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

(11) EP 1 223 564 A1

(12) DEMANDE DE BREVET EUROPEEN

(43) Date de publication:
17.07.2002 Bulletin 2002/29

(51) Int Cl.[7]: **G07F 7/08**

(21) Numéro de dépôt: **01402850.0**

(22) Date de dépôt: **05.11.2001**

(84) Etats contractants désignés:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Etats d'extension désignés:
AL LT LV MK RO SI

(30) Priorité: **10.11.2000 FR 0014468**

(71) Demandeurs:
- **Briault, Jules Amédée Adéodat**
  75013 Paris (FR)
- **Tartiere, Patrick Roland Gabriel**
  94880 Noiseau (FR)

(72) Inventeurs:
- **Briault, Jules Amédée Adéodat**
  75013 Paris (FR)
- **Tartiere, Patrick Roland Gabriel**
  94880 Noiseau (FR)

(74) Mandataire: **Rinuy, Santarelli**
14, avenue de la Grande Armée,
B.P. 237
75822 Paris Cédex 17 (FR)

(54) Procédé et dispositif de filtrage de l'accès à une zone surveillée

(57) Le filtrage de l'accès à une zone surveillée, notamment un lieu public, est effectué par application d'un critère d'accès, et comporte les étapes suivantes :

- on analyse un document censé être une pièce d'identité du candidat à l'accès et on y saisit optiquement exclusivement des données nécessaires à l'application du critère d'accès,
- on applique ce critère d'accès aux données saisies, par vérification de la non-conformité à une liste donnée,
- on autorise l'accès si ce critère d'accès est satisfait, par exemple par suppression temporaire d'un rayonnement infra-rouge, sinon on déclenche une alarme, et
- on supprime les données saisies.

De manière avantageuse, il y a en outre une étape d'impression de ticket, reproduisant les données auxquelles on a appliqué le critère d'accès.

Un tel filtrage peut s'appliquer à l'entrée des casinos, par comparaison de l'identité à la liste des interdits de jeux.

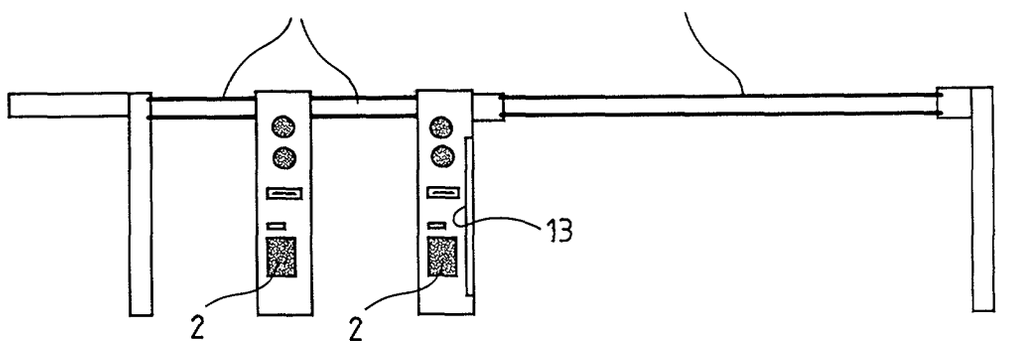


Fig. 2

EP 1 223 564 A1

Description

[0001] L'invention concerne le contrôle de l'accès à certaines zones ou lieux publics, tels que les casinos, soumis à certaines conditions ou restrictions d'accès.

[0002] Ainsi qu'on le sait, les casinos sont des lieux publics dont l'accès est interdit à certaines personnes, sur demande de celles-ci, de leurs proches ou du Ministre de l'Intérieur, en France. Ainsi les casinos doivent mettre en place un système de filtrage permettant de refouler les joueurs indésirables, sans toutefois dissuader les autres personnes d'entrer.

[0003] Il faut savoir que les casinos sont responsables de ce qui se déroule dans leurs locaux, par exemple les émotions intempestives en cas de succès (ou de perte), et doivent notamment payer les gros lots à tous les joueurs ayant gagné, indépendamment de savoir s'ils sont « interdits » ou non.

[0004] Il existe donc un besoin de filtrer l'accès à de tels endroits, d'une manière permettant de refouler les personnes « interdites» d'une manière telle qu'il soit possible de prouver, si ces personnes réussissent à entrer, que cela résulte d'un comportement frauduleux, sans pour autant rebuter les autres visiteurs.

[0005] Le besoin de contrôler l'accès à des zones données est un problème classique, bien résolu lorsqu'il s'agit de ne laisser passer que des personnes habilitées : il suffit de leur délivrer un badge, et de conditionner le passage à la présentation d'une manière appropriée de celui-ci. Il est à noter qu'il s'agit de lieux privés.

[0006] Mais l'accès à un lieu public tel qu'un casino répond à des contraintes très différentes, dans la mesure où il ne s'agit pas de laisser entrer des personnes faisant partie d'une liste préétablie, mais au contraire de refouler des personnes faisant partie d'une telle liste préétablie ; en outre, alors que ce paramètre n'a aucune importance dans le cas où l'accès est réservé à quelques personnes préidentifiées, l'accès à des zones telles que des casinos doit rester aussi attrayant que possible aux personnes non inscrites sur la liste des « interdits », c'est à dire que l'accès doit rester facile pour les personnes « normales » dont on ne sait rien a priori, et dont il est par exemple exclu de demander la présentation d'un badge.

[0007] L'invention a pour objet de répondre à cet objectif, en se fondant sur la simple présentation d'une pièce d'identité (il est normalement admis qu'il ne peut rien être demandé de plus).

[0008] L'invention propose à cet effet un procédé de filtrage d'accès à une zone surveillée, notamment un lieu public, par application d'un critère d'accès selon lequel :

- on analyse un document censé être une pièce d'identité du candidat à l'accès et on y saisit optiquement, sélectivement des données nécessaires à l'application du critère d'accès,
- on applique ce critère d'accès aux données saisies, ce critère étant la non conformité des données saisies sur le document présenté à des données d'une base de données concernant des personnes interdites d'accès,
- on autorise l'accès si ce critère d'accès est satisfait, sinon on déclenche une alarme, et
- on supprime les données saisies.

[0009] Il faut noter que l'invention ne prévoit rien en cas de présentation de fausse pièce d'identité. Cela peut paraître un vice rédhibitoire, dissuadant l'homme de métier de s'intéresser à la solution de l'invention : pourtant cette absence de contrôle n'empêche pas qu'il y ait, selon l'invention, contrôle de l'identité de chaque personne à l'intérieur de l'enceinte de sorte que, en cas de problème à l'intérieur de celle-ci (problème de comportement, incident de santé, ou gain d'un gros lot dans le cas d'un casino) les responsables locaux puissent invoquer que l'entrée n'a pu se faire que par manoeuvre frauduleuse et que leur responsabilité n'est pas engagée, n'étant soumis qu'à une obligation de moyens et non pas à une obligation de résultat.

[0010] Il est à noter que cette absence de contrôle de l'authenticité de la pièce d'identité permet d'entrer avec une simple photocopie d'une de ses pièces d'identité authentiques. En outre, cette absence de contrôle d'authenticité permet que le contrôle d'accès puisse être appliqué à chacun(e) avec un temps de traitement supportable.

[0011] Selon des dispositions préférées de l'invention, éventuellement combinées :

- Avant de saisir les données nécessaires à l'application du critère d'accès, il est avantageusement prévu d'identifier le type de pièce d'identité auquel appartient le document présenté, ce qui permet de ne pas avoir de contrainte quant au document à présenter (selon les habitudes de chacun, c'est la carte d'identité ou le passeport, voire un permis de conduire qui sera présenté).
- L'étape d'identification du type de pièce d'identité comporte par exemple la recherche dans le document présenté d'une caractéristique de chacun de plusieurs types de pièces d'identité présélectionnés (qu'il s'agisse du format, ou de signes particuliers), et on saisit les données dans une zone choisie en fonction du type de pièce d'identité ainsi reconnu. Les types de pièces d'identité présélectionnés comportent avantageusement la carte d'identité, le permis de conduire et le passeport. De manière préférée, les types de pièces d'identité présélectionnés comportent en France, l'ancien et le nouveau type de carte d'identité.
- De manière tout à fait avantageuse, lorsque le critère d'accès est satisfait on imprime un ticket comportant les données ayant servi à l'application du critère d'accès. Cela a le gros avantage, quoique le

dispositif ait supprimé toute trace des filtrages effectués, de pouvoir exiger de toute personne qu'elle prouve par la présentation de ce ticket qu'elle a passé de bonne foi le dispositif de filtrage.

- De manière préférée, l'on autorise le passage vers la zone surveillée, lorsque le critère d'accès est satisfait, par suppression d'une barrière de rayonnement infra-rouge, et on autorise tout passage depuis la zone surveillée vers l'extérieur. De la sorte seules les entrées sont filtrées tandis que les sorties sont libres, ce qui est important en cas d'urgence.
- De manière avantageuse, notamment pour des raisons de sécurité, l'on compte les entrées et les sorties (soit séparément, le nombre de personnes présentes étant la différence entre les entrées et les sorties, soit par un seul compteur qui augmente lors de chaque entrée et qui diminue lors de chaque sortie ; mais ce premier cas a l'avantage de donner des informations cumulées, par exemple sur la journée).

[0012] L'invention propose en outre un dispositif de filtrage de l'accès à une zone surveillée comportant un dispositif central de traitement, un dispositif d'acquisition numérique capable de saisir une image d'un document censé être une pièce d'identité, un dispositif de reconnaissance de caractères adapté à saisir des données dans l'image saisie par le dispositif d'acquisition numérique, une zone contenant les éléments constitutifs d'un critère d'accès qui sont des données d'identification de personnes interdites d'accès, le critère d'accès étant satisfait lorsque les données saisies sur le document ne sont pas conformes à ces données d'identification, un dispositif d'accès à ouverture commandée, le dispositif central étant adapté à appliquer le critère d'accès aux données saisies par le dispositif de reconnaissance de caractères et, si le critère est satisfait, à commander l'ouverture du dispositif d'accès, sinon à déclencher une alarme, puis à supprimer les données saisies, le dispositif de reconnaissance de caractère étant conçu en sorte de ne saisir que des données nécessaires au critère d'accès.

[0013] Selon des dispositions préférées de l'invention, par analogie à ce qui a été dit à propos du procédé :

- Le dispositif central est de préférence en outre adapté à faire reconnaître par le dispositif de reconnaissance de caractères le type de document d'identité auquel appartient le document scruté par le dispositif de balayage. Le dispositif de reconnaissance de caractères est de préférence adapté à reconnaître au moins une carte d'identité, un permis de conduire, et un passeport. De manière encore plus préférée, le dispositif de reconnaissance de caractères est en outre adapté à reconnaître l'ancien et le nouveau type de carte d'identité.
- Selon une caractéristique particulièrement avantageuse de l'invention, il y a en outre un dispositif d'impression de ticket, le dispositif central étant adapté à déclencher ce dispositif lorsque le critère d'accès est satisfait, en faisant imprimer les données saisies sur le document.
- Le dispositif d'accès à ouverture commandée comporte avantageusement une barrière de rayonnement infra-rouge qui est supprimée lorsque le critère d'accès est satisfait. De manière également préférée, ce dispositif d'accès comporte en outre une barrière de rayonnement infra-rouge à double faisceau, adaptée à déclencher une alarme lorsqu'un passage a lieu dans le sens de l'entrée, et à ne déclencher aucune alarme lorsqu'un passage a lieu dans le sens de la sortie. En pratique, pour favoriser des entrées multiples, réduisant ainsi toute gêne pour les candidats à l'accès, il y a de préférence plusieurs dispositifs d'accès chacun muni d'un dispositif d'acquisition numérique connecté au dispositif central.
- Ainsi que cela a été dit à propos du procédé de l'invention, pour des raisons de sécurité notamment, le dispositif central est avantageusement conçu en sorte de pouvoir compter les entrées et les sorties dans la zone surveillée.
- Le dispositif d'acquisition numérique peut être un dispositif de balayage au scanner, ou tout autre élément numérique tel que caméra, etc...
- Une caméra, par exemple numérique, peut être ajoutée pour, par exemple, prendre une image du candidat à l'accès pour, notamment, la comparer à la photo de la pièce d'identité.

[0014] Des objets, avantages et caractéristiques de l'invention ressortent de la description qui suit, donnée à titre d'exemple illustratif non limitatif, en regard des dessins annexés sur lesquels :

* la figure 1 est un schéma matériel synoptique d'un dispositif de filtrage selon l'invention,
* la figure 2 est une vue de dessus du système d'accès de ce dispositif de filtrage,
* la figure 3 est une vue de face de ce système d'accès,
* la figure 4 est une vue schématique de la vitre de lecture du dispositif de balayage du dispositif de filtrage,
* la figure 5 est un schéma fonctionnel synoptique du dispositif de filtrage,
* la figure 6 est un schéma de la partie « analyse d'identité » du schéma de la figure 5,
* la figure 7 est une vue de dessus d'un exemple de ticket de passage, et
* la figure 8 est une vue de derrière de ce ticket de passage.

[0015] Les figure 1 à 8 décrivent conjointement un dispositif de filtrage adapté à contrôler l'accès à une zone, notamment un lieu public, tel que la zone de jeu d'un

casino, en fonction de la comparaison de données sélectivement prélevées sur un document censé être une pièce d'identité à une base de données relative à des personnes interdites d'accès.

[0016] Ce dispositif est, dans l'exemple considéré, capable de saisir des données sur plusieurs types de pièces d'identité possibles, d'émettre des tickets de passage témoignant du passage par le dispositif de filtrage et de suivre la fréquentation de l'endroit (notamment nombre de personnes présentes à tout instant considéré, par comptage des entrées ainsi que des entrées, voire mémorisation des nombres en fonction du moment de la journée et élaboration de statistiques de fréquentation).

[0017] Mais il faut comprendre qu'il s'agit d'une version particulièrement performante de dispositif selon l'invention.

[0018] Ainsi que cela ressort de la figure 1 ce dispositif comporte

- un dispositif central 1de traitement,
- un dispositif 2 d'acquisition numérique, ici du type scanner (en variante, il peut s'agir d'une caméra),
- un dispositif 3 de reconnaissance de caractères, ou OCR,
- une base de données 4,
- un dispositif 5 d'impression de ticket,
- un dispositif 6 d'accès à ouverture commandée, avantageusement franchissable dans les deux sens,
- un dispositif 7 de surveillance des accès,
- une télécommande 8.

[0019] Le dispositif central de traitement 1 est le coeur du dispositif de filtrage et communique avec tous les autres éléments, qui sont logiciels ou matériels pour en coordonner les interventions. Il comporte des éléments de démarrage, non détaillés.

[0020] Le dispositif 2 d'acquisition numérique (ici un scanner) est un dispositif matériel connu en soi qui sert à la lecture, d'une manière appropriée, la pièce d'identité que doit présenter tout candidat à l'accès. C'est un dispositif de numérisation de documents au moyen de capteurs optiques. Il génère un fichier du document numérisé.

[0021] Le dispositif 3 de reconnaissance de caractères est un dispositif logiciel connu en soi qui permet de convertir tout ou partie d'une image en caractères ASCII, caractères utilisables ultérieurement par un traitement de texte ; selon l'invention il est utilisé pour saisir exclusivement les caractères dont la combinaison est nécessaire à une comparaison aux données saisies dans les listes d'interdits (en pratique le nom, les prénoms, la date et le lieu de naissance).

[0022] La base de données 4 est un élément logiciel (fichier informatique) contenant toutes les données identifiant les personnes « interdites d'accès ».

[0023] Le dispositif 5 d'impression de ticket est un élément matériel de tout type connu approprié, comprenant une imprimante (non représentée) permettant l'impression d'un ticket destiné à être pris par toute personne autorisée à entrer et à permettre à celle-ci de prouver, sur toute demande du personnel du casino, qu'elle est entrée de manière régulière : ce ticket peut être exigé, par exemple en combinaison avec la pièce d'identité présentée à l'entrée, en préalable à tout versement de gain.

[0024] Le dispositif 6 d'accès à ouverture commandée comporte les éléments matériels déterminant les passages d'entrée et de sortie du dispositif de filtrage.

[0025] Ce dispositif 6 est représenté aux figures 2 et 3. Dans cet exemple de réalisation, la communication de la zone surveillée avec l'extérieur se fait par l'une de deux voies étroites formant portillon, désignées par la référence 11 ou par une voie de grande largeur 12. Chacune de ces voies est munie d'une barrière à rayonnement infra-rouge (il y a de préférence deux rayons décalés horizontalement, voir ci-dessous) ; le dispositif représenté ne comporte donc pas de barrière matérielle, susceptible de gêner la sortie en cas d'urgence. Sur un côté de chaque portillon se trouvent successivement la fenêtre du dispositif d'acquisition numérique 2 constitué d'un scanner, la sortie d'un dispositif 5 d'impression de ticket et des voyants, par exemple vert et rouge, visualisant le résultat du filtrage (passage autorisé ou non). Lorsque le passage est autorisé, la barrière de rayonnement infra-rouge est momentanément désactivée de manière à laisser passer la personne qui vient d'être autorisée. Un franchissement intempestif des barrières 11 ou 12 depuis l'extérieur déclenche une alarme sonore, tandis qu'un franchissement depuis l'intérieur vers l'extérieur est en permanence autorisé, ce qui explique que les barrières 11 soient des barrières d'entrée tandis que la barrière 12 est appelée barrière de sortie. Il peut y avoir une vitre 13 entre les barrières d'entrée et la barrière de sortie.

[0026] Le dispositif 7 de surveillance des accès permet la surveillance, le comptage, l'analyse des gens entrant et sortant de la zone en considération, ainsi que les personnes présentes dans cette zone à un instant donné, ce qui permet de réagir en fonction des normes de sécurité. Il permet aussi, couplé aux caisses, de déterminer le taux de transformation par tranches horaires.

[0027] En pratique, le dispositif de filtrage est secondé par un ou plusieurs vigiles pour pouvoir réagir lors d'un franchissement intempestif des accès ou lors d'une vérification d'identité.

[0028] En variante non représentée, il y a en outre une caméra permettant la prise en photo, de préférence numérique, de chaque candidat à l'accès, par exemple en vue d'une comparaison éventuelle à la photo que comporte la pièce d'identité, par exemple par l'un des vigiles précités de façon automatique.

[0029] La télécommande 8 permet, lorsqu'elle est activée, de couper temporairement le faisceau des barriè-

res, permettant ainsi l'entrée dans la zone sous surveillance sans contrôle d'identité. Une telle télécommande est par exemple à la disposition du directeur du Casino, aux fonctionnaires de la police des jeux ainsi qu'à tout employé en ayant reçu autorisation pour une quelconque raison. Cette télécommande peut être à rayonnement infra-rouge ou du type radio (des détecteurs correspondants étant prévus sur les éléments délimitant les barrières.

[0030] Le dispositif représenté est conçu pour permettre la saisie sélective de paramètres d'identification du candidat au passage sur plusieurs types de pièces d'identité, par exemple :

* la carte d'identité selon le nouveau format,
* la carte d'identité selon l'ancien format (tant que celui-ci est en usage),
* le passeport (il est à noter que cette pièce est d'un format unique pour tous les ressortissants de l'Union Européenne, de sorte que le dispositif n'est pas limité aux citoyens français), et
* le permis de conduire.

[0031] Dans la mesure où les formats de ces pièces ne sont pas identiques, il peut y avoir une règle de présentation de la pièce soumise par le candidat au passage sur la vitre du scanner, au moins aussi grande que la plus grande de ces pièces d'identité ; à titre d'exemple (voir la figure 4) la pièce doit être présentée avec le bord supérieur longeant le bord supérieur de la vitre le coin supérieur droit occupant le coin supérieur droit de la vitre. En variante, il peut y avoir reconnaissance du format indépendamment du sens de présentation du document.

[0032] Le fonctionnement du dispositif est schématisé à la figure 5. On suppose bien entendu que le démarrage du dispositif a déjà eu lieu.

[0033] Lorsqu'un franchissement est tenté par les barrières d'entrée (partie gauche du schéma), le dispositif détecte d'abord le sens de franchissement (ce qui est permis par la présence de deux rayonnements décalés horizontalement dans les barrières 11 et 12). Si le sens de franchissement est vers la sortie, quoique les barrières 11 soient en principe destinées à l'entrée, aucune réaction n'est déclenchée, si ce n'est que le comptage des sorties est incrémenté. Si par contre le sens est celui de l'entrée, le circuit central de traitement vérifie s'il est en configuration de service (c'est à dire que la fonction de gestion d'identité est en service) ; si cela n'est pas le cas, il déclenche un éventuel signal lumineux et incrémente un compteur d'entrée ; si par contre il est en mode de gestion d'identité, il teste le résultat d'une analyse d'identité.

[0034] Une telle analyse est décrite plus en détail à la figure 6.

[0035] Elle commence par une phase de démarrage, déclenchée par exemple par l'apposition d'un document sur la vitre du scanner (ou en regard d'un autre dispositif d'acquisition numérique utilisé) ou par l'enfoncement par le candidat au passage d'un bouton de démarrage.

[0036] Elle se poursuit par un balayage du document présenté sur la vitre du scanner, avec numérisation puis mémorisation/acquisition de la totalité du document. Le fichier mémorisé est traité par le dispositif OCR pour, en un premier temps, reconnaître le type de document.

[0037] Cette reconnaissance peut se faire par reconnaissance du format du document (en effet, les quatre types de documents cités ci-dessus ont des formats différents) ; toutefois, il est aussi possible de reconnaître le type de document à partir de caractéristiques spécifiques de chacun de ces types de documents (à partir de la position de la photo ou de la signature par rapport au coin supérieur droit, ou par reconnaissance d'une empreinte digitale sur les anciennes cartes d'identité, par la présence du sigle REPUBLIQUE FRANCAISE au début de la carte d'identité de nouvelle génération, des chiffres devant les nom et prénoms dans le permis de conduire, ou par la présence des numéros d'un passeport).

[0038] C'est ensuite, après que le format de la pièce d'identité a été identifié, que l'on saisit, exclusivement, les caractères à comparer avec les données stockés dans la base de données 4, en pratique le nom du porteur, ses prénoms, sa date de naissance et le lieu de cette naissance. Aucune autre indication, non comparable avec les données de cette base, n'est saisie à ce stade.

[0039] En d'autres termes, il y a une phase de reconnaissance du type de pièce d'identité au cours de laquelle seules des informations générales caractéristiques du type de pièce d'identité sont saisies, suivie d'une phase où il y a saisie d'une partie seulement des informations spécifiques du porteur de la pièce considérée.

[0040] En effet, à partir de la connaissance du format (c'est à dire du type) de la pièce d'identité, il est possible de déterminer où se trouvent les données précitées, et il n'y a saisie de caractères que dans ces zones préidentifiées. Cela garantit qu'aucune donnée confidentielle, non utile, n'est saisie, et permet une grande rapidité de traitement, puisqu'il n'y a saisie que d'une partie des caractères apparaissant sur la pièce d'identité.

[0041] Ensuite, par interrogation de la base de données et comparaison du fichier texte constitué à partir des caractères saisis au contenu de celle-ci, le dispositif de filtrage est en mesure de décider si (voir à nouveau la figure 5) s'il y a concordance entre la chaîne de caractères et un ensemble de données de la base relatif à une personne « interdite d'accès ».

[0042] S'il y a concordance, ce qui signifie que l'accès doit être refusé au porteur de la pièce d'identité analysée, un signal est émis, par exemple sonore et/ou lumineux indiquant au porteur que l'accès lui est interdit et alertant le vigile à proximité de manière qu'il puisse vérifier que ce porteur n'essaye pas de forcer le passage. Toutes les données saisies par le dispositif d'analyse

d'identité sont supprimées et l'opération de filtrage est terminée.

[0043] Le critère d'accès peut en outre comporter le contrôle d'âge (majorité ?) du candidat à l'accès.

[0044] En variante non représentée, il peut être prévu une conservation des données de ce candidat refusé et éventuelle incrémentation du compteur général (dans ce cas, on compte le nombre de candidats à l'accès) ou d'un compteur spécifique (nombre de candidats refusés).

[0045] S'il n'y a pas concordance, ce qui signifie qu'il n'y a aucune raison d'interdire l'accès au porteur, une opération d'impression de ticket est déclenchée, avec une sous-opération de vérification que le porteur prend bien ce ticket (un voyant est avantageusement allumé tant que ce ticket n'est pas pris : les rayons infra-rouge de la barrière 11 concernée sont interrompus lorsqu'il est détecté que le ticket a été pris, le compteur des entrées est incrémenté, toutes les informations saisies lors de l'analyse d'identité sont supprimées et l'opération de filtrage est terminée.

[0046] Si la procédure d'analyse d'identité ne peut conclure (parce que la format de la pièce d'identité n'est pas reconnu), un signal est émis, par exemple uniquement lumineux ou plus discrètement vers un dispositif porté par le vigile posté à proximité pour que celui-ci puisse trancher lui-même sur la possibilité de laisser passer le porteur de la pièce d'identité non reconnue.

[0047] Si par contre il y a tentative de franchissement de la barrière 12, s'il est détecté que ce n'est pas dans le sens de la sortie, il y a déclenchement d'une alerte, à moins qu'il y ait eu au préalable une désactivation par la télécommande ayant eu pour effet de couper le faisceau infra-rouge ; il y a avantageusement incrémentation du nombre des entrées avant retour à l'état de veille (case « gestion des accès » en haut de la figure).

[0048] Si par contre il est détecté que la tentative de franchissement se fait dans le sens de la sortie il y simplement incrémentation du nombre des sorties.

[0049] Bien entendu toutes les sous-opérations mentionnées ci-dessus ne sont pas nécessaires. Ainsi il est envisageable de ne pas prévoir de télécommande, même si cela apparaît être un élément facilitant l'emploi du système par la direction du casino. De même il peut ne pas y avoir d'impression de ticket, quoique celui-ci soit un moyen commode pour le casino de subordonner le paiement de tout gain à la présentation de ce ticket ; en outre celui-ci permet à ce casino de faire la preuve de ce qu'il a satisfait à son obligation de moyens pour empêcher les « interdits de jeu » d'accéder aux zones de jeu (toute personne ne pouvant pas présenter son ticket d'entrée peut être présumé être entré en fraude). Il est par ailleurs clair que la présence de compteurs n'est qu'une option permettant de suivre la fréquentation de la zone surveillée (il peut bien sûr n'y avoir qu'un seul compteur incrémenté lors de chaque entrée et décrémenté lors de chaque sortie, quoique l'on perde alors toute information sur le total des entrées).

[0050] Par ailleurs, lorsqu'il est possible d'exiger que la pièce d'identité soit d'un type donné, aucune phase préalable de reconnaissance de type de pièce d'identité n'est nécessaire, de sorte qu'il peut être possible dans ce cas de limiter la scrutation de la pièce d'identité présentée sur la scanner à la zone de ce document contenant les données nécessaires à la comparaison des données de la base de données.

[0051] Pourtant il est à noter que quelle que soit la configuration adoptée, le dispositif de l'invention ne gêne en aucune manière une éventuelle évacuation d'urgence de la zone surveillée (au contraire, si le comptage des sorties est assez performant, il peut même être possible de s'assurer que personne n'est resté dans la zone).

[0052] Pour assurer le respect des règles en ce qui concerne le respect des libertés individuelles, il peut y avoir une partie du système qui est scellée par les autorités des jeux, ce qui peut rassurer les joueurs soucieux de ne pas laisser de trace lors de leur passage.

[0053] Un exemple de ticket est donné aux figures 7 et 8. On y voit, par exemple la date, voire l'heure d'entrée et un numéro d'entrée. Selon une disposition particulièrement avantageuse de l'invention, il y a en outre une reproduction des données saisies sur la pièce d'identité soumise à l'analyse. Cela permet de contrôler ces données lors du paiement de gains, au vu de la pièce d'identité présentée à ce moment. Il peut y avoir en outre rappel de passages pertinents du Règlement Intérieur, notamment en ce qui concerne l'obligation de présenter ce ticket.

[0054] Ainsi, selon un aspect de l'invention, indépendant de la comparaison à une liste de personnes interdites d'accès, il y a un filtrage d'accès selon lequel :

- on analyse un document censé être une pièce d'identité, et on saisit exclusivement les données nécessaires à une opération de discrimination selon un critère d'accès,
- on applique cette opération de discrimination et, si le critère d'accès est satisfait on édite un ticket visualisant ces données saisies et on autorise le passage, et si le critère n'est pas satisfait on déclenche une alarme, et
- on supprime toutes les informations saisies.

[0055] Un tel filtrage s'applique non seulement au filtrage de l'accès à des casinos en fonction de la non-appartenance à une liste d'interdits, mais aussi à d'autres lieux, par exemple des lieux interdits aux mineurs (le critère de discrimination étant la comparaison de l'âge au seuil de 18 ans), toute personne à l'intérieur des lieux étant tenue de pouvoir montrer son ticket sur la moindre demande de responsables de ces lieux et prouver sa cohérence avec une pièce d'identité (pas nécessairement la même que celle ayant servi au filtrage, mais contenant les mêmes données que celles ayant servi à ce filtrage.

[0056] La description qui précède a mentionné un scanner 2 en tant que dispositif d'acquisition numérique. D'autres dispositifs sont possibles, tels qu'une caméra numérique couplée à un logiciel de reconnaissance adapté par exemple à reconnaître le type de document par comparaison à une bibliothèque d'images de référence. Le choix d'une telle caméra numérique peut permettre une acquisition bien plus rapide qu'avec un dispositif à balayage.

Revendications

1. Procédé de filtrage d'accès à une zone surveillée, notamment un lieu public, par application d'un critère d'accès selon lequel :

   - on analyse un document censé être une pièce d'identité du candidat à l'accès et on y saisit optiquement, exclusivement des données nécessaires à l'application du critère d'accès,
   - on applique ce critère d'accès aux données saisies, ce critère est la non conformité des données saisies sur le document présenté à des données d'une base de données concernant des personnes interdites d'accès,
   - on autorise l'accès si ce critère d'accès est satisfait, sinon on déclenche une alarme, et
   - on supprime les données saisies.

2. Procédé selon la revendication 1, **caractérisé en ce que**, avant de saisir les données nécessaires à l'application du critère d'accès, on identifie le type de pièce d'identité auquel appartient le document présenté.

3. Procédé selon la revendication 2, **caractérisé en ce que** l'identification du type de pièce d'identité comporte la reconnaissance de son format parmi ceux de plusieurs types de pièces présélectionnés.

4. Procédé selon la revendication 2 ou la revendication 3, **caractérisé en ce que** l'étape d'identification du type de pièce d'identité comporte la recherche dans le document présenté d'une caractéristique de chacun de plusieurs types de pièces d'identité présélectionnés, et on saisit les données dans une zone choisie en fonction du type de pièce d'identité ainsi reconnu.

5. Procédé selon la revendication 3 ou la revendication 4, **caractérisé en ce que** les types de pièces d'identité présélectionnés comportent la carte d'identité, le permis de conduire et le passeport.

6. Procédé selon la revendication 5, **caractérisé en ce que** les types de pièces d'identité présélectionnés comportent l'ancien et le nouveau type de carte d'identité.

7. Procédé selon l'une quelconque des revendications 1 à 6, **caractérisé en ce que** lorsque le critère d'accès est satisfait on imprime un ticket comportant les données ayant servi à l'application du critère d'accès.

8. Procédé selon l'une quelconque des revendications 1 à 7, **caractérisé en ce que** l'on autorise le passage vers la zone surveillée, lorsque le critère d'accès est satisfait, par suppression d'une barrière de rayonnement infra-rouge, et on autorise tout passage depuis la zone surveillée vers l'extérieur.

9. Procédé selon l'une quelconque des revendications 1 à 8, **caractérisé en ce qu'**on saisit les données au moyen d'une caméra numérique.

10. Procédé selon l'une quelconque des revendications 1 à 9, **caractérisé en ce que** l'on compte les entrées et les sorties.

11. Dispositif de filtrage de l'accès à une zone surveillée notamment lieu public, comportant un dispositif central (1) de traitement, un dispositif (2) d'acquisition numérique capable de saisir une image d'un document censé être une pièce d'identité, un dispositif de reconnaissance de caractères adapté à saisir des données dans l'image saisie par le dispositif d'acquisition numérique, une zone contenant les éléments constitutifs d'un critère d'accès, lesquels sont des données d'identification de personnes interdites d'accès, le critère d'accès étant satisfait lorsque les données saisies sur le document ne sont pas conformes à ces données d'identification, un dispositif d'accès à ouverture commandée, le dispositif central étant adapté à appliquer le critère d'accès aux données saisies par le dispositif de reconnaissance de caractères et, si le critère est satisfait, à commander l'ouverture du dispositif d'accès, sinon à déclencher une alarme, puis à supprimer les données saisies, le dispositif de reconnaissance de caractère étant conçu en sorte de ne saisir que des données nécessaires au critère d'accès.

12. Dispositif selon la revendication 11, **caractérisé en ce que** le dispositif central est en outre adapté à faire reconnaître par le dispositif de reconnaissance de caractères le type de document d'identité auquel appartient le document scruté par le dispositif de balayage.

13. Dispositif selon la revendication 11 ou la revendication 12, **caractérisé en ce que** le dispositif central est en outre adapté à faire reconnaître par le dispositif d'acquisition numérique le format auquel appar-

tient le document.

14. Dispositif selon la revendication 12, **caractérisé en ce que** le dispositif d'acquisition numérique ou le dispositif de reconnaissance de caractères est adapté à reconnaître au moins une carte d'identité, un permis de conduire, et un passeport.

15. Dispositif selon la revendication 14, **caractérisé en ce que** le dispositif d'acquisition numérique ou le dispositif de reconnaissance de caractères est en outre adapté à reconnaître l'ancien et le nouveau type de carte d'identité française.

16. Dispositif selon l'une quelconque des revendications 11 à 15, **caractérisé en ce qu'**il comporte en outre un dispositif (5) d'impression de ticket, le dispositif central étant adapté à déclencher ce dispositif lorsque le critère d'accès est satisfait, en faisant imprimer les données saisies sur le document.

17. Dispositif selon l'une quelconque des revendications 11 à 16, **caractérisé en ce que** le dispositif (6, 11, 12) d'accès à ouverture commandée comporte une barrière de rayonnement infra-rouge qui est supprimée lorsque le critère d'accès est satisfait.

18. Dispositif selon la revendication 17, **caractérisé en ce qu'**il comporte en outre une barrière de rayonnement infra-rouge à double faisceau, adaptée à déclencher une alarme lorsqu'un passage a lieu dans le sens de l'entrée, et à ne déclencher aucune alarme lorsqu'un passage a lieu dans le sens de la sortie.

19. Dispositif selon l'une quelconque des revendications 11 à 18, **caractérisé en ce qu'**il y a plusieurs dispositifs d'accès (6, 11) chacun muni d'un dispositif d'acquisition numérique connectée au dispositif central.

20. Dispositif selon l'une quelconque des revendications 11 à 18, **caractérisé en ce** le dispositif d'acquisition numérique est une caméra numérique.

21. Dispositif selon l'une quelconque des revendications 11 à 20, **caractérisé en ce que** le dispositif central est adapté à compter les entrées et les sorties dans la zone surveillée.

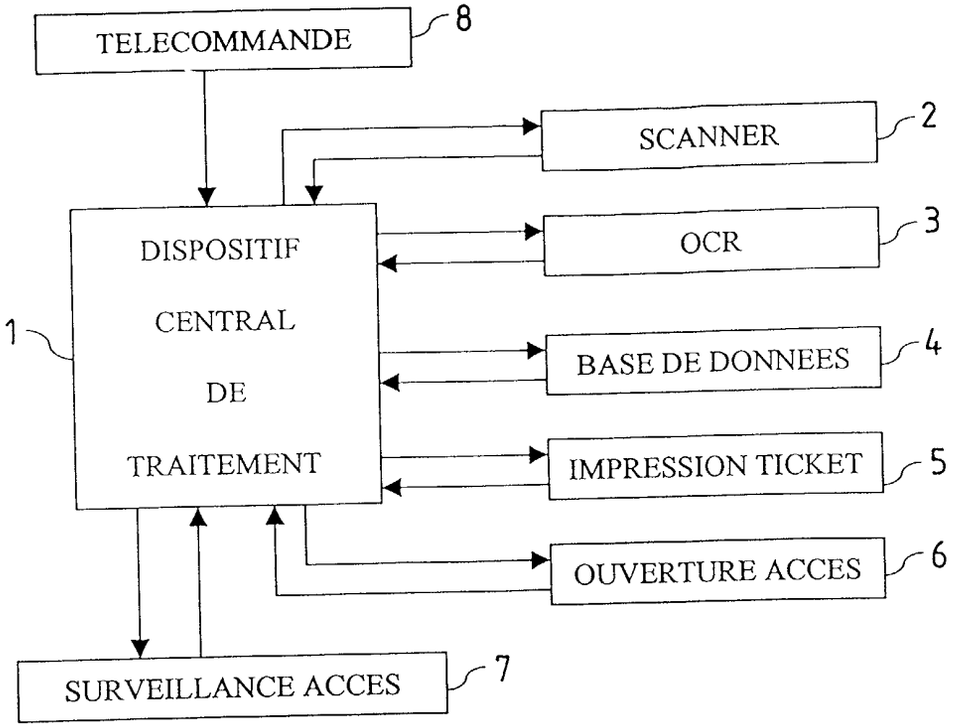

TELECOMMANDE
8
SCANNER
2
DISPOSITIF
CENTRAL
DE
TRAITEMENT
1
OCR
3
BASE DE DONNEES
4
IMPRESSION TICKET
5
OUVERTURE ACCES
6
SURVEILLANCE ACCES
7

Fig. 1

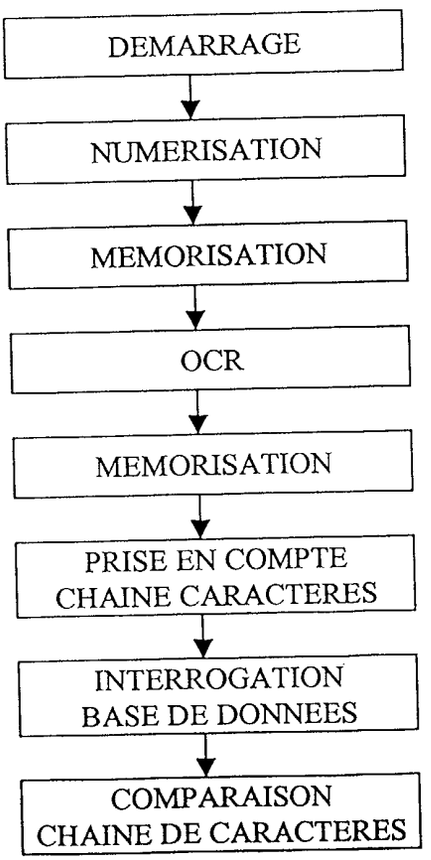

DEMARRAGE
NUMERISATION
MEMORISATION
OCR
MEMORISATION
PRISE EN COMPTE
CHAINE CARACTERES
INTERROGATION
BASE DE DONNEES
COMPARAISON
CHAINE DE CARACTERES

Fig. 6

Fig. 2

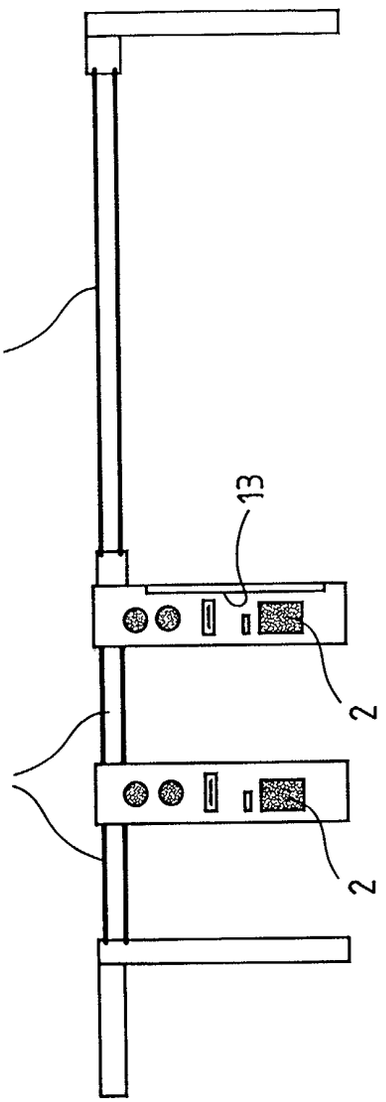
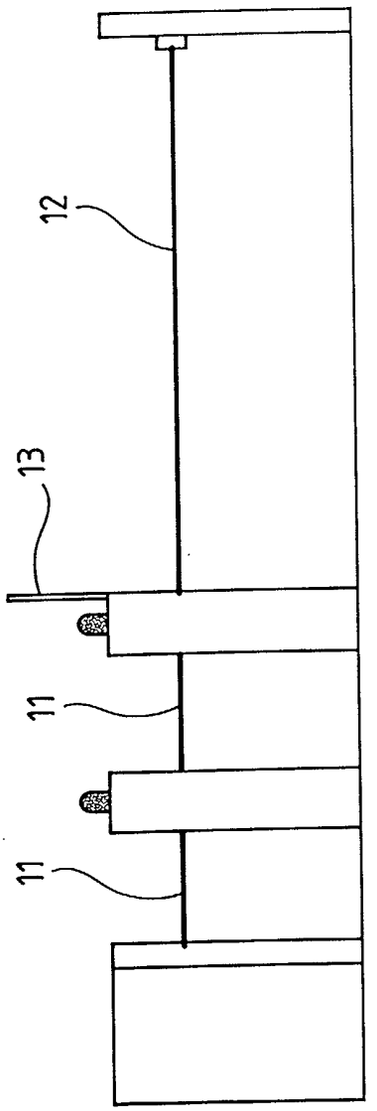


Fig. 3



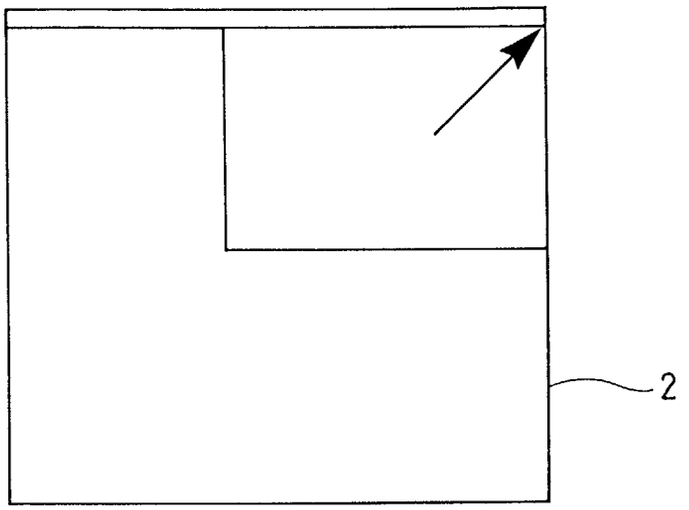


Fig. 4

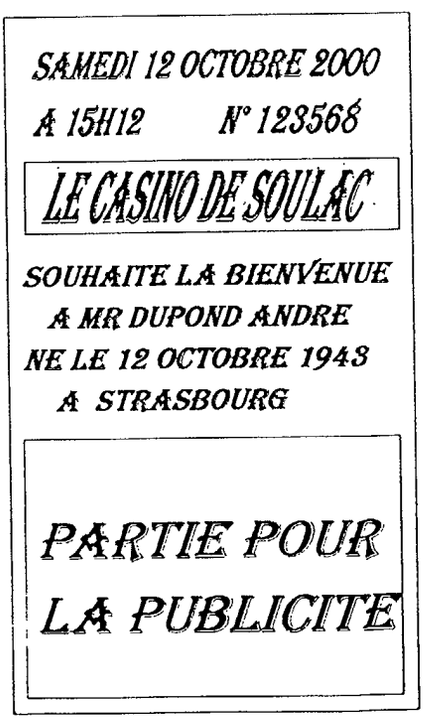


Fig. 7

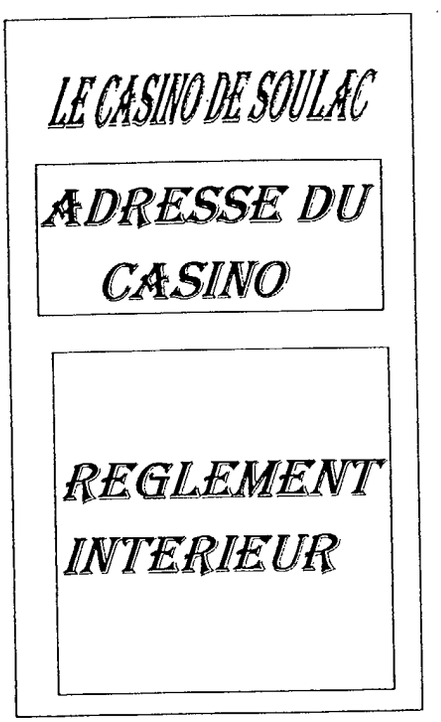


Fig. 8

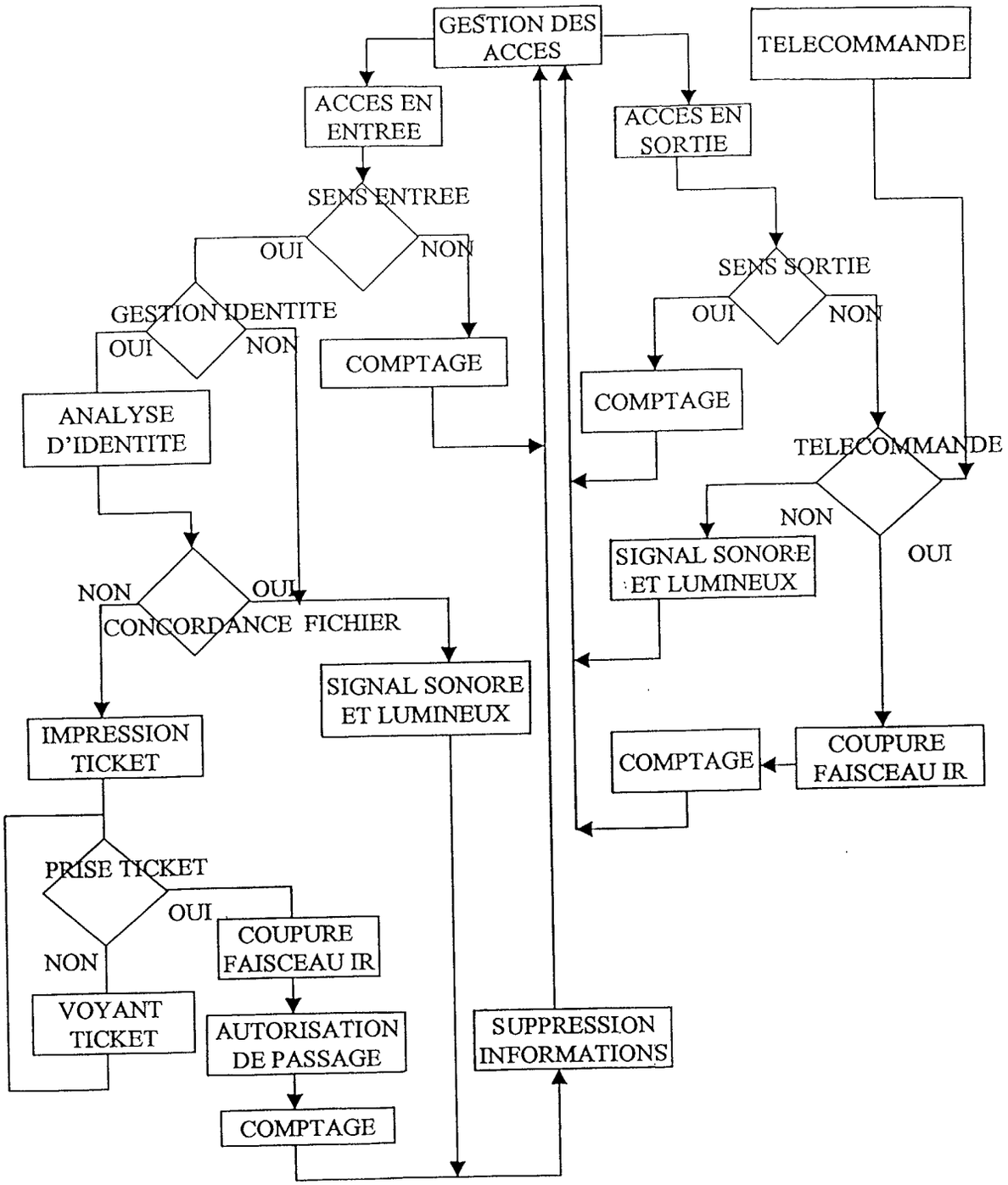

GESTION DES ACCES
TELECOMMANDE
ACCES EN ENTREE
ACCES EN SORTIE
SENS ENTREE
OUI
NON
SENS SORTIE
OUI
NON
GESTION IDENTITE
OUI
NON
COMPTAGE
COMPTAGE
ANALYSE D'IDENTITE
TELECOMMANDE
NON
OUI
SIGNAL SONORE ET LUMINEUX
NON
OUI
CONCORDANCE FICHIER
SIGNAL SONORE ET LUMINEUX
IMPRESSION TICKET
COMPTAGE
COUPURE FAISCEAU IR
PRISE TICKET
OUI
NON
COUPURE FAISCEAU IR
VOYANT TICKET
AUTORISATION DE PASSAGE
SUPPRESSION INFORMATIONS
COMPTAGE

Fig. 5

Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande
EP 01 40 2850

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (Int.Cl.7)
X	WO 00 31691 A (RITTER RUDOLF ;SWISSCOM AG (CH)) 2 juin 2000 (2000-06-02) * abrégé * * page 2, ligne 7 - page 5, ligne 8 * * page 8, ligne 23 - page 13, ligne 3 *	1,2,7,8, 11,12, 16-19	G07F7/08
X Y	US 5 864 623 A (COHEN TODD ET AL) 26 janvier 1999 (1999-01-26) * le document en entier *	1,2,9, 11,12,20 3-5,13, 14	
Y	WO 00 10141 A (SHIN MIN CHUL) 24 février 2000 (2000-02-24) * abrégé * * page 5, ligne 1 - page 6, ligne 11 *	3-5,13, 14	
A	US 5 103 079 A (BARAKAI SIMON ET AL) 7 avril 1992 (1992-04-07) * abrégé * * colonne 1, ligne 1 - colonne 2, ligne 48 *	1,11	
			DOMAINES TECHNIQUES RECHERCHES (Int.Cl.7) G07C G07F

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
LA HAYE	2 avril 2002	Teutloff, H

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)

ANNEXE AU RAPPORT DE RECHERCHE EUROPEENNE RELATIF A LA DEMANDE DE BREVET EUROPEEN NO. EP 01 40 2850

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.

02-04-2002

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 0031691 A	02-06-2000	WO 0031691 A1	02-06-2000
		AU 1139399 A	13-06-2000
US 5864623 A	26-01-1999	CA 2219098 A1	24-04-1999
WO 0010141 A	24-02-2000	US 6196460 B1	06-03-2001
		AU 5486999 A	06-03-2000
		BR 9913007 A	08-05-2001
		CN 1312932 T	12-09-2001
		EP 1112556 A1	04-07-2001
		NO 20010716 A	06-04-2001
		WO 0010141 A1	24-02-2000
US 5103079 A	07-04-1992	FR 2633411 A1	29-12-1989
		DE 68909126 D1	21-10-1993
		DE 68909126 T2	13-01-1994
		EP 0349413 A1	03-01-1990
		ES 2046506 T3	01-02-1994

EPO FORM P0460

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