(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
19 janvier 2012 (19.01.2012)

PCT

(10) Numéro de publication internationale
WO 2012/007668 Al

(51) Classification internationale des brevets :
G06N 5/02 (2006.01)

(21) Numéro de la demande internationale :
PCT/FR201 1/05 1520

(22) Date de dépôt international :
29 juin 201 1 (29.06.201 1)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
10 55665 12 juillet 2010 (12.07.2010) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **MORPHO** [FR/FR]; 27 rue Leblanc, F-75015 Paris (FR).

(72) Inventeur; et
(75) Inventeur/Déposant *(pour US seulement)* : **CHABANNE, Hervé** [FR/FR]; c/o Morpho, 27 rue Leblanc, F-75015 Paris (FR).

(74) Mandataires : ATTALI, Pascal et al; Cabinet Plasseraud, 52 rue de la Victoire, F-75440 Paris Cedex 09 (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclarations en vertu de la règle 4.17 :

— *relative à la qualité d'inventeur (règle 4.1 7.iv))*

Publiée :

— *avec rapport de recherche internationale (Art. 21(3))*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues (règle 48.2.h))*

(54) Title : METHODS, SYSTEMS AND DEVICES FOR BIOMETRIC VERIFICATION

(54) Titre : PROCEDES, SYSTEMES ET DISPOSITIFS DE VERIFICATION BIOMETRIQUE

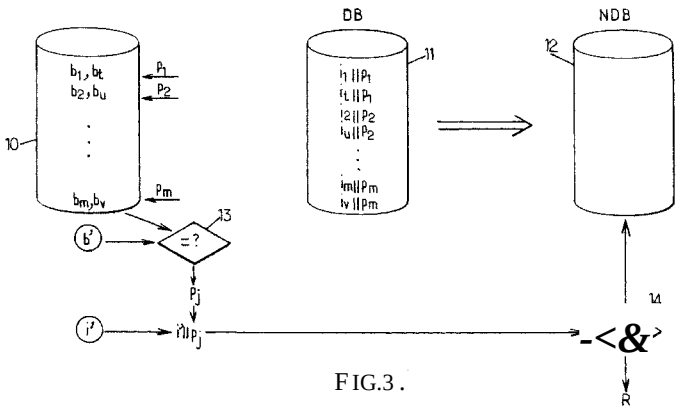

FIG.3 .

(57) Abstract : The invention relates to a method for constructing a négative identity database relating to persons for the purpose of biométrie vérification, said négative identity database being correlated with a biométrie database (10) storing groups of biométrie data (b_1, b_2,..., b_m) relating to said persons. The method includes: obtaining a respective identity datum (i_1,i_2, - · -,i_m) relating to each of said persons; creating an association between each obtained identity datum relating to a respective person, and a pointer (pi,p_2,...,p_m) directed to a group stored in the biométrie database that includes a biométrie datum relating to said respective person; and constructing a négative identity database (12) from the set matching the set of created associations.

(57) Abrégé :

[Suite sur la page suivante]

WO 2012/007668 A1

Procédé de construction d'une base de données d'identité négative relative à des individus à des fins de vérification biométrique en relation avec une base de données biométrique (10) stockant des groupes de données biométriques (bi, b_2,..., b_m) relatives auxdits individus. Le procédé comprend : l'obtention d'une donnée d'identité (i_1,i_2, - · ',im) respective relativement à chacun desdits individus; la réalisation d'une association entre chaque donnée d'identité obtenue relativement à un individu respectif et un pointeur (pi,p_2,...,p_m) désignant un groupe stocké dans la base de données biométrique qui inclut une donnée biométrique relative audit individu respectif; et la construction d'une base de données d'identité négative (12) à partir de l'ensemble complémentaire de l'ensemble des associations réalisées.

PROCEDES, SYSTEMES ET DISPOSITIFS DE VERIFICATION BIOMETRIQUE

La présente invention concerne la vérification biométrique.

La vérification biométrique s'entend traditionnellement de l'authentification ou de l'identification d'individus, humains ou animaux, à partir de données biométriques, relatives à des caractéristiques d'un ou plusieurs attributs biologiques de ces individus, comme les minuties d'empreintes digitales, une forme générale de doigts de la main, les veines d'une main ou d'un doigt, des caractéristiques de la voix, des caractéristiques de l'iris de l'œil, etc.

Une telle vérification biométrique utilise conventionnellement une base de données stockant des données biométriques relatives à des individus ayant préalablement fait l'objet d'une phase d'inscription dite "enrôlement" pour se voir délivrer, lors d'une vérification biométrique, un droit quelconque (délivrance d'un permis de conduire, d'un titre de transport, d'une indemnisation, autorisation d'accès à un local, etc.).

Un exemple très simple de vérification biométrique est illustré sur la figure **1,** où l'on distingue une base de données **1** stockant un ensemble de données biométriques b_1, b_2,..., b_N relatives à des individus enrôlés.

Ces données biométriques b_1, b_2, ..., b_N sont par exemple des images représentant tel ou tel attribut biologique d'individus respectifs (par exemple des images d'empreintes digitales, d'iris, etc.), des caractéristiques relatives à un attribut biologique (par exemple un type, une position et une orientation de minuties dans le cas d'empreintes digitales), ou autre.

Avantageusement, une représentation numérique des données biométriques peut être utilisée, de façon à en simplifier la manipulation et à rendre ces données intégrables dans un algorithme cryptographique.

A titre d'exemple non limitatif, les données biométriques b_1, b_2,..., b_N stockées dans la base de données **1** peuvent consister chacune en un vecteur numérique, par exemple binaire. De nombreuses façons d'obtenir un vecteur numérique à partir d'informations biométriques sont connues.

Dans l'exemple de la figure 1, la vérification biométrique se passe de la manière suivante relativement à un individu donné. On obtient une donnée biométrique b', par exemple dans sa représentation sous forme de vecteur numérique, de l'individu considéré. Cette donnée b' est comparée à tout ou partie des données $b_1, b_2, \ldots, b_N$ stockées dans la base de données 1 (référence 2).

En cas de concordance ou de proximité suffisante, on peut en déduire que l'individu considéré correspond à un individu enrôlé (cas d'une identification) ou à l'individu enrôlé qu'il prétend être (cas d'une authentification). Ce résultat est noté R sur la figure 1.

La base de données biométrique 1 est parfois reliée à une base de données d'identité d'individus (par exemple sous forme alphanumérique). C'est notamment le cas, dans un scénario d'authentification, pour conclure qu'un individu est ou non l'individu enrôlé qu'il prétend être.

Un lien univoque (c'est-à-dire 1 pour 1) entre données biométriques et données d'identité stockées dans ces bases de données pourrait permettre au propriétaire de ces bases de connaître trop facilement la correspondance entre les deux types de données. Ceci peut constituer un problème lorsque ledit propriétaire n'est pas une personne de confiance, ou lorsque des contraintes, par exemple d'ordre législatif, interdisent cette situation. En outre, toute personne indélicate, autre que le propriétaire des bases de données, parvenant à accéder auxdites bases de données pourrait se servir de la correspondance entre les deux types de données pour usurper l'identité d'individus enrôlés.

Il est possible de protéger les données biométriques et/ou d'identité à l'aide d'un algorithme cryptographique, de façon à compliquer la tâche d'une telle personne indélicate. Mais, outre le fait de complexifier la vérification biométrique, cela ne protège pas les données contre le propriétaire des bases de données, car c'est généralement lui qui maîtrise l'algorithme cryptographique et en détient les clés.

Il a également été proposé d'utiliser un "lien faible" entre une base de données biométrique 1 et une base de données d'identité. Un tel lien faible ne permet pas d'établir une correspondance univoque entre données biométriques

et données d'identité. Mais il autorise tout de même une vérification biométrique avec un niveau de succès acceptable. La mise en place de cette technique de lien faible est cependant relativement complexe.

Un exemple schématique en est donné en référence à la figure 2. La base de données biométrique 3 stocke des groupes de plusieurs données biométriques. Dans l'exemple illustré, ces groupes sont constitués de deux éléments, bien qu'un plus grand nombre d'éléments soit tout-à-fait envisageable. De la même façon, la base de données d'identité 4 stocke des groupes de plusieurs données d'identité, en l'occurrence deux dans l'exemple de la figure 2. Le nombre de groupes et/ou d'éléments par groupe peut éventuellement différer entre la base de données biométrique 3 et la base de données d'identité 4.

Le lien l entre les deux bases de données 3 et 4 fait correspondre à chaque groupe de données biométriques, par exemple $(bi.b_t)$, un groupe respectif de données d'identité, par exemple (ii,i_t).

Une personne ayant accès aux bases de données 3 et 4, y compris leur propriétaire, ne peut pas retrouver, avec certitude et sans investigation supplémentaire, la correspondance entre une donnée biométrique et une donnée d'identité (mais seulement entre deux groupes).

Une vérification biométrique reste néanmoins possible. Ainsi, comme illustré sur la figure 2, si un individu avec une biométrie b' et une identité i' se présente pour une authentification par exemple, on vérifie la présence de b' dans la base de données biométrique 3 (étape 5), puis on retrouve le groupe de données d'identité (i_{α},ip) correspondant au groupe de données biométriques auquel b' appartient selon le lien faible l. Un résultat R peut alors être déduit d'une comparaison entre i' et les éléments du groupe $(i_{\alpha},i\beta)$. Si i' correspond à une des données d'identité i_{α} ou i_{β}, on peut par exemple conclure que l'individu est bien celui qu'il prétend être.

Le recours à un tel lien faible améliore donc la situation. Mais le problème redevient entier lorsque plusieurs bases de données biométrique et/ou d'identité sont utilisées en relation avec de mêmes individus, par exemple dans le cadre de plusieurs applications indépendantes. Dans ce cas en effet,

une intersection entre les groupes de données biométriques et/ou d'identité peut permettre de retrouver une correspondance entre certaines données biométriques et des données d'identité respectives.

Un but de la présente invention est de limiter une partie au moins des inconvénients des techniques antérieures décrites ci-dessus.

L'invention propose ainsi un procédé de construction d'une base de données d'identité négative relative à des individus à des fins de vérification biométrique en relation avec une base de données biométrique stockant des groupes de données biométriques relatives auxdits individus. Le procédé comprend les étapes suivantes :

- obtenir une donnée d'identité respective relativement à chacun desdits individus ;

- réaliser une association entre chaque donnée d'identité obtenue relativement à un individu respectif et un pointeur désignant un groupe stocké dans la base de données biométrique qui inclut une donnée biométrique relative audit individu respectif ; et

- construire une base de données d'identité négative à partir de l'ensemble complémentaire de l'ensemble des associations réalisées.

La génération d'une telle base de données négative permet un certain niveau de protection des données d'identité et de leur lien avec des données biométriques stockées dans la base de données biométrique.

Si les groupes de données biométriques stockées dans la base de données biométrique comprennent chacun plusieurs éléments, on bénéficie en plus d'une protection du type "lien faible" tel que mentionné plus haut. Pour autant, la protection des données d'identité conférée par la présente invention peut résister notamment à l'intersection de plusieurs bases de données qui seraient utilisées relativement à de mêmes individus, par exemple dans le cadre de plusieurs applications indépendantes.

En variante, la protection apportée intrinsèquement par l'usage d'une base de données négative peut permettre d'utiliser des groupes de données biométriques ne comportant qu'un seul élément.

Selon des modes de réalisation avantageux qui peuvent être combinés de toutes les manières envisageables :

- ladite association réalisée comprend une concaténation entre chaque donnée d'identité et le pointeur correspondant. Une telle association est particulièrement simple. Son obtention et son stockage sont peu consommateurs en capacité de calcul et de mémorisation ;

- ladite association réalisée consiste en une fonction secrète entre chaque donnée d'identité et le pointeur correspondant. On complique ainsi un peu plus l'identification de chacune de ces informations pour une personne ayant accès au contenu de la base de données d'identité négative ;

- la base de données d'identité négative est construite pour stocker ledit ensemble complémentaire sous une forme condensée. On complique ainsi un peu plus la tâche d'une personne ayant accès au contenu de la base de données d'identité négative ;

- la forme condensée dudit ensemble complémentaire est obtenue par application d'un algorithme de type préfixe ; et/ou

- la base de données d'identité négative est construite pour stocker ledit ensemble complémentaire sous une forme randomisée On complique ainsi un peu plus la tâche d'une personne ayant accès au contenu de la base de données d'identité négative pour retrouver des données d'identité et leur lien avec des données biométriques correspondantes.

L'invention propose aussi un système ou dispositif pour la construction d'une base de données d'identité relative à des individus à des fins de vérification biométrique en relation avec une base de données biométrique stockant des groupes de données biométriques relatives auxdits individus. Le système ou dispositif est apte à obtenir une donnée d'identité respective relativement à chacun desdits individus et comprend :

- une unité pour réaliser une association entre chaque donnée d'identité obtenue relativement à un individu respectif et un pointeur désignant un

groupe stocké dans la base de données biométrique qui inclut une donnée biométrique relative audit individu respectif ;

- une unité de construction d'une base de données d'identité négative à partir de l'ensemble complémentaire de l'ensemble des associations réalisées.

Ces unités peuvent être de toute forme envisageable, e.g. électronique et/ou informatique.

L'invention propose encore un procédé de vérification biométrique relativement à un individu, utilisant une base de données d'identité négative construite comme mentionné plus haut en relation avec une base de données biométrique stockant des groupes de données biométriques. Ce procédé de vérification biométrique comprend les étapes suivantes :

- obtenir une donnée biométrique relative audit individu ;

- retrouver un pointeur désignant un groupe stocké dans la base de données biométrique qui inclut une donnée biométrique correspondant à la donnée biométrique relative audit individu ;

- obtenir une donnée d'identité relative audit individu ;

- réaliser une association entre la donnée d'identité relative audit individu et ledit pointeur ;

- vérifier la présence ou l'absence de ladite association dans la base de données d'identité négative.

Avantageusement, la vérification biométrique comprend en outre la génération d'une conclusion en fonction d'un résultat de ladite vérification. Cette conclusion peut être générée dans un cas d'authentification et/ou d'identification.

L'invention propose également un système ou dispositif pour la mise en œuvre d'une vérification biométrique relativement à un individu telle que mentionnée ci-dessus. Ce système ou dispositif est apte à obtenir une donnée d'identité relative audit individu et comprend :

- une unité d'obtention d'une donnée biométrique relative audit individu ;

- une unité pour retrouver un pointeur désignant un groupe stocké dans la base de données biométrique qui inclut une donnée biométrique correspondant à la donnée biométrique relative audit individu ;

- une unité pour réaliser une association entre la donnée d'identité relative audit individu et ledit pointeur ;

- une unité de vérification de la présence ou de l'absence de ladite association dans la base de données d'identité négative.

Ces unités peuvent être de toute forme envisageable, e.g. électronique et/ou informatique.

D'autres particularités et avantages de la présente invention apparaîtront dans la description ci-après d'exemples de réalisation non limitatifs, en référence aux dessins annexés, dans lesquels :

- la figure 1, déjà commentée, est un schéma illustrant un exemple simple de vérification biométrique selon l'art antérieur ;
- la figure 2, déjà commentée, est un schéma illustrant un autre exemple simple de vérification biométrique selon l'art antérieur ;
- la figure 3 est un schéma illustrant une construction de base de données d'identité négative et une vérification biométrique selon un exemple non-limitatif de réalisation de l'invention ;
- la figure 4 est un schéma illustrant la notion de base de données négative.

Selon un premier aspect de l'invention, on construit une base de données d'identité relative à des individus à des fins de vérification biométrique. Cette construction peut être faite une fois pour toute, après enrôlement de tous les individus concernés, ou bien au fur et à mesure que de nouveaux individus font l'objet d'un enrôlement.

A cet effet, on obtient une donnée d'identité respective relativement à chaque individu. La donnée d'identité relative à l'individu a est notée i_a par la suite, a représentant un entier quelconque. La donnée d'identité peut être obtenue après que l'individu concerné a décliné son identité. Elle peut aussi être obtenue par consultation d'un document officiel (carte d'identité, passeport, permis de conduire, etc.), ou autre.

La donnée d'identité obtenue peut prendre n'importe quelle forme envisageable. Elle peut par exemple consister en une concaténation d'informations relatives audit individu, telles que son nom, son prénom, sa date de naissance, son numéro de sécurité sociale et/ou autre. Elle est avantageusement unique pour un individu donné, de façon à éviter toute ambiguïté. Son format peut par exemple être alphanumérique. Un format entièrement numérique est également possible. A titre d'exemple, la donnée d'identité peut résulter d'une binarisation d'informations d'identité, de manière à présenter un format binaire (série de 'O' et de '1').

La base de données d'identité négative dont la construction constitue le premier aspect de l'invention est destinée à être utilisée en relation avec une base de données biométrique. Cette dernière est éventuellement construite en même temps que la base de données d'identité négative, ou bien avant celle-ci. Elle stocke des groupes de données biométriques relatives à des individus.

Dans l'exemple de la figure 3, la base de données biométrique 10 utilisée stocke des groupes de deux données biométriques, à savoir (b_1,b_t), (b_2,b_u),. ..,(b_m,b_v), où b_a désigne une donnée biométrique relative à un individu a correspondant, a représentant un entier quelconque. On notera que les groupes pourraient comprendre un nombre de données biométriques supérieur à deux. Ce nombre pourrait d'ailleurs varier d'un groupe à un autre. Tout ou partie des groupes pourraient même ne comprendre qu'une seule donnée biométrique (on a dans ce cas un lien fort entre les deux types de données). On notera également que le nombre total de données biométriques stockées dans la base de données biométrique 10 peut correspondre ou non au nombre total de données d'identité destinées à être couvertes par la base de données d'identité.

Les données biométriques b_1, b_2,. . , b_m stockées dans la base de données biométrique 10 peuvent prendre toute forme envisageable. Il peut par exemple s'agir d'images représentant un attribut biologique (empreinte digitale, iris, réseau veineux, etc.). En variante ou en complément, il peut s'agir de caractéristiques relatives à un attribut biologique (par exemple un type, une position et une orientation de minuties dans le cas d'empreintes digitales), ou

autre. Ces données biométriques peuvent être acquises à l'aide d'un capteur biométrique approprié.

Dans un cas de figure avantageux, plusieurs données biométriques relatives à un même individu pourraient être stockées dans la base de données biométrique 10. Ces données biométriques pourraient se rapporter à des types de biométrie différents. A titre d'exemple non limitatif, une donnée biométrique relative à une empreinte digitale et une donnée biométrique relative à un iris pourraient être utilisées pour un même individu. Dans ce cas, les différentes données biométriques relatives à un même individu sont stockées dans un même groupe de données biométriques au sein de la base de données biométrique 10, de façon à ne pas permettre de retrouver trop facilement l'identité dudit individu par recoupement d'information. Autrement dit, certains au moins des groupes de données biométriques stockés dans la base de données biométrique 10 peuvent comprendre des données biométriques relatives à de mêmes individus et/ou à des individus différents.

De façon avantageuse, les données biométriques b_1, b_2,..., b_m sont stockées dans la base de données biométrique 10 sous la forme de vecteurs numériques, par exemple binaires.

Chaque groupe de données biométriques stocké dans la base de données biométrique 10 peut être identifié à l'aide d'un pointeur respectif. Ainsi, les groupes (bi,bt),(b2,b_u),.. .,(b_m,b_v) sont désignés respectivement par les pointeurs pi,p_2,...,p_m- Ces pointeurs pointent par exemple chacun vers une entrée de la base de données biométrique 10 où le groupe de données biométriques correspondant est stocké. Dans l'exemple non limitatif illustré sur la figure 3, chaque pointeur pointe vers une ligne de la base de données biométrique 10 où le groupe de données biométriques correspondant est stocké. Bien d'autres exemples de pointeurs peuvent être utilisés, comme cela apparaîtra à l'homme du métier.

Pour construire la base de données d'identité, on réalise une association entre chaque donnée d'identité obtenue i_1,î2, -.-,i_m et un pointeur pi.P2,...,Pm désignant un groupe stocké dans la base de données biométrique 10 qui inclut au moins une donnée biométrique relative à l'individu

correspondant. A titre d'exemple, une association est réalisée entre la donnée d'identité h (relative à l'individu 1) et le pointeur p_1 qui pointe vers le groupe (bi,b_t) stocké dans la base de données biométrique 10 et qui inclut la donnée biométrique b_1 (également relative à l'individu 1). De même, une association est réalisée entre la donnée d'identité i_t et le même pointeur p_1 qui pointe vers le groupe (bi,b_t), etc.

On notera que, bien que l'exemple de la figure 2 présente un même nombre m de données biométriques et de données d'identité, il pourrait en être différemment. Ce serait par exemple le cas si des leurres sont utilisés en tant que données biométriques et/ou données d'identité, de manière à rendre plus difficile la détection de correspondances entre données biométriques et données d'identité.

Dans un mode de réalisation avantageux, l'association entre une donnée d'identité i_a et un pointeur p_a correspondant comprend, voire consiste en une concaténation de ces deux paramètres, dans un ordre quelconque. Cette association peut donc s'écrire $i_a \,||\, p_a$, où le symbole $||$ désigne une concaténation (c'est-à-dire une mise bout à bout des champs qu'il sépare). Une représentation numérique, par exemple binaire, de $i_a \,||\, p_a$ peut avantageusement être utilisée, bien que toute autre représentation soit également envisageable. Comme illustré sur l'exemple de la figure 2, l'ensemble des associations réalisées pour l'ensemble des individus peut donc s'écrire $h \,||\, p_1$, $i_t \,||\, pi$, $i_2 \,||\, p2$, $i_u \,||\, P2, \ldots$, $i_m \,||\, pm$, $i_v \,||\, pm$.

En variante ou en complément, l'association entre une donnée d'identité i_a et un pointeur p_a correspondant pourrait comprendre, voire consister en n'importe quelle fonction f_a de i_a et de p_a, soit $f_a(i_a,p_a)$, telle qu'une somme, un produit ou autre. La fonction f_a en question pourrait d'ailleurs varier selon les individus a. Avantageusement, la ou les fonctions utilisées pourraient être secrètes, c'est-à-dire n'être connues que du responsable de la construction de la base de données d'identité. Ceci permet de rendre un peu plus difficile la tâche d'une personne indélicate qui, ayant accès aux valeurs $f_a(i_a,P_a)$, chercheraient à en déduire les données d'identité i_a.

Plutôt que de construire une base de données d'identité positive

regroupant l'ensemble des associations réalisées, comme la base de données 11 de la figure 2, on construit une base de données d'identité négative à partir de l'ensemble complémentaire de l'ensemble des associations réalisées.

La notion de base de données négative et des méthodes de construction d'une telle base de données sont connues, bien que dans des domaines techniques sans rapport avec la vérification biométrique. On peut par exemple citer l'article de Fernando Esponda, Elena S. Ackley, Stéphanie Forrest et Paul Helman de Septembre 2004, "On-line Négative Databases". Third International Conférence on Artificial Immune Systems (ICARIS 2004) Proceedings, pp. 175-1 88, ou encore l'article de Fernando Esponda intitulé "Everything That's Not Important", IEEE Computational Intelligence 3:2 (mai 2008).

La figure 4 illustre schématiquement la notion de base de données négative relativement à des vecteurs binaires de longueur 4. Ces vecteurs binaires sont représentés en haut de la figure 4 sous la forme d'un arbre 9 dont les branches supérieures correspondent aux bits de poids le plus fort et les branches inférieures correspondent aux bits de poids le plus faible.

Parmi l'ensemble des vecteurs binaires possibles, on considère le sous-ensemble consistant dans les cinq vecteurs binaires suivants : 0001, 0010, 0 110, 1100 et 1101. Les feuilles de l'arbre 9 correspondant à ces cinq vecteurs binaires sont marquées par des croix.

Une représentation positive des cinq vecteurs binaires dudit sous-ensemble pourrait éventuellement être stockée dans une base de données positive, telle que la base DB 7 qui apparaît en bas à gauche de la figure 4.

Une base de données négative NDB correspondante peut être construite en désignant les vecteurs binaires complémentaires dudit sous-ensemble, lesquels correspondent aux feuilles de l'arbre 9 non marquées d'une croix sur la figure 4.

La base de données négative NDB peut lister les vecteurs binaires complémentaires dudit sous-ensemble un à un, dans une représentation similaire à celle de la DB (i.e. 0000, 001 1, 0100, 0101, 0 111, 1000, 1001, 10 10, 101 1, 1110 et 1111).

En variante, la représentation des vecteurs binaires utilisée dans NDB peut avantageusement être une représentation condensée, ce qui limite l'espace de stockage nécessaire.

Dans la NDB 8 illustrée en bas à droite de la figure 4, la représentation adoptée a été obtenue à l'aide d'un algorithme de type préfixe. Cela signifie que les données stockées dans la NDB 8 ne font apparaître que les préfixes (c'est-à-dire les bits de poids les plus forts) des vecteurs binaires qui ne font pas partie dudit sous-ensemble, les bits de poids les plus faibles étant absents ou bien remplacés par un caractère, comme une étoile (*), qui indique que ces bits peuvent prendre la valeur 0 ou 1.

Un tel mode de représentation condensé est simple et peut être obtenu facilement par un parcours visuel de l'arbre 9.

Une méthode de construction d'une base de données négative à l'aide d'un algorithme préfixe a été formalisée par Esponda, Stéphanie Forrest et Paul Helman dans l'article "Enhancing Privacy through Négative Représentations of Data", UNM Computer Science Technical Report TR-CS-2004-18, de mars 2004.

Selon cette méthode, on désigne par l la longueur des vecteurs binaires du sous-ensemble considéré (c'est-à-dire les vecteurs binaires de longueur l qui seraient stockées dans une base de données positive), par w_i un préfixe de longueur i et par W_i un ensemble de vecteurs de longueur i (une partie des préfixes w_i).

Les étapes mises en œuvre par cette méthode sont les suivantes :

1. i := 0

2. W_i := {} (l'ensemble vide)

3. W_(i+1) := ensemble des vecteurs de longueur i+1 avec un préfixe de longueur i dans W_i et qui n'est pas un préfixe d'un vecteur du sous-ensemble considéré

4. pour tout x dans W_{i+1}

5. créer un vecteur y avec préfixe x et des étoiles (*) pour compléter en

un vecteur de longueur l (une étoile représente une position qui peut prendre la valeur 0 ou la valeur 1)

6. ajouter le champ à la base de données négative

7. i := i + 1

8. W_i := l'ensemble des préfixes de longueur i du sous-ensemble considéré

9. Retour à l'étape 3 tant que kl.

Une telle méthode conduit à une base de données négative de taille de l'ordre de (2*N*l^2) où N est le nombre de vecteurs binaires du sous-ensemble considéré (c'est-à-dire le nombre d'entrées d'une base de données positive correspondante).

On peut en outre avantageusement rendre aléatoire ("randomiser") la représentation pour augmenter la sécurité, en particulier à partir d'une version non déterministe de l'algorithme précédent. A cet effet, on peut par exemple utiliser une permutation aléatoire pour faire apparaître des étoiles au début ou au milieu des vecteurs, remplacer aléatoirement certaines étoiles par les valeurs associées 0,1 , ou autre.

Un exemple d'algorithme permettant de randomiser la représentation de la base de données négative est exposé dans l'article "Enhancing Privacy through Négative Représentations of Data", UNM Computer Science Technical Report TR-CS-2004-18, mars 2004, de Fernando Esponda, Stéphanie Forrest, et Paul Helman.

D'autres algorithmes de randomisation créant une base de données négative qui correspond à une représentation approximative du complémentaire d'une base de données positive peuvent bien sûr être utilisés, comme cela apparaîtra à l'homme du métier.

Par ailleurs, dans le cadre de la présente invention, toute autre méthode de construction d'une base de données négative peut être utilisée, en remplacement ou en complément d'un algorithme de type préfixe, comme cela apparaîtra à l'homme du métier.

On peut par exemple citer la méthode de construction d'une base de données négative basée sur l'utilisation de fonction de hachage cryptographique, telle que proposée dans l'article de George Danezis, Claudia Diaz, Sébastian Faust, Emilia Kàsper, Carmela Troncoso et Bart Preneel, "Efficient Négative Databases from Cryptographie Hash Functions", in Proceedings of the 10th Information Security Conférence (ISC 2007), LNCS, J. A. Garay (éd.), Springer-Verlag, 12 pages, 2007. On peut encore citer l'article de Fernando Esponda, Elena S. Ackley, Paul Helman, Haixia Jia et Stéphanie Forrest, "Protecting Data Privacy through Hard-to-Reverse Négative Databases", International Journal of Information Security (IJIS), Volume 6, Number 6, pp.403-415, Octobre 2007.

Si l'on est en présence de données non binaires, la construction d'une base de données négative pourra également tenir compte de ce fait.

L'usage d'une base de données négative présente plusieurs avantages, par rapport à celui d'une base de données positive classique.

Tout d'abord, retrouver les données positives à partir des données complémentaires stockées dans une base de données négative n'est pas une opération simple, surtout si le nombre de données considérées est conséquent et/ou si la représentation des données complémentaires est elle-même rendue complexe par une condensation, une randomisation, ou autre. Les données positives sont ainsi un peu mieux protégées que si elles étaient stockées directement dans une base de données positive.

De plus, le parcours d'une base de données négative peut être facilité et rendu plus naturel par rapport à celui d'une base de données positive. En effet, rechercher la présence d'une donnée dans une base de données positive nécessite de comparer cette donnée à chacune des données stockées, une à une. En revanche, détecter l'absence de cette même donnée dans une base de données négative peut nécessiter un nombre d'opérations plus faible pour obtenir le même résultat. Par exemple, lorsque la base de données négative a été construite avec un algorithme de type préfixe, il suffira de vérifier que la donnée en question ne possède pas un des préfixes apparaissant dans la base de données négative.

La présente invention tire profit de ces avantages des bases de données négatives pour permettre une vérification biométrique particulièrement pertinente.

Ainsi en référence à l'exemple de la figure 3, on peut déterminer l'ensemble complémentaire (le complément) de l'ensemble des associations réalisées telles que décrites plus haut, par exemple $i_1 || p_1$, it || Pi, i_2 |ı P2, i_u ıı p2..-., i_m ıı P_m, i_v || Pm- Et une base de données négative NDB 12 peut être construite à partir de cet ensemble complémentaire. La base de données négative NDB 12 peut par exemple stocker cet ensemble complémentaire, seul ou éventuellement accompagné d'autres données.

La forme prise par l'ensemble complémentaire dans la base de données négative NDB 12 peut être quelconque. Avantageusement, une forme condensée telle que décrite plus haut pourra être utilisée. Cette forme condensée peut être obtenue par application d'un algorithme de type préfixe ou tout autre algorithme envisageable.

En variante ou en complément, une randomisation de la représentation des données complémentaires telle que mentionnée plus haut pourra éventuellement être mise en œuvre.

Etant donnée la nature des données stockées dans la base de données négative NDB 12 et leur mode de représentation, on comprendra qu'une personne indélicate ayant accès au contenu de cette base de données ne pourra pas que difficilement en déduire de l'information pertinente sur les individus enrôlés.

En effet, un premier obstacle à franchir pour ce faire serait de reconstruire une base de données positive pour retrouver les associations entre données d'identité et pointeurs, ce qui n'est pas nécessairement simple comme rappelé plus haut. La puissance de calcul requise pour ce faire devient vite considérable lorsque le nombre d'individus enrôlés dépasse plusieurs centaines, plusieurs milliers, voire plus.

Et même si la personne indélicate y parvenait, il lui serait encore difficile de retrouver le lien entre une donnée biométrique stockée dans la base de données biométrique 10 et une donnée d'identité correspondante, sans

connaître au préalable la fonction ayant permis l'association entre la donnée d'identité i_a et le pointeur p_a, ainsi que l'information pointée par le pointeur p_a au sein de la base de données biométrique 10. Cette difficulté est encore accrue lorsque l'information désignée par le pointeur p_a ne consiste pas en une donnée biométrique unique (comme c'est le cas dans l'exemple de la figure 2).

Certaines de ces difficultés s'appliquent également, dans une certaine mesure, au propriétaire des bases de données lui-même.

Du fait de cette protection, il n'est pas nécessaire d'utiliser un algorithme cryptographique qui de toute façon était sans efficacité vis-à-vis du propriétaire des bases de données. On évite ainsi de complexifier les opérations mises en œuvre pour la vérification biométrique. Le recours supplémentaire à un algorithme cryptographique n'est cependant pas exclu.

De plus, si plusieurs bases de données d'identité négatives sont utilisées en relation avec de mêmes individus, par exemple dans le cadre de plusieurs applications indépendantes, une intersection entre ces bases de données ne permet pas de retrouver des données d'identité et leur lien avec des données biométriques correspondantes. Le retour à des données d'identité positives pour réaliser une intersection nécessiterait à nouveau une puissance de calcul trop importante et ne permettrait même pas nécessairement d'aboutir à un quelconque résultat.

La construction d'une base de données négative telle qu'elle vient d'être décrite peut être réalisée à l'aide d'un système ou d'un dispositif comprenant des unités appropriées à cet effet. Ce système ou dispositif peut par exemple comprendre un dispositif électronique et/ou informatique comprenant un module de traitement de données et éventuellement associé à un terminal de capture biométrique.

Tout ou partie des opérations mentionnées plus haut peuvent être mises en œuvre à l'aide d'un programme d'ordinateur comprenant des instructions appropriées, lorsqu'il est chargé et exécuté sur des moyens informatiques.

Un deuxième aspect de l'invention concerne la vérification biométrique d'un individu, en utilisant une base de données négative construite comme

décrit plus haut.

La vérification biométrique comprend l'obtention d'une donnée biométrique b' relative audit individu. Cette donnée biométrique est avantageusement de même nature et/ou de même format que les données biométriques $b_1, b_2, \ldots, b_m$ stockées dans la base de données biométrique 10. Son obtention peut éventuellement comprendre une acquisition à l'aide d'un capteur biométrique approprié. Elle peut le cas échéant être suivie par une numérisation de la donnée acquise, de manière à la mettre sous une forme numérique souhaitée.

Il peut être vérifié si la donnée biométrique b' obtenue correspond à une donnée biométrique stockée dans la base de données biométrique 10, soit de façon exacte soit à quelques différences acceptables près. Cette vérification peut par exemple résulter d'une comparaison de la donnée biométrique b' avec tout ou partie des données biométriques stockées dans la base de données biométrique 10 (étape 13).

En supposant que la donnée biométrique b' correspond à la donnée biométrique b_j stockée dans la base de données biométrique 10, on peut alors déterminer le groupe auquel la donnée biométrique b_j appartient. Le pointeur p_j correspondant peut également être retrouvé.

Lorsque la base de données biométrique 10 stocke plusieurs données biométriques relatives à de mêmes individus (au sein d'un même groupe pour un individu donné), la vérification biométrique peut de la même façon comprendre l'obtention de plusieurs données biométriques b' à comparer à tout ou partie des données biométriques stockées dans la base de données biométrique 10, pour retrouver le pointeur correspondant. Dans ce cas, le pointeur en question pourrait par exemple être celui qui désigne le groupe stocké dans la base de données biométrique 10 qui inclut des données biométriques correspondant à chacune des données biométriques relatives à l'individu qui fait l'objet de la vérification biométrique.

La vérification biométrique comprend en outre l'obtention d'une donnée d'identité i' relative à l'individu considéré. Cette obtention peut utiliser les mêmes moyens que lors de la construction de la base de données d'identité.

Elle peut par exemple être obtenue après que l'individu considéré a décliné son identité et/ou par consultation d'un document officiel (carte d'identité, passeport, permis de conduire, etc.), ou autre. La donnée d'identité i' est avantageusement de même nature et/ou de même format que les données d'identité $h, i_2, \ldots, i_m$ obtenues au préalable.

Une association est ensuite réalisée entre la donnée d'identité i' et le pointeur P_j retrouvé. Cette association est avantageusement de même nature et/ou de même format que celles qui ont été réalisées dans le cadre de la construction de la base de données d'identité. Ainsi, une telle association peut par exemple consister en la concaténation $i' || p_j$.

Puis on vérifie si l'association $i' || P_j$ ainsi réalisée est présente dans la base de données d'identité négative NDB 12. En variante, on vérifie l'absence de $i' || P_j$ dans la NDB 12, comme illustré à l'étape 14 de la figure 3. Une conclusion R peut être déduite de cette vérification.

Du fait de la nature négative de la base de données d'identité, l'absence de l'association $i' || pj$ dans la NDB 12 peut être interprétée comme le fait que l'individu considéré correspond bien à un individu enrôlé dont la donnée biométrique b' et la donnée d'identité i' sont en cohérence. Il s'agit d'un cas d'authentification réussi.

En cas de présence de l'association $i' || p_j$ dans la NDB 12, une conclusion R pouvant être tirée serait que la donnée d'identité i' n'est pas cohérente avec la donnée biométrique b'. On peut donc douter que l'individu considéré corresponde à l'individu enrôlé qu'il prétend être. La vérification biométrique peut alors être considérée comme ayant échoué. En variante, une ou plusieurs vérifications supplémentaires pourraient être mises en œuvre pour affiner le résultat de la vérification biométrique. A titre d'exemple, une nouvelle acquisition biométrique et/ou le recours à d'autres informations d'identité pourraient être utilisés en remplacement ou en complément de b' et/ou i'.

On notera que la situation décrite ci-dessus correspond à un cas d'authentification. En variante ou en complément, la base de données d'identité négative NDB 12 pourrait être utilisée à des fins d'identification d'individus.

Un cas d'application particulièrement intéressant de la présente

invention concerne la délivrance d'un titre d'identité. Un tel titre d'identité n'est alors délivré à un individu que lorsque la biométrie et l'identité de ce dernier correspondent à celles d'un individu enrôlé, conformément aux opérations décrites ci-dessus. En protégeant les identités grâce notamment à l'usage d'une base de données négative, on empêche une personne indélicate d'usurper une identité existante en vue de se faire délivrer abusivement un titre d'identité.

Dans le cas où la comparaison effectuée à l'étape 13 ne permet pas de trouver, dans la base de données biométrique 10, une donnée biométrique qui corresponde suffisamment à b', on peut conclure directement que l'individu considéré ne correspond pas à un individu enrôlé. On peut également réaliser une association de la donnée d'identité i' avec tout ou partie des pointeurs p_a, pour tenter de trouver une association qui serait absente de la base de données d'identité négative NDB 12. Ce cas peut par exemple correspondre à l'omission du stockage de la donnée biométrique pertinente dans la base de données biométrique 10, ou bien à un stockage corrompu ou erroné de cette donnée biométrique, ou autre.

D'autres types d'utilisation de la base de données d'identité négative NDB 12 en relation avec la base de données biométrique 10 peuvent également être envisagés, comme cela apparaîtra à l'homme du métier.

La vérification biométrique telle qu'elle vient d'être décrite peut être réalisée à l'aide d'un système ou d'un dispositif comprenant des unités appropriées à cet effet. Ce système ou dispositif peut par exemple comprendre un dispositif électronique et/ou informatique comprenant un module de traitement de données et éventuellement associé à un terminal de capture biométrique.

Tout ou partie des opérations de vérification biométrique mentionnées plus haut peuvent être mises en œuvre à l'aide d'un programme d'ordinateur comprenant des instructions appropriées, lorsqu'il est chargé et exécuté sur des moyens informatiques.

REVENDICATIONS

1. Procédé de construction d'une base de données d'identité négative relative à des individus à des fins de vérification biométrique en relation avec une base de données biométrique (10) stockant des groupes de données biométriques (b_1, b_2,..., b_m) relatives auxdits individus, le procédé comprenant les étapes suivantes :

- obtenir une donnée d'identité (i_1, i_2,...,i_m) respective relativement à chacun desdits individus ;

- réaliser une association entre chaque donnée d'identité obtenue relativement à un individu respectif et un pointeur (pi,p_2,...,Pm) désignant un groupe stocké dans la base de données biométrique qui inclut une donnée biométrique relative audit individu respectif ; et

- construire une base de données d'identité négative (12) à partir de l'ensemble complémentaire de l'ensemble des associations réalisées.

2. Procédé selon la revendication 1, dans lequel ladite association réalisée comprend une concaténation (h || p_1, i_t || p_1, i_2 || P2, i_u || p2,..., i_m || Pm, i_v || pm) entre chaque donnée d'identité (i_1,i_2,...,i_m) et le pointeur correspondant (p_1,p_2,...,p_m).

3. Procédé selon la revendication 1 ou 2, dans lequel ladite association réalisée consiste en une fonction secrète chaque donnée d'identité (i_1,i_2,...,i_m) et le pointeur correspondant (pi,p2,...,Pm)-

4. Procédé selon l'une quelconque des revendications précédentes, dans lequel la base de données d'identité négative (12) est construite pour stocker ledit ensemble complémentaire sous une forme condensée.

5. Procédé selon la revendication 4, dans lequel la forme condensée dudit ensemble complémentaire est obtenue par application d'un algorithme de type préfixe.

6. Procédé selon l'une quelconque des revendications précédentes, dans lequel la base de données d'identité négative (12) est construite pour stocker ledit ensemble complémentaire sous une forme randomisée.

7. Système ou dispositif pour la construction d'une base de données d'identité relative à des individus à des fins de vérification biométrique en relation avec une base de données biométrique (10) stockant des groupes de données biométriques (bi, b_2,..., b_m) relatives auxdits individus, le système ou dispositif étant apte à obtenir une donnée d'identité (h,i_2,...,i_m) respective relativement à chacun desdits individus et comprenant :

- une unité pour réaliser une association entre chaque donnée d'identité obtenue relativement à un individu respectif et un pointeur (p_1,p_2, ...,p_m) désignant un groupe stocké dans la base de données biométrique qui inclut une donnée biométrique relative audit individu respectif ;

- une unité de construction d'une base de données d'identité négative (12) à partir de l'ensemble complémentaire de l'ensemble des associations réalisées.

8. Procédé de vérification biométrique relativement à un individu, utilisant une base de données d'identité négative (12) construite selon l'une quelconque des revendications 1 à 6 en relation avec une base de données biométrique (10) stockant des groupes de données biométriques (bi, b_2, ..., b_m), le procédé de vérification biométrique comprenant les étapes suivantes :

- obtenir une donnée biométrique (b') relative audit individu ;

- retrouver un pointeur (p_j) désignant un groupe stocké dans la base de données biométrique qui inclut une donnée biométrique correspondant à la donnée biométrique relative audit individu ;

- obtenir une donnée d'identité (F) relative audit individu ;

- réaliser une association (i' || p_j) entre la donnée d'identité relative audit individu et ledit pointeur ;

- vérifier la présence ou l'absence de ladite association dans la base de données d'identité négative.

9. Procédé selon la revendication 8, comprenant en outre la génération d'une conclusion (R) en fonction d'un résultat de ladite vérification.

10. Système ou dispositif pour la mise en œuvre d'une vérification biométrique relativement à un individu selon la revendication 8 ou 9, le système ou dispositif étant apte à obtenir une donnée d'identité (i') relative audit individu et comprenant :

- une unité d'obtention d'une donnée biométrique (b') relative audit individu ;

- une unité pour retrouver un pointeur (p_j) désignant un groupe stocké dans la base de données biométrique qui inclut une donnée biométrique correspondant à la donnée biométrique relative audit individu ;

- une unité pour réaliser une association ($i' \,||\, P_j$) entre la donnée d'identité relative audit individu et ledit pointeur ;

- une unité de vérification de la présence ou de l'absence de ladite association dans la base de données d'identité négative (12).

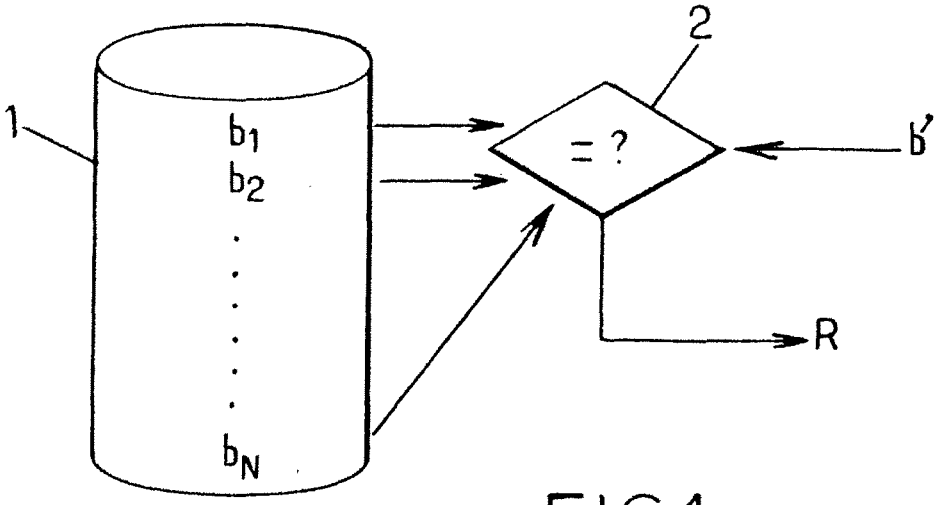

FIG.1.

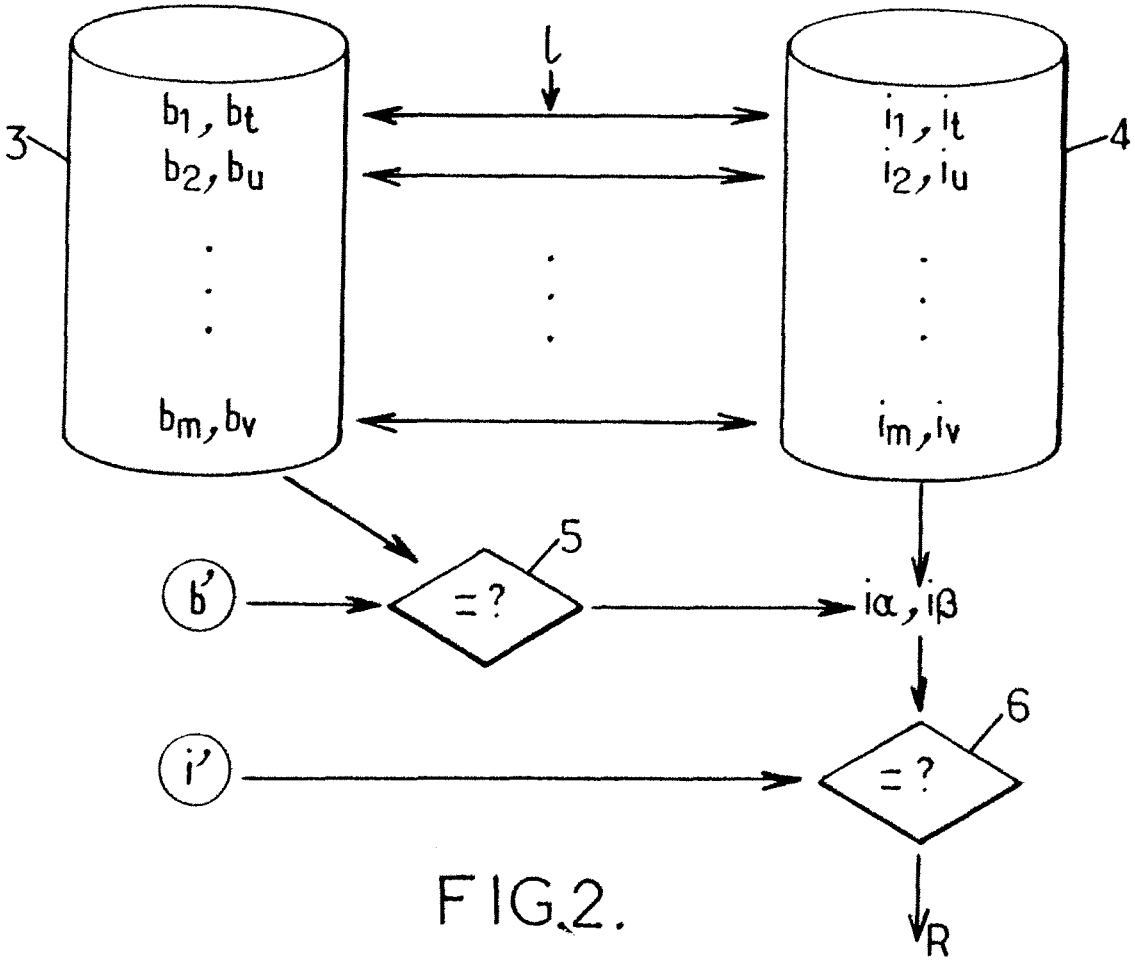

FIG.2.

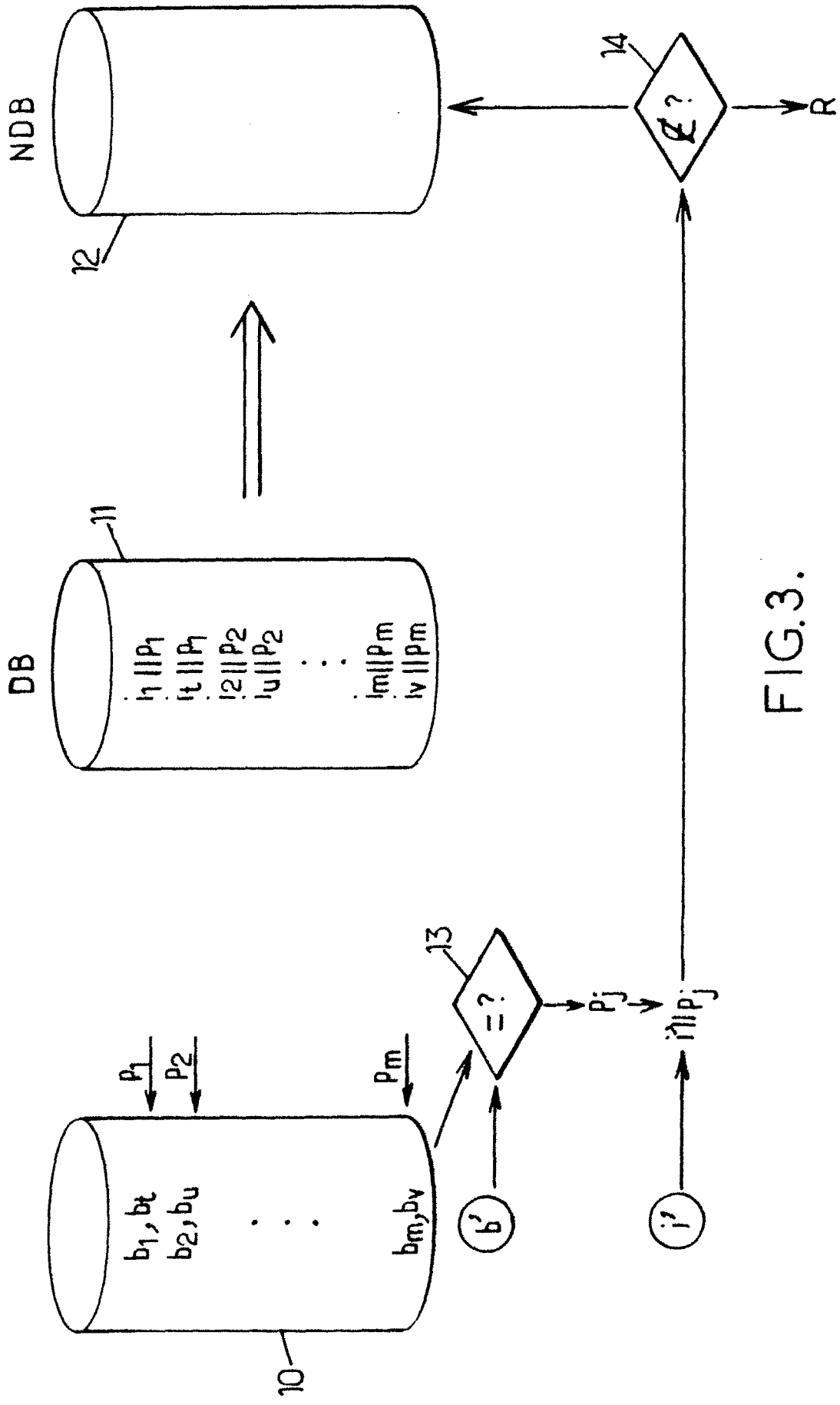
NDB
12
14
R
DB
11
i1 ||P1
it ||P1
i2 ||P2
iu ||P2
im ||Pm
iv ||Pm
13
P1
P2
Pm
b1, bt
b2, bu
bm, bv
10
b'
i'
Pj
i' ||Pj

FIG.3.

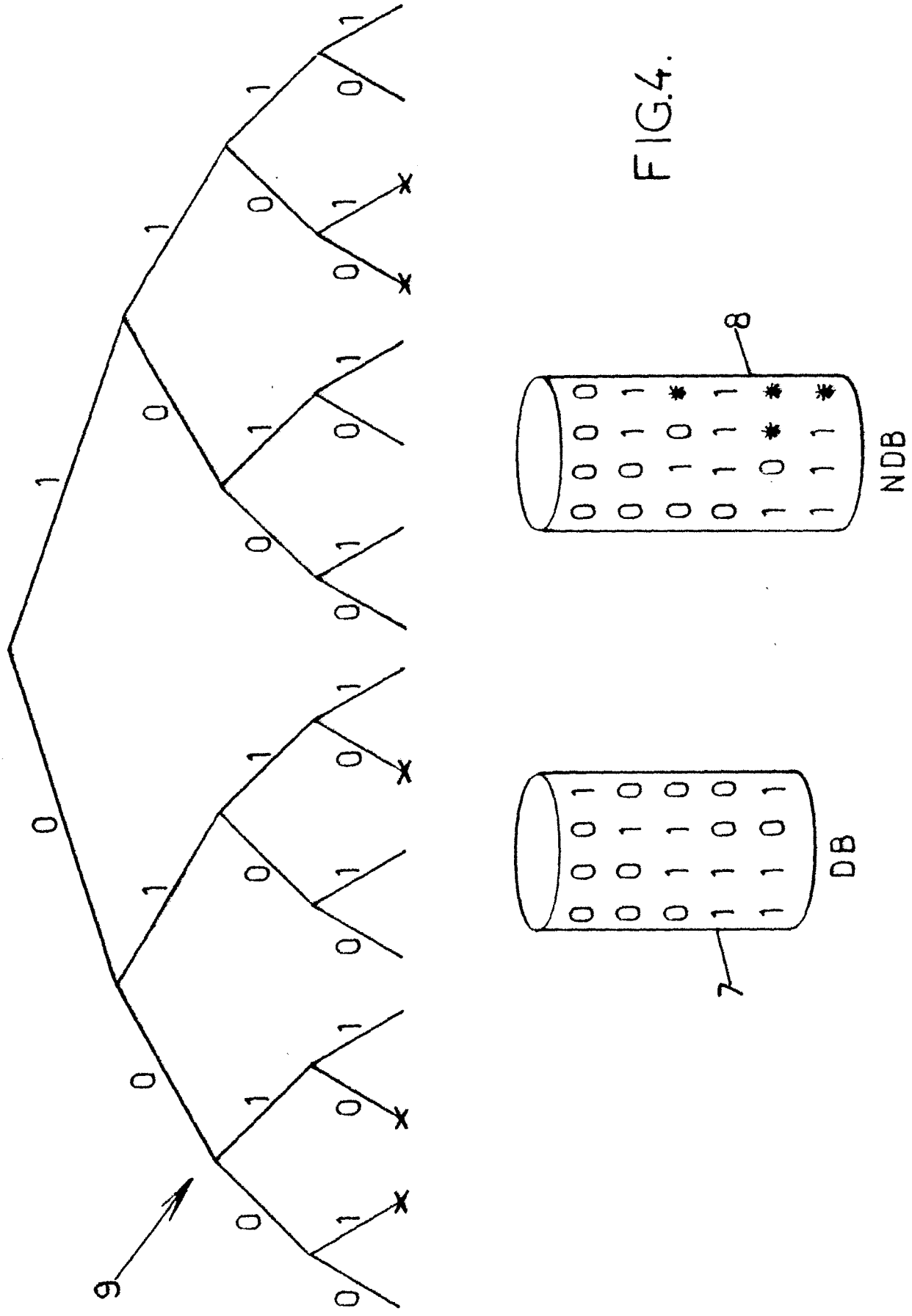

FIG.4.

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2011/051520

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06N5/02
ADD.

According to International Patent Classification (IPC) orto both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification **System** followed **by** classification **symbols)**
G06N G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 2005/121924 A2 (KONINKL PHILIPS ELECTRONICS NV [NL] ; KEVENAAR THOMAS A M [NL] ; AKKERMA) 22 December 2005 (2005-12-22) abstract page 1 - page 6 -----	1-10
Y	ESPONDA F: "Everything that is not important: Négative databases [Research Frontier] ", IEEE COMPUTATIONAL INTELLIGENCE MAGAZINE, IEEE, US, vol. 3, no. 2, 1 May 2008 (2008-05-01) , pages 60-63 , XP011207740, ISSN: 1556-603X the whole document -----	1-10

-/- .

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Spécial catégories of cited documents :

"A" document defining the gênerai state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" documentwhich may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other spécial reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published priorto the international filing date but laterthan the priority date claimed

"T" later document published after the international filing date or priority date and not in conflictwith the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such docu¬ments, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 December 2011	23/12/2011

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Valenci a, Eri ka

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2011/051520

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	FERNANDO ESPONDA ET AL: "Négati ve représentati ons of i nformati on" , INTERNATIONAL JOURNAL OF INFORMATION SECURITY, SPRINGER, BERLIN , DE, vol . 8 , no. 5 , 14 Apri l 2009 (2009-04-14) , pages 331-345 , XP019744017 , ISSN : 1615-5270, D0I : D01 : 10. 1007/S10207-009-0078-1 abstract	1-10
A	GEORGE DANEZIS ET AL: " Effi ci ent Négati ve Databases from Cryptographi e Hash Functi ons" , 9 October 2007 (2007-10-09) , INFORMATION SECURITY; [LECTURE NOTES I N COMPUTER SCI ENCE] , SPRINGER BERLIN HEIDELBERG, BERLIN , HEIDELBERG, PAGE(S) 423 - 436, XP019101591 , ISBN : 978-3-540-75495-4 abstract	5 , 6
A	US 2008/177569 Al (CHEN LI REN [US] ET AL) 24 July 2008 (2008-07-24) abstract	1-10

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2011/051520

Patent document oited in searoh report	Publication date	Patent family member(s)	Publication date
Wo 2005121924 A2	22-12-2005	JP 2008538146 A	09-10-2008
		KR 20070024569 A	02-03-2007
		US 2007226512 Al	27-09-2007
		W0 2005121924 A2	22-12-2005
US 2008177569 Al	24-07-2008	CN 101583967 A	18-11-2009
		EP 2126826 A2	02-12-2009
		JP 2010517181 A	20-05-2010
		US 2008177569 Al	24-07-2008
		W0 2008092043 A2	31-07-2008

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2011/051520

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. G06N5/02
ADD.

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
G06N G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)
EPO-Internal

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	WO 2005/121924 A2 (KONINKL PHILIPS ELECTRONICS NV [NL] ; KEVENAAR THOMAS A M [NL] ; AKKERMA) 22 décembre 2005 (2005-12-22) abrégé page 1 - page 6 -----	1-10
Y	ESPONDA F: "Everything that is not important: Négative databases [Research Frontier] ", IEEE COMPUTATIONAL INTELLIGENCE MAGAZINE, IEEE, US, vol. 3, no. 2, 1 mai 2008 (2008-05-01) , pages 60-63 , XP011207740, ISSN: 1556-603X le document en entier ----- -/- ·	1-10

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
16 décembre 2011	23/12/2011

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Valenciа, Erika

1

Formulaire PCT/ISA/210 (deuxième feuille) (avril 2005)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2011/051520

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	FERNANDO ESPONDA ET AL: "Négati ve représentati ons of i nformati on" , INTERNATIONAL JOURNAL OF INFORMATION SECURITY, SPRINGER, BERLIN , DE, vol . 8, no. 5, 14 avri l 2009 (2009-04-14) , pages 331-345 , XP019744017 , ISSN : 1615-5270, D0I : D01 : 10. 1007/S10207-009-0078-1 abrégé	1-10
A	GEORGE DANEZIS ET AL: " Effi ci ent Négati ve Databases from Cryptographi e Hash Functi ons" , 9 octobre 2007 (2007-10-09) , INFORMATION SECURITY; [LECTURE NOTES I N COMPUTER SCI ENCE] , SPRINGER BERLIN HEIDELBERG, BERLIN , HEIDELBERG, PAGE(S) 423 - 436, XP019101591 , ISBN : 978-3-540-75495-4 abrégé	5 , 6
A	US 2008/177569 Al (CHEN LI REN [US] ET AL) 24 jui l l et 2008 (2008-07-24) abrégé	1-10

1

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2011/051520

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 2005121924 A2	22-12-2005	JP 2008538146 A	09-10-2008
		KR 20070024569 A	02-03-2007
		US 2007226512 Al	27-09-2007
		WO 2005121924 A2	22-12-2005
US 2008177569 Al	24-07-2008	CN 101583967 A	18-11-2009
		EP 2126826 A2	02-12-2009
		JP 2010517181 A	20-05-2010
		US 2008177569 Al	24-07-2008
		W0 2008092043 A2	31-07-2008