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

(11) **EP 1 747 526 B1**

(12) **FASCICULE DE BREVET EUROPEEN**

(45) Date de publication et mention de la délivrance du brevet:
11.01.2012 Bulletin 2012/02

(21) Numéro de dépôt: **05749585.5**

(22) Date de dépôt: **11.05.2005**

(51) Int Cl.:
G06K 9/00 *(2006.01)* ***H04L 9/32*** *(2006.01)*

(86) Numéro de dépôt international:
PCT/EP2005/052151

(87) Numéro de publication internationale:
WO 2005/111915 (24.11.2005 Gazette 2005/47)

(54) **Procédé de masquage d'une donnée numérique, telle que par exemple une empreinte biometrique**

Verfahren zur Maskierung eines digitalen Datenelements wie etwa eines biometrischen Abdrucks und Verwendung dafür zur Sicherung eines Sicherheitsdokuments

Method of masking a digital datum, such as a biometric print, and use thereof for securing a security document

(84) Etats contractants désignés:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU MC NL PL PT RO SE SI SK TR

(30) Priorité: **14.05.2004 FR 0405236**

(43) Date de publication de la demande:
31.01.2007 Bulletin 2007/05

(73) Titulaire: **Gemalto SA**
92190 Meudon (FR)

(72) Inventeurs:
- **NACCACHE, David**
  F-75018 Paris (FR)
- **BRIER, Eric**
  F-13400 Aubagne (FR)
- **CORON, Jean-Sébastien**
  L-2551 Luxembourg (LU)
- **CARDONNEL, Cédric**
  F-13470 Carnoux en Provence (FR)

(56) Documents cités:
US-B1- 6 185 316 **US-B1- 6 697 947**

Il est rappelé que: Dans un délai de neuf mois à compter de la publication de la mention de la délivrance du brevet européen au Bulletin européen des brevets, toute personne peut faire opposition à ce brevet auprès de l'Office européen des brevets, conformément au règlement d'exécution. L'opposition n'est réputée formée qu'après le paiement de la taxe d'opposition. (Art. 99(1) Convention sur le brevet européen).

EP 1 747 526 B1

Printed by Jouve, 75001 PARIS (FR)

Description

[0001] L'invention a pour objet les systèmes d'identification et / ou d'authentification biométrique. Ces systèmes manipulent des données biométriques de tous types telles que par exemple des empreintes digitales, des empreintes numériques de l'oeil, de la peau, du visage, ou même de la voix.

[0002] L'utilisation d'empreintes biométriques est de plus en plus envisagée pour compléter des mots de passe utilisateur ou une signature manuelle, notamment pour des applications nécessitant un haut niveau de sécurité. En effet, l'utilisation d'une empreinte biométrique est un bon complément à un mot de passe ou une signature manuelle, dans la mesure où une empreinte biométrique peut difficilement être dérobée à son propriétaire réel et ne peut pas non plus être imitée, copiée. En contrepartie de cette sécurité et dans la mesure où une empreinte biométrique ne peut pas être remplacée, il est indispensable d'empêcher l'accès direct à cette empreinte afin de garantir la sécurité des personnes et la fiabilité de l'empreinte.

[0003] Pour cela, on peut par exemple envisager des procédés de masquage connus pour masquer l'empreinte biométrique à sécuriser. L'empreinte masquée peut être ensuite utilisée en lieu et place de l'empreinte claire, pour signer un message, authentifier l'identité d'une personne, etc. L'intérêt de tels procédés est l'utilisation de fonctions de hachage, qui sont des fonctions à sens unique, c'est-à-dire qu'elles ne peuvent pas être inversées. En d'autres termes, connaissant une empreinte masquée par une fonction de hachage à partir d'une empreinte claire, il n'est pas possible de retrouver l'empreinte claire, même en connaissant tous les paramètres de la fonction de hachage.

[0004] Il est bien connu par ailleurs qu'il n'est pas possible de prendre deux empreintes biométriques strictement identiques d'un même individu à des instants différents. D'abord parce qu'il est très difficile de positionner, de manière strictement identique mais à des instants différents, un même instrument de mesure adapté pour relever la dite empreinte biométrique. Ensuite par ce que l'environnement (température, humidité, etc.) et l'état de santé général (stress, maladie de peau, etc.) de l'individu au moment où l'empreinte est relevée peut perturber le résultat du relevé.

[0005] Or, avec les fonctions de hachage connues, partant de deux données initiales peu différentes, les données masquées correspondantes sont très différentes et décorrélées, de sorte qu'il n'est pas possible, en les comparant, d'en déduire si les données initiales sont identiques à quelques erreurs près ou pas. Il n'est donc pas possible d'utiliser les fonctions de hachage connues pour masquer une empreinte biométrique.

[0006] Le document US 6 697 947 B1 (MATYAS JR, STEPHEN, MICHAEL ET AL; 24 février 2004) décrit un schéma de masquage de données biométriques qui utilise une fonction peu sensible aux erreurs basée sur une opération d'exponentiation modulaire.

[0007] Un premier objet de l'invention est de proposer un procédé de masquage utilisant une nouvelle fonction de hachage, mieux adaptée pour masquer des empreintes biométriques que les fonctions de hachage connues. Dans un mode préféré de mise en oeuvre, le procédé de masquage selon l'invention est utilisé pour sécuriser une empreinte biométrique.

[0008] Enfin, un deuxième objet de l'invention est une utilisation du procédé de masquage de l'invention pour sécuriser un document de sécurité tel que par exemple un chèque bancaire.

[0009] Le premier objet de l'invention est atteint par un procédé de masquage d'une donnée claire b de n bits, caractérisé en ce qu'on produit une donnée masquée m en utilisant la fonction de hachage suivante : $m = \prod_{i=1}^{n} q_i^{b_i} \bmod p$, où p est un nombre premier, bi est le bit de rang i de la donnée claire b, qi est le nombre premier de rang i d'un ensemble de nombres premiers $(q_1, ..., q_n)$. De préférence, p est un nombre premier de grande taille et les éléments de l'ensemble de nombres premiers sont de petite taille.

[0010] Par rapport aux fonctions de hachage connues, la fonction $m = \prod_{i=1}^{n} q_i^{b_i} \bmod p$ a pour principal intérêt d'être tolérante aux erreurs, comme on le verra mieux par la suite, elle est de ce fait particulièrement bien adaptée pour masquer des données biométriques.

[0011] Dans un mode préféré de mise en oeuvre, le procédé de masquage ci-dessus est appliqué à une empreinte biométrique. Pour cela, au cours du procédé, on détermine un ensemble de s minuties réelles caractéristiques de la dite empreinte, on mélange et on range les minuties réelles avec t fausses minuties, on forme une donnée mélangée b de n = s + t bits telle que, pour tout i :

$b_i = 1$ si le rang i correspond à une minutie réelle et
$b_i = 0$ si le rang i correspond à une fausse minutie.

et on applique la fonction de hachage selon l'invention à cette donnée mélangée pour produire une donnée masquée.

[0012] De préférence, les minuties réelles et les fausses minuties sont mélangées de façon aléatoire.

[0013] Le deuxième objet de l'invention concerne quant à lui un procédé de sécurisation d'un document de sécurité, par exemple d'un chèque bancaire, au cours duquel, après avoir obtenu une donnée de référence par masquage d'une empreinte biométrique selon un procédé tel que décrit ci-dessus,

- on mémorise la dite donnée de référence sur ou dans le document de sécurité, ou
- on associe à la dite donnée de référence un code - barre que l'on mémorise sur ou dans le document de sécurité, la donnée de référence et le code - barre étant également mémorisés dans une table.

[0014] Des exemples préférés de mise en oeuvre de l'invention sont décrits ci-dessous.

[0015] On va tout d'abord détailler le procédé de masquage selon l'invention. Pour masquer une donnée claire $b = (b_n, ..., b_1)$ de n bits, on utilise la fonction de hachage suivante:

$$m = \prod_{i=1}^{n} q_i^{b_i} \bmod p$$

[0016] La fonction utilise comme paramètres un ensemble $(q_n, ..., q_1)$ de petits nombres premiers, par exemple des nombres entiers d'environ 60 bits. La fonction utilise également un paramètre p, qui est un entier de grande taille, par exemple d'environ 1024 bits. p est choisi de préférence tel que $2*q_n\text{^}2t < p < 4*q_n\text{^}2t$, où t est un nombre d'erreurs acceptées.

[0017] Contrairement aux fonctions de hachage connues, la fonction selon l'invention est peu sensible aux erreurs, c'est-à-dire que, connaissant deux données m, μ masquées par cette fonction, il est possible de dire si les données claires d'origine b, β correspondantes sont identiques, à au maximum t erreurs près.

[0018] En effet, m, μ sont obtenues par les relations :

$$m = \prod_{i=1}^{n} q_i^{b_i} \bmod p \quad \text{et} \quad \mu = \prod_{i=1}^{n} q_i^{\beta_i} \bmod p,$$

[0019] On définit de plus :

$$\lambda = \frac{m}{\mu} \bmod (p) = \frac{a}{\alpha} \bmod p$$

avec

$$a = \prod_{i \in \Delta_i} q_i \bmod p \quad \text{et} \quad \alpha = \prod_{i \in \Gamma_i} q_i \bmod p$$

où Δ_i est l'ensemble des indices i compris entre 1 et n pour lesquels $b_i = 1$ et $\beta_i = 0$, et où Γ_i est l'ensemble des indices i compris entre 1 et n pour lesquels $b_i = 0$ et $\beta_i = 1$. La somme des tailles des ensembles Δ_i et Γ_i est au plus égale à t, t étant le nombre de bits de β différents des bits de b de même rang, correspondant au nombre maximum d'erreurs acceptées.

[0020] a et α, qui sont des produits de petits nombres premiers q_i, sont également des petits nombres, qui vérifient de plus la relation : $a*\lambda = \alpha \bmod p$. A partir de cette dernière égalité et du nombre λ, il est alors possible de retrouver les nombres a et α. Une décomposition de a et α en nombres premiers permet finalement factoriser a et α. La décomposition est facilitée en tirant partie du fait que a et α se décomposent en principe en de petits nombres premiers. Si a et α se décomposent sur l'ensemble $(q_n, ..., q_1)$, alors on en déduit que les données d'origine b et β sont identiques, à au plus t erreurs près.

[0021] On va maintenant décrire un mode préféré de mise en oeuvre du procédé de masquage utilisant la fonction

de masquage décrite ci-dessus, pour le masquage d'une empreinte biométrique.

[0022] Dans l'exemple ci-dessous, l'empreinte biométrique physique que l'on cherche à masquer est une empreinte digitale caractérisée par un nombre s prédéfini de minutiae réelles. Une minutie réelle est un détail d'une empreinte en un point donné de l'empreinte physique, comme par exemple une rupture d'une ligne, une fourche sur une ligne, etc. Numériquement, une minutie peut être traduite par une chaîne de caractères incluant des informations sur la position et la forme de la minutie.

[0023] Selon l'invention, pour masquer l'empreinte physique, on ajoute d'abord à l'ensemble des minuties réelles un ensemble de t fausses minuties, également définies par une chaîne de caractères mais qui ne correspondent pas à une minutie réelle de l'empreinte physique. Dans un exemple, une fausse minutie est définie de manière totalement aléatoire, et on ajoute un ensemble de t = 80 fausses minuties à un ensemble de s = 20 minuties réelles.

[0024] L'ordre des minuties réelles et des fausses minutiae est mélangé, par exemple de façon aléatoire, puis on forme une donnée mélangée $b = (b_n, ..., b_1)$ de n = s + t bits telle que, pour tout i :

$b_i = 1$ si le rang i correspond à une minutie réelle et
$b_i = 0$ si le rang i correspond à une fausse minutie.

[0025] La donnée mélangée b est ensuite masquée par le procédé de masquage selon l'invention pour produire une donnée masquée m telle que :

$$m = \prod_{i=1}^{n} q_i^{b_i} \bmod p$$

[0026] La donnée masquée m peut ensuite être mémorisée dans une base de données, sur une carde d'identité, dans une mémoire d'une carte à puce, etc. La donnée masquée m peut être utilisée comme donnée de référence, par exemple pour vérifier l'identité d'une personne, de la manière suivante.

[0027] Pour vérifier l'identité d'une personne, il suffit :

- de relever une nouvelle empreinte biométrique physique sur la personne puis de calculer l'ensemble de s minuties réelles correspondant,
- d'ajouter t fausses minuties, de mélanger les fausses minuties et les vraies minuties, de déterminer la donnée mélangée β associée à la nouvelle empreinte biométrique, puis de masquer β par la fonction $\mu = \prod_{i=1}^{n} q_i^{\beta_i} \bmod p$ pour obtenir une nouvelle donnée masquée μ,
- de déterminer s'il y a concordance entre la donnée référence m précédemment mémorisée et la donnée μ masquée obtenue à partir de la nouvelle empreinte réelle qui vient d'être relevée.

[0028] Pour déterminer s'il y a concordance entre m et μ :

- on calcule $\lambda = \frac{m}{\mu} \bmod p = \frac{a}{\alpha} \bmod p$, puis a et α à partir de la relation $a^*\lambda = \alpha \bmod p$, avec a et α petits devant l'entier p, par l'algorithme des fractions continues par exemple.
- on décompose ensuite a et α en facteurs premiers, puis
  - il y a concordance si a et α se décomposent sur au plus t éléments de l'ensemble des nombres premiers (q_n , ..., q_l),
  - il n'y a pas concordance sinon

[0029] Une application envisagée du procédé de masquage selon l'invention vise à sécuriser un document de sécurité tel que par exemple un chèque bancaire. Pour cela, selon l'invention, une empreinte biométrique du propriétaire du document de sécurité est masquée par un procédé de masquage tel que décrit ci-dessus, pour produire une donnée de référence.

[0030] Selon un premier mode de réalisation, la donnée de référence est mémorisée sur ou dans le document de sécurité, par exemple par impression.

[0031] Selon un deuxième mode de réalisation, la donnée de référence est associée à un code - barre, le couple donnée de référence / code - barre associé est mémorisé dans une base de donnée, et le code - barre est mémorisé,

par exemple par impression, sur le document de sécurité.

[0032] Il suffit ensuite, lorsque le document de sécurité est transmis par exemple, de prendre simultanément avec le document de sécurité une empreinte biométrique de la personne qui transmet le dit document puis de vérifier que l'empreinte biométrique de la personne qui transmet le document correspond bien à l'empreinte incluse dans la donnée de référence mémorisée sur le document ou associée au code - barre mémorisé sur le document.

[0033] Dans le premier mode de réalisation, la vérification pourra être faite par toute personne , la donnée de référence étant mémorisée directement sur le document. Dans le deuxième mode de réalisation, la vérification pourra être faite par toute personne ayant accès à la base de données, et qui n'est pas nécessairement la personne qui reçoit le document.

[0034] Le code - barre est réalisé selon des techniques connues, on pourra utiliser par exemple un code - barre à une dimension, constitué d'une série de barres verticales d'épaisseur et d'écartement variables. Le choix de la forme du code - barre est en pratique fonction du nombre de données de référence à mémoriser, chaque donnée de référence correspondant à des personnes différentes.

[0035] De préférence, la base de données dans laquelle les couples donnée de référence / code - barre associé sont mémorisés est accessible pour vérification uniquement à un nombre restreint de personnes, selon le niveau de sécurité souhaité : l'accès peut par exemple être autorisé pour toute personne amenée à recevoir des documents de sécurité ou, de manière plus restreinte, uniquement à une autorité certificatrice.

[0036] Dans un exemple pratique, le document de sécurité est un chèque bancaire et l'empreinte digitale de son propriétaire est mémorisée sur le chèque sous la forme d'un code - barre. Un commerçant dispose d'un dispositif de lecture et de masquage d'une empreinte doté de moyens pour lire une empreinte, la masquer puis imprimer la donnée masquée associée. La banque émettrice du chèque a seule le droit d'accès à la base de données dans laquelle sont mémorisés la donnée masquée de référence (correspondant à l'empreinte initiale masquée) et le code - barre associé ; cet accès lui permet de vérifier que l'empreinte laissée par la personne qui a présenté le chèque au commerçant, et que ce dernier a masqué et imprimé sur le chèque, correspond bien à celle du propriétaire du chèque.

Revendications

1. Procédé de masquage d'une donnée claire b de n bits, **caractérisé en ce qu'**on produit une donnée masquée m en utilisant la fonction de hachage suivante : $m = \prod_{i=1}^{n} q_i^{b_i} \bmod p$, où p est un nombre premier, bi est le bit de rang i de la donnée claire b, q_i est le nombre premier de rang i d'un ensemble de nombres premiers (q_1, ..., q_n).

2. Procédé de masquage selon la revendication 1, dans lequel p est un nombre premier de grande taille et les éléments de l'ensemble de nombres premiers sont de petite taille.

3. Procédé de masquage selon l'une quelconque des revendications 1 et 2, appliqué à une empreinte biométrique, **caractérisé en ce qu'**on détermine un ensemble de s minuties réelles caractéristiques de la dite empreinte, **en ce qu'**on mélange et on range les minuties réelles avec t fausses minuties, **en ce qu'**on forme une donnée mélangée b de n = s + t bits telle que, pour tout i :

   b_i = 1 si le rang i correspond à une minutie réelle et
   b_i = 0 si le rang i correspond à une fausse minutie,

   et **en ce qu'**on applique la fonction de hachage à cette donnée mélangée pour produire une donnée masquée.

4. Procédé selon la revendication 3, dans lequel les minuties réelles et les fausses minuties sont mélangées de façon aléatoire.

5. Procédé de sécurisation d'un document de sécurité, par exemple d'un chèque bancaire, au cours duquel, après avoir obtenu une donnée de référence par masquage d'une empreinte biométrique selon un procédé selon la revendication 3 et 4,

   • on mémorise la dite donnée de référence sur ou dans le document de sécurité, ou
   • on associe à la dite donnée de référence un code - barre que l'on mémorise sur ou dans le document de sécurité, la donnée de référence et le code -barre étant par ailleurs mémorisés dans une table.

6. Procédé de vérification d'un document de sécurité sécurisé par un procédé selon la revendication 5, procédé de vérification au cours duquel :

- on numérise une empreinte biométrique physique d'une personne présentant le document de sécurité,
- on masque l'empreinte numérisée par un procédé selon l'une des revendications 3 à 4, pour produire une donnée masquée,
- on compare la donnée masquée avec une donnée de référence, puis
- on accepte le document de sécurité si la donnée masquée et la donnée de référence sont identiques à un taux d'erreur près prédéfini, ou on refuse le titre sinon.

7. Procédé selon la revendication 6, dans lequel, lors de l'étape de comparaison, si un code - barre associé à la donnée de référence est mémorisé sur le document de sécurité, alors :

- on lit le code - barre et on recherche dans une table la donnée de référence associée au code - barre, puis
- on compare la donnée de référence avec la donnée masquée.

Claims

1. Method of masking a plain datum b having n bits, **characterised in that** a masked datum m is produced using the following hash function: $m = \prod_{i=1}^{n} q_i^{b_i} \bmod p$, where p is a prime number, b_i is the bit at position i of plain datum b, and q_i is the prime number at position i in a set of prime numbers (q_i...,q_n) .

2. Masking method according to claim 1, in which p is a large prime number and the components of the set of prime numbers are small.

3. Masking method according to either one of the claims 1 or 2, applied to a biometric print, **characterised in that** it consists in determining a set of s real minutiae, which are characteristic of said print, mixing and arranging the real minutiae with t false minutiae, and forming a mixed biometric datum b having n = s + t bits, such that, for any i:

b_i = 1 if position i corresponds to a real minutia and
b_i = 0 if position i corresponds to a false minutia

and the hash function according to the invention is applied to this mixed datum in order to produce a masked datum.

4. Method according to claim 3, in which the real minutiae and the false minutiae are mixed in a random fashion.

5. Method of securing a security document, for example a bank cheque, during which, after having obtained a reference datum by masking a biometric print according to a method according to claim 3 and 4,

- said reference datum is stored on or in the security document, or
- a barcode is associated with said reference datum, which is stored on or in the security document, the reference datum and the barcode also being stored in a table.

6. Method of verifying a security document secured by a method according to claim 5, verification method during which;

- a physical biometric print of a person presenting the security document is digitised,
- the digitised print is masked using a method according to one of the claims from 3 to 4, to produce a masked datum,
- the masked datum is compared with a reference datum, and then
- the security document is accepted if the masked datum and the reference datum are identical with a predefined rate of error, and the document is refused otherwise.

7. Method according to claim 6, in which, during the comparison step, if a barcode associated with the reference datum is stored on the security document, then:

- the barcode is read and the reference datum associated with the barcode is searched in a table, and then
- the reference datum is compared with the masked datum.

Patentansprüche

1. Maskierungsverfahren einer klaren Angabe b von n Bits, **dadurch gekennzeichnet, dass** man eine maskierte Angabe m erzeugt, indem man die folgende Hash-Funktion verwendet: $m = \prod_{i=1}^{n} q_i^{b_i} \bmod p$, wobei p eine Primzahl ist, b_i der Bit des Rangs i der klaren Angabe b ist, q_i die Primzahl des Rangs i einer Einheit von Primzahlen (q_1, ..., q_n) ist.

2. Maskierungsverfahren gemäß Anspruch 1, bei dem p eine große Primzahl ist und die Elemente der Einheit von Primzahlen klein sind.

3. Maskierungsverfahren gemäß einem der Ansprüche 1 und 2, angewendet auf einen biometrischen Abdruck, **dadurch gekennzeichnet, dass** man eine Einheit von s echten Minutien bestimmt, die charakteristisch sind für den genannten Abdruck, dass man die echten Minutien mit t falschen Minutien vermischt und ordnet, dass man eine gemischte Angabe b von n = s + t Bits bildet, so dass für ganz i:

   b_i - 1, wenn der Rang i einer echten Minutie entspricht, und
   b_1 = 0, wenn der Rang i einer falschen Minutie entspricht,

   und dass man die Hash-Funktion auf diese gemischte Angabe anwendet, um eine maskierte Angabe zu erzeugen.

4. Verfahren gemäß Anspruch 3, bei dem die echten Minutien und die falschen Minutien zufällig gemischt werden.

5. Sicherungsverfahren einer Sicherheitsunterlage, beispielsweise eines Bankschecks, bei dem man, nach Erhalt einer Referenzangabe durch Maskierung eines biometrischen Abdrucks gemäß einem Verfahren nach Anspruch 3 und 4,

   . die genannte Referenzangabe auf oder in der Sicherheitsunterlage speichert, oder
   . die genannte Referenzangabe mit einem Strichcode verbindet, den man auf oder in der Sicherheitsunterlage speichert, wobei die Referenzangabe und der Strichcode ferner in einer Tabelle gespeichert werden.

6. Prüfverfahren einer Sicherheitsunterlage, die durch ein Verfahren nach Anspruch 5 gesichert wurde, Prüfverfahren bei dem man:

   . einen physischen biometrischen Abdruck einer Person digitalisiert, die die Sicherheitsunterlage präsentiert,
   . den digitalisierten Abdruck nach einem Verfahren gemäß einem der Ansprüche 3 bis 4 maskiert, um eine maskierte Angabe zu erzeugen,
   . die maskierte Angabe mit einer Referenzangabe vergleicht, und
   . die Sicherheitsunterlage akzeptiert, wenn die maskierte Angabe und die Referenzangabe bis auf eine Vorbestimmte Fehlerrate identisch sind, oder man die Unterlage ansonsten ablehnt.

7. Verfahren gemäß Anspruch 6, bei dem man während des Vergleichsschritts, wenn ein Strichcode, verbunden mit der Referenzangabe, auf der Sicherheitsunterlage gespeichert ist:

   . den Strichcode liest und in einer Tabelle die mit dem Strichcode verbundene Referenzangabe sucht, und
   . die Referenzangabe mit der maskieren Angabe vergleicht.

RÉFÉRENCES CITÉES DANS LA DESCRIPTION

Cette liste de références citées par le demandeur vise uniquement à aider le lecteur et ne fait pas partie du document de brevet européen. Même si le plus grand soin a été accordé à sa conception, des erreurs ou des omissions ne peuvent être exclues et l'OEB décline toute responsabilité à cet égard.

Documents brevets cités dans la description

- US 6697947 B1, MATYAS JR, STEPHEN, MICHAEL
  [0006]