



(22) **Date de dépôt/Filing Date:** 2007/01/19

(41) **Mise à la disp. pub./Open to Public Insp.:** 2007/07/23

(45) **Date de délivrance/Issue Date:** 2015/06/23

(30) **Priorité/Priority:** 2006/01/23 (FR06 00580)

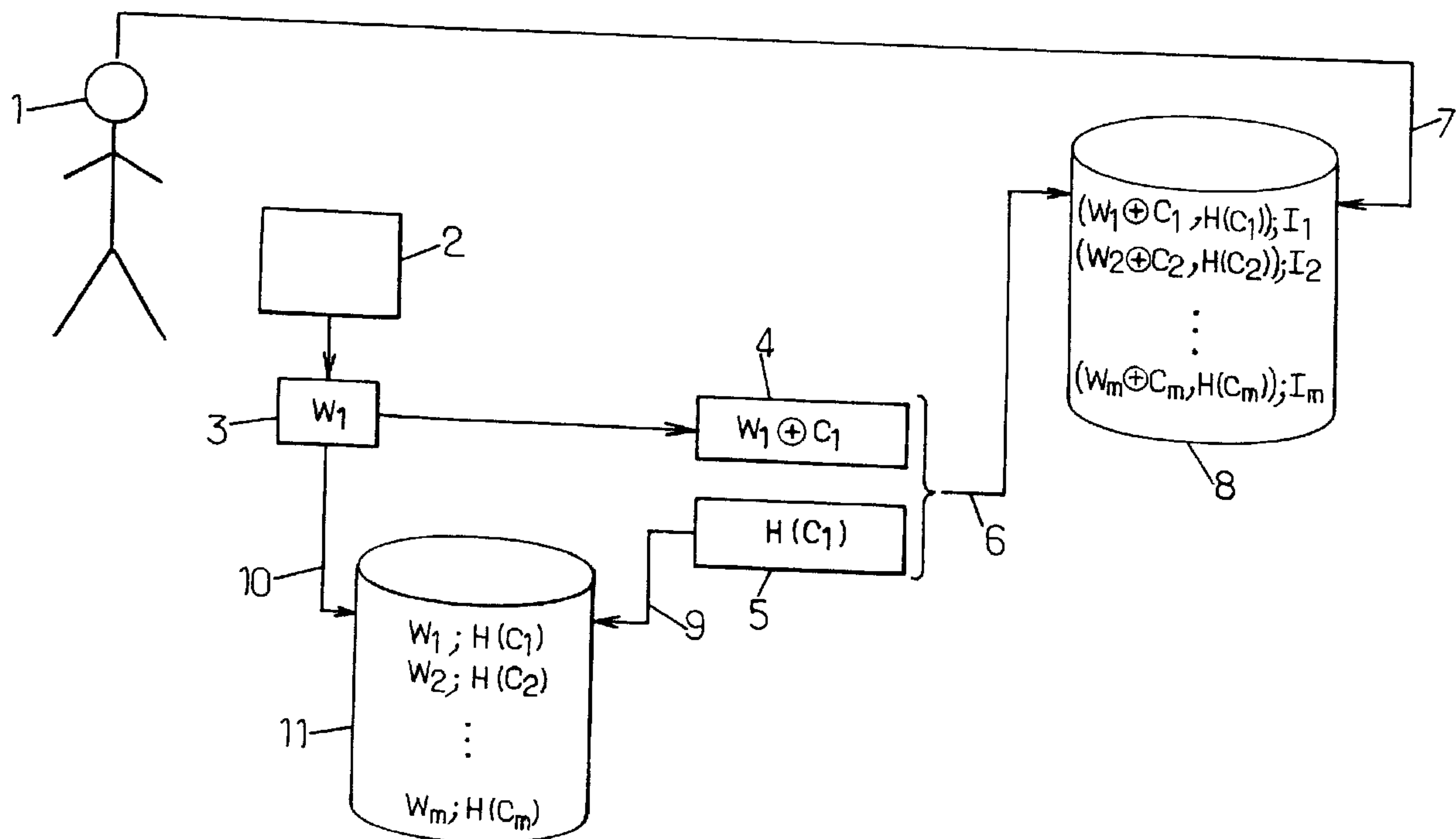
(51) **Cl.Int./Int.Cl.** **G07C 11/00** (2006.01),
G07C 9/00 (2006.01)

(72) **Inventeurs/Inventors:**
BRINGER, JULIEN, FR;
WELTI, PAUL, FR

(73) **Propriétaire/Owner:**
MORPHO, FR

(74) **Agent:** GOUDREAU GAGE DUBUC

(54) **Titre : PROCÉDES DE DETERMINATION D'UN IDENTIFIANT ET DE VERIFICATION BIOMETRIQUE ET SYSTEMES ASSOCIES**
(54) **Title: METHODS FOR THE DETERMINATION OF AN IDENTIFIER AND FOR BIOMETRIC VERIFICATION AND RELATED SYSTEMS**



(57) **Abrégé/Abstract:**

L'invention concerne un procédé de détermination d'un identifiant de pouvoir discriminant déterminé à partir d'une donnée biométrique. Selon ce procédé, on obtient une donnée biométrique relative à un individu (1). On convertit la donnée biométrique en une chaîne numérique (W_1). On associe un mot (C_1) d'un code correcteur d'erreurs à l'individu. On ajoute le mot du code correcteur d'erreurs à la chaîne numérique. On détermine un identifiant ($H(C_1)$) relatif à l'individu par application d'une fonction de hachage (H) au mot du code correcteur d'erreurs, la fonction de hachage étant choisie pour assurer audit identifiant le pouvoir discriminant déterminé.



ABRÉGÉ**PROCEDES DE DETERMINATION D'UN IDENTIFIANT ET DE
VERIFICATION BIOMETRIQUE ET SYSTEMES ASSOCIES**

L'invention concerne un procédé de détermination d'un identifiant de pouvoir discriminant déterminé à partir d'une donnée biométrique. Selon ce procédé, on obtient une donnée biométrique relative à un individu (1). On convertit la donnée biométrique en une chaîne numérique (w_1). On associe un mot (c_1) d'un code correcteur d'erreurs à l'individu. On ajoute le mot du code correcteur d'erreurs à la chaîne numérique. On détermine un identifiant ($H(c_1)$) relatif à l'individu par application d'une fonction de hachage (H) au mot du code correcteur d'erreurs, la fonction de hachage étant choisie pour assurer audit identifiant le pouvoir discriminant déterminé.

Figure 1

**PROCEDES DE DETERMINATION D'UN IDENTIFIANT ET DE
VERIFICATION BIOMETRIQUE ET SYSTEMES ASSOCIES**

La présente invention concerne l'utilisation de données biométriques.

Il est connu d'utiliser des données biométriques d'individus dans le
5 cadre de multiples applications.

A titre d'exemple, la vérification de l'identité d'un individu peut se baser sur une comparaison d'une donnée biométrique mesurée sur un individu déclinant son identité avec une donnée biométrique préalablement obtenue en correspondance avec ladite identité.

10 Selon un autre exemple, on peut subordonner à une vérification biométrique la délivrance d'un droit, la délivrance d'un droit étant à comprendre dans son acception la plus large (délivrance d'un permis de conduire, d'un titre de transport, d'une indemnisation, autorisation d'accès à un local, etc.).

Un problème tient à la nature des données biométriques utilisées.
15 Celles-ci peuvent en effet présenter un pouvoir discriminant très variable. Le pouvoir discriminant correspond à la faculté de caractériser de façon plus ou moins précise un individu.

Ainsi, une donnée biométrique telle que la forme générale d'une main ou la longueur de quelques doigts de la main est relativement peu
20 discriminante, puisque deux individus quelconques ont une probabilité relativement élevée de présenter la même donnée. A l'inverse, une donnée biométrique telle que l'empreinte digitale des dix doigts des mains ou des caractéristiques de l'iris des yeux est relativement discriminante, si bien que deux individus quelconques ont une probabilité relativement faible de présenter
25 la même donnée.

Certaines applications requièrent l'utilisation de données biométriques avec un fort pouvoir discriminant, car elles s'adressent exclusivement ou quasi exclusivement à des individus particuliers. On peut penser par exemple à une application visant à donner accès à un site stratégique à un personnel
30 spécialisé.

Au contraire, pour d'autres applications dont l'enjeu est moindre,

l'utilisation de données biométriques avec un faible pouvoir discriminant peut être préférée, recommandée voire rendue obligatoire.

En effet, un inconvénient des données biométriques très discriminantes est qu'elles sont susceptibles de représenter une entrave à la protection de la
5 vie privée ("privacy"), puisqu'elles peuvent permettre de caractériser complètement un individu. Ainsi, il n'est pas exclu qu'une application mettant en œuvre des données biométriques très discriminantes puisse être détournée pour retrouver des données relatives à ses utilisateurs (notamment personnelles, par exemple l'identité) en dehors du contexte normal d'utilisation.

10 Cet inconvénient peut pousser certains individus souhaitant rester dans l'anonymat à ne pas utiliser des applications mettant en œuvre des données biométriques jugées trop discriminantes.

En outre, dans certains pays, la législation est telle qu'une application donnée peut être refusée si elle utilise des données biométriques très
15 discriminantes, tandis qu'elle serait acceptée si elle utilisait des données biométriques avec un pouvoir discriminant inférieur. Typiquement, il peut être requis que le niveau de discrimination mis en œuvre soit proportionnel à l'enjeu de sécurité de l'application visée.

Le fait que des applications nécessitent d'utiliser des données
20 biométriques de pouvoirs discriminants différents nécessite d'adapter les moyens d'obtention et de traitement des données biométriques à chaque application, ce qui est fastidieux et implique un coût de mise en œuvre relativement élevé.

Un but de la présente invention est de limiter ces inconvénients.

25 L'invention propose ainsi un procédé de détermination d'un identifiant de pouvoir discriminant déterminé à partir d'une donnée biométrique. Le procédé comprend les étapes suivantes relativement à un individu :

- obtenir une donnée biométrique relative à l'individu ;
- convertir la donnée biométrique en une chaîne numérique ;
- 30 - associer un mot d'un code correcteur d'erreurs à l'individu ;

- 3 -

- ajouter le mot du code correcteur d'erreurs à la chaîne numérique ; et
- déterminer un identifiant relatif à l'individu par application d'une fonction de hachage au mot du code correcteur d'erreurs, la fonction de hachage étant choisie pour assurer audit identifiant le pouvoir discriminant déterminé.

5

L'identifiant ainsi obtenu provient donc d'une donnée biométrique relative à l'individu. Il possède cependant un pouvoir discriminant qui lui est propre et qui sera inférieur à celui de la donnée biométrique initiale. En d'autres termes, l'identifiant correspond à une dégradation maîtrisée de la donnée biométrique initiale.

10

De plus, cette dégradation est irréversible, c'est à dire que grâce aux propriétés de la fonction de hachage, il peut être quasiment impossible de retrouver le mot de code en connaissant son hachage seulement.

Le pouvoir discriminant de cet identifiant est déterminé, éventuellement à l'avance, par exemple en référence à un niveau de discrimination souhaité pour une application prévoyant une vérification utilisant ledit identifiant. Le pouvoir discriminant peut ainsi être choisi selon les besoins. Il pourra notamment être choisi suffisamment faible pour garantir un certain niveau de protection de la vie privée lorsque cela est nécessaire.

15

L'invention propose aussi un procédé de vérification biométrique utilisant un premier support de données stockant de façon associée, pour au moins un individu d'un ensemble d'individus, une identité relative audit individu, le résultat d'un ajout d'un premier mot d'un code correcteur d'erreurs associé audit individu à une première chaîne numérique obtenue à partir d'une donnée biométrique relative audit individu et au moins un identifiant de pouvoir discriminant déterminé obtenu par application d'une fonction de hachage au premier mot du code correcteur d'erreurs. Le procédé comprend les étapes suivantes relativement à un individu de l'ensemble d'individus :

20

25

- obtenir une donnée biométrique relative à l'individu ;
- convertir la donnée biométrique en une deuxième chaîne numérique ;

30

- 4 -

- déterminer un deuxième mot du code correcteur d'erreurs correspondant sensiblement à l'ajout à la deuxième chaîne numérique du résultat de l'ajout du premier mot du code correcteur d'erreurs à la première chaîne numérique stocké sur le premier support de données en association avec l'identité relative audit individu ;
- appliquer ladite fonction de hachage au deuxième mot du code correcteur d'erreurs ; et
- comparer le résultat de l'application de ladite fonction de hachage au deuxième mot du code correcteur d'erreurs avec l'identifiant de pouvoir discriminant déterminé stocké sur le premier support de données en association avec l'identité relative audit individu.

Une telle vérification biométrique est réalisée en utilisant un identifiant ayant un pouvoir discriminant conforme aux attentes. Elle se base en outre sur une donnée biométrique initiale, qui peut être obtenue par exemple à l'aide de moyens d'acquisition classiques, quel que soit le niveau de discrimination souhaité.

De façon avantageuse, une pluralité d'identifiants de pouvoirs discriminants déterminés distincts peut être stockée pour un individu donné. On choisira alors l'identifiant de la pluralité ayant le pouvoir discriminant le plus en adéquation avec le niveau de discrimination souhaité pour l'application à mettre en œuvre.

Ainsi, à partir d'une même mesure biométrique, des vérifications de niveaux de discrimination différents pourront être mises en œuvre selon les besoins. Cela implique une économie appréciable dans les moyens à déployer (capteurs biométriques par exemple) et une grande simplicité de mise en œuvre.

L'invention propose aussi un procédé d'identification utilisant un premier support de données stockant de façon associée, pour chaque individu d'un ensemble d'individus, une identité relative audit individu, le résultat d'un ajout d'un premier mot d'un code correcteur d'erreurs associé audit individu à une première chaîne numérique obtenue à partir d'une donnée biométrique relative audit individu et au moins un identifiant de pouvoir discriminant

- 5 -

déterminé obtenu par application d'une fonction de hachage au premier mot du code correcteur d'erreurs. Le procédé comprend les étapes suivantes relativement à un individu de l'ensemble d'individus :

- obtenir une donnée biométrique relative à l'individu ;
- 5 - convertir la donnée biométrique en une deuxième chaîne numérique ;
- déterminer une pluralité de deuxièmes mots du code correcteur d'erreurs correspondant chacun sensiblement à l'ajout à la deuxième chaîne numérique du résultat de l'ajout du premier mot du code correcteur d'erreurs à la première chaîne numérique stocké sur le
- 10 premier support de données pour un individu dudit ensemble d'individus ;
- appliquer ladite fonction de hachage à chaque deuxième mot du code correcteur d'erreurs ;
- comparer le résultat de l'application de ladite fonction de hachage à
- 15 chaque deuxième mot du code correcteur d'erreurs avec l'identifiant correspondant de pouvoir discriminant déterminé stocké sur le premier support de données ;
- déterminer l'identité dudit individu, ladite identité correspondant à une identité stockée sur le premier support de données en association avec
- 20 un identifiant pour lequel ladite comparaison révèle une égalité.

L'invention propose aussi un système comprenant des moyens pour obtenir une donnée biométrique et des moyens de traitement numérique agencés pour mettre en œuvre le procédé susmentionné de détermination d'un identifiant de pouvoir discriminant déterminé à partir d'une donnée biométrique.

25 L'invention propose aussi un système comprenant des moyens pour obtenir une donnée biométrique et des moyens de traitement numérique agencés pour mettre en œuvre le procédé susmentionné de vérification biométrique.

30 L'invention propose aussi un système comprenant des moyens pour obtenir une donnée biométrique et des moyens de traitement numérique agencés pour mettre en œuvre le procédé susmentionné d'identification.

L'invention propose aussi un produit programme d'ordinateur comprenant des instructions de code adaptées à la mise en œuvre du procédé susmentionné de détermination d'un identifiant de pouvoir discriminant déterminé à partir d'une donnée biométrique, lorsqu'il est chargé et exécuté par
5 des moyens informatiques.

L'invention propose aussi un produit programme d'ordinateur comprenant des instructions de code adaptées à la mise en œuvre du procédé susmentionné de vérification biométrique, lorsqu'il est chargé et exécuté par des moyens informatiques.

10 L'invention propose aussi un produit programme d'ordinateur comprenant des instructions de code adaptées à la mise en œuvre du procédé susmentionné d'identification, lorsqu'il est chargé et exécuté par des moyens informatiques.

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

- la figure 1 est un schéma représentant des étapes d'une phase d'enrôlement permettant la détermination d'un identifiant selon l'invention ;
- 20 - la figure 2 est un schéma représentant des étapes de vérification biométrique selon l'invention ;
- la figure 3 est un schéma représentant des étapes supplémentaires de vérification biométrique selon un mode de réalisation de l'invention ;
- les figures 4 à 7 sont des exemples simplifiés de chaînes numériques
25 utilisées dans le cadre de vérifications biométriques selon les principes de l'invention.

La figure 1 montre un individu 1 pour lequel on souhaite déterminer un identifiant de pouvoir discriminant déterminé, au cours d'une phase dite d'enrôlement. Ce pouvoir discriminant peut par exemple être choisi pour être
30 conforme à un niveau de discrimination requis par une application mettant en œuvre une vérification biométrique. L'identifiant ainsi déterminé pourra alors être exploité dans la vérification biométrique, en apportant la garantie que les

exigences de l'application en termes de discrimination seront respectées.

La détermination de l'identifiant est réalisée comme suit.

Une donnée biométrique est d'abord obtenue pour l'individu 1. Cette donnée biométrique peut être de différents types. De préférence, elle
5 présentera un pouvoir discriminant relativement élevé. Le pouvoir discriminant est parfois caractérisé par un taux de "fausses acceptances" qui correspond à la probabilité de confondre deux personnes quelconques lors de l'analyse de leurs données biométriques. La donnée biométrique obtenue dans le cas présent sera donc avantageusement choisie pour présenter un taux de fausses
10 acceptances inférieur à un seuil prédéterminé, par exemple 10^{-6} . Il peut ainsi s'agir d'empreintes digitales ou de caractéristiques de l'iris de l'œil par exemple.

L'obtention de la donnée biométrique est avantageusement réalisée par acquisition à l'aide d'un capteur 2. Ce capteur est adapté à la donnée
15 biométrique qu'on souhaite obtenir. Ainsi, il peut par exemple s'agir d'un capteur classique d'empreintes digitales ou de caractéristiques de l'iris.

Une fois obtenue, la donnée biométrique de l'individu 1 est convertie en une chaîne numérique, comme cela est connu en soi. La chaîne numérique w_1 ainsi obtenue (étape 3) est par exemple une chaîne d'éléments binaires.

20 L'obtention de la chaîne w_1 , lorsque la donnée biométrique comprend des empreintes digitales, peut comprendre une pré-orientation des images d'empreintes selon une direction, et une extraction de certaines caractéristiques (par exemple minuties ou directions des sillons). Lorsque la donnée biométrique est relative à l'iris, un code d'iris peut être extrait. Ces
25 méthodes, connues en soi, peuvent dépendre d'un type de correction d'erreurs utilisé (l'application d'une telle correction d'erreurs est décrit ci-après). Certaines méthodes sont décrites dans les articles mentionnés ci-dessous. Bien sûr, d'autres méthodes sont également possibles.

Par ailleurs, un mot d'un code correcteur d'erreurs c_1 , qui peut être
30 choisi de façon aléatoire parmi les différents mots du code, est associé à l'individu 1. Ce mot est une chaîne numérique, par exemple une chaîne binaire, présentant de préférence une taille identique à celle de la chaîne binaire w_1 .

A cet effet, divers codes correcteurs d'erreurs peuvent être utilisés. A titre d'exemples non limitatifs, on peut citer le code BCH de longueur 511 décrit par P. Tuyls, A. Akkermans, T. Kevenaar, G.-J. Schrijen, A. Bazen et R. Veldhuis, dans l'article "Practical Biometric Authentication with Template
5 Protection", AVBPA 2005, LNCS 3546, 2005, publié en 2005, ou bien le code concaténé Hadamard/Reed-Solomon décrit par R. Anderson, J. Daugman & F. Hao, dans l'article "Combining cryptography with biometrics effectively", Technical report UCAM-CL-TR-640, University of Cambridge, publié en juillet 2005. Bien sûr, d'autres codes correcteurs d'erreurs pourraient être utilisés.

10 Une fois associé à l'individu 1, le mot du code correcteur d'erreurs c_1 est ajouté à la chaîne binaire w_1 (étape 4). Comme cela est classique en traitement numérique, on entend par "ajout", l'opération de OU exclusif ($\oplus$), de sorte que l'ajout des deux chaînes binaires soit tel que deux éléments binaires identiques de même rang appartenant aux deux chaînes respectivement
15 donnent lieu à un "0", tandis que deux éléments binaires distincts de même rang appartenant aux deux chaînes respectivement donnent lieu à un "1". On obtient ainsi une nouvelle chaîne binaire $w_1 \oplus c_1$.

On calcule en outre un identifiant $H(c_1)$ à partir du mot de code c_1 , la fonction H étant une fonction de hachage (étape 5). On rappelle qu'une
20 fonction de hachage est une fonction de compression permettant d'obtenir une information plus courte qu'une information initiale à laquelle elle est appliquée. Elle a en outre comme propriété de délivrer des résultats très différents à partir d'informations initiales qui diffèrent même légèrement, c'est-à-dire qu'elles accentuent les différences entre des informations distinctes, de façon à éviter
25 qu'on puisse retrouver facilement l'information initiale à partir du résultat du hachage.

Dans le cadre de l'invention, la fonction de hachage H est choisie de façon telle que l'identifiant $H(c_1)$ résultant ait un pouvoir discriminant déterminé. Autrement dit, la fonction de hachage choisie implique une probabilité de
30 collision, i.e. une probabilité d'aboutir à un même condensé à partir de chaînes distinctes, correspondant au taux de fausses acceptances présenté par l'identifiant $H(c_1)$.

Avantageusement, la fonction de hachage est choisie pour avoir un espace d'arrivée équiprobable comprenant un nombre de valeurs possibles correspondant sensiblement au pouvoir discriminant déterminé de l'identifiant.

A titre d'exemple non limitatif, on peut utiliser une fonction de hachage
 5 H dérivée de la fonction SHA-1 décrite dans le standard FIPS 180-1, "Secure hash standard", publié en avril 1993 par l'organisme Federal Information Processing Standards, et qui produit des condensés de 160 éléments binaires. Bien d'autres fonctions de hachage sont bien sûr également utilisables.

Ainsi, si l'on souhaite que l'identifiant à déterminer puisse prendre une
 10 valeur parmi un nombre de valeurs possibles égal à 2^n , avec $n < 160$, on peut alors choisir une fonction de hachage H telle que pour toute chaîne binaire x de longueur l, on ait $H(x) = [SHA-1(x)]_{i_1, \dots, i_n}$, où $[X]_{i_1, \dots, i_n}$ désigne les éléments binaires de rang $i_1, \dots, i_n$ de la chaîne binaire x. Ainsi, $H(c_1) = [SHA-1(c_1)]_{i_1, \dots, i_n}$, c'est-à-dire que l'identifiant déterminé est une chaîne de n éléments binaires
 15 correspondant aux éléments binaires de rang $i_1, \dots, i_n$ de la chaîne binaire résultant de l'application de la fonction SHA-1 au mot de code c_1 . Dans cet exemple, $H(c_1)$ a donc un pouvoir discriminant de 2^n . En effet, du fait des propriétés de la fonction H, un individu quelconque a une chance sur 2^n d'avoir le même identifiant $H(c_1)$ que l'individu 1, et ce, même si un autre mot de code
 20 c_2 a été associé à cet individu.

Dans l'exemple susmentionné, on pourra donc définir le pouvoir discriminant de l'identifiant à déterminer par simple fixation du nombre n. Si l'on souhaite pouvoir effectuer une vérification biométrique de façon peu discriminante, on choisira n relativement faible (par exemple inférieur à 20). A
 25 l'inverse, si l'on souhaite pouvoir effectuer une vérification biométrique de façon discriminante, on choisira n relativement élevé (par exemple supérieur à 20).

De façon avantageuse, les informations obtenues relativement à l'individu 1, à savoir $w_1 \oplus c_1$ et $H(c_1)$, sont ensuite stockées de façon associée sur un support de données (étape 6). Elles sont en outre associées à une
 30 identité I_1 de l'individu 1. Cette identité, qui peut par exemple consister en le nom et le prénom de l'individu 1, mais éventuellement d'autres types d'informations, peut être déclinée par l'individu 1 lui-même (étape 7) ou bien

être obtenue par d'autres moyens. Elle est avantageusement vérifiée avant d'être stockée sur le support de données.

Dans l'exemple illustré sur la figure 1, toutes ces informations sont mémorisées dans une base de données d'identités 8 destinée à stocker les informations d'un ensemble d'individus 1-m. Selon une variante, les informations $w_1 \oplus c_1$, $H(c_1)$ et I_1 pourraient être stockées en association sur un jeton biométrique détenu avantageusement par l'individu 1. D'autres supports de données sont également envisageables, dans la mesure où ils peuvent ensuite être interrogés dans le cadre d'une vérification biométrique.

On notera que, dans la base de données 8, la chaîne binaire w_1 caractérisant l'individu 1 n'est pas stockée en tant que telle, mais seulement sous la forme $w_1 \oplus c_1$. Ainsi, une personne ayant accès à cette base de données ne pourra pas trouver un lien entre l'identité I_1 et la chaîne binaire w_1 de l'individu 1. Si cette personne connaît l'identité I_1 , elle sera incapable d'en déduire la chaîne binaire w_1 , à partir de la base de données 8. De même, si cette personne connaît la chaîne binaire w_1 , elle sera incapable d'en déduire l'identité I_1 , à partir de la base de données 8.

De façon avantageuse, la chaîne binaire w_1 de l'individu 1 et l'identifiant obtenu $H(c_1)$ sont en outre stockés l'un avec l'autre, sur un deuxième support de données qui peut aussi être une base de données 11 ou tout autre support envisageable (étapes 9 et 10). La base de données biométriques 11 ne comprend pas d'informations d'identités, telles que l'identité I_1 de l'individu 1, si bien qu'elle garantit la protection de la vie privée.

On notera que tout ou partie des opérations décrites ci-dessus peuvent être mises en œuvre par un système utilisant avantageusement un programme d'ordinateur. Ce système peut consister en un simple dispositif, qui comprend alors le capteur 2 et les moyens de traitement numérique nécessaires au traitement des chaînes binaires, ou bien être distribué entre différents dispositifs aptes à communiquer entre eux de toute manière envisageable.

On s'intéresse ci-après, en référence à la figure 2, à une vérification biométrique effectuée à l'aide d'un identifiant de pouvoir discriminant déterminé tel que décrit plus haut. Cette vérification biométrique peut être mise en œuvre

dans le cadre d'une application quelconque. Elle peut par exemple être le prélude à la délivrance d'un droit, comme définie en introduction. L'application visée requiert un niveau de discrimination donné, en référence auquel le pouvoir discriminant de l'identifiant décrit plus haut a pu être déterminé.

5 Sur l'exemple de la figure 2, l'individu 1, qui a subi préalablement une phase d'enrôlement décrite en référence à la figure 1, fait désormais l'objet d'une vérification biométrique. A cet effet, une donnée biométrique de l'individu 1 est obtenue. La donnée biométrique en question est du même type que celle obtenue lors de l'enrôlement. Elle peut avantageusement être obtenue avec un
10 capteur qui peut être le même ou du même type que le capteur 2 de la figure 1.

La donnée biométrique obtenue est ensuite convertie en une chaîne numérique, dans les mêmes conditions que lors de l'enrôlement (étape 12). Dans l'exemple décrit, on obtient ainsi une chaîne binaire w'_1 , qui peut différer plus ou moins de la chaîne binaire w_1 . Ces différences sont liées à la non
15 reproductibilité des mesures biométriques réalisées à l'aide du capteur 2. A titre d'exemple, deux mesures successives d'empreinte digitale peuvent différer du fait de la variation de l'inclinaison du doigt ou de la pression exercée par le doigt sur le capteur entre les deux mesures.

Par la suite, on calcule une nouvelle chaîne binaire par ajout de w'_1
20 avec la chaîne $w_1 \oplus c_1$ préalablement stockée dans la base de données 8 ou tout support de données équivalent (étape 13). La chaîne $w_1 \oplus c_1$ correspondant à l'individu 1 est retrouvée dans la base de données 8, par exemple à l'aide de l'identité I_1 déclinée par l'individu 1.

Le résultat de ce nouvel ajout, à savoir $w'_1 \oplus w_1 \oplus c_1$, peut consister en
25 un mot c'_1 du code correcteur d'erreurs auquel le mot c_1 appartient. Dans le cas contraire, on utilise avantageusement l'algorithme de décodage associé audit code correcteur d'erreurs, de manière à retrouver le mot c'_1 du code correcteur d'erreurs le plus proche de $w'_1 \oplus w_1 \oplus c_1$. Le succès de cette opération tient au fait que le code correcteur d'erreurs est prévu pour corriger un certain nombre
30 d'erreurs dans les chaînes binaires, les différences entre w'_1 et w_1 étant alors vues comme des erreurs.

La fonction de hachage H telle qu'utilisée dans la phase d'enrôlement

décrite plus haut est ensuite appliquée au nouveau mot de code c'_1 (étape 14). Le condensé $H(c'_1)$ en résultant est alors comparé à l'identifiant $H(c_1)$ stocké dans la base de données 8 pour l'individu 1 (étape 15). L'identifiant $H(c_1)$ est retrouvé dans la base de données 8, par exemple à l'aide de l'identité I_1
5 déclinée par l'individu 1.

En cas d'égalité entre $H(c'_1)$ et $H(c_1)$, la vérification biométrique peut être considérée comme réussie, c'est-à-dire qu'on considère que l'individu 1 faisant l'objet de la vérification est bien celui qui avait fait préalablement l'objet de l'enrôlement décrit en référence à la figure 1. On peut ainsi réaliser une
10 authentification à partir de l'identité I_1 déclinée par l'individu 1.

En effet, les éventuelles différences entre les chaînes w_1 et w'_1 , sous réserve de ne pas être excessives sont estompées grâce aux propriétés du code correcteur d'erreurs. De cette façon, dans le cas décrit en référence à la figure 2, on peut espérer obtenir un mot de code c'_1 égal à c_1 . En conséquence,
15 $H(c'_1)=H(c_1)$, et l'authentification de l'individu 1 est réussie.

A l'inverse, si l'individu faisant l'objet de la vérification biométrique prétend, à tort, avoir l'identité I_1 , il y a de fortes chances pour que le mot de code c'_1 obtenu pour cet individu selon les principes décrits plus haut soit différent de c_1 . Dans ce cas, $H(c'_1)$ peut différer de $H(c_1)$, et l'authentification
20 échoue. Mais, étant données les propriétés de la fonction H , il est malgré tout possible que $H(c'_1)=H(c_1)$, alors même que c'_1 diffère de c_1 . Dans ce dernier cas, l'authentification est considérée, à tort, comme réussie. L'individu ayant usurpé l'identité I_1 pourra alors éventuellement se faire passer pour l'individu 1. Il s'agit donc d'un cas de fausse acceptation que l'application visée est prévue
25 pour tolérer.

Cette incertitude est liée au relativement faible pouvoir discriminant de l'identifiant $H(c_1)$. En contrepartie, ce faible niveau de discrimination empêche toute personne ayant accès à la base de données 8 de retrouver l'identité I_1 de l'individu 1, à partir de son identifiant $H(c_1)$, puisque plusieurs individus peuvent
30 avoir le même identifiant $H(c_1)$. La protection de la vie privée de l'individu 1 est ainsi assurée.

On comprendra qu'une vérification biométrique a pu ainsi être réalisée

- 13 -

avec un faible niveau de discrimination pour protéger la vie privée de l'individu 1, à partir d'une donnée biométrique pourtant relativement discriminante.

A la suite de la vérification réalisée à l'étape 15, d'autres étapes peuvent éventuellement être mises en œuvre selon l'application visée. Par exemple, la délivrance d'un droit pourra être faite à l'individu 1 dans ce cas.

La figure 3 montre un exemple de vérification biométrique incluant des étapes de vérification supplémentaires par rapport à l'exemple de la figure 2. Les étapes 12-14 sont identiques à celles de la figure 2.

En outre, après obtention de la chaîne binaire w'_1 relative à l'individu 1, on retrouve dans la base de données biométriques 11 ou tout autre support de données équivalent, la chaîne binaire w_1 correspondante, c'est-à-dire celle qui présente le plus de similitudes avec w'_1 et qui est donc susceptible de caractériser le même individu 1 (étape 16).

On retrouve ensuite l'identifiant $H(c_1)$ préalablement stocké dans la base de données biométriques 11 en association avec w_1 , lors de la phase d'enrôlement.

Puis, on compare $H(c'_1)$ avec l'identifiant $H(c_1)$ (étape 17). En cas d'égalité, on peut alors conclure que l'individu 1 a déjà fait l'objet d'un enregistrement biométrique dans la base de données 11 lors d'un enrôlement préalable.

Cette vérification peut être utile par exemple pour éviter que l'individu 1 puisse faire l'objet de plusieurs enrôlements successifs qui pourraient éventuellement lui permettre de se faire délivrer plus d'une fois un même droit (par exemple plusieurs permis de conduire avec des identités différentes, etc.).

Là encore, le relativement faible pouvoir discriminant de l'identifiant $H(c_1)$ empêche toute personne ayant accès à la base de données 11 de retrouver la chaîne binaire w_1 caractérisant l'individu 1, à partir de cet identifiant $H(c_1)$, puisque plusieurs individus peuvent avoir le même identifiant $H(c_1)$. La protection de la vie privée de l'individu 1 est ainsi assurée.

On notera que tout ou partie des opérations décrites en référence aux figures 2 et 3 peuvent être mises en œuvre par un système utilisant

avantageusement un programme d'ordinateur. Ce système peut consister en un simple dispositif, qui comprend alors le capteur 2 et les moyens de traitement numérique nécessaires au traitement des chaînes binaires, ou bien être distribué entre différents dispositifs aptes à communiquer entre eux de toute manière envisageable. Ce système peut être le même que celui décrit en référence à la figure 1 et utilisé pour l'enrôlement. Les deux systèmes peuvent également être distincts.

Dans un mode de réalisation de l'invention, plusieurs identifiants ayant des pouvoirs discriminants distincts sont déterminés pour l'individu 1. Ainsi, t identifiants $H_1(c_1)$, $H_2(c_1)$, ..., $H_t(c_1)$ ayant des pouvoirs discriminants décroissants peuvent être obtenus et stockés relativement à l'individu 1 selon les principes décrits en référence à la figure 1.

En fonction de l'application qu'on souhaite mettre en œuvre, une vérification biométrique est réalisée, comme décrit en référence à la figure 2 ou 3, en utilisant l'identifiant dont le pouvoir discriminant correspond au niveau de discrimination requis pour ladite application. Ainsi, une application nécessitant une forte discrimination pourra nécessiter une vérification biométrique utilisant l'identifiant $H_1(c_1)$, tandis qu'une application nécessitant une faible discrimination pourra nécessiter une vérification biométrique utilisant l'identifiant $H_t(c_1)$ par exemple.

Le niveau de discrimination souhaité peut faire l'objet d'une détermination préalable, voire d'une négociation avec l'individu concerné.

Dans ce cas de figure, on comprendra que des vérifications biométriques avec des niveaux de discrimination différents peuvent être réalisées à partir d'une seule et unique donnée biométrique et donc à l'aide d'un seul capteur, de façon transparente pour l'individu qui la subit. La protection de la vie privée de l'individu est cependant garantie dans tous les cas où cela est nécessaire, même si une donnée biométrique relativement discriminante est initialement acquise pour ledit individu.

Les figures 4 à 7 montrent des exemples numériques simplifiés permettant de mieux comprendre encore le fonctionnement de l'invention décrite ci-dessus.

- 15 -

Sur la figure 4, on a représenté une chaîne binaire w_1 supposée caractériser un individu 1. Dans l'exemple illustré, pour des raisons de clarté et de simplification, la chaîne binaire w_1 ne comporte que 14 éléments binaires, ce qui est relativement peu discriminant ($2^{14}=16384$ valeurs possibles au total).

5 Dans la réalité, une telle chaîne binaire pourrait comprendre avantageusement un nombre plus élevé d'éléments binaires, par exemple 20 éléments binaires ou plus.

Par ailleurs, le code correcteur d'erreurs C utilisé est constitué de quatre mots distincts, à savoir $m_1=11111110000000$, $m_2=00000001111111$,
 10 $m_3=11111111111111$ et $m_4=00000000000000$. Etant donné le format de ces quatre mots, on comprendra que le code correcteur d'erreurs C est capable de corriger trois erreurs sans ambiguïté. En effet, une chaîne binaire présentant trois différences avec un de ces quatre mots, par exemple m_1 , comprendra un plus grand nombre de différences encore avec les trois autres mots, si bien
 15 qu'elle pourra être assimilée à m_1 sans hésitation. Bien sûr, le code C choisi pour cet exemple est un cas simplifié. Dans la pratique, des codes correcteurs d'erreurs plus complexes, comme ceux cités plus haut, pourront avantageusement être utilisés.

Lors de l'enrôlement de l'individu 1, un mot du code C, à savoir m_3 , est
 20 associé à cet individu 1, de façon éventuellement arbitraire. Avec les notations adoptées plus haut, on a donc $c_1=m_3$. Puis, on détermine la chaîne binaire $w_1 \oplus c_1$, c'est-à-dire $w_1 \oplus m_3$, comme illustré sur la figure 4.

De plus, une fonction de hachage est appliquée au code $c_1=m_3$. Dans l'exemple décrit, la fonction de hachage H utilisée consiste à sélectionner le
 25 deuxième élément binaire d'une chaîne binaire, en partant de la gauche. Ainsi, $H(c_1)$ est égal à 1, comme montré sur la figure 4 par un encadrement de l'élément binaire sélectionné. Bien sûr, une telle fonction de hachage est particulièrement simple, pour des raisons de clarté. En pratique, des fonctions de hachage plus complexes, comme celles mentionnées plus haut, pourront
 30 être utilisées.

A l'issue de l'enrôlement de l'individu 1, on dispose donc des deux informations suivantes : $w_1 \oplus c_1=01100001111001$ et $H(c_1)=1$. Ces informations

sont avantageusement stockées sur un support de données pour pouvoir être retrouvées dans une phase de vérification ultérieure.

La figure 5 illustre un cas de vérification biométrique relativement à l'individu 1. Une nouvelle chaîne binaire w'_1 est obtenue pour l'individu 1, à partir d'une nouvelle mesure biométrique par exemple. Cette chaîne binaire w'_1 comporte trois différences avec la chaîne binaire w_1 . Les éléments binaires qui diffèrent ont été entourés dans la chaîne binaire w'_1 de la figure 5.

Puis, conformément aux principes décrits plus haut, on calcule la chaîne binaire $w'_1 \oplus w_1 \oplus c_1$, puis on cherche à déterminer le mot c'_1 du code C dont cette chaîne est la plus proche. On constate que la chaîne $w'_1 \oplus w_1 \oplus c_1$ comprend trois différences avec le mot m_3 . La correction d'erreurs permet alors d'assimiler cette chaîne $w'_1 \oplus w_1 \oplus c_1$ au mot de code m_3 . Selon les notations précédemment adoptées, on a donc $c'_1 = m_3$.

De ce fait, le calcul de $H(c'_1)$ permet de retrouver $H(m_3)$ c'est-à-dire la valeur binaire 1, comme indiqué par l'encadrement du deuxième élément binaire du mot c'_1 sur la figure 5.

Puisque $H(c'_1) = H(c_1) = 1$, la vérification biométrique est valide. L'individu 1 est authentifié avec succès. Il pourra ensuite bénéficier éventuellement de la délivrance d'un droit par exemple.

La figure 6 illustre un cas de vérification biométrique relativement à un individu 2 essayant de se faire passer pour l'individu 1.

Une chaîne binaire w_2 caractérisant l'individu 2 est obtenue, à partir d'une mesure biométrique par exemple. Cette chaîne w_2 diffère largement de la chaîne w_1 relative à l'individu 1. Onze éléments binaires (entourés sur la figure 6) sont en effet différents entre ces deux chaînes.

Lors de la vérification biométrique, on calcule la chaîne $w_2 \oplus w_1 \oplus c_1$, puis on détermine le mot c_2 du code C le plus proche de cette chaîne, à l'aide des propriétés de décodage d'erreurs du code. Dans le présent exemple, la chaîne $w_2 \oplus w_1 \oplus c_1$ présente trois différences avec le mot m_4 (éléments binaires entourés), si bien qu'on conclut que $c_2 = m_4$.

Le deuxième élément binaire de c_2 (encadré sur la figure 6) étant un 0,

- 17 -

on a donc $H(c_2)=0$. $H(c_2)$ diffère donc de $H(c_1)$, de sorte que la vérification est un échec. L'individu 2 n'a donc pas pu se faire passer pour l'individu 1.

Dans l'exemple de la figure 7, un individu 3 caractérisé par une chaîne binaire w_3 tente de se faire passer pour l'individu 1. Il y parvient puisque la
 5 chaîne binaire $w_3 \oplus w_1 \oplus c_1$ est assimilée au mot de code $c_3=m_1$ et que $H(c_3)=H(m_1)=H(m_3)=H(c_1)=1$, comme cela apparaît sur la figure 3.

Cet exemple correspond à un cas de fausse acceptation, toléré par l'application visée. Cette fausse acceptation est due au faible pouvoir discriminant de l'identifiant $H(c_1)$ qui ne peut prendre que deux valeurs 0 ou 1.
 10 Ainsi, quelle que soit la chaîne binaire w_i relative à un individu i , on a une chance sur deux pour que $H(c_i)=H(c_1)$.

Ce niveau d'incertitude est acceptable pour l'application visée. Il permet en outre de ne pas pouvoir retrouver l'identité I_i d'un individu i à partir de son identifiant $H(c_i)$, même pour une personne ayant accès à la structure de
 15 données stockant I_i et $H(c_i)$ en association.

La présente invention peut également être utilisée dans des applications d'identification, c'est-à-dire pour retrouver l'identité d'un individu à partir de sa biométrie.

Ainsi, si l'on se réfère à nouveau à la figure 2, on cherche désormais à
 20 obtenir l'identité de l'individu 1. Les étapes 12 à 14 sont mises en œuvre comme décrit plus haut, si ce n'est que la chaîne w'_1 est ajoutée à toutes les chaînes $w_1 \oplus c_1$, $w_2 \oplus c_2, \dots, w_m \oplus c_m$ stockées dans la base de données 8 relativement à des individus distincts, ou à au moins une pluralité d'entre ces chaînes.

25 On vérifie ensuite, pour chaque condensé $H(c'_1)$, $H(c'_2), \dots, H(c'_m)$ obtenu, si celui-ci correspond à l'identifiant $H(c_1)$, $H(c_2), \dots, H(c_m)$ correspondant, stocké dans la base de données 8.

Lorsqu'une égalité est détectée, on peut en déduire une identité de l'individu considéré. Par exemple si $H(c'_1)=H(c_1)$, on peut alors conclure que
 30 l'individu 1 possède l'identité I_1 stockée en association avec $H(c_1)$.

On notera cependant que la détermination univoque de l'identité ne

- 18 -

sera a priori possible que pour des tailles de bases inférieures à une certaine limite déterminée par le pouvoir discriminant. En général, plusieurs identités peuvent correspondre.

REVENDEICATIONS

1. Procédé de vérification biométrique utilisant un premier support de données (8) stockant de façon associée, pour au moins un individu (1) d'un ensemble d'individus, une identité (I_1) relative audit individu, le résultat ($w_1 \oplus c_1$) d'un ajout d'un premier mot (c_1) d'un code correcteur d'erreurs associé audit individu à une première chaîne numérique (w_1) obtenue à partir d'une donnée biométrique relative audit individu et au moins deux identifiants de pouvoirs discriminants déterminés distincts obtenus par application de fonctions de hachage respectives au premier mot du code correcteur d'erreurs, le procédé comprenant les étapes suivantes relativement à un individu (1) de l'ensemble d'individus :

obtenir une donnée biométrique relative à l'individu;
convertir la donnée biométrique en une deuxième chaîne numérique w'_1);
déterminer un deuxième mot (c'_1) du code correcteur d'erreurs correspondant sensiblement à l'ajout à la deuxième chaîne numérique (w'_1) du résultat ($w_1 \oplus c_1$) de l'ajout du premier mot du code correcteur d'erreurs à la première chaîne numérique stocké sur le premier support de données (8) en association avec l'identité (I_1) relative audit individu;
déterminer un niveau de discrimination souhaité;
déterminer un identifiant ($H(c_1)$) stocké sur le premier support de données en association avec l'identité relative audit individu, ayant un pouvoir discriminant correspondant sensiblement au niveau de discrimination souhaité;
appliquer au deuxième mot (c'_1) du code correcteur d'erreurs la fonction de hachage par application de laquelle ledit identifiant déterminé a été obtenu; et
comparer le résultat ($H(c'_1)$) de l'application de ladite fonction de hachage au deuxième mot du code correcteur d'erreurs avec l'identifiant déterminé ($H(c_1)$).

2. Procédé selon la revendication 1, dans lequel certaines au moins des fonctions de hachage appliquées au premier mot du code correcteur d'erreurs sont choisies pour avoir un espace d'arrivée équiprobable comprenant un nombre de valeurs possibles correspondant sensiblement au pouvoir discriminant déterminé de l'identifiant respectif.

3. Procédé selon la revendication 1 ou 2, comprenant en outre la délivrance d'un droit lorsque la comparaison révèle une égalité entre le résultat ($H(c'_1)$) de l'application de ladite fonction de hachage au deuxième mot du code correcteur d'erreurs et l'identifiant déterminé ($H(c_1)$).

4. Procédé selon l'une quelconque des revendications 1 à 3, utilisant en outre un deuxième support de données (11) stockant de façon associée, pour au moins ledit individu (1) de l'ensemble d'individus, la première chaîne numérique (w_1) obtenue à partir d'une donnée biométrique relative audit individu et les identifiants de pouvoirs discriminants déterminés distincts obtenus par application de fonctions de hachage respectives au premier mot (c_1) du code correcteur d'erreurs associé audit individu, le procédé comprenant en outre les étapes suivantes relativement audit individu (1) de l'ensemble d'individus :

10 retrouver la première chaîne numérique (w_1) stockée sur le deuxième support de données (11) et correspondant sensiblement à ladite deuxième chaîne numérique (w'_1) ;

15 retrouver un identifiant ($H(c_1)$) stocké sur le deuxième support de données (11) en association avec la première chaîne numérique (w_1) retrouvée, ayant un pouvoir discriminant correspondant sensiblement au niveau de discrimination souhaité; et

 comparer le résultat ($H(c'_1)$) de l'application de la fonction de hachage (H) par application de laquelle l'identifiant retrouvé a été obtenu au deuxième mot (c'_1) du code correcteur d'erreurs avec l'identifiant retrouvé ($H(c_1)$).

20 5. Système de vérification biométrique comprenant des moyens (2) pour obtenir une donnée biométrique et des moyens (12-17) de traitement numérique agencés pour mettre en œuvre le procédé tel que défini selon l'une quelconque des revendications 1 à 4.

25 6. Produit programme d'ordinateur comprenant une mémoire physique stockant des instructions de code adaptées à la mise en œuvre du procédé tel que défini selon l'une quelconque des revendications 1 à 4, lorsqu'il est chargé et exécuté par des moyens informatiques.

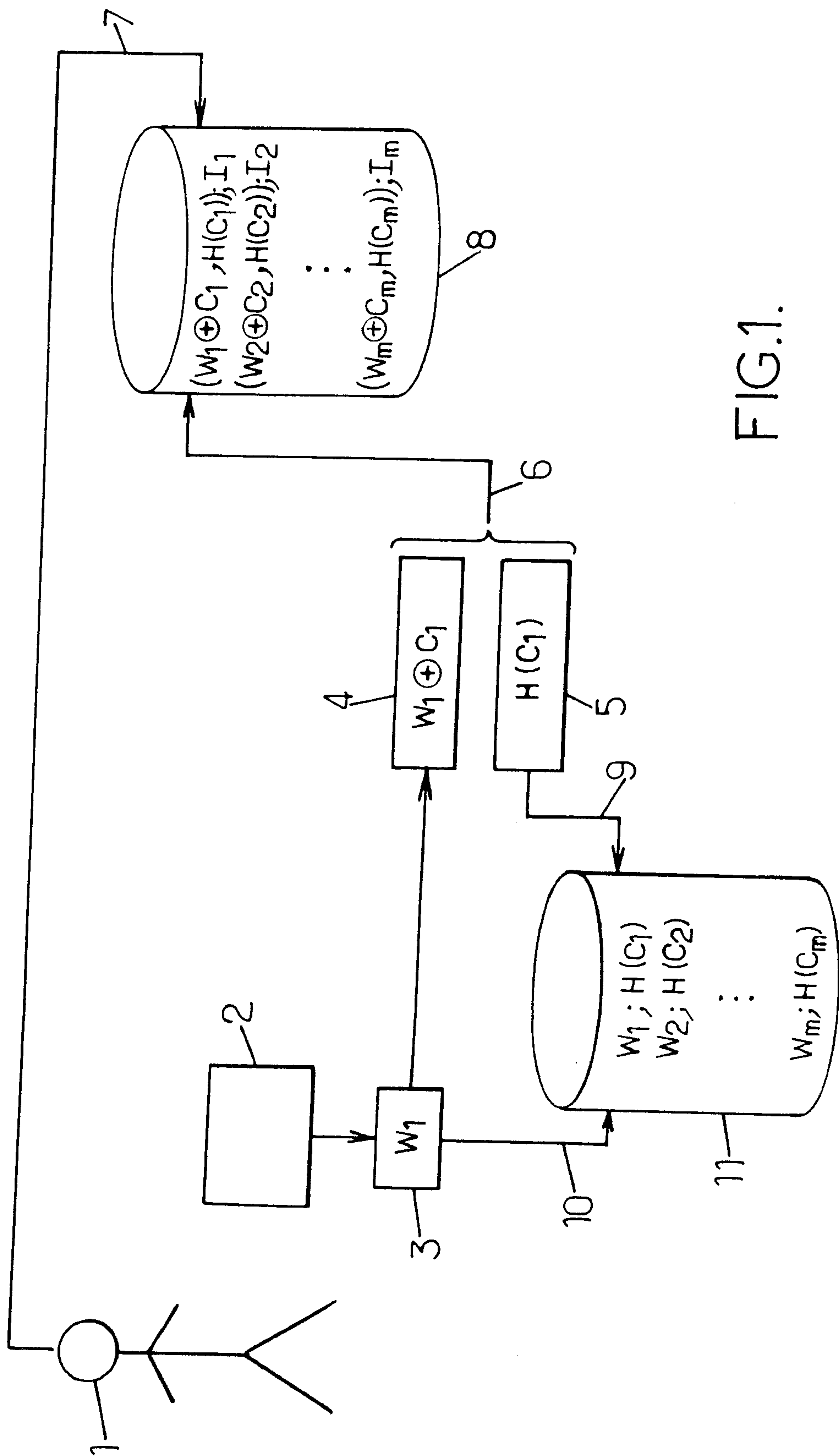


FIG.1.

2/5

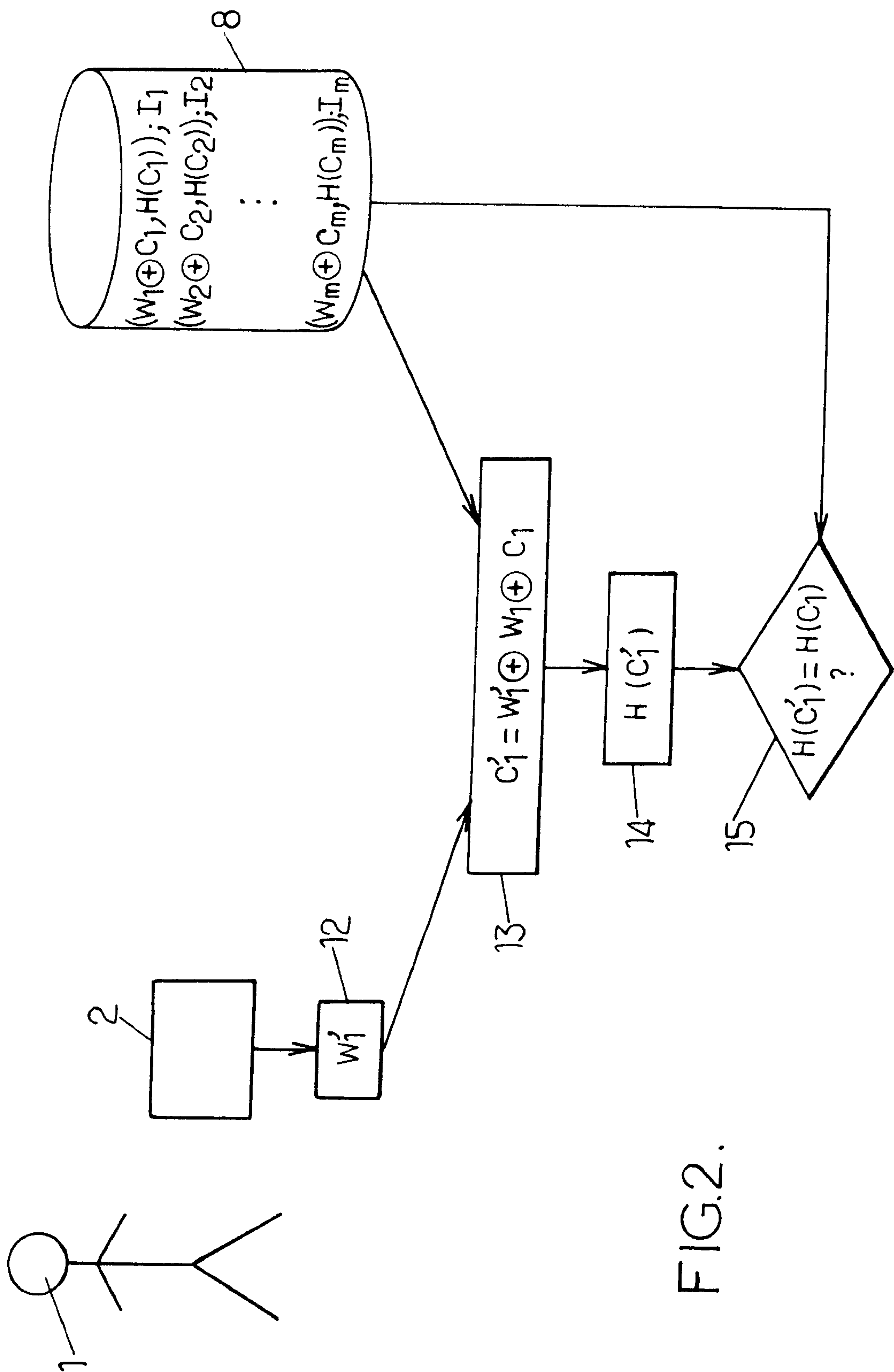


FIG. 2.

3/5

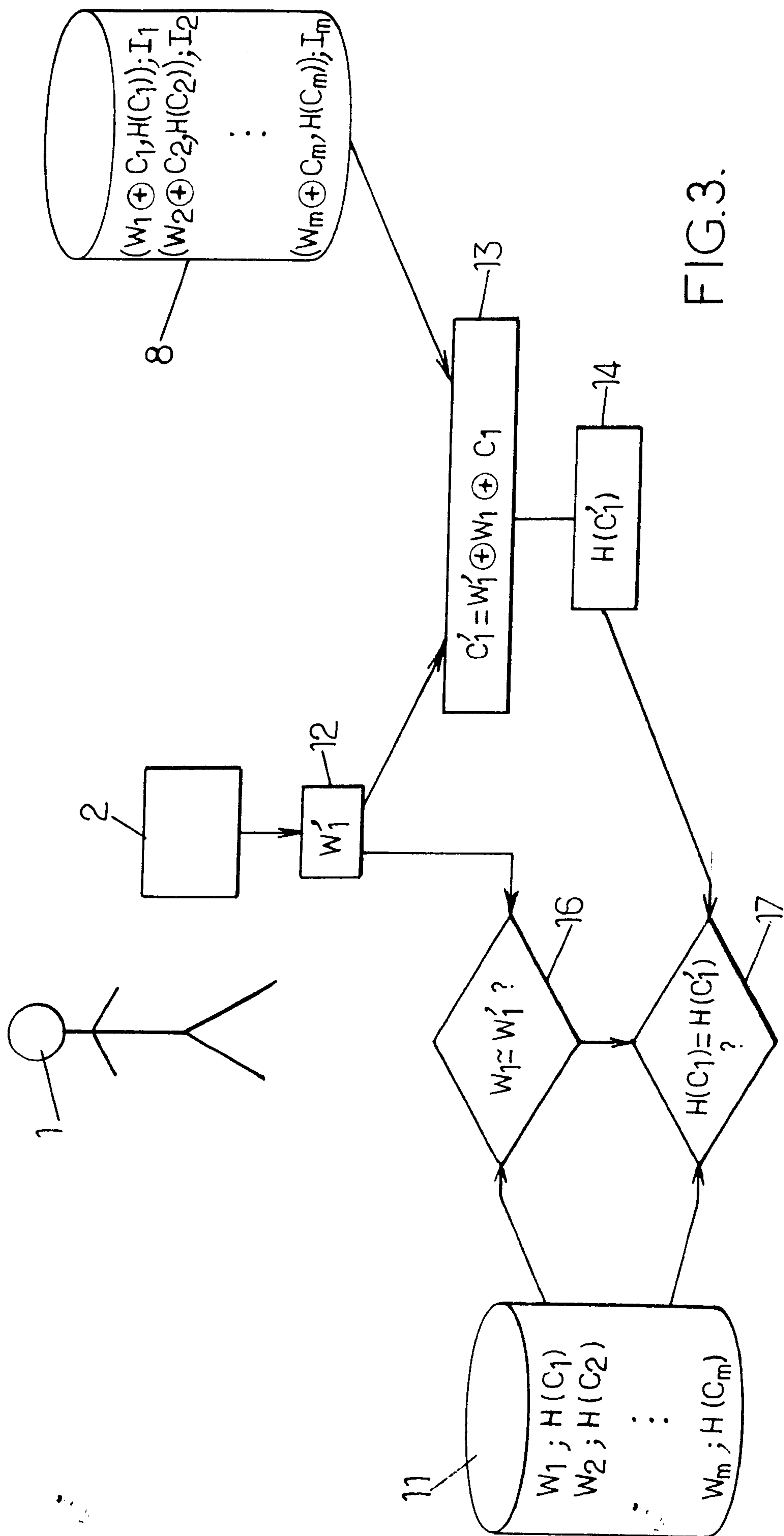


FIG. 3.

4/5

$$\begin{array}{cccccccccccccccc}
 w_1 = & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
 c_1 = m_3 = & 1 & \boxed{1} & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\
 & & & & & & & & & & & & & & \\
 w_1 \oplus c_1 = & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1
 \end{array}$$

FIG.4.

$$\begin{array}{cccccccccccccccc}
 w'_1 = & 1 & \textcircled{1} & 0 & 1 & 1 & 1 & 1 & \textcircled{1} & 0 & 0 & 0 & 1 & 1 & \textcircled{1} \\
 w'_1 \oplus w_1 \oplus c_1 = & 1 & \textcircled{0} & 1 & 1 & 1 & 1 & 1 & \textcircled{0} & 1 & 1 & 1 & 1 & 1 & \textcircled{0} \\
 c'_1 = & 1 & \boxed{1} & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 = m_3 \\
 & & & & & & & & & & & & & & \\
 & & & & & & & & & & & & & &
 \end{array}$$

FIG.5.

