(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 634 570**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **88 09959**

(51) Int Cl⁵ : G 06 K 9/62.

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 22 juillet 1988.

(30) **Priorité :**

(43) **Date de la mise à disposition du public de la demande :** BOPI « Brevets » n° 4 du 26 janvier 1990.

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *Renaud REITTER, Catherine ANDRE et Marie Josèphe REVILLET.* — FR.

(72) **Inventeur(s) :** Renaud Reitter ; Catherine Andre ; Marie-Josèphe Revillet.

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

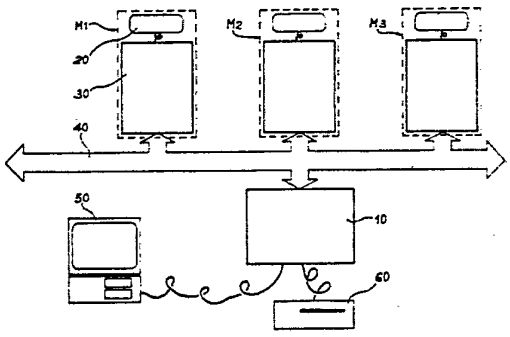
(74) **Mandataire(s) :** Brevatome.

(54) Système d'authentification multibiométrique.

(57) Système d'authentification biométrique.

Le système de l'invention comprend un organe central 10 et des modules d'authentification M1, M2, M3 utilisant des caractères biométriques différents. Ces modules sont mis en œuvre par l'organe central selon l'authentification à effectuer.

Application au contrôle d'accès.



FR 2 634 570 - A1

Vente des fascicules à l'IMPRIMERIE NATIONALE, 27, rue de la Convention — 75732 PARIS CEDEX 15

DESCRIPTION

SYSTEME D'AUTHENTIFICATION MULTI-BIOMETRIQUE

La présente invention a pour objet un système d'authentification multi-biométrique.

Elle trouve une application dans la mise en oeuvre de procédures de contrôle d'accès. Par "contrôle d'accès", on désigne aussi bien un contrôle d'accès physique (accès à un laboratoire, un établissement, une salle, etc.) qu'un contrôle d'accès à un système informatique ou à des données informatiques.

Lors d'un contrôle d'accès biométrique, on exige de l'usager qu'il présente un caractère biométrique, lequel est authentifié par un système approprié. Ce caractère biométrique peut être la voix, les empreintes digitales, la signature manuscrite, le fond de l'oeil, la forme de la main, etc. Les informations saisies par un capteur approprié sont comparées à une référence et le résultat de la comparaison permet d'autoriser ou de refuser l'accès demandé. La référence est préalablement mémorisée soit dans une carte à mémoire détenue par l'utilisateur, soit dans une base de données reliée au système.

Il existe de nombreux systèmes d'authentification biométrique utilisant l'un ou l'autre des caractères précités. Le fonctionnement de ces systèmes repose sur le test d'un seul caractère biométrique ; ce test est très souvent associé à la vérification d'un code confidentiel.

Si, pour des raisons accidentelles (aphonie, dégradation momentanée de l'empreinte digitale, infection oculaire, blessure au poignet...), l'usager n'est pas dans des conditions normales pour subir une authentification, il se trouve rejeté, même s'il est de bonne

foi. En outre, pour certains systèmes, l'usager doit se prêter aux contraintes apportées par la vérification d'un code confidentiel.

L'unicité du paramètre d'authentification implique, pour le confort de l'usager et la sécurité de l'accès, des taux d'erreur très faibles pour le système de reconnaissance. Il en résulte des temps d'exécution longs et un côut élevé du fait de la grande complexité des logiciels et des capteurs.

Le but de l'invention est justement de remédier à ces inconvénients. A cette fin, l'invention propose de combiner plusieurs moyens d'authentification biométrique mettant en oeuvre des caractères biométriques différents, ces moyens étant sous la commande d'un organe central de contrôle et de gestion.

En raison de la multiplicité des moyens possibles d'authentification, le système de l'invention échappe aux nuisances extérieures (bruit ambiant dans le cas de l'authentification vocale, atmosphère hostile, produits salissants, humidité, pour les autres moyens d'authentification) qui risquent de gêner son fonctionnement puisque l'organe central peut sélectionner celui des moyens d'authentification qui échappe auxdites nuisances sans qu'il soit nécessaire de modifier la structure du système.

Le système de l'invention permet également d'adapter le moyen d'authentification retenu à l'usager, d'après la stabilité de ses caractères biométriques.

La combinaison des moyens d'authentification permet aussi de hiérarchiser les accès et de gérer le degré de sécurité suivant les niveaux d'accès. Une authentification basée sur un ensemble de caractères biométriques autorise l'accès au niveau de sécurité le plus élevé, alors qu'une authentification basée sur un caractère unique autorise l'accès au niveau

de sécurité le plus faible.

Selon une autre variante de mise en oeuvre il est possible d'augmenter le degré de sécurité en laissant à l'organe central l'initiative du choix du test biométrique à opérer, ce choix étant déterminé par un mécanisme aléatoire, l'usager devant naturellement posséder des références pour chaque type d'authentification, dans l'incertitude du caractère qui sera choisi.

On comprend ainsi que le système de l'invention ne se contente pas de juxtaposer des systèmes d'authentification différents mais qu'il combine, à travers l'organe central, différents moyens d'authentification. De cette combinaison découlent des fonctions nouvelles (affranchissement vis-à-vis des nuisances extérieures, hiérarchisation des contrôles, choix aléatoire, etc...) et des résultats nouveaux et avantageux (abaissement du coût, modularité, souplesse, fiabilité).

De façon plus précise, la présente invention a pour objet un système d'authentification biométrique caractérisé par le fait qu'il comprend :

- un organe central de contrôle et de gestion,
- plusieurs modules d'authentification biométrique aptes à effectuer chacun un test d'authentification à l'aide d'un caractère biométrique déterminé, ce caractère étant différent d'un module à l'autre,
- un moyen de liaison entre l'organe central et les différents modules, cet organe central étant apte à commander la mise en oeuvre d'au moins un des modules et de recueillir le résultat du test effectué par chaque module mis en oeuvre.

De toute façon, les caractéristiques de l'invention apparaîtront mieux à la lumière de la description qui va suivre. Cette description porte sur des exemples de réalisation donnés à titre explicatif et

nullement limitatif et elle se réfère à des dessins annexés, sur lesquels :

- la figure 1 montre l'architecture du système de l'invention,
- la figure 2 illustre un exemple d'adaptation du système à des niveaux d'accès hiérarchisés,
- la figure 3 montre un module d'authentification à empreintes digitales.

La figure 1 se réfère à un mode de réalisation utilisant des cartes électroniques. Il va de soi que l'invention n'est pas limitée à cette technique même si elle semble, à l'heure actuelle, la plus avantageuse.

L'architecture de la figure 1 montre :

- une carte mère 10 constituant un organe central de contrôle et de gestion ; cette carte comprend un microprocesseur, par exemple du type 68000 de MOTOROLA, une mémoire de programme, une mémoire de travail et des liaisons série ;
- divers modules M1, M2, M3, etc... d'authentification biométrique, comprenant chacun un capteur 20 et une carte spécifique de traitement 30 ;
- un bus 40, par exemple du type VME commercialisé par la Société MOTOROLA ;
- divers organes comme un ordinateur hôte 50 et un lecteur de carte à mémoire 60.

Le fonctionnement de ce système est le suivant.

Le système est articulé autour de la carte mère comportant le microprocesseur. Cette carte assure la coordination des différentes cartes qui lui sont reliées par l'intermédiaire du bus et la gestion des échanges avec l'extérieur.

Les fonctions propres au mode d'authentification utilisé sont regroupées sur la carte prévue à cet effet, afin d'assurer la modularité de l'ensemble.

Les calculs les plus complexes sont effectués sur cette carte, à l'aide de circuits spécialisés (corrélateur, processeur de traitement de signal, etc.). Des calculs plus élémentaires peuvent être traités par le microprocesseur de la carte mère.

Il n'existe a priori aucune hiérarchie fonctionnelle entre les différentes cartes qui constituent le système de l'invention. La position des cartes spécifiques sur le bus est indifférente. Le choix de cette architecture renforce la modularité du système et permettra d'y adapter tous les développements futurs (nouveaux moyens d'authentification, utilisation de processeurs ou d'algorithmes plus performants, etc.).

Le dialogue système-utilisateur s'effectue par exemple par l'intermédiaire d'un écran à cristaux liquides et de touches de fonctions reliées à la carte mère.

Différentes références peuvent être stockées dans une carte à mémoire. Dans ce cas, le lecteur de carte 60 est intégré au système.

Les liaisons séries situées sur la carte mère permettent de communiquer avec l'ordinateur hôte.

Il est possible d'envisager plusieurs modes de fonctionnement du système suivant le niveau de sécurité choisi :

a) Dans le cas d'un accès à un seul niveau de sécurité, le système peut, de façon aléatoire, choisir un moyen d'authentification pour lequel l'usager possède une référence. En cas d'échec de l'authentification, le système peut soit autoriser un nouvel essai avec le même moyen, soit en choisir un autre.

b) Dans le cas d'un accès à plusieurs niveaux de sécurité (cas par exemple d'un système informatique dans lequel on distingue une partie accessible à tout utilisateur et une autre réservée aux responsables

du système) une combinaison de différents moyens d'authentification permet de hiérarchiser les accès.

Cette dernière variante est illustrée sur la figure 2 :

- pour l'accès au premier niveau N1, un seul paramètre est testé à l'aide d'un module M1,
- pour l'accès au deuxième niveau N2, un test supplémentaire est effectué par le module M2,
- et ainsi de suite.

L'usager, pour avoir accès au niveau de sécurité le plus élevé (N3) devra passer avec succès les tests des niveaux inférieurs (N1, N2).

Il est également possible d'associer le niveau de sécurité le plus faible au moyen d'authentification le moins performant.

Quel que soit le mode de fonctionnement choisi, pour chaque type d'authentification, l'information est issue d'un capteur adapté au caractère biométrique choisi. Cette information est transférée sur la carte et traitée par celle-ci, qui opère en liaison avec la carte mère.

On peut décrire trois types d'authentification, lesquels sont, du reste, de type connu :

a. Authentification par empreintes digitales :

La figure 3 montre la structure du module d'authentification utilisé. Il comprend trois éléments : un capteur optique 20, une carte d'acquisition et de numérisation 30/1 et une carte de corrélation 30/2.

Le capteur 20 a fait l'objet d'une demande de brevet français N° EN/88 02803 du 4 Mars 1988.

L'image de l'empreinte est obtenue de la façon suivante : l'utilisateur place son index 21 sur un prisme 23 de section triangulaire droite, éclairé en parallèle par un système 26 sur l'une de ses faces carrées. L'image latente est transportée par le faisceau

émergeant de l'autre face carrée du prisme, dévié par réflexion totale sur le prisme 24. Cette image est formée par un objectif spécial 27 sur le plan d'une matrice 29 du type dispositif à couplage de charges (CCD).

Après saisie par un circuit 31, l'image est numérisée mise sous forme binaire par le circuit 32 puis stockée dans une mémoire rapide 34, appelée mémoire image, sur la carte de corrélation 30/2.

La référence de l'usager est transférée de la carte à mémoire ou de la base de données vers une mémoire appelée mémoire de référence 35. Cette mémoire représente la partie la plus significative de l'empreinte.

Un circuit 36 effectue la corrélation entre les données de la mémoire image et celles de la mémoire de référence.

Les résultats de la corrélation sont envoyés au microprocesseur 68000 de la carte mère par le bus 40. Ces résultats valident ou non l'authentification.

Une carte vidéo optionnelle permet de contrôler sur un moniteur vidéo la saisie de l'empreinte digitale.

b. Authentification par la voix :

L'authentification de la voix est actuellement basée sur la reconnaissance d'un mot de passe. Elle ne nécessite qu'une seule carte spécifique, de type connu.

Le signal vocal est capté par un microphone puis mis en forme sur une carte afin d'y être échantillonné et numérisé. Les informations résultant de la conversation sont transmises à un processeur de traitement de signal (par exemple DSP 56000 de MOTOROLA), qui possède ses propres mémoires de travail et de pro-

gramme. Ce processeur extrait les paramètres du signal vocal qui servent à la comparaison avec la référence. Le résultat de la comparaison est transmis à la carte mère.

L'utilisation du processeur de traitement de signal peut être étendue à la synthèse de la parole, ce qui améliore ainsi la convivialité du système.

c. Authentification par la signature manuscrite :

L'authentification par signature manuscrite ne nécessite pas de carte spécifique. L'usager dépose sa signature sur une tablette à numériser, à l'aide d'un stylo spécial relié à la tablette. Une liaison série assure le transfert des données à la carte mère (position, vitesse, accélération).

Le microprocesseur situé sur la carte mètre effectue l'analyse des paramètres dynamiques calculés à partir des informations issues de la tablette. En fonction des résultats obtenus il valide ou non l'authentification.

REVENDICATIONS

1. Système d'authentification multi-biométrique caractérisé par le fait qu'il comprend :

- un organe central (10) de contrôle et de gestion,
- plusieurs modules (M1, M2, M3) d'authentification biométrique aptes à effectuer chacun un test d'authentification à l'aide d'un caractère biométrique déterminé, ce caractère étant différent d'un module à l'autre,
- un moyen de liaison (40) entre l'organe central (10) et les différents modules (M1, M2, M3), cet organe central étant apte à commander la mise en oeuvre d'au moins un des modules, de recueillir le résultat du test effectué par chaque module mis en oeuvre et de combiner les résultats obtenus.

2. Système selon la revendication 1, caractérisé par le fait que les caractères biométriques utilisés sont pris dans le groupe qui comprend notamment la voix, les empreintes digitales, la signature manuscrite, le fond de l'oeil, la forme de la main.

3. Système selon la revendication 1, caractérisé par le fait que l'organe central (10) de contrôle et de gestion est apte à choisir de manière aléatoire la mise en oeuvre d'un module d'authentification (M1, M2, M3).

4. Système selon la revendication 1, caractérisé par le fait que l'organe central (10) de contrôle et de gestion est apte à hiérarchiser la mise en oeuvre des modules d'authentification, un premier module (M1) étant mis en oeuvre pour un premier test, un deuxième module (M2) n'étant mis en oeuvre que si le premier test a été passé avec succès et ainsi de suite.

5. Système selon la revendication 1, caractérisé par le fait que l'organe central de contrôle et de gestion est constitué par une carte électronique comprenant un microprocesseur, une mémoire de programme, une mémoire de travail et des liaisons série.

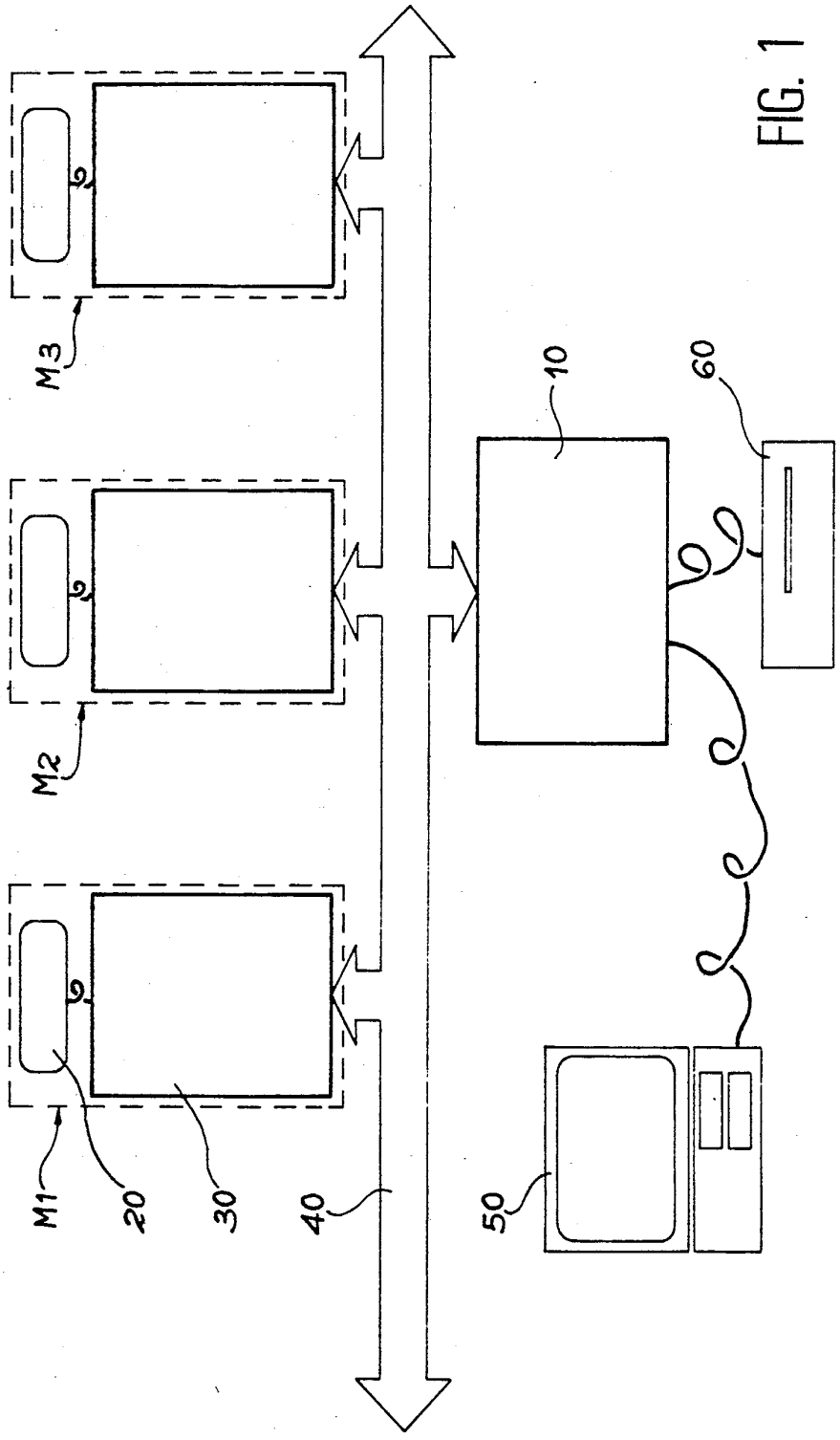


FIG. 1

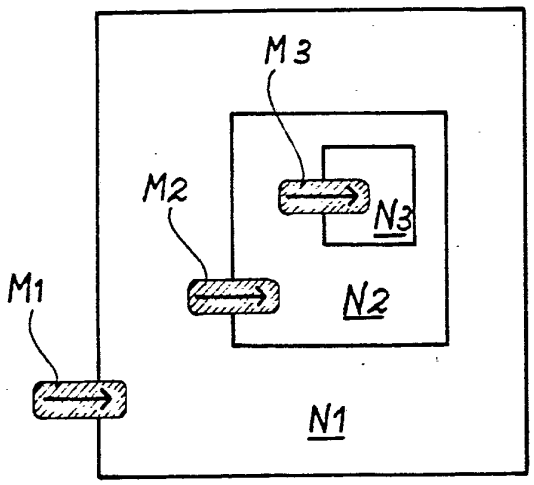


FIG. 2

FIG. 3

