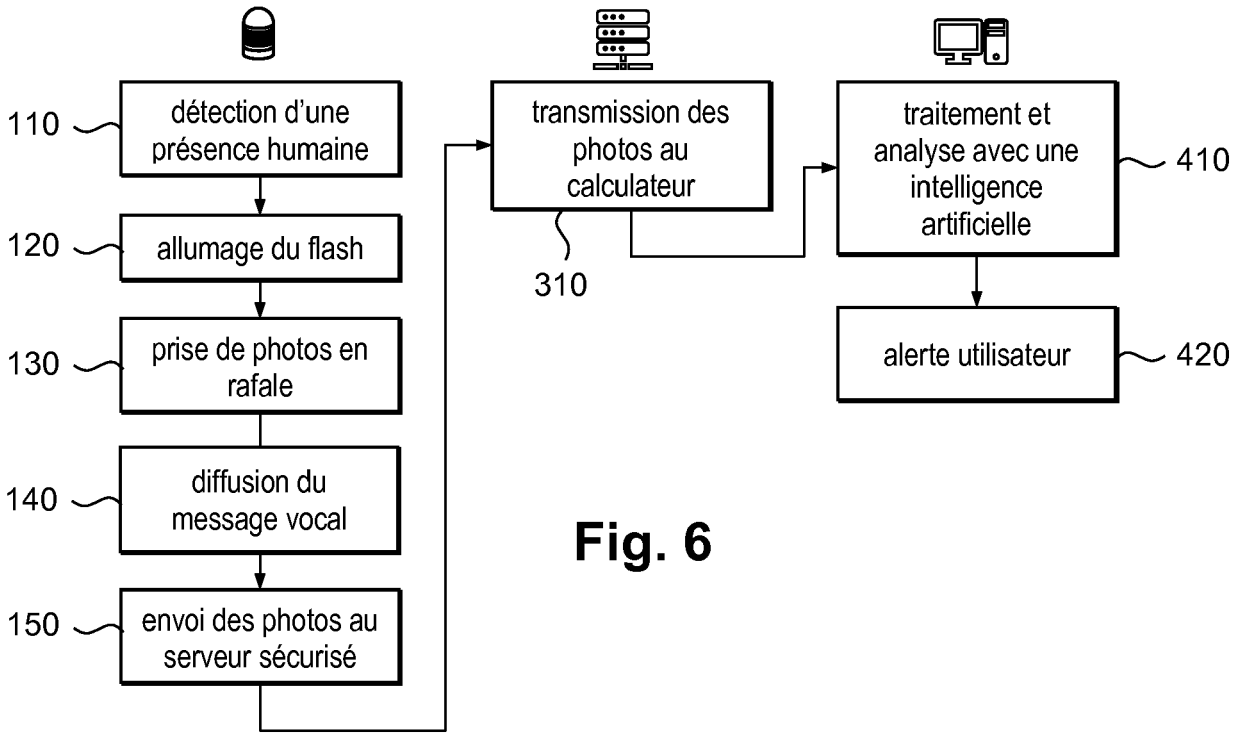

110
détection d'une présence humaine
120
allumage du flash
130
prise de photos en rafale
140
diffusion du message vocal
150
envoi des photos au serveur sécurisé
transmission des photos au calculateur
310
traitement et analyse avec une intelligence artificielle
410
alerte utilisateur
420

Fig. 6

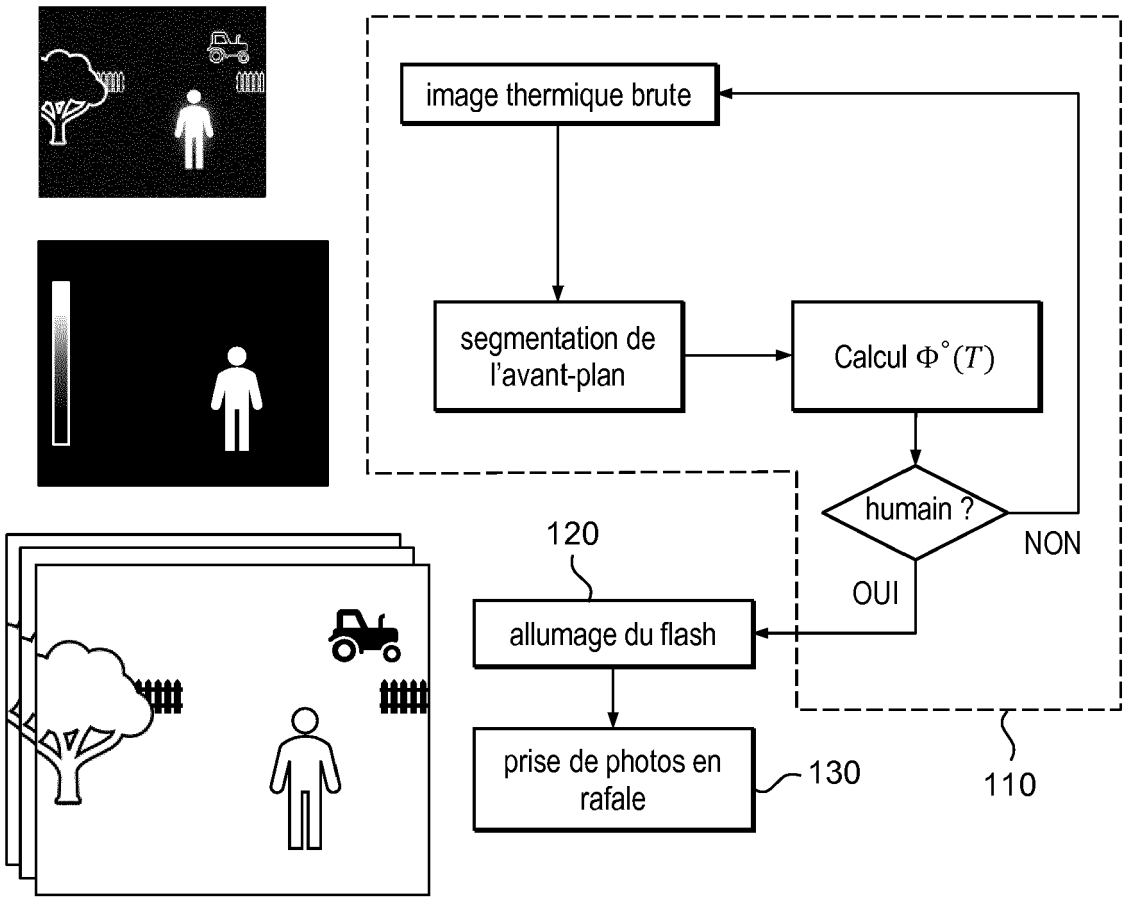


image thermique brute
segmentation de l'avant-plan
Calcul $\Phi^{\circ}(T)$
humain ?
NON
OUI
120
allumage du flash
prise de photos en rafale
130
110

Fig. 7

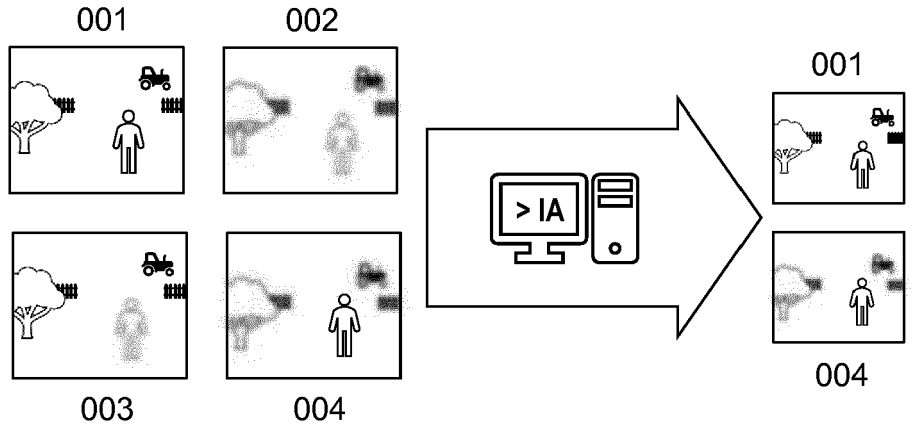

001
002
003
004
> IA
001
004

Fig. 8

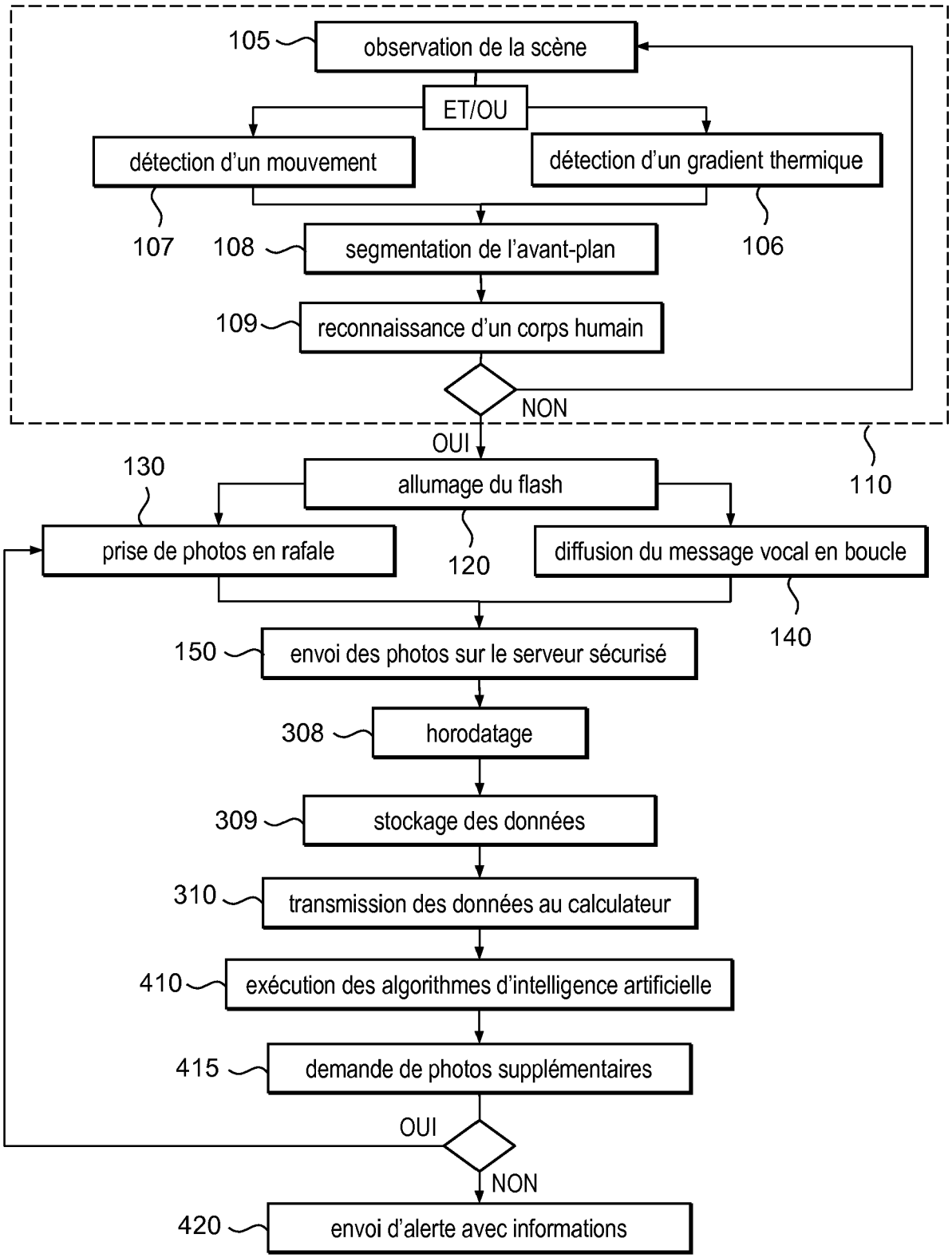
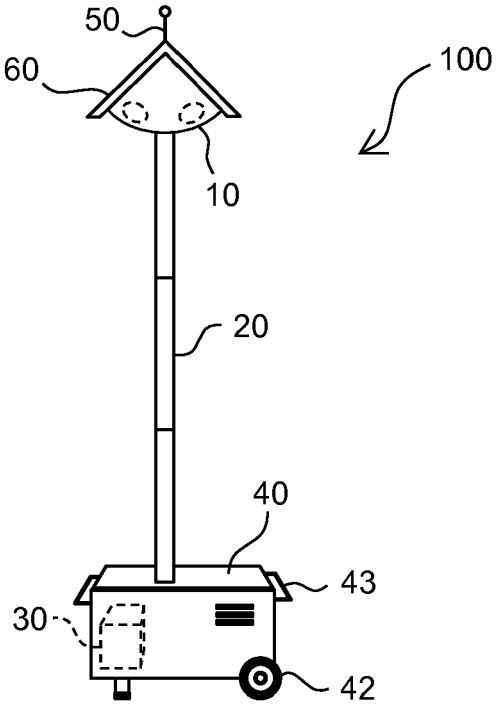

105
observation de la scène
ET/OU
détection d'un mouvement
détection d'un gradient thermique
107
108
segmentation de l'avant-plan
106
109
reconnaissance d'un corps humain
NON
OUI
110
130
allumage du flash
prise de photos en rafale
120
diffusion du message vocal en boucle
140
150
envoi des photos sur le serveur sécurisé
308
horodatage
309
stockage des données
310
transmission des données au calculateur
410
exécution des algorithmes d'intelligence artificielle
415
demande de photos supplémentaires
OUI
NON
420
envoi d'alerte avec informations

Fig. 9

Fig. 10


50
60
100
10
20
40
43
30
42

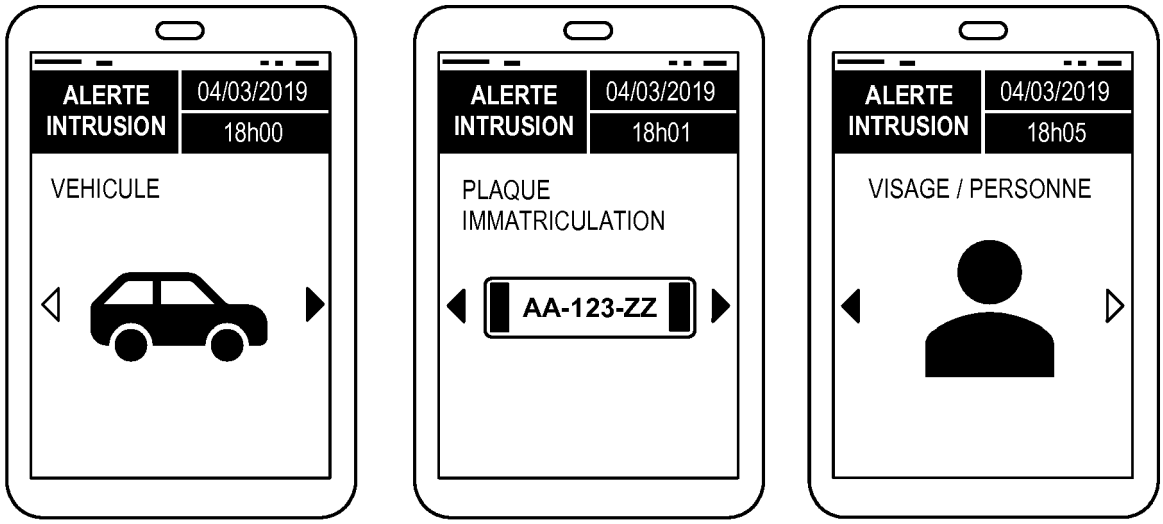

ALERTE INTRUSION
04/03/2019
18h00
VEHICULE
ALERTE INTRUSION
04/03/2019
18h01
PLAQUE IMMATRICULATION
AA-123-ZZ
ALERTE INTRUSION
04/03/2019
18h05
VISAGE / PERSONNE

Fig. 11

Europäisches Patentamt
European Patent Office
Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande
EP 19 30 5379

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (IPC)
X Y	US 2018/151039 A1 (LEMBERGER ELLIOTT [US] ET AL) 31 mai 2018 (2018-05-31) * alinéas [0072] - [0073] * * alinéas [0085] - [0086] * * alinéa [0088] * * alinéa [0092] * * alinéa [0094] * * alinéa [0097] * * alinéa [0099] * * alinéa [0116] * * alinéa [0120] * * alinéas [0122] - [0125] * * alinéa [0128] * * alinéa [0130] * * alinéa [0132] * * figures 4,10-12 * -----	1,3-5,7,8 2,6,9-15	INV. G08B13/196
Y	JP 2018 182399 A (CROSS KK) 15 novembre 2018 (2018-11-15) * alinéas [0007] - [0008] * * alinéas [0012] - [0013] * * alinéa [0041] * * figure 1a * -----	2,6,9	DOMAINES TECHNIQUES RECHERCHES (IPC) G08B
Y	US 2018/069838 A1 (LEE DAVID D [US] ET AL) 8 mars 2018 (2018-03-08) * alinéa [0028] * * alinéa [0046] * * alinéa [0053] * * alinéa [0055] * * alinéas [0057], [0058] * * alinéa [0059] * * alinéa [0062] * * alinéas [0066], [0067] * * alinéa [0068] * * figures 2d,4 * ----- -/--	10-15	

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
Munich	12 décembre 2019	Meister, Mark

CATEGORIE DES DOCUMENTS CITES

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 antérieur, mais publié à la date de dépôt ou après cette date
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C02)

Europäisches Patentamt
European Patent Office
Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande
EP 19 30 5379

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (IPC)
Y	KR 101 750 676 B1 (JUNG KYUNG HEE [KR]) 26 juin 2017 (2017-06-26) * alinéas [0024] - [0026] * * alinéa [0038] * * alinéas [0044] - [0046] * * alinéa [0048] * * alinéa [0078] * * figure 1 * -----	10,15	
Y	EP 3 142 355 A1 (AXIS AB [SE]) 15 mars 2017 (2017-03-15) * alinéa [0038] * * alinéa [0044] * * alinéas [0045] - [0047] * * alinéa [0050] * * alinéa [0055] * * alinéa [0060] * * figures 2,3 * -----	13	
			DOMAINES TECHNIQUES RECHERCHES (IPC)

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
Munich	12 décembre 2019	Meister, Mark

CATEGORIE DES DOCUMENTS CITES

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 antérieur, mais publié à la date de dépôt ou après cette date
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C02)

Europäisches Patentamt
European Patent Office
Office européen des brevets

Numéro de la demande

EP 19 30 5379

REVENDICATIONS DONNANT LIEU AU PAIEMENT DE TAXES

La présente demande de brevet européen comportait lors de son dépôt les revendications dont le paiement était dû.

☐ Une partie seulement des taxes de revendication ayant été acquittée dans les délais prescrits, le présent rapport de recherche européenne a été établi pour les revendications pour lesquelles aucun paiement n'était dû ainsi que pour celles dont les taxes de revendication ont été acquittées, à savoir les revendication(s):

☐ Aucune taxe de revendication n'ayant été acquittée dans les délais prescrits, le présent rapport de recherche européenne a été établi pour les revendications pour lesquelles aucun paiement n'était dû.

ABSENCE D'UNITE D'INVENTION

La division de la recherche estime que la présente demande de brevet européen ne satisfait pas à l'exigence relative à l'unité d'invention et concerne plusieurs inventions ou pluralités d'inventions, à savoir:

voir feuille supplémentaire B

☒ Toutes les nouvelles taxes de recherche ayant été acquittées dans les délais impartis, le présent rapport de recherche européenne a été établi pour toutes les revendications.

☐ Comme toutes les recherches portant sur les revendications qui s'y prêtaient ont pu être effectuées sans effort particulier justifiant une taxe additionnelle, la division de la recherche n'a sollicité le paiement d'aucune taxe de cette nature.

☐ Une partie seulement des nouvelles taxes de recherche ayant été acquittée dans les délais impartis, le présent rapport de recherche européenne a été établi pour les parties qui se rapportent aux inventions pour lesquelles les taxes de recherche ont été acquittées, à savoir les revendications:

☐ Aucune nouvelle taxe de recherche n'ayant été acquittée dans les délais impartis, le présent rapport de recherche européenne a été établi pour les parties de la demande de brevet européen qui se rapportent à l'invention mentionnée en premier lieu dans les revendications, à savoir les revendications:

☐ Le present rapport supplémentaire de recherche européenne a été établi pour les parties de la demande de brevet européen qui se rapportent a l'invention mentionée en premier lieu dans le revendications (Règle 164 (1) CBE)

Europäisches Patentamt
European Patent Office
Office européen des brevets

ABSENCE D'UNITÉ D'INVENTION
FEUILLE SUPPLÉMENTAIRE B

Numéro de la demande
EP 19 30 5379

La division de la recherche estime que la présente demande de brevet européen ne satisfait pas à l'exigence relative à l'unité d'invention et concerne plusieurs inventions ou pluralités d'inventions, à savoir :

1. revendications: 1-9

Dispositif de détection d'intrusion, pour sécuriser une zone déterminée, comportant une unité de surveillance, comprenant au moins un capteur d'image et un moyen d'éclairage, un support, un boîtier électronique, comportant un module de communication sans-fil, un dispositif d'alimentation électrique, et une antenne, ledit au moins un capteur d'image étant une caméra infrarouge pourvue de moyens de détection de présence commandant ses prises d'images, le module de communication sans-fil étant apte à communiquer sur un réseau de téléphonie mobile, le capteur d'image comportant trois caméras infrarouges disposées en triangle équilatéral de sorte que leurs axes forment deux à deux un angle de 120°, le moyen d'éclairage comprenant un flash photographique pour chaque caméra infrarouge.

---

2. revendications: 10-15

Système de détection d'intrusion, pour sécuriser une zone déterminée, comportant une unité de surveillance, comprenant au moins un capteur d'image et un moyen d'éclairage, un support, un boîtier électronique, comportant un module de communication sans-fil, un dispositif d'alimentation électrique, et une antenne, ledit au moins un capteur d'image étant une caméra infrarouge pourvue de moyens de détection de présence commandant ses prises d'images, le module de communication sans-fil étant apte à communiquer sur un réseau de téléphonie mobile, et serveur sécurisé par une blockchain et un calculateur implémentant au moins un algorithme d'intelligence artificielle, et procédé pour la sécurisation d'une zone déterminée, le procédé mettant en oeuvre ledit système de détection d'intrusion.

EPO FORM P0402

ANNEXE AU RAPPORT DE RECHERCHE EUROPEENNE RELATIF A LA DEMANDE DE BREVET EUROPEEN NO. EP 19 30 5379

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche européenne visé ci-dessus.
Lesdits members sont contenus au fichier informatique de l'Office européen des brevets à la date du
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets.

12-12-2019

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2018151039 A1	31-05-2018	US 2018151039 A1	31-05-2018
		WO 2018098448 A1	31-05-2018
JP 2018182399 A	15-11-2018	AUCUN	
US 2018069838 A1	08-03-2018	US 2018069838 A1	08-03-2018
		WO 2018044676 A1	08-03-2018
KR 101750676 B1	26-06-2017	AUCUN	
EP 3142355 A1	15-03-2017	CN 106504197 A	15-03-2017
		EP 3142355 A1	15-03-2017
		JP 6602731 B2	06-11-2019
		JP 2017096915 A	01-06-2017
		KR 20170030049 A	16-03-2017
		TW 201737204 A	16-10-2017
		US 2017069069 A1	09-03-2017

EPO FORM P0460

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No.12/82

RÉFÉRENCES CITÉES DANS LA DESCRIPTION

Cette liste de références citées par le demandeur vise uniquement à aider le lecteur et ne fait pas partie du document de brevet européen. Même si le plus grand soin a été accordé à sa conception, des erreurs ou des omissions ne peuvent être exclues et l'OEB décline toute responsabilité à cet égard.

Documents brevets cités dans la description

- US 20170116836 A1 **[0007]**