



(11) **EP 4 421 761 A1**

(12) **DEMANDE DE BREVET EUROPEEN**

(43) Date de publication:
28.08.2024 Bulletin 2024/35

(51) Classification Internationale des Brevets (IPC):
G07C 9/37 (2020.01)

(21) Numéro de dépôt: **24157491.2**

(52) Classification Coopérative des Brevets (CPC):
G07C 9/37; G07C 9/10

(22) Date de dépôt: **14.02.2024**

(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 ME MK MT NL NO PL PT RO RS SE SI SK SM TR
Etats d'extension désignés:
BA
Etats de validation désignés:
GE KH MA MD TN

(72) Inventeurs:
• **DESPIEGEL, Vincent**
92400 COURBEVOIE (FR)
• **BAUDRY, Christelle**
92400 COURBEVOIE (FR)
• **GENTRIC, Stéphane**
92400 COURBEVOIE (FR)
• **MORISSON, Nicolas**
92400 COURBEVOIE (FR)

(30) Priorité: **27.02.2023 FR 2301776**

(71) Demandeur: **IDEMIA Identity & Security France**
92400 Courbevoie (FR)

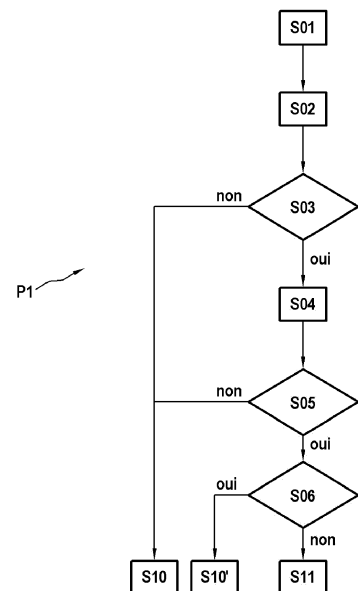
(74) Mandataire: **Idemia**
2, place Samuel de Champlain
92400 Courbevoie (FR)

(54) **PROCÉDÉ DE SÉCURISATION D'UN ACCÈS À UNE ZONE CIBLE PAR DES PERSONNES AVEC DÉTERMINATION DE LA DIFFICULTÉ À OBTENIR UNE INFORMATION BIOMÉTRIQUE**

(57) Procédé de sécurisation d'un accès à une zone cible (ZC) par des personnes, dans lequel, pour une personne :

- dans une première zone (Z1) située en amont de la zone cible, on met en oeuvre un suivi (S01) de la personne lorsqu'elle circule dans la première zone dans la direction de la zone cible, au moyen d'une caméra (400) qui observe au moins une portion de la première zone,
- on obtient (S02) une information biométrique de la personne suivie pour vérifier (S03) si cette personne correspond à une personne préenregistrée,
- on détermine (S04) un indicateur de sécurité indiquant un niveau de difficulté à obtenir une information biométrique pour la personne suivie et l'on vérifie (S05) si une condition de sécurité est vérifiée à partir de l'indicateur,
- on génère (S10) un signal d'alerte.

[Fig. 1]



EP 4 421 761 A1

Description

Domaine Technique

[0001] L'invention se rapporte au domaine de la sécurisation de l'accès à une zone cible vers laquelle des personnes circulent. L'invention trouve application dans la sécurisation de l'accès à un avion, un train, un bateau, ou encore un bâtiment.

Technique antérieure

[0002] L'accès à des zones présentant un certain niveau de sécurité peut être limité à uniquement des personnes qui sont autorisées à y pénétrer. Par exemple, lors de l'embarquement dans un avion, on réalise en général une vérification (par un opérateur) de l'identité des personnes et de leur titre de transport avant de permettre aux personnes d'avancer vers un accès à un avion (typiquement une passerelle aéroportuaire).

[0003] Le développement des solutions basées sur la biométrie permet de se passer de ce contrôle par un opérateur. Dans un contexte dans lequel on utilise la biométrie, les personnes qui veulent avoir accès à un avion se préenregistrent pour un vol avec leurs informations biométriques (typiquement une image du visage), et la reconnaissance des informations biométriques donne accès à l'avion sans qu'aucun opérateur n'intervienne.

[0004] Des solutions basées sur la biométrie permettent de ne plus avoir de portique, la reconnaissance se faisant lors du passage des personnes dans une zone en direction par exemple de l'avion. Une telle zone peut être un couloir observé par des caméras qui vont réaliser un suivi des personnes et vérifier leur biométrie sur les images acquises.

[0005] Il existe dans l'art antérieur des couloirs dans lesquels plusieurs personnes peuvent passer simultanément (par exemple des groupes de moins de 4 personnes) dans une zone observée par une ou plusieurs caméras dans laquelle les informations biométriques de ces personnes sont obtenues pour vérifier qu'elles sont bien préenregistrées pour accéder à l'avion.

[0006] Cette dernière solution est la moins incommode pour les personnes qui circulent sans aucune entrave telle qu'un portique, mais elle est aussi moins sécurisée qu'un contrôle par un opérateur. En fait, cette solution est une solution dans laquelle les portiques sont ouverts par défaut et peuvent se fermer si une personne non autorisée est présente.

[0007] Il existe peu de solutions suffisamment sécurisées dans lesquelles un groupe de personnes peuvent passer (et non pas des personnes une à une).

[0008] De l'état de la technique antérieure, on connaît les documents suivants :

- US 20210358244,
- ES 2860352,
- US 11080955,

- EP3494553,
- KR20170111804, et
- EP3179452.

[0009] Les solutions décrites dans ces documents ne sont pas faites pour laisser passer plusieurs personnes ou pas suffisamment sécurisées ou trop incommode pour les personnes.

10 Objet et résumé de l'invention

[0010] La présente invention répond à ce besoin en proposant un procédé de sécurisation d'un accès à une zone cible par des personnes, dans lequel, pour une personne (par exemple une personne parmi plusieurs personnes qui circulent vers la zone cible) :

- dans une première zone située en amont de la zone cible, on met en oeuvre un suivi de la personne lorsqu'elle circule dans la première zone dans la direction de la zone cible, au moyen d'une caméra qui observe au moins une portion de la première zone (plusieurs caméras peuvent être utilisées, avec des champs d'observation qui se chevauchent, par exemple pour couvrir toute la première zone),
- on obtient une information biométrique (par exemple une information permettant la reconnaissance faciale) de la personne suivie (et donc au moyen du suivi qui utilise la caméra) pour vérifier si cette personne correspond à une personne préenregistrée,
- on détermine un indicateur de sécurité indiquant un niveau de difficulté à obtenir une information biométrique pour la personne suivie (et donc au moyen du suivi qui utilise la caméra) et l'on vérifie si une condition de sécurité est vérifiée à partir de l'indicateur, si la personne correspond à une personne préenregistrée et si la condition de sécurité relative à l'indicateur n'est pas vérifiée, alors on génère un signal d'alerte, et si la personne ne correspond pas à une personne préenregistrée, alors on génère un signal d'alerte (par exemple le même signal d'alerte que celui généré si la condition de sécurité relative à l'indicateur n'est pas vérifiée, ou un signal d'alerte différent).

[0011] Ainsi, l'invention propose d'utiliser un indicateur supplémentaire et une vérification d'une condition de sécurité supplémentaire pour générer ou non un signal d'alerte. En particulier, ce signal d'alerte est généré alors même que la personne a été reconnue par sa biométrie. En fait, l'indicateur de sécurité peut indiquer qu'un niveau de sécurité trop faible lors de l'obtention de l'information biométrique a été atteint, puisque celle-ci a été difficile à obtenir.

[0012] L'indicateur de sécurité indique en fait un niveau de coopération de la personne lorsqu'elle circule vers la zone cible, cette coopération étant mesurable par la difficulté qu'il y a à obtenir l'information biométrique.

[0013] Le signal d'alerte, par exemple celui généré si la condition de sécurité relative à l'indicateur n'est pas vérifiée, peut être un signal visuel, un signal sonore, ou encore un signal qui déclenche un actionneur (par exemple pour fermer un accès). Avec ce signal d'alerte, on peut inviter un opérateur à mettre en oeuvre une vérification de l'identité de la personne. Il est préférentiellement restitué au voisinage de la sortie de la première zone.

[0014] Selon un mode de mise en oeuvre particulier, le signal d'alerte désigne la personne.

[0015] Par exemple, le signal d'alerte peut être restitué au moyen d'un module d'affichage sur lequel la personne est désignée.

[0016] Par exemple, si le module d'affichage comprend des lunettes de réalité augmentée (par exemple du type Hololens (marque déposée)), un marqueur peut apparaître au voisinage de la personne sur ces lunettes, de sorte que l'opérateur qui porte ces lunettes perçoit l'alerte et la personne concernée.

[0017] Si le module d'affichage est un écran, cet écran peut montrer les images observées par la caméra (ou une autre caméra) et afficher un marqueur au voisinage de la personne visible sur ces images.

[0018] Selon un mode de mise en oeuvre particulier, le procédé comprend la génération d'un autre signal d'alerte désignant une autre personne pour laquelle on a obtenu une information biométrique pour une vérification montrant que cette personne correspond à une personne préenregistrée (en d'autres termes, la vérification basée sur la biométrie montre que cette autre personne est bien une personne préenregistrée) et pour laquelle la condition de sécurité est vérifiée.

[0019] Dans ce mode de réalisation particulier une alerte désigne une personne pourtant correspondant à une personne préenregistrée, c'est-à-dire dont l'identité est biométrique est vérifiée, et pour laquelle la condition de sécurité était vérifiée : cela permet de limiter l'impact d'un biais dans l'utilisation de l'indicateur de sécurité.

[0020] L'autre personne est aussi une personne qui circule ou a circulé à travers la première zone dans la direction de la zone cible.

[0021] Selon un mode de réalisation particulier, l'autre personne est choisie au moyen d'une donnée aléatoire.

[0022] En d'autres termes, l'autre personne est choisie aléatoirement, ce qui limite encore plus l'impact d'un biais dans la détermination de l'indicateur de sécurité. En fait, cela limite non seulement l'impact d'un biais relatif à la détermination de l'indicateur de sécurité, mais cela limite aussi l'impact d'un biais dans l'obtention de l'information biométrique et/ou dans la vérification basée sur la biométrie, ou encore d'un biais d'un opérateur si un opérateur a aussi la possibilité de générer des signaux d'alerte.

[0023] Aussi, on peut mettre en oeuvre le choix de l'autre personne de manière régulière, c'est-à-dire en répétant le choix d'une autre personne à intervalle de temps donné ou de nombre de personnes donné ayant transité de la première zone à la zone cible fixe, de manière à

limiter l'impact sur les personnes qui circulent vers la zone cible. Avantagement, l'occurrence de mise en oeuvre du choix peut également être conditionnée à la charge des opérateurs.

[0024] Selon un mode de mise en oeuvre particulier, l'indicateur de sécurité est basé sur une visibilité du visage de la personne.

[0025] La visibilité du visage d'une personne peut être affectée par un angle de vue (une personne détourne la tête par rapport à une caméra), par le port d'un accessoire (lunettes, écharpe, masque, etc). Un visage peu visible rend difficile l'obtention d'une information biométrique, en particulier si l'on utilise une technique de reconnaissance faciale.

[0026] Par exemple, l'indicateur de sécurité peut être basé sur l'une des méthodes décrites dans le document « Face Image Quality Assessment : A Literature Survey » (TORSTEN SCHLETT ET AL, ACM Computing Surveys, Volume 54 Issue 10 Janvier 2022). D'autres méthodes peuvent être utilisées.

[0027] La visibilité du visage peut également être définie au moyen de la norme ISO/IEC 39794-5, dans sa partie 5, Annexe D.1 (décembre 2019), et l'on peut évaluer la conformité avec cette norme pour déterminer une visibilité d'un visage.

[0028] Selon un mode de mise en oeuvre particulier, le signal d'alerte ou l'autre signal d'alerte, lorsqu'il existe, ne comporte aucune information biométrique additionnelle de la personne ou de l'autre personne, une information biométrique additionnelle étant une information biométrique qui diffère de l'information biométrique obtenue.

[0029] Une information biométrique additionnelle peut être une information provenant d'une base de données, qui peut ne pas être disponible dans l'environnement où la présente méthode est mise en oeuvre (typiquement l'environnement peut être un aéroport). Le choix des informations biométriques additionnelles est effectué en fonction de l'environnement.

[0030] A titre indicatif, dans ce mode de réalisation, le signal d'alerte ou l'autre signal d'alerte ne comportant aucune information biométrique additionnelle peut être une image de la personne acquise par exemple lors de son passage dans la première zone, et elle peut ne contenir aucune information d'identité (nom, etc.) ou d'empreinte.

[0031] Par exemple, le signal peut être un marqueur visible au voisinage de la personne sur des lunettes de réalité augmentée. Un opérateur n'aura ainsi accès à aucune donnée sensible en termes de sécurité mais pourra réaliser une vérification d'identité basée sur un document d'identité, si cela est nécessaire.

[0032] Selon un mode de mise en oeuvre particulier, le signal d'alerte est destiné à être produit dans une deuxième zone située entre la première zone et la zone cible, et éventuellement, l'autre signal est destiné à être restitué dans une deuxième zone située entre la première zone et la zone cible.

[0033] La première zone est la zone dans laquelle circulent les personnes pour permettre leur reconnaissance basée sur la biométrie. Dans la deuxième zone, d'autres personnes telles que des opérateurs peuvent être présentes. C'est dans cette deuxième zone que le signal d'alerte est restitué (par exemple, il est visible sur un module d'affichage présent dans la deuxième zone), ou alors il est émis de sorte qu'il soit audible dans la deuxième zone s'il s'agit d'un signal sonore.

[0034] Selon un mode de mise en oeuvre particulier, une troisième zone est séparée de la première zone au moyen d'une séparation empêchant les personnes de passer de la première zone et éventuellement de la deuxième zone à la troisième zone (lorsque la deuxième zone est prévue, par exemple), la troisième zone étant hors d'un champ de suivi par la caméra et d'un champ d'obtention de l'information biométrique (typiquement dans la première zone), et la troisième zone débouche sur la zone cible ou sur la deuxième zone, et comprenant un portique de contrôle situé avant l'accès à la zone cible ou à la deuxième zone.

[0035] La troisième zone est une zone alternative à la première (et éventuellement à la deuxième). Pour des personnes qui n'ont pas partagé préalablement leurs informations biométriques, le passage par la troisième zone permet d'avoir accès à la zone cible mais en passant par un portique de contrôle ne nécessitant pas d'être préenregistré. Par exemple, un opérateur peut être présent au portique de contrôle.

[0036] A titre indicatif, le procédé peut comprendre la génération d'un autre signal d'alerte désignant une personne ayant circulé à travers la troisième zone.

[0037] Selon un mode de mise en oeuvre particulier, on contrôle des portiques de blocage d'accès dans un état bloqué en se basant sur le résultat de l'étape de vérification de la condition de sécurité (typiquement, si plusieurs conditions de sécurité sont non-vérifiées) et/ou sur le résultat de l'étape de vérification de la correspondance biométrique (typiquement, si plusieurs personnes ne correspondent pas à une personne préenregistrée) d'une pluralité de personnes.

[0038] Ces portiques de blocage d'accès peuvent être situés entre la première zone et la zone cible, notamment entre la deuxième zone et la zone cible.

[0039] Dans ce mode de mise en oeuvre, on considère que la vérification de la condition de sécurité et que la vérification de la correspondance biométrique de la personne, sont problématiques pour une pluralité de personnes et l'on bloque complètement l'accès à la zone cible en commandant les portiques de blocage d'accès. Par exemple, les portiques de blocage peuvent être contrôlés dans un état bloqué si, pendant une période de temps donnée, un nombre de personnes supérieur à un seuil donné (par exemple égal à un nombre d'opérateurs capables de réaliser des vérifications) a conduit à la génération de signaux d'alertes (condition de sécurité non vérifiée ou échec de la correspondance biométrique).

[0040] Selon un mode de mise en oeuvre particulier,

pour plusieurs personnes :

- dans la première zone située en amont de la zone cible, on met en oeuvre un suivi des plusieurs personnes lorsqu'elles circulent dans la première zone dans la direction de la zone cible, au moyen de la caméra,
- on obtient une information biométrique de chaque personne suivie parmi les plusieurs personnes pour vérifier si chaque personne correspond à une personne préenregistrée,
- on détermine l'indicateur de sécurité pour chaque personne suivie et l'on vérifie si une condition de sécurité est vérifiée à partir de l'indicateur pour chaque personne suivie,
- pour chaque personne suivie, si la personne correspond à une personne préenregistrée et si la condition de sécurité relative à l'indicateur n'est pas vérifiée, alors on génère un signal d'alerte, et pour chaque personne qui ne correspond pas à une personne préenregistrée, alors on génère un signal d'alerte (par exemple le même signal d'alerte que celui généré si la condition de sécurité relative à l'indicateur n'est pas vérifiée, ou un signal d'alerte différent).

[0041] Ainsi, plusieurs personnes sont suivies et dès que la condition de sécurité n'est pas vérifiée pour une personne préenregistrée, on émet une alerte.

[0042] Cette alerte peut désigner la personne parmi les plusieurs personnes.

[0043] Selon un mode de mise en oeuvre, on contrôle les portiques de blocage d'accès dans un état bloqué en se basant sur la vérification de la condition de sécurité et sur la vérification de la correspondance biométrique des plusieurs personnes.

[0044] Par exemple, par « en se basant sur », on peut comprendre que l'on compare à un seuil donné une valeur basée sur les indicateurs de plusieurs personnes et la vérification de correspondance des plusieurs personnes. Par exemple, au-delà d'un nombre donné de personnes avec une condition de sécurité non vérifiée et au-delà d'un nombre donné de personnes non préenregistrées, on peut bloquer complètement l'accès à la zone cible.

[0045] Selon un mode de mise en oeuvre particulier, la zone cible est un accès à un avion ou un accès à un train ou un accès à un bateau ou un accès à un bâtiment.

[0046] L'invention est particulièrement bien adaptée à ces accès.

[0047] L'invention propose également un dispositif de sécurisation d'un accès à une zone cible par des personnes, comprenant :

un module d'obtention d'un flux d'images issue d'une caméra qui observe au moins une partie d'une première zone dans laquelle une personne circule dans la direction de la zone cible,
un module de suivi de la personne au moyen de la

caméra,
 un module d'obtention d'une information biométrique de la personne suivie configuré pour vérifier si cette personne correspond à une personne préenregistrée,
 un module de détermination d'un indicateur de sécurité pour la personne configuré pour vérifier si une condition de sécurité relative à l'indicateur est vérifiée,
 un module configuré pour générer un signal d'alerte si la personne correspond à une personne préenregistrée et si la condition de sécurité relative à l'indicateur n'est pas vérifiée, et pour générer un signal d'alerte si la personne ne correspond pas à une personne préenregistrée.

[0048] Ce dispositif peut être configuré pour la mise en oeuvre de tous les modes de mise en oeuvre du procédé tel que décrit ci-avant.

[0049] Par exemple, ce procédé peut avoir une structure de système informatique, et les modules peuvent être implémentés au moyen d'instructions de programme d'ordinateur stockées dans une mémoire non-volatile du système informatique qui, lorsqu'elles sont exécutées par un processeur du système informatique, exécutent les étapes du procédé tel que décrit ci-avant.

[0050] L'invention propose également un système comprenant le dispositif de sécurisation défini ci-avant et ladite caméra (éventuellement une pluralité de caméras).

[0051] Dans ce système, la caméra et le dispositif sont en communication.

[0052] L'invention vise également une installation comprenant le système tel que défini ci-avant et la première zone.

[0053] Système comprenant un dispositif de sécurisation tel que défini ci-avant et ladite caméra.

[0054] Selon un mode de réalisation particulier, le système comprend en outre un module de restitution du signal d'alerte généré si la personne correspond à une personne préenregistrée et si la condition de sécurité relative à l'indicateur n'est pas vérifiée, et/ou si la personne ne correspond pas à une personne préenregistrée,

le module de restitution du signal d'alerte comprenant des lunettes de réalité augmentée (par exemple des lunettes Hololens (marque déposée)) ou une tablette (une tablette avec un écran) ou un portique d'alerte équipé d'un dispositif de signalisation (par exemple sous la forme d'un portique tel qu'on en trouve à la sortie d'un commerce, ou encore sous la forme d'une borne de visualisation).

[0055] Installation comprenant le système tel que défini ci-avant et la première zone.

[0056] L'installation comprend donc à la fois le système et cette zone qui peut être une zone d'un bâtiment.

[0057] L'installation peut comprendre la deuxième zone et/ou la troisième zone définies ci-avant.

[0058] Selon un mode de réalisation particulier, la zone cible est un accès à un avion ou un accès à un train ou un accès à un bateau ou un accès à un bâtiment.

5 Brève description des dessins

[0059] D'autres caractéristiques et avantages de la présente invention ressortiront de la description faite ci-dessous, en référence aux dessins annexés qui en illustrent un exemple dépourvu de tous caractères limitatifs.

[0060] Sur les figures :

[Fig. 1] La figure 1 montre schématiquement les étapes d'un procédé selon un exemple.

[Fig. 2] La figure 2 montre un autre exemple dans lequel plusieurs personnes sont suivies.

[Fig. 3] La figure 3 montre un dispositif et un système selon un exemple.

[Fig. 4] La figure 4 montre une installation de type aéroport.

[Fig. 5] La figure 5 montre une installation de type gare ferroviaire.

Description détaillée d'un mode de réalisation

[0061] On va maintenant décrire un procédé et un système de sécurisation d'un accès à une zone cible par des personnes.

[0062] Ce procédé et ce système sont particulièrement adaptés à des zones cibles que sont un accès à un avion (typiquement une plateforme aéroportuaire) ou un accès à un train (un quai) ou un accès à un bateau ou un accès à un bâtiment.

[0063] Aussi, le procédé et le système visent la circulation des personnes permettant la vérification de leur identité en se basant sur la biométrie, dans une zone dans laquelle les personnes circulent sans entrave et dans la direction de la zone cible, pour permettre la vérification de leur identité. Le procédé et le système trouvent donc application dans les accès sécurisés pour lesquels il n'est pas nécessaire de vérifier manuellement systématiquement l'identité des personnes. En langue anglaise, on peut appeler ces accès des accès « free flow ».

[0064] Sur la figure 1, on a représenté de manière schématique et sous forme d'ordinogramme les étapes d'un procédé de sécurisation d'un accès à une zone cible par des personnes, ces étapes concernant une personne, par exemple une personne parmi plusieurs qui circulent vers la zone cible (procédé P1). Par circule, on entend circuler à pieds ou au moyen d'un dispositif aidant la mobilité tel qu'un fauteuil roulant, etc.

[0065] Le procédé P1 est mis en oeuvre en utilisant une ou plusieurs caméras d'observation qui observent

chacune une première zone. La première zone peut être un couloir dans lequel plusieurs personnes peuvent circuler simultanément et même côte-à-côte.

[0066] Dans une première étape S01, on met en oeuvre un suivi de la personne, par exemple en utilisant des algorithmes de traitement d'image qui identifient des personnes et réalisent un suivi (« tracking » en langue anglaise). La personne du métier saura choisir un algorithme utilisable à cette fin, qui permet de localiser sur un flux vidéo où se trouve une même personne. Le flux vidéo peut comprendre des images provenant de plusieurs caméras, par exemple avec des champs d'observation qui se chevauchent et des signaux issus des caméras fusionnés, de sorte que le suivi des personnes peut être consolidé.

[0067] On peut noter que le suivi d'une personne peut être un suivi de son corps entier et/ou uniquement de son visage.

[0068] Dans une deuxième étape S02, on obtient une information biométrique de la personne suivie. Cela permet de réaliser, à l'étape S03, une vérification du caractère préenregistré de la personne.

[0069] Par exemple, pour réaliser l'étape S02, on peut utiliser tout algorithme connu de reconnaissance faciale, notamment sur la base des images acquises lors du suivi de personnes lors de l'étape S01 par la caméra 400. Par exemple, on peut utiliser un algorithme qui délivre une signature, notamment biométrique, utilisée pour vérifier à l'étape S03 si la personne est préenregistrée dans une base de données, ce préenregistrement utilisant également la biométrie.

[0070] Si la personne n'est pas préenregistrée, on met en oeuvre l'étape S10 d'alerte.

[0071] On peut noter que l'étape S10 peut n'être mise en oeuvre que si la personne a traversé la première zone pour atteindre soit la zone cible soit la deuxième zone si elle est présente, comme tel est le cas sur les exemples décrits en référence aux figures 4 et 5. Ce mode de mise en oeuvre étant avantageux pour une première zone dite « ouverte » telle qu'un hall de gare.

[0072] L'alerte peut être une alerte globale, qui ne désigne pas la personne parmi plusieurs personnes qui circulent vers la zone cible. Par exemple, le signal d'alerte peut être restitué au moyen d'un portique d'alerte situé à la sortie de la première zone, par exemple entre la première zone et une deuxième zone, ce portique d'alerte étant équipé avec un dispositif de signalisation qui clignote/sonne lorsque le signal d'alerte est généré (ces portiques d'alerte étant semblables à ceux situés à la sortie d'un commerce). Plusieurs portiques d'alerte peuvent être utilisés. Le signal d'alerte peut également être restitué sur un module d'affichage comme un écran de tablette ou des lunettes de réalité augmentée (par exemple du type Hololens (marque déposée)). Plusieurs de ces modes de restitution de l'alerte peuvent être combinés.

[0073] Préférentiellement, l'alerte désigne la personne. Par exemple, le signal d'alerte peut être restitué au

moyen d'un module d'affichage sur lequel la personne est désignée.

[0074] Par exemple, si le module d'affichage comprend des lunettes de réalité augmentée (par exemple du type Hololens (marque déposée)), un marqueur peut apparaître au voisinage de la personne sur ces lunettes, de sorte que l'opérateur qui porte ces lunettes perçoit l'alerte. Si le module d'affichage est un écran, cet écran peut montrer les images observées par la caméra (ou une autre caméra) et afficher un marqueur au voisinage de la personne visible sur ces images.

[0075] Pour une alerte qui désigne une personne, on peut aussi utiliser un ou plusieurs portiques d'alerte, configurés pour que l'alerte soit restituée lorsque la personne passe au travers (on notera que la largeur des portiques d'alerte est avantageusement choisie de sorte que plusieurs personnes à la fois passent dans un portique d'alerte, en laissant notamment suffisamment de place pour le passage d'une personne à mobilité réduite).

[0076] L'alerte qui désigne une personne peut être configurée pour qu'un opérateur soit invité à réaliser une vérification de l'identité de la personne non enregistrée, et à cet effet elle est restituée de sorte qu'un opérateur puisse la percevoir.

[0077] Pour une personne préenregistrée, on peut mettre en oeuvre l'étape S04 de détermination d'un indicateur de sécurité indiquant un niveau de difficulté à obtenir une information biométrique pour la personne suivie et l'on vérifie si une condition de sécurité est vérifiée à partir de l'indicateur.

[0078] Dans le présent exemple, l'indicateur est relatif à une visibilité du visage de la personne. En mesurant cette visibilité, on obtient une information sur le niveau de coopération de la personne avec le système d'accès basé sur la biométrie.

[0079] En fait, la dissimulation du visage avec des lunettes, un chapeau, etc. peut affecter l'obtention de l'information biométrique. Cette information mesurable reflète bien le niveau de coopération de la personne.

[0080] A titre indicatif, on pourra utiliser l'une des méthodes décrite dans le document « Face Image Quality Assessment : A Literature Survey » (TORSTEN SCHLETT ET AL, ACM Computing Surveys, Volume 54 Issue 10 Janvier 2022).

[0081] A l'étape S05, on vérifie si une condition de sécurité est vérifiée à partir de l'indicateur. Cette étape peut comprendre une comparaison à un seuil donné.

[0082] Si la condition de sécurité n'est pas vérifiée, on met en oeuvre l'étape S10 de génération d'un signal d'alerte décrite ci-avant.

[0083] En d'autres termes, la personne est une personne préenregistrée mais sa coopération n'est pas à un niveau attendu, et l'on génère le signal d'alerte.

[0084] Si la condition de sécurité est vérifiée, on peut mettre en oeuvre l'étape S06 dans laquelle, selon une donnée aléatoire, on décide ou non de générer un autre signal d'alerte.

[0085] S'il est décidé de générer un signal sur la base

de la donnée aléatoire, on met en oeuvre l'étape S10' de génération d'un autre signal d'alerte.

[0086] L'étape S10' est analogue à l'étape S10. Préférentiellement, les signaux générés par les étapes S10' et S10 sont identiques, de sorte qu'il n'est pas possible de distinguer une alerte justifiée au vu des vérifications S03 et S05 d'une alerte basée sur la donnée aléatoire. Ces signaux peuvent être restitués de la manière identique.

[0087] L'utilisation d'une donnée aléatoire permet d'éviter l'impact qu'aurait un biais dans la vérification des informations biométriques ou la détermination de l'indicateur de sécurité.

[0088] S'il n'est pas décidé de générer un signal sur la base de la donnée aléatoire, le procédé se termine à l'étape S11.

[0089] Sur la figure 2, on a représenté un exemple dans lequel on a mis en oeuvre le procédé P1 pour n personnes, les n personnes passant à travers la première zone dans la direction de la zone cible.

[0090] Cela correspond à la mise en oeuvre d'un procédé dans lequel, pour n personnes :

- dans la première zone située en amont de la zone cible, on met en oeuvre un suivi des plusieurs personnes lorsqu'elles circulent dans la première zone dans la direction de la zone cible, au moyen de la caméra,
- on obtient une information biométrique de chaque personne suivie parmi les plusieurs personnes pour vérifier si chaque personne correspond à une personne préenregistrée,
- on détermine ledit indicateur de sécurité pour chaque personne suivie et l'on vérifie si une condition de sécurité est vérifiée à partir de l'indicateur pour chaque personne suivie,
- pour chaque personne suivie, si la personne correspond à une personne préenregistrée et si la condition de sécurité relative à l'indicateur n'est pas vérifiée, alors on génère un signal d'alerte.

[0091] Ultérieurement, on peut mettre en oeuvre l'étape S20 dans laquelle on contrôle des portiques de blocage d'accès dans un état bloqué en se basant sur toutes les vérifications de la condition de sécurité et sur toutes les vérifications de la correspondance des n personnes.

[0092] Ces portiques de blocage peuvent être agencés entre la première zone et la zone cible, notamment entre une deuxième zone et la zone cible comme cela sera visible sur les figures 4 et 5 décrites ultérieurement.

[0093] Par exemple, au-delà d'un seuil donné de personnes pour lesquelles la condition de sécurité n'était pas vérifiée, on peut contrôler les portiques de blocage dans un état bloqué. Au-delà d'un autre seuil donné de personnes qui ne correspondent pas à des personnes préenregistrées, on peut contrôler les portiques de blocage dans un état bloqué.

[0094] Dans les étapes représentées aux figures 1 et

2, lorsque des signaux d'alerte sont générés, on peut ne transmettre aucune information biométrique des personnes concernées avec les alertes. Cela assure la sécurité des informations biométriques tout en permettant à des opérateurs de réaliser des contrôles des personnes avec par exemple leurs documents d'identité. Cela peut être réalisé avec un signal d'alerte qui indique la position d'une personne désignée par une alerte (comme un marqueur). En fait, aucune information permettant la mise en oeuvre de l'étape S03 n'est transmise.

[0095] Sur la figure 3, on a représenté un système 200 comprenant un dispositif 100 configuré pour la mise en oeuvre des étapes de procédé décrites ci-avant.

[0096] Le système 200 et le dispositif sont configurés pour la sécurisation de l'accès à la zone cible ZC représentée sur la figure, à partir de la première zone Z1.

[0097] A cet effet, le système comporte des caméras 400 qui observent la première zone, ici chacune une portion.

[0098] Le dispositif 100 a une structure de système informatique et il comporte un processeur 101 et une mémoire non volatile 102 qui comprend des instructions de programme d'ordinateur.

[0099] Le dispositif 100 est en communication (par exemple au moyen d'un réseau de communication) avec une base de données biométriques 300 dans laquelle sont mémorisées des informations biométriques de personnes préenregistrées. La base de données biométrique peut être centralisée, par exemple gérée par un état, ou encore locale et gérée par l'entité accueillant la zone cible (typiquement l'aéroport).

[0100] Le système 200 comporte également un module 500 configuré pour restituer les alertes générées, par exemple un dispositif d'affichage (écran, lunettes de réalité augmentée).

[0101] Dans la mémoire non volatile, on a mémorisé des instructions :

- des instructions 111 pour l'obtention d'un flux d'images issues d'une caméra qui observe au moins une partie de la première zone Z1 dans laquelle une personne circule dans la direction de la zone cible ZC, formant un module d'obtention quand elles sont exécutées par le processeur,
- des instructions 112 de suivi de la personne au moyen des caméras 400 et de détermination de sa signature, notamment biométrique, formant un module de suivi de la personne quand elles sont exécutées par le processeur,
- des instructions 113 d'obtention d'une information biométrique de la personne suivie et pour vérifier si cette personne correspond à une personne préenregistrée, notamment par comparaison de la signature déterminée avec la base des personnes préenregistrées 300, formant un module de mise en correspondance biométrique quand elles sont exécutées par le processeur,
- des instructions 114 de détermination d'un indica-

teur de sécurité indiquant un niveau de difficulté à obtenir une information biométrique pour la personne, les instructions 114 étant en outre des instructions pour vérifier si une condition de sécurité relative à l'indicateur est vérifiée, notamment par comparaison de l'indicateur à un seuil, formant un module de détermination quand elles sont exécutées par le processeur,

- des instructions 115 pour générer un signal d'alerte si la personne correspond à une personne préenregistrée et si la condition de sécurité relative à l'indicateur n'est pas vérifiée, et pour générer un signal d'alerte si la personne ne correspond pas à une personne préenregistrée, formant un module de génération quand elles sont exécutées par le processeur.

[0102] La mémoire non volatile 102 comporte également des instructions 116 qui, quand elles sont exécutées par le processeur 101, mettent en oeuvre l'étape S20 décrite ci-avant.

[0103] En outre, la mémoire non volatile peut comporter des instructions pour générer un autre signal d'alerte pour une personne choisie aléatoirement, pour par exemple mettre en oeuvre l'étape S10' décrite ci-avant.

[0104] La figure 4 montre une configuration de zone cible qui peut être celle pour un aéroport (ou un port).

[0105] Par exemple, la zone cible peut être une plateforme aéroportuaire débouchant sur un avion (non représenté).

[0106] Deux caméras 400 sont représentées pour la première zone. Par exemple, on peut utiliser des caméras agencées à une hauteur de 2m, préférentiellement équiréparties de manière à couvrir entièrement le volume/espace de la zone 1. A titre indicatif, et si plusieurs caméras sont utilisées, elles peuvent avoir des champs d'observation qui se chevauchent (cela permet de fusionner les données issues des caméras), cela pouvant être obtenu en choisissant des caméras avec des champs d'observation approprié (par exemple fish-eye/grand-angle/etc.). Préférentiellement, l'intégralité de la première zone est observée par les caméras.

[0107] Ici, la première zone débouche, dans le sens de circulation qui va du bas vers le haut sur la figure, sur une deuxième zone Z2. La deuxième zone Z2 est une zone dans laquelle le module 500 est agencé pour que l'alerte soit restituée dans cette zone.

[0108] Par exemple, un ou plusieurs opérateurs peuvent être présents dans cette zone et, sur la base de l'alerte, ils peuvent contrôler des personnes désignées par des alertes.

[0109] On peut rejoindre la zone cible ZC au moyen d'un chemin alternatif, ici une troisième zone Z3. La troisième zone est séparée de la première zone au moyen d'une séparation 610 empêchant les personnes de passer de la première zone et de la deuxième zone à la troisième zone.

[0110] La séparation 610 peut être opaque ou non, de sorte que la troisième zone Z3 est hors du champ d'ob-

servation des caméras 400, c'est-à-dire hors du champ de suivi et de contrôle biométrique automatisé. Ainsi, on n'utilise pas d'informations biométriques des personnes qui circulent dans la troisième zone Z3. Cette zone permet, pour des raisons personnelles, de ne pas avoir à transmettre d'informations pour un préenregistrement. Par contre, un portique de contrôle 600 est agencé entre la troisième zone Z3 et la deuxième zone Z2, avec par exemple un opérateur.

[0111] De manière optionnelle, on a en outre agencé une caméra 410 observant la deuxième zone, permettant par exemple, sur la base du suivi qui a été réalisé dans la première zone, de continuer ce suivi et de produire des alertes qui désigne bien les bonnes personnes, ce qui est notamment utile dans le cas d'un groupe consé-

quent de personnes non coopératives.

[0112] Entre d'une part la deuxième zone, et/ou la troisième zone, et d'autre part la zone cible, on a agencé des portiques de blocage d'accès 700 qui peuvent être contrôlés au cours de l'étape S20.

[0113] Ces portiques de blocage d'accès 700 peuvent, quand ils sont ouverts, permettre des accès aisés, typiquement avec une largeur de l'ordre préférentielle d'au moins 1,20 m, en fonction de la configuration du lieu (porte de train, porte d'embarquement...).

[0114] Des portiques d'alerte 800 ont été représentés sur la figure entre la première zone Z1 et la deuxième zone Z2. Ces portiques d'alerte 800 peuvent restituer un signal d'alerte comme le module 500 (qu'ils peuvent remplacer), par exemple avec dispositif de signalisation 801 qui produit un signal lumineux ou sonore (monté ici sur les portiques d'alerte 800 mais qui peut être placé ailleurs). La restitution du signal d'alerte peut être déclenchée par exemple quand une personne désignée par une alerte passe à travers l'un des portiques d'alerte 800, de largeur plus étroite que la largeur de la zone 1 (ici, pour toute la zone 1, on a représenté trois portiques d'alerte). Ces portiques d'alerte 800 peuvent, quand ils sont ouverts, permettre des accès aisés, typiquement avec une largeur de l'ordre de 1.20 m à 1.50 m. La figure 5 montre une autre configuration, plus adaptée à un accès à un train, dans laquelle la troisième zone et la première zone débouchent sur la deuxième zone. Les portiques de blocage d'accès sont agencés entre la deuxième zone et la zone cible ZC.

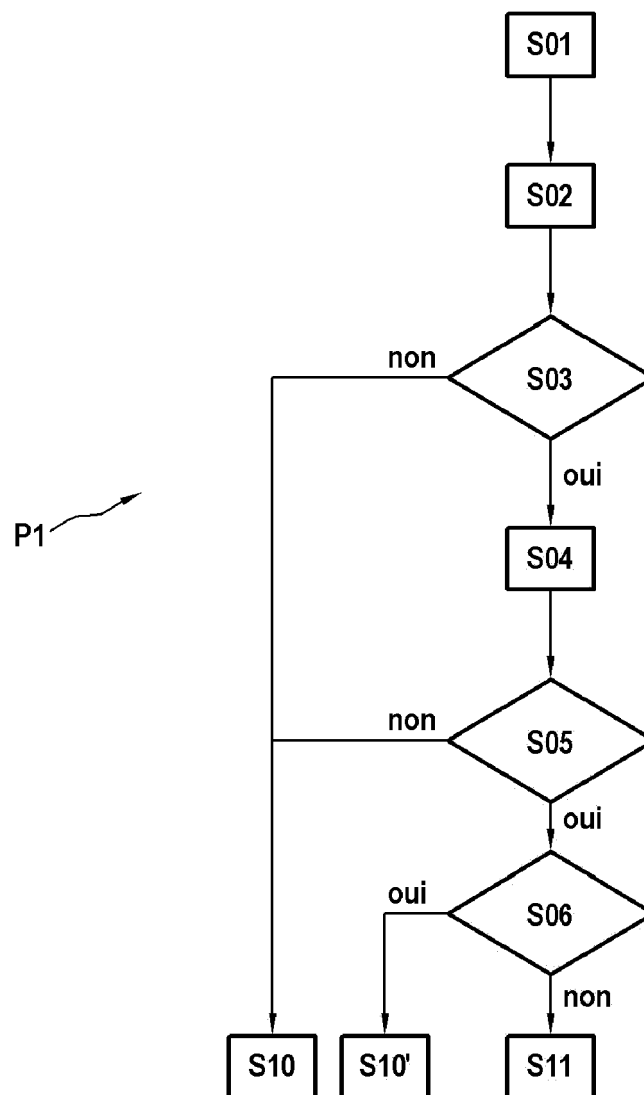
[0115] Comme illustré sur les figures 4 et 5, les portiques d'alerte 800 sont initialement et par défaut ouverts, ne comportant pas nécessairement de moyen de fermeture, alors que les portiques de blocage d'accès 700 sont initialement et par défaut ouverts, mais comportent des moyens de fermeture (par exemple des battants de porte, une fermeture coulissante) qui sont alors passés en position fermée lorsqu'on contrôle S20 les portiques 700 de blocage d'accès dans un état bloqué, de manière à empêcher l'accès à la zone cible ZC.

Revendications

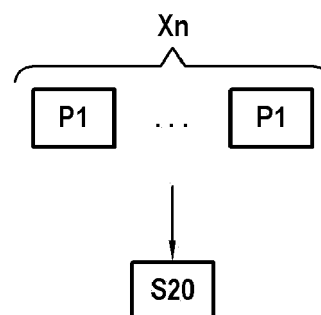
1. Procédé de sécurisation d'un accès à une zone cible (ZC) par des personnes, dans lequel, pour une personne :
 - dans une première zone (Z1) située en amont de la zone cible, on met en oeuvre un suivi (S01) de la personne lorsqu'elle circule dans la première zone dans la direction de la zone cible, au moyen d'une caméra (400) qui observe au moins une portion de la première zone,
 - on obtient (S02) une information biométrique de la personne suivie pour vérifier (S03) si cette personne correspond à une personne préenregistrée,
 - on détermine (S04) un indicateur de sécurité indiquant un niveau de difficulté à obtenir une information biométrique pour la personne suivie et l'on vérifie (S05) si une condition de sécurité est vérifiée à partir de l'indicateur,
 - si la personne correspond à une personne préenregistrée et si la condition de sécurité relative à l'indicateur n'est pas vérifiée, alors on génère (S10) un signal d'alerte, et si la personne ne correspond pas à une personne préenregistrée, alors on génère un signal d'alerte.
2. Procédé selon la revendication 1, dans lequel le signal d'alerte désigne la personne.
3. Procédé selon la revendication 2, comprenant la génération (S10') d'un autre signal d'alerte désignant une autre personne pour laquelle on a obtenu une information biométrique pour une vérification montrant que cette personne correspond à une autre personne préenregistrée et pour laquelle la condition de sécurité est vérifiée.
4. Procédé selon la revendication 3, dans lequel l'autre personne est choisie au moyen d'une donnée aléatoire.
5. Procédé selon l'une quelconque des revendications 1 à 3, dans lequel l'indicateur de sécurité indiquant un niveau de difficulté à obtenir une information biométrique pour la personne suivie est basé sur une visibilité du visage de la personne suivie.
6. Procédé selon l'une quelconque des revendications 1 à 5, dans lequel le signal d'alerte ou, lorsque le procédé est pris dans son rattachement à la revendication 3 ou 4, l'autre signal d'alerte, ne comporte aucune information biométrique additionnelle de la personne ou de l'autre personne, une information biométrique additionnelle étant une information biométrique qui diffère de l'information biométrique obtenue.
7. Procédé selon l'une quelconque des revendications 1 à 6, dans lequel le signal d'alerte est destiné à être produit dans une deuxième zone située entre la première zone et la zone cible, et lorsque le procédé est pris dans son rattachement à au moins la revendication 3, l'autre signal est destiné à être restitué dans une deuxième zone située entre la première zone et la zone cible.
8. Procédé selon l'une quelconque des revendications 1 à 6, dans lequel une troisième zone est séparée de la première zone au moyen d'une séparation empêchant les personnes de passer de la première zone et éventuellement de la deuxième zone à la troisième zone,
 - la troisième zone étant hors d'un champ de suivi par la caméra et d'un champ d'obtention de l'information biométrique, et
 - la troisième zone débouche sur la zone cible ou sur la deuxième zone, et comprenant un portique de contrôle (600) situé avant l'accès à la zone cible ou à la deuxième zone.
9. Procédé selon l'une quelconque des revendications 1 à 8, dans lequel on contrôle (S20) des portiques (700) de blocage d'accès dans un état bloqué en se basant sur la vérification de la condition de sécurité et sur la vérification de la correspondance biométrique d'une pluralité de personnes.
10. Procédé selon l'une quelconque des revendications précédentes, dans lequel, pour plusieurs personnes :
 - dans la première zone située en amont de la zone cible, on met en oeuvre un suivi des plusieurs personnes lorsqu'elles circulent dans la première zone dans la direction de la zone cible, au moyen de la caméra,
 - on obtient une information biométrique de chaque personne suivie parmi les plusieurs personnes pour vérifier si chaque personne correspond à une personne préenregistrée,
 - on détermine ledit indicateur de sécurité pour chaque personne suivie et l'on vérifie si une condition de sécurité est vérifiée à partir de l'indicateur pour chaque personne suivie,
 - pour chaque personne suivie, si la personne correspond à une personne préenregistrée et si la condition de sécurité relative à l'indicateur n'est pas vérifiée, alors on génère un signal d'alerte, et pour chaque personne qui ne correspond pas à une personne préenregistrée, alors on génère un signal d'alerte (par exemple le même signal d'alerte que celui généré si la condition de sécurité relative à l'indicateur n'est pas vérifiée, ou un signal d'alerte différent.

11. Procédé selon les revendications 9 et 10, dans lequel on contrôle les portiques (700) de blocage d'accès dans un état bloqué en se basant sur la vérification de la condition de sécurité et sur la vérification de la correspondance biométriques des plusieurs personnes 5
12. Procédé selon l'une quelconque des revendications 1 à 11, dans lequel la zone cible est un accès à un avion ou un accès à un train ou un accès à un bateau ou un accès à un bâtiment. 10
13. Dispositif de sécurisation d'un accès à une zone cible par des personnes, comprenant : 15
- un module (101, 111) d'obtention d'un flux d'images issue d'une caméra qui observe au moins une partie d'une première zone dans laquelle une personne circule dans la direction de la zone cible, 20
- un module (101, 112) de suivi de la personne au moyen de la caméra,
- un module (101, 113) d'obtention une information biométrique de la personne suivie configuré pour vérifier si cette personne correspond à une personne préenregistrée, 25
- un module (101, 114) de détermination d'un indicateur de sécurité indiquant un niveau de difficulté à obtenir une information biométrique pour la personne configuré pour vérifier si une condition de sécurité relative à l'indicateur est vérifiée, 30
- un module (101, 115) configuré pour générer un signal d'alerte si la personne correspond à une personne préenregistrée et si la condition de sécurité relative à l'indicateur n'est pas vérifiée, et pour générer un signal d'alerte si la personne ne correspond pas à une personne préenregistrée. 35
- 40
14. Système comprenant un dispositif de sécurisation selon la revendication 13 et ladite caméra.
15. Système selon la revendication 14, comprenant en outre un module de restitution du signal d'alerte généré si la personne correspond à une personne préenregistrée et si la condition de sécurité relative à l'indicateur n'est pas vérifiée, et/ou si la personne ne correspond pas à une personne préenregistrée, le module de restitution du signal d'alerte comprenant des lunettes de réalité augmentée (500) ou une tablette (500) ou un portique (800) d'alerte équipé d'un dispositif de signalisation (801). 1 45
- 50
- 55

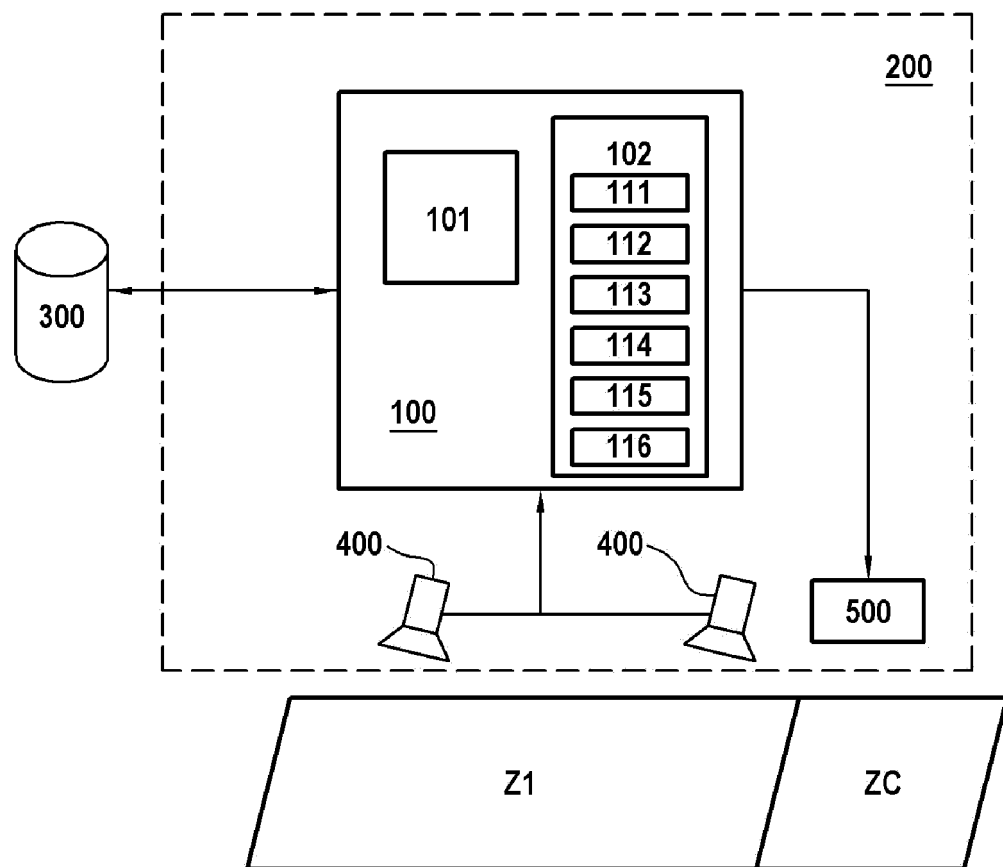
[Fig. 1]



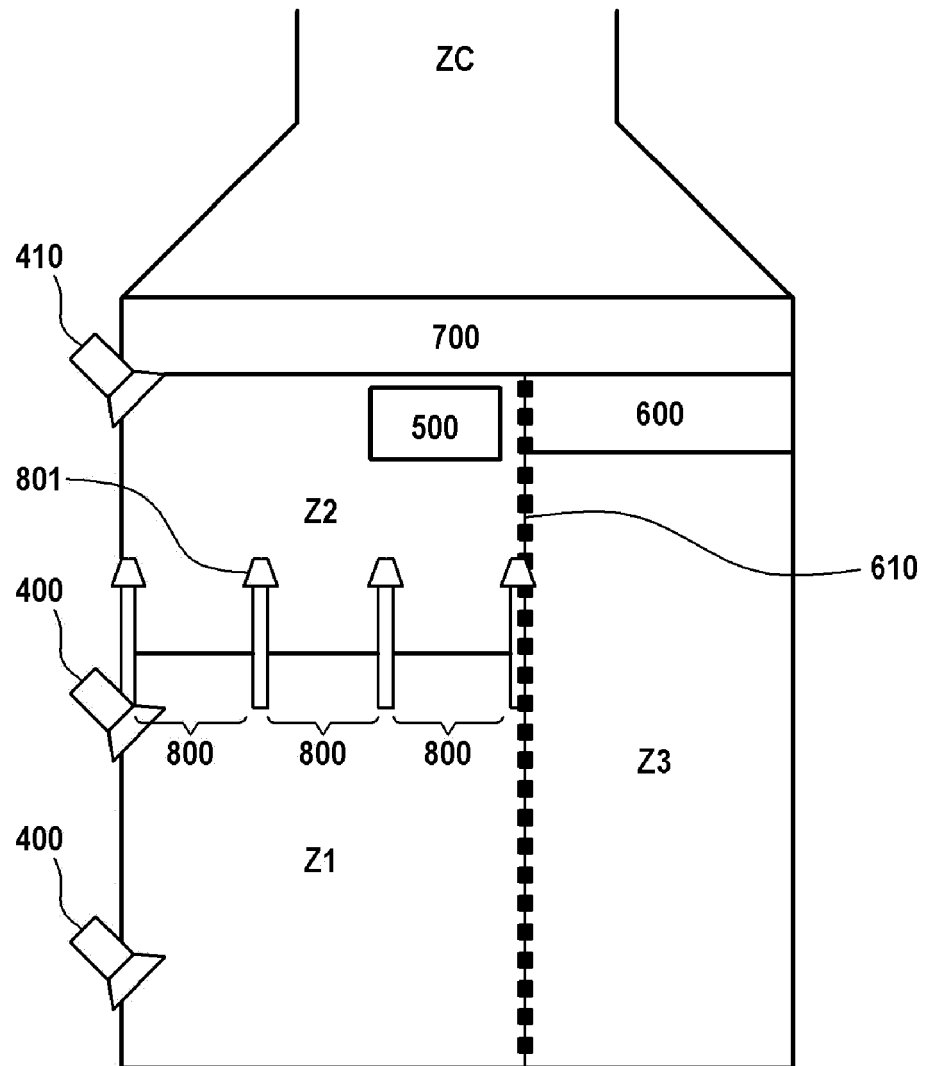
[Fig. 2]



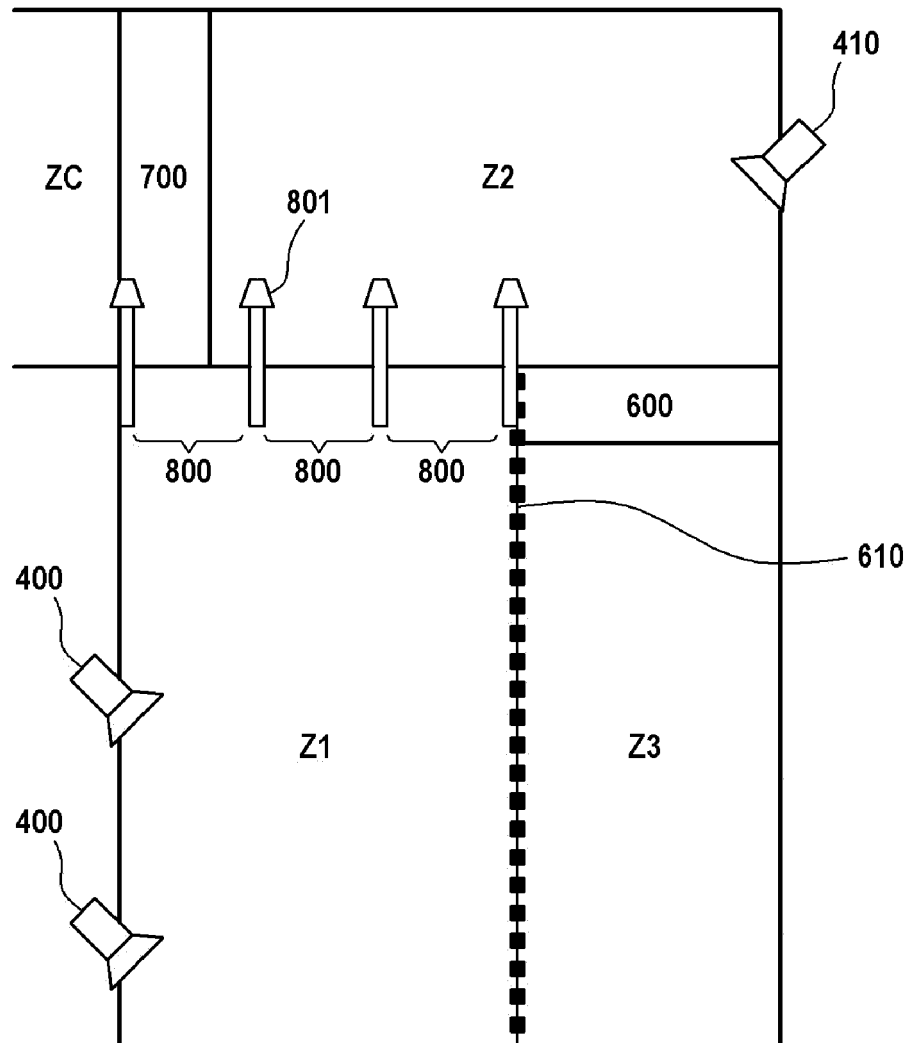
[Fig. 3]



[Fig. 4]



[Fig. 5]





RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande

EP 24 15 7491

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	EP 3 907 709 A1 (ROYAL CARIBBEAN CRUISES LTD [US]; TASCENT INC [US]) 10 novembre 2021 (2021-11-10) * abrégé * * * figures 1-5B * * alinéa [0005] - alinéa [0097] * -----	1-15	INV. G07C9/37
X	US 2019/147676 A1 (MADZHUNKOV YORDAN [BG] ET AL) 16 mai 2019 (2019-05-16) * abrégé * * * alinéa [0009] - alinéa [0276] * -----	1-15	
X	US 2018/047230 A1 (NYE JAMES E [US]) 15 février 2018 (2018-02-15) * abrégé * * * alinéa [0005] - alinéa [0200] * -----	1,13	
			DOMAINES TECHNIQUES RECHERCHES (IPC)
			G07C
Le présent rapport a été établi pour toutes les revendications			
Lieu de la recherche		Date d'achèvement de la recherche	Examineur
La Haye		21 juin 2024	Pañeda Fernández, J
CATEGORIE DES DOCUMENTS CITES		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	
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			

EPO FORM 1503 03.82 (P04C02)

**ANNEXE AU RAPPORT DE RECHERCHE EUROPEENNE
RELATIF A LA DEMANDE DE BREVET EUROPEEN NO.**

EP 24 15 7491

5 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 membres 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.

21-06-2024

10	Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
	EP 3907709 A1	10-11-2021	EP 3907709 A1	10-11-2021
			US 2021350642 A1	11-11-2021
			US 2022230493 A1	21-07-2022
15	-----	-----	-----	-----
	US 2019147676 A1	16-05-2019	US 2019147676 A1	16-05-2019
			US 2019213816 A1	11-07-2019
			US 2019325682 A1	24-10-2019
	-----	-----	-----	-----
20	US 2018047230 A1	15-02-2018	AUCUN	
	-----	-----	-----	-----
25				
30				
35				
40				
45				
50				
55				

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 20210358244 A [0008]
- ES 2860352 [0008]
- US 11080955 B [0008]
- EP 3494553 A [0008]
- KR 20170111804 [0008]
- EP 3179452 A [0008]

Littérature non-brevet citée dans la description

- **TORSTEN SCHLETT et al.** Face Image Quality Assessment : A Literature Survey. *ACM Computing Surveys*, Janvier 2022, vol. 54, 10 [0026]
- **TORSTEN SCHLETT et al.** Face Image Quality Assessment : A Literature Survey. *ACM Computing Surveys*, Janvier 2022, vol. 54 (10 [0080])