(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2012-511202
(P2012-511202A)
(43)公表日　平成24年5月17日(2012.5.17)

(51)Int.Cl.		F I			テーマコード（参考）
G06T 7/00	(2006.01)	G06T	7/00	510B	5B043
G06F 21/20	(2006.01)	G06F	15/00	330F	5B285

審査請求 未請求　予備審査請求 未請求　（全 24 頁）

(21)出願番号　特願2011-539086 (P2011-539086)
(86)(22)出願日　平成21年12月4日 (2009.12.4)
(85)翻訳文提出日　平成23年8月5日 (2011.8.5)
(86)国際出願番号　PCT/FR2009/052420
(87)国際公開番号　WO2010/066992
(87)国際公開日　平成22年6月17日 (2010.6.17)
(31)優先権主張番号　0858364
(32)優先日　平成20年12月8日 (2008.12.8)
(33)優先権主張国　フランス(FR)

(71)出願人　508256673
モルフォ
フランス・Ｆ－７５０１５・パリ・リュ・ルブラン・２７・ル・ポナン・ドゥ・パリ
(74)代理人　100108453
弁理士　村山　靖彦
(74)代理人　100064908
弁理士　志賀　正武
(74)代理人　100089037
弁理士　渡邊　隆
(74)代理人　100110364
弁理士　実広　信哉
(72)発明者　ブルーノ・キンダルジ
フランス・Ｆ－７５０１５・パリ・リュ・ルブラン・２７・サジェム・セキュリテ内
最終頁に続く

(54)【発明の名称】識別または許可の方法ならびに関連するシステムおよび安全モジュール

(57)【要約】
本発明は、生体計測データを獲得するための少なくとも1つのセンサー(2)、およびデジタル化アルゴリズム(Φ)により各組の生体計測データ($b_1,\cdots,b_N$)から得られたデジタルデータセット($c_1,\cdots,c_N$)を格納する安全モジュール(4)を含むシステムを使用した識別または許可の方法に関する。前記方法により、センサーにより獲得された生体計測データ(b')が取得され、獲得済み生体計測データにデジタル化アルゴリズムを適用してデジタル値(c')が取得され、前記デジタルデータセットのデジタルデータの少なくとも一部が、取得済みデジタル値に対する前記データの近似度に従って安全モジュールで分類され、生体計測データ(b_N)が、前記生体計測データの組から、分類における対応するデジタルデータの位置を考慮して取得される。

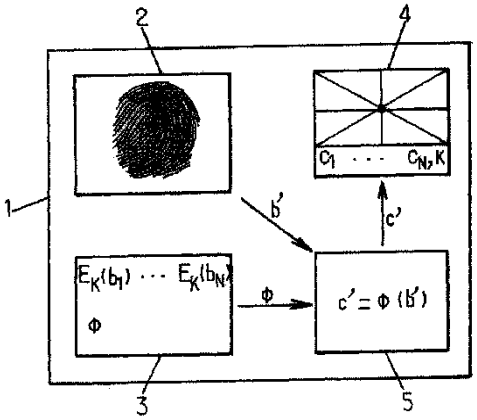


FIG.2.

【特許請求の範囲】
【請求項１】
生体計測データを獲得するための少なくとも1つのセンサー(2)およびデジタル化アルゴリズム(Φ)によって1組の各生体計測データ($b_1,\cdots,b_N$)を起点に取得された1組のデジタルデータ($c_1,\cdots,c_N$)を格納する1つの安全モジュール(4)を含むシステムを使用した識別または許可の方法であって、
/a/前記センサーによって獲得された生体計測データ値(b’)を取得するステップと、
/b/獲得された前記生体計測データに前記デジタル化アルゴリズムを適用してデジタル値(c’)を取得するステップと、
/c/前記安全モジュール内で、前記デジタルデータの組からの少なくとも一部のデジタルデータの順位付けを、近似基準による取得された前記デジタル値に対するそれぞれの近似度に従い実行するステップと、
/d/前記生体計測データの組から生体計測データ値(b_{i1})を、前記順位付け内の前記対応するデジタルデータの位置を考慮して取得するステップと、
を含むことを特徴とする方法。
【請求項２】
/e/前記生体計測データの組($b_1,\cdots,b_N$)から取得された前記生体計測データ(b_{i1})と前記センサー(2)によって獲得された前記生体計測データ(b’)との対応を確認するステップと、
/f/対応がない場合、前記順位付けでより低い位置にあるデジタルデータ値に対応する生体計測データ値(b_{i2})を前記生体計測データの組から取得するステップと、
をさらに含むことを特徴とする請求項1に記載の方法。
【請求項３】
前記安全モジュール(4)は、安全な方法で互いに通信するために設定された少なくとも2つのサブセクションに分けられ、
前記サブセクションの1つは、前記ステップ/c/を担当し、
前記サブセクションのもう1つは、前記ステップ/e/を担当することを特徴とする請求項2に記載の方法。
【請求項４】
前記近似基準がハミング距離のようなデジタル距離の計算を利用することを特徴とする請求項1から3のいずれか一項に記載の方法。
【請求項５】
前記デジタル化アルゴリズムが、前記生体計測データの組の前記生体計測データ値の1つと同じ個人に関係する生体計測データ値を、前記生体計測データの組からの前記生体計測データ値に対応する前記デジタルデータ値によって、前記近似基準を満たすデジタル値に対応させるよう構成された量子化アルゴリズムであることを特徴とする請求項1から4のいずれか一項に記載の方法。
【請求項６】
前記生体計測データの組($b_1,\cdots,b_N$)からの前記生体計測データ値の少なくとも一部が、前記安全モジュール(4)の外部にあるメモリ(3)に符号化されて保存され、前記安全モジュールが、前記符号化された生体計測データを復号するよう構成されることを特徴とする請求項1から5のいずれか一項に記載の方法。
【請求項７】
前記生体計測データの組($b_1,\cdots,b_N$)からの前記生体計測データ値の少なくとも一部が符号化されずに前記安全モジュール(4)に保存されることを特徴とする請求項1から6のいずれか一項に記載の方法。
【請求項８】
前記デジタルデータの組($c_1,\cdots,c_N$)からの前記デジタルデータのサイズが、前記生体計測データの組($b_1,\cdots,b_N$)からの前記各生体計測データのサイズより小さいことを特徴とする請求項1から7のいずれか一項に記載の方法。

【請求項９】
前記安全モジュール(4)が、各デジタル化アルゴリズムによって1組の各生体計測データを起点に各々取得された少なくとも2組のデジタルデータを保存し、少なくとも2つのデジタル値が、獲得された前記生体計測データ(b’)に前記各デジタル化アルゴリズムを適用して取得され、前記安全モジュール内で、前記デジタルデータの組の各々からの前記デジタルデータの少なくとも一部が、近似基準による前記対応するデジタル値に対するそれぞれの近似度に従って分類され、生体計測データ値が前記生体計測データの組から、前記順位付け内の前記対応するデジタルデータの位置を考慮して取得されることを特徴とする請求項1から8のいずれか一項に記載の方法。
【請求項１０】
前記安全モジュール(4)が、各デジタル化アルゴリズムにより少なくとも第1および第2の各組の各生体計測データを起点に各々取得された少なくとも第1および第2の組のデジタルデータを保存することを特徴とする請求項1から9のいずれか一項に記載の方法。
【請求項１１】
少なくとも1つの各センサーによって獲得された少なくとも1つの生体計測データ値が取得され、
少なくとも第1および第2のデジタル値が、前記デジタル化アルゴリズムの各々を前記獲得済み生体計測データに適用することによって取得され、
前記安全モジュール内で、少なくとも前記第1および第2の組のデジタルデータからの前記デジタルデータの少なくとも一部について、少なくとも前記第1および第2のデジタル値の各々に対するそれぞれの近似度に従って順位付けが実施され、
前記第1または第2の組の生体計測データの1つからの生体計測データ値は、少なくとも前記順位付け内の前記対応するデジタルデータの位置が考慮されていることを特徴とする請求項10に記載の方法。
【請求項１２】
各センサーによって獲得された少なくとも第1および第2の生体計測データ値が取得され、
少なくとも第1および第2のデジタル値が、それぞれ少なくとも前記第1および前記第2の獲得済み生体計測データに前記各デジタル化アルゴリズムを適用することによって取得され、
前記安全モジュール内で、前記第2組のデジタルデータからの一部のデジタルデータに対し、前記第2デジタル値に対するそれぞれの近似度に従い順位付けが実行され、
生体計測データ値は、前記第2組の生体計測データから、前記順位付け内の前記第2デジタルデータ値の位置を考慮して取得され、
前記第1デジタル値から特定された前記第1組の生体計測データからの一部の生体計測データと同じ個人に関係する前記第2組の生体計測データからの一部の生体計測データに対応するよう、前記第2組のデジタルデータから前記一部のデジタルデータが選択されることを特徴とする請求項10に記載の方法。
【請求項１３】
前記システムは、前記センサーを備えると共に、前記安全モジュール(4)が結合されている端末(1)を具備するローカルシステムであることを特徴とする請求項1から12のいずれか一項に記載の方法。
【請求項１４】
前記システムは、前記生体計測データ($E_K(b_1),...,E_K(b_N)$、$E_K(d_1),...,E_K(d_N)$)の少なくとも一部を保存する集中データベース(13)およびセンサーを含む少なくとも1つの分散端末(14、15)を含む分散システムであることを特徴とする請求項1から12のいずれか一項に記載の方法。
【請求項１５】
請求項1から14のいずれか一項に記載の方法を実施するための識別または許可のシステムであって、

生体計測データを獲得するための少なくとも1つのセンサー(2)およびデジタル化アルゴリズム(Φ)により1組の各生体計測データ($b_1,\cdots,b_N$)から取得された1組のデジタルデータ($c_1,\cdots,c_N$)を保存する安全モジュール(4)を含み、

/a/前記センサーによって獲得された生体計測データ値(b')を取得する手段と、

/b/前記獲得済み生体計測データに前記デジタル化アルゴリズムを適用してデジタル値(c')を割り出すための処理装置と、

/c/前記安全モジュール内で、前記デジタルデータの組からの前記デジタルデータの少なくとも一部の順位付けを、近似基準による取得済みの前記デジタル値に対するそれぞれの近似度に従い実行するための順位付け装置と、

/d/前記生体計測データの組から生体計測データ値(b_{i1})を、前記順位付け内の前記対応するデジタルデータの位置を考慮して取得するための識別または許可の装置と、

を含むことを特徴とするシステム。

【請求項１６】

生体計測データを獲得するための少なくとも1つのセンサー(2)を含む、請求項1から14のいずれか一項に記載の方法を実施するための識別または許可のシステムで使用する安全モジュール(4)であって、

デジタル化アルゴリズム(Φ)により1組の各生体計測データ($b_1,\cdots,b_N$)から取得された1組のデジタルデータ($c_1,\cdots,c_N$)を格納するためのメモリを含み、

前記センサーによって獲得された生体計測データ(b')に前記デジタル化アルゴリズムを適用することによってデジタル値(c')を取得するための手段と、

前記デジタルデータの組からの前記デジタルデータの少なくとも一部の順位付けを、近似基準による取得済みの前記デジタル値に対するそれぞれの近似度に従い実行するための順位付け装置と、

前記生体計測データの組から生体計測データ値(b_{i1})を、前記順位付け内の前記対応するデジタルデータの位置を考慮して取得するための識別または許可の装置と、

をさらに含むことを特徴とする安全モジュール。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、生体計測データに基づく識別および/または許可に関する。

【背景技術】

【０００２】

識別とは通常、個人の生体計測データの1つに基づき当該個人の同一性を回復することにある。

【０００３】

これは図1に概略的に示されており、各個人に関係し、登録段階と呼ばれる段階で以前取得された生体計測データ$b_1,\cdots,b_N$を保存する生体計測データベースM、およびかかる生体計測データを獲得できる生体計測センサーCを含むシステムによって実行される。

【０００４】

生体計測データは任意の種類であってよく、虹彩、1つまたは複数の指紋、細部、顔、手のひら、指または手の血管網、前記の特徴の組合せなどの個人の特徴に関係しうる。

【０００５】

個人が識別のため現れた場合、この個人に関係する生体計測データ値b'がセンサーCによって取得され、次いで、生体計測データ$b_1,\cdots,b_N$の1つb_{i1}との対応が得られるまで、これらの生体計測データの各々と比較される。

【０００６】

この生体計測データb_{i1}を用いて、生体計測データb'が獲得されている個人の同一性i_{i1}が見出される。この同一性i_{i1}は例えば生体計測データb_{i1}との関係で保存される。

【０００７】

取得された生体計測データb_{i1}が、生体計測データb'が獲得されている個人の同一性を

見出すために使用されるのではなく、この個人に何らかの種類の許可、例えばサイトへのアクセスの許可、製品、文書の納入の許可などを与えるために使用されることにより、許可は上述の識別から単純に区別される。したがって許可の場合、b’が登録データベース中の個人の1人からもたらされるものとして、同一性(結果的にこの場合には保存する必要がない)の読取りまたはリターン(return)を試みることなく、b’が検知されているという応答を要求するだけでよい。

【０００８】

生体計測データの複雑かつ不安定な性質により、一連の前述の比較処理は、膨大な量の計算につながる。そのため、識別または許可の結果は、比較的長い時間を経てようやく得られる。また、必要な処理能力からして、比較的大きなシステムを使用しなければならない。

【０００９】

識別または許可の信頼性を大きく低下させることなく計算量を抑制する試みがこれまでなされてきた。

【００１０】

「IEEE Transactions on Information Forensics and Security」で2008年6月に発表されたFeng Hao、John Daugman、Piotr Zielinskiによる記事「A fast search algorithm for a large fuzzy database」はこの一例である。

【００１１】

これは、限定されたサイズのデジタル値を保持するだけのために、虹彩の2進コードへの変換、例えば回転、入れ替えおよび抽出を利用する考えを促進している。そのため、こうしたデジタル値に基づく比較は、生体計測データに対して直接実行される上述の比較と比べて、大幅に簡略化される。

【００１２】

上述した手法のもう1つの欠点は、生体計測データの保護レベルの低さにある。

【００１３】

これは、生体計測データ$b_1,\cdots, b_N$が直接使用される場合に特に当てはまる。

【００１４】

こうした生体計測データが符号化されて生体計測データベースMに保存される場合でも、こうした生体計測データの符号化されていないバージョンがシステムにより、特に獲得された生体計測データ値b’と比較する目的で処理される。

【００１５】

よって、犯意を持ってシステムにアクセスする者が、生体計測データの保護されていないバージョンを取得する可能性がある。そのため、対応する個人の同一性の保護が保証されない。

【００１６】

前述の記事「A fast search algorithm for a large fuzzy database」の教示に従い、生体計測データに代えてメモリをさほど必要としないデジタル値を利用する場合でも、こうしたデジタル値はその発生元である生体計測データに関する情報を提供する。したがって、対応する個人の同一性は、このシナリオでも保護されない。

【先行技術文献】

【非特許文献】

【００１７】

【非特許文献１】「IEEE Transactions on Information Forensics and Security」で2008年6月に発表されたFeng Hao、John Daugman、Piotr Zielinskiによる記事「A fast search algorithm for a large fuzzy database」

【非特許文献２】IEEEによって2008年6月に発表されたC. Chen、R.N.J. Veldhuis、T.A.M. KevenaarおよびA.H.M. Akkermansによる記事「Biometric binary string generation with detection rate optimized bit allocation」

【非特許文献３】SPIEによって2006年2月に発表されたM. van der Veen、T. Kevenaar、G

.J. Schrijen、T.H. AkkermansおよびF. Zuoによる記事「Face biometrics with renewable templates」

【発明の概要】

【発明が解決しようとする課題】

【００１８】

本発明の1つの目的は、生体計測データが獲得されている個人の同一性の保護を向上させることである。

【課題を解決するための手段】

【００１９】

そのため、本発明は、生体計測データを獲得するための少なくとも1つのセンサーおよびデジタル化アルゴリズムによって1組の各生体計測データを起点に取得された1組のデジタルデータを保存する1つの安全モジュールを含むシステムを使用する識別または許可の方法を提供し、本方法は以下のステップを含む。

/a/センサーによって獲得された生体計測データ値を取得する。

/b/獲得された生体計測データにデジタル化アルゴリズムを適用してデジタル値を取得する。

/c/安全モジュール内で、前記デジタルデータの組からの少なくとも一部のデジタルデータの順位付けを、近似基準による取得済みデジタル値に対するそれぞれの近似度に従い実行する。

/d/前記生体計測データの組から生体計測データ値を、順位付け内の対応するデジタルデータの位置を考慮して取得する。

【００２０】

安全モジュールを利用することで、安全モジュールが含むデジタルデータに犯意を持った者がアクセスすることに対する保護が得られる。このため、こうしたデジタルデータに、かかる犯意を持った者はアクセスできない。

【００２１】

また、前記デジタルデータの取得起点である生体計測データは、例えば符号化によって、かつ/または安全モジュール内への保存によってそれ自体を保護することができる。したがって、前記生体計測データが関係する個人の同一性が保護される。

【００２２】

また、生体計測データではなくデジタルデータの保存および有利に単純な処理は、処理時間が限られているさほど高度ではないシステムによる実施を可能にすることができる。

【００２３】

前述のデジタル化アルゴリズムは、例えば、前記生体計測データの組の生体計測データ値の1つと同じ個人に関係する生体計測データ値を、前記生体計測データの組からの前記生体計測データ値に対応するデジタルデータ値によって前記近似基準を満たすデジタル値に対応させるよう構成された量子化アルゴリズムであってよい。

【００２４】

有利な形で、以下のステップを実行できる。

/e/前記生体計測データの組から取得された生体計測データとセンサーによって獲得された生体計測データとの対応を確認する。

/f/対応がない場合、順位付けでより低い位置にあるデジタルデータ値に対応する生体計測データ値を前記生体計測データの組から取得する。

【００２５】

こうした確認は、識別または許可を信頼できるものにしている。確認による処理の複雑性はなおも、従来技術の系統的な生体計測上の比較に比べてさらに低下している。

【００２６】

この場合、安全モジュールは安全な方法で互いに通信するために設定された少なくとも2つのサブセクションに分けられ、前記サブセクションの1つはステップ/c/を担当し、前記サブセクションのもう1つはステップ/e/を担当する。

【００２７】
有利な形で、1つまたは複数の組の生体計測データからもたらされる数組のデジタルデータを使用できる。
【００２８】
安全モジュールは、例えば、各デジタル化アルゴリズムによって少なくとも第1および第2の各組の各生体計測データから各々取得された少なくとも第1および第2の組のデジタルデータを保存することができる。
【００２９】
この状況において実施できる1つの有利な実施形態に従い、少なくとも1つの各センサーによって獲得された少なくとも1つの生体計測データ値が取得され、少なくとも第1および第2のデジタル値が、デジタル化アルゴリズムの各々を前記獲得済み生体計測データに適用することによって取得され、安全モジュール内では、少なくとも第1および第2の組のデジタルデータからのデジタルデータの少なくとも一部について、少なくとも第1および第2のデジタル値の各々に対するそれぞれの近似度に従って順位付けが実行され、少なくとも第1または第2の組の生体計測データの1つからの生体計測データ値は、順位付け内の対応するデジタルデータの位置を考慮する。
【００３０】
こうして個人は、その個人の入手可能な生体計測上の特徴(顔、指紋、虹彩など)の少なくとも1つを獲得することによって識別または許可されうる。
【００３１】
この同じ状況において実施できる1つの有利な実施形態に従い、各センサーによって獲得された少なくとも第1および第2の生体計測データ値が取得され、少なくとも第1および第2のデジタル値が、それぞれ少なくとも第1および第2の獲得済み生体計測データに各デジタル化アルゴリズムを適用することによって取得され、安全モジュール内で、第2組のデジタルデータからの一部のデジタルデータに対し、第2デジタル値に対するそれぞれの近似度に従い順位付けが実行され、前記順位付け内の第2デジタルデータ値の位置を考慮して第2組の生体計測データから生体計測データ値が取得され、第1デジタル値から特定された第1組の生体計測データからの一部の生体計測データと同じ個人に関係する第2組の生体計測データからの一部の生体計測データに対応するため、第2組のデジタルデータから前記一部のデジタルデータが選択される。
【００３２】
こうして、順位付けが限定的な量のデータに対してのみ実行されるため、識別または許可を容易にすることができる。そのため、識別または許可の信頼性を低下させることなく、収束に要する時間をしかるべく減らすことができる。
【００３３】
本発明の別の対象は、前述の方法を実施するための識別または許可のシステムであって、このシステムは、生体計測データを獲得するための少なくとも1つのセンサーおよびデジタル化アルゴリズムによって1組の各生体計測データから取得された1組のデジタルデータを保存する1つの安全モジュールを含み、このシステムは以下を含む。
/a/センサーによって獲得された生体計測データ値を取得する手段。
/b/獲得された生体計測データにデジタル化アルゴリズムを適用してデジタル値を割り出すための処理装置。
/c/安全モジュール内で、前記デジタルデータの組からのデジタルデータの少なくとも一部の順位付けを、近似基準による取得済みデジタル値に対するそれぞれの近似度に従い実行するための順位付け装置。
/d/前記生体計測データの組から生体計測データ値を、順位付け内の対応するデジタルデータの位置を考慮して取得するための識別または許可の装置。
【００３４】
問題のシステムは、センサーを含む、(例えば、組み込みまたは外部通信により)安全モジュールが結び付いた端末を含むローカルシステムからなることができる。安全モジュー

ルは、例えば端末内に含めることができるマイクロチップの形をとることができる。
【００３５】
変形として、システムは分散型であってよい。その場合、システムは、生体計測データの少なくとも一部を保存する集中データベースおよびセンサーを含む少なくとも1つの分散端末を含むことができる。この場合、使用される各安全モジュールは集中データベースと結び付くことができ、分散端末の少なくとも1つと結び付くことができ、またはある部分が集中データベースと結び付き、別の部分が分散端末の少なくとも1つと結び付くことができる。
【００３６】
本発明はまた、生体計測データを獲得するための少なくとも1つのセンサーを含む、前述の方法を実施するための識別または許可のシステム内で使用する安全モジュールを提供し、安全モジュールはデジタル化アルゴリズムによって1組の各生体計測データから取得された1組のデジタルデータを保存するためのメモリを含む。安全モジュールは以下をさらに含む。
- センサーによって獲得された生体計測データにデジタル化アルゴリズムを適用することによってデジタル値を取得するための手段。
- 前記デジタルデータの組からのデジタルデータの少なくとも一部の順位付けを、近似基準による取得済みデジタル値に対するそれぞれの近似度に従い実行するための順位付け装置。
- 前記生体計測データの組から生体計測データ値を、順位付け内の対応するデジタルデータの位置を考慮して取得するための識別または許可の装置。
【００３７】
本発明の他の特徴および利点は、非限定的な例示的実施形態に関する後の説明において、下記の添付の図面を参照することで明らかになろう。
【図面の簡単な説明】
【００３８】
【図１】既に論じた、従来技術による生体計測データに基づく識別または許可を示す図である。
【図２】本発明による識別または許可のシステムの第1の非限定的例を示す図である。
【図３】本発明の枠組み内で実施できる連続ステップを示す図である。
【図４】本発明による識別または許可のシステムの第2の非限定的例を示す図である。
【発明を実施するための形態】
【００３９】
図2は、本発明による識別または許可のシステムの第1の例を示している。
【００４０】
この例では、システムは、虹彩、1つまたは複数の指紋、細部、顔、手のひら、指または手の血管網、前記の特徴の組合せなどの個人の一定の特徴に関係しうる、任意の種類であってよい生体計測データを獲得できるセンサー2を含む端末1を備える。
【００４１】
端末1はまた、安全モジュール4、すなわち、含まれるデータを物理的に保護する装置を備える。図2の例では、安全モジュールはマイクロチップからなり、マイクロチップは、例えば設計段階で、またはプリント回路板の挿入によって端末1に含まれ、この端末1内で取り外し可能なスマートカードであってよい。
【００４２】
端末1は各個人に関係する1組の生体計測データ$b_1,\cdots,b_N$を保存する。これらの生体計測データは、例えば対応する個人の以前の登録によってもたらされる。これらは、端末1のセンサー2、またはその他の適切な手段、例えば端末1から独立したセンサーによって取得された可能性がある。
【００４３】
これらの生体計測データは、端末1のメモリ3に保存できる。この場合、犯意を持った者

が端末1にアクセスしてデータにアクセスするのを回避するため、符号化されて保存されるのが好ましい。図2の例では、これは参照$E_K(b_1),\cdots,E_K(b_N)$によって表されており、Eは符号化アルゴリズムを示し、Kは復号化キーを示している。

【００４４】

この解決法は、2つの水準のデータ保護を同時に保証するという点で有利である。実際、以下で詳述する安全モジュール4によるデジタルデータの物理的保護に加えて、安全モジュール4とは別にメモリ3に生体計測データを符号化した形で保存することにより、こうした生体計測データ自体が別の形でも保護される。

【００４５】

使用される復号化アルゴリズムは、対称、非対称など、任意の種類であってよい。アルゴリズムAESおよびDESは、使用可能な復号化アルゴリズムの非限定的な例である。有利なことに、選択される復号化アルゴリズムは、必要な処理時間を限定するために、対応する復号化アルゴリズムを比較的迅速に実行できるよう選択されうる。

【００４６】

マイクロチップ4は、復号化アルゴリズムおよび/または適切な復号化キー(これは図2のマイクロチップ4内の復号化キーKを参照することにより記号化される)を、メモリ3に保存された符号化バージョンを起点に生体計測データ$b_1,\cdots,b_N$を回復できる方法で有利に保存する。

【００４７】

変形として、マイクロチップ4に十分な記憶容量がある場合、生体計測データ$b_1,\cdots,b_N$はマイクロチップ4に保存できる。この場合、マイクロチップ4は物理的保護を保証するため、生体計測データは符号化されずに保存されうる。

【００４８】

これらの2つの保存方法の組合せ、すなわち、メモリ3に生体計測データの一部を符号化して保存し、マイクロチップ4に生体計測データの一部を符号化せずに保存することも考えられる。

【００４９】

さらに、生体計測データ$b_1,\cdots,b_N$は端末1の外に保存してよく、例えば外部データベースからアクセス可能であってよい。

【００５０】

1組のデジタルデータ$c_1,\cdots,c_N$はさらに、デジタル化アルゴリズムΦによって各生体計測データ$b_1,\cdots,b_N$を起点に取得される。この場合、$c_1=\Phi(b_1),\cdots,c_N=\Phi(b_N)$である。

【００５１】

デジタル化アルゴリズムΦは、デジタルデータ値と生体計測データ値とを対応させるアルゴリズムである。こうして取得されるデジタルデータ$c_1,\cdots,c_N$は、生体計測データと比べてサイズが縮小されている可能性がある。非限定的な例を挙げると、このデジタル化アルゴリズムは、キロバイト級の生体計測データb_iをわずか数百バイト、またはさらに小規模のデジタルデータ値c_iに対応させる。そのため、デジタルデータと生体計測データとのサイズの比率は1対10またはそれ以上になる(1対100の比率になることも考えられる)。

【００５２】

換言すれば、デジタル化アルゴリズムΦは、有利な形でメモリをさほど必要としないデジタルデータへの生体計測データの投影(projection)のためのアルゴリズムと見なすことができる。

【００５３】

1つの有利な場合では、デジタルデータ値を取得するために実行されるデジタル化により、対応する生体計測データは、大きなデータベースに対する確実な識別(positive identification)が非効果的になる点まで低下する。

【００５４】

デジタル化アルゴリズムΦはさらに、$b_1,\cdots,b_N$からの生体計測データ値の1つb_iと同じ個人に関する生体計測データb'を、生体計測データb_iに対応するデジタルデータ値c_iに

よって近似基準を満たすデジタル値c’に対応させるよう構成される量子化アルゴリズムからなることができる。

【００５５】

換言すれば、かかる量子化アルゴリズムΦによって生体計測データ値b’からデジタル値c’が取得されている場合、c’と$c_1,\cdots,c_N$からのデジタルデータ値c_iとの近似性は、一定の統計的誤り確率を伴って、生体計測データb’およびc_iに対応する生体計測データb_iが同じ個人に関係することを明らかにしている。

【００５６】

この統計的誤り確率は、偽陽性、すなわち、デジタル値間に近似性があるが、対応する生体計測データが関係する個人が同じではない場合、および偽陰性、すなわち、1人の同じ個人からもたらされた2つの生体計測データに対応するデジタル値間に近似性がない場合に関係する。

【００５７】

この性質により、量子化アルゴリズムΦを用いて、限定的なサイズのデジタル値を起点に、一定の信頼できる水準で個人の生体計測データを回復することができる。

【００５８】

使用される近似基準は、ハミング距離、ユークリッド距離などのデジタル距離の計算を利用することができる。この場合、量子化アルゴリズムΦにより、b_iと同じ個人に関係する生体計測データ値b’を起点にc’が取得された可能性が高いことを$d(c_i,c')<d$が示唆し、$c_i=\Phi(b_i)$であって、$d(c_i,c')$は例えばc_iとc’とのハミング距離を表し、dは所与の距離のしきい値を表してよい。

【００５９】

他のデジタル距離ももちろん考えられる。デジタル距離が例えば、c_iおよびc’を形成するデジタルチェーン内で相違するデジタル値の数を表す場合もある。こうしたデジタルチェーンが2進法の場合、かかるデジタル距離は例えばc_iとc’との排他的な論理和演算によって取得できる。

【００６０】

当業者には明らかな他の種類の近似基準も可能である。

【００６１】

デジタル化アルゴリズムは任意の既知のアルゴリズムであってよい。非限定的な例として、IEEEによって2008年6月に発表されたC. Chen、R.N.J. Veldhuis、T.A.M. KevenaarおよびA.H.M. Akkermansによる記事「Biometric binary string generation with detection rate optimized bit allocation」、およびSPIEによって2006年2月に発表されたM. van der Veen、T. Kevenaar、G.J. Schrijen、T.H. AkkermansおよびF. Zuoによる記事「Face biometrics with renewable templates」に説明されているアルゴリズムが挙げられる。

【００６２】

デジタル化アルゴリズムは、例えば端末1のメモリ3に保存される。変形として、マイクロチップ4または端末1の外部に保存することができる。

【００６３】

デジタルデータ$c_1,\cdots,c_N$の全てがマイクロチップ4に保存され、その保護が保証される。このため、犯意を持ちうる者は、こうしたデジタルデータ$c_1,\cdots,c_N$にアクセスできず、したがって、デジタルデータ$c_1,\cdots,c_N$の発生元である生体計測データ$b_1,\cdots,b_N$に関して何かを発見できるような情報をこれらから集めることはできない。

【００６４】

さらに、デジタルデータ$c_1,\cdots,c_N$のサイズが対応する生体計測データ$b_1,\cdots,b_N$のサイズよりはるかに小さいことから、デジタルデータ$c_1,\cdots,c_N$はさらに、記憶容量の少ないマイクロチップ4に保存でき、これは生体計測データ$b_1,\cdots,b_N$自体には通常当てはまるとは限らない。

【００６５】

個人が識別または許可を求めて現れた場合、当該個人の生体計測データ値の1つb’がセンサー2によって獲得される。センサー2が図2とは対照的に端末1の外部にある場合、このセンサーによって獲得された生体計測データ値b’は、識別または許可のため端末1に適切な手段によって転送される。

【００６６】

デジタル値c’は後に、センサー2によって獲得された生体計測データ値b’にデジタル化アルゴリズムΦを適用することで得られる。デジタル値c’は例えば、生体計測データ値b’のバージョンおよびデジタル化アルゴリズムΦのバージョンが以前送信された際の送信先である端末1の処理装置5によって決定される。

【００６７】

変形として、c’の計算はマイクロチップ4自体によって実行できる。さらに別の変形によると、c’の計算は端末1の外部にある装置によって実行でき、これは端末1へのその後の転送を想定している。

【００６８】

いずれの場合でも、デジタル値c’は識別または許可のためマイクロチップ4に提供される。

【００６９】

図3に示されているように、マイクロチップ4は処理するデジタルデータ$c_1,\cdots,c_N$との関係でこのデジタル値c’の分析を、デジタルデータ$c_1,\cdots,c_N$を前述の近似基準によるc’に対するそれぞれの近似度で順位付けする方法で実施する。

【００７０】

これは例えば、デジタル値c’とデジタルデータ値$c_1,\cdots,c_N$の各々とのデジタル距離を計算し(ステップ6)、こうして計算された距離が増える順番で値$c_1,\cdots,c_N$を順位付けすることによって得られる。その結果、例えば、デジタルデータ$c_1,\cdots,c_N$の順位付けを表す、$1,\cdots,N$から選択されたインデックス$i_1,\cdots,i_N$の順位リストが生成されうる。

【００７１】

図3の例では、c’の近似度がマイクロチップ4でテストされ、デジタルデータ$c_1,\cdots,c_N$の各々が対象となるが、マイクロチップ4によってデジタルデータ$c_1,\cdots,c_N$の一部のみでこの順位付けを行ってもよい。

【００７２】

例えば、最初のp個のデジタルデータ値$c_1,\cdots,c_P$、$(p<N)$のみを、c’に対する近似度のテスト対象とすることができる。変形として、デジタルデータ$c_1,\cdots,c_N$の全部または一部でこうしたテストを実施できるが、c’に対する近似度が十分に高いデジタルデータのみを順位付けの対象とすることができる。

【００７３】

次いで、順位付けを利用して、$b_1,\cdots,b_N$の中から、b’と同じ個人に関係する確率が最も高い生体計測データを特定する。

【００７４】

図3の例では、リスト7の中でインデックスi_1が最初である。これは、前述の近時基準に照らして、対応するデジタルデータ値c_{i1}がc’に最も近いことを意味する。

【００７５】

使用されるデジタル化アルゴリズムΦが上記で定めたような量子化アルゴリズムである場合、その性質は、$c_{i1}=\Phi(b_{i1})$の生体計測データb_{i1}がb’と同じ個人に関係する確率が高いことを意味する。

【００７６】

検索を容易にするため、この場合、インデックスi_1に基づき、デジタルデータ値c_{i1}に生体計測データ値b_{i1}が対応する状況において、デジタルデータ$c_1,\cdots,c_N$がマイクロチップ4に保存される順番が、生体計測データ$b_1,\cdots,b_N$が例えばメモリ3に保存される順番と同じであることが有利でありうる。とはいえ、任意のデジタルデータ値c_iに対応する生体計測データb_iが回復できる限り、様々な順番が可能である。

【００７７】
また図3の例では、マイクロチップ4はこの生体計測データb_{i1}を取得することができ、その理由は、マイクロチップ4がそれをメモリに含めること、またはマイクロチップ4が端末1のメモリ3からその符号化バージョン$E_K(b_{i1})$を受信(ステップ8)できることにある。後者の場合、マイクロチップ4は、アルゴリズムおよび/またはメモリに保存されたキーによって符号化バージョンを復号した後、生体計測データ値b_{i1}を処理する(ステップ9)。
【００７８】
この生体計測データ値b_{i1}は、識別または許可のために現れた個人を識別または許可するために直接使用されうる。保護をしかるべく保証するマイクロチップ4からこの値b_{i1}が出ることはない点が注目される。
【００７９】
有利な形で、識別または許可の信頼性を高めるために追加の確認が実施される。この追加の確認として、ステップ9で取得された生体計測データb_{i1}とセンサーによって獲得された生体計測データb’との比較を実行することができる(ステップ10)。この生体計測上の比較では、使用される生体計測データの性質により、任意の従来型のアルゴリズムを実施できる。これはマイクロチップ4で実施してよい。
【００８０】
この比較により、生体計測データb’とb_{i1}との対応が十分に信頼できる水準で明らかになった場合、生体計測データb_{i1}がb’と同じ個人を真に表していると考えられ、その結果、これに基づいて識別または許可の処理を進めることができる。許可の場合には図3に示されているように値OKがしかるべく返され、または識別の場合には生体計測データb_{i1}に対応する同一性i_{i1}が返されてよい。
【００８１】
なお、(図1と同様に)図3で使用される記号「=」は、比較される生体計測データと完全に等しいことを意味するとは限らないが、これらのデータ間の生体計測近似度テストに対応し、生体計測学の分野では周知のとおり「合致」と呼ばれることがある。
【００８２】
一方、(「合致」という意味で)対応がない場合、前述の順位付けでより低い位置にあるデジタルデータ値に対応する別の生体計測データ値を取得することによって処理を続けることが考えられる。変形として、処理をそこで中止して、失敗(NOK)を示すこともできる。
【００８３】
処理を続ける例を挙げると、必要に応じて復号後に、ステップ7で設定された順位付けに従い、デジタル値c’に対する近似度が2番目に高いデジタルデータ値c_{i2}に対応する生体計測データ値b_{i2}を取得することができる(ステップ11および12)。
【００８４】
このプロセスは、b’と同じ個人に対応する生体計測データ値が$b_1,\cdots,b_N$から十分に信頼できる水準で得られるまで、有利な形で続けることができる。
【００８５】
これまで述べてきたことから、識別または許可を実現するのに必要な計算の量が限定的であることが理解されよう。その理由は、ステップ6で実行される距離の計算が、サイズが縮小されたデジタル値に適用されるため複雑性が低下することにある。よって、ステップ9で取得される生体計測データb_{i1}は、比較的短い処理時間で特定されうる。さらに、処理能力が限定的なマイクロチップ4でも、こうした単純な計算を実施できる。
【００８６】
それでも、ステップ10以降を参照して説明したような一定の生体計測データ値間で追加の確認が実施される選択的場合には、さらなる複雑性が求められる。だが、大半の場合、こうした複雑性の確認の数は、既に紹介したデジタル化アルゴリズムΦの潜在的性質のおかげで依然として少ない。
【００８７】

図2および3を参照して説明した例の改善により、数組のデジタルデータ$c_1 \cdots c_N$が、各デジタル化アルゴリズムΦを利用してそれぞれ生体計測データ$b_1 \cdots b_N$を起点に取得されうる。

【００８８】

この場合、上記のステップは、数組のデジタルデータ$c_1 \cdots c_N$の各々に関して実施できる。特に、生体計測データ値b’にデジタル化アルゴリズムの1つを適用してそれぞれ得られるデジタル値c’を計算できる。次いで、前述したような近似基準に従いマイクロチップ4内で、これらの組の各々からのデジタルデータの少なくとも一部の順位付けを実行することができる。

【００８９】

次いで、$b_1 \cdots b_N$から生体計測データ値を、様々な組のデジタルデータ$c_1 \cdots c_N$に関して実施された様々な順位付けを考慮して取得できる。例えば、実施された様々な順位付けを考慮して、1,…,Nから最も高い位置にあるインデックスを、対応する生体計測データ値を取得するために第1近似データとして確保できる。別の例によると、各順位付けの最上位にある様々なデジタルデータに対応する生体計測データを選択し、各々は、そのうちの1つを確保するためだけに追加の確認の対象とすることができる。

【００９０】

当業者には明らかなように、様々な順位付け内のデジタルデータの位置を考慮して、$b_1 \cdots b_N$から生体計測データ値を取得する他の可能性も考えられる。

【００９１】

様々な組のデジタルデータを考慮した共通の順位付けを実行することも可能である。

【００９２】

いずれの場合でも、数組のデジタルデータを使用することで、関連する生体計測データ値の選択が信頼できるものになることが理解されよう。また、デジタルデータのサイズが縮小されているため、処理能力と記憶容量が限定的なマイクロチップ4でも、様々な組のデジタルデータを保存して前述のデジタル処理演算を実行することができる。

【００９３】

前述の改善と組み合わせることができる別の改善では、数組の生体計測データ$b_1 \cdots b_N$を使用することが可能である。この場合、様々な組のデジタルデータ$c_1 \cdots c_N$はそれぞれ、各デジタル化アルゴリズムによりこれらの組の生体計測データの1つに対応する。

【００９４】

例えば、前記生体計測データの組は様々な生体計測上の特徴、例えばそれぞれの指からの指紋、1つの特徴としての指紋およびその他の特徴としての顔、1つの特徴としての指紋およびその他の特徴としての血管網、指紋、虹彩および掌紋、または考えられるこれらの任意の組合せに関係しうる。

【００９５】

このシナリオでは、様々な組の生体計測データの性質に従い設計された1つまたは複数のセンサーによって、1つまたは複数のb’獲得を実施できる。次いで、各生体計測データb’から各デジタル値c’を取得できる。

【００９６】

ここでは捕捉される生体計測データが登録時よりも少ない場合があることに留意すべきである(例えば、登録時には10本の指が捕捉される一方、このステップでは1本の指のみが捕捉される場合、目標はこの10本の指のうち少なくとも1本を見つけることである)。

【００９７】

捕捉された生体計測データの正確な状況(例えば、10本の指のうちどれか、右または左どちらの人差し指かなど)を特定することは不可能であり、ただ1組の可能性のある性質しか特定できない場合もある。次いで、登録中に使用され、この1組の可能性に対応する全てのデジタル化アルゴリズムが、同数のデジタル値を取得するために適用されうる。これらのデジタル値から生成される順位付けによりその後、生体計測データ値を取得することができ、同時にb’の正確な性質を回復することができる。

【００９８】
前述したステップの実施の結果、利用可能な数組の生体計測データの少なくとも一部からいくつかの生体計測データを取得することができる。
【００９９】
そして、識別または許可の処理を進めるためにいくつかの戦略を考えることができる。例えば、識別または許可される個人に対応する確率が最も高いデータを確保するためだけに、取得された生体計測データの各々は、同じ性質を持つ獲得済みの生体計測データと比較されうる。換言すれば、様々な組の生体計測データの生体計測データ間の結び付きを心配することなく、すなわち、(例えば、右ではなく左の人差し指のような、指が置かれたときの誤りを補正するために)こうした生体計測データが同じ個人に結び付いているか否かを重要視することなく、少なくとも1つの「合致」データ値が求められる。
【０１００】
変形として、取得された様々な生体計測データ全てが同じ個人に関係するまで追加の確認を実施することができる。換言すれば、生体計測データ間の結び付きを考慮して、すなわち登録済み個人に関して「強化された」順位付けを適用することができる。
【０１０１】
別の変形として、少なくとも2つの異なる生体計測上の特徴を使用することができ、1つは、個人の迅速な選択(考え得る候補のリストアップ)を目的としており、もう1つは、正確な方法で、この選択から、捕捉された生体計測上の特徴に対応する個人を識別できるようにする。換言すれば、第1の順位付けを使用して、第2の順位付けが実行される候補の選択を(例えば、順位付けにおける最初のk個の位置を考慮して)行う。そこで第2の順位付けは、第2の生体計測上の特徴にデジタル化アルゴリズムを適用して取得されたデジタル値と、選択された個人に関係するデジタルデータのみとの間の近似度に基づいている。
【０１０２】
これは、例えば、デジタル化されていなかったり、デジタル値と結び付いていなかったりすることもある、第1のあまり際立っていない生体計測上の特徴を、第2の非常に際立った生体計測上の特徴を使用する前に使用することによって実行できる(例えば、候補を選択する際の顔と、識別する際の虹彩、または候補を選択する際の血管網と、識別する際の指紋)。
【０１０３】
当業者には明らかなように、他の可能性も存在する。
【０１０４】
さらに、図2を参照して説明したシステム以外のシステムも、本発明を実施することができる。例えば、はるかに大きなシステムを使用することができる。この後者の場合、安全モジュールは、例えばHSM(ハードウェアセキュリティモジュール)タイプの1つまたは複数の安全装置を含むことができる。
【０１０５】
マイクロチップより大きく能力が高いが、この種のモジュールはまた、犯意を持った者がデータの内容にアクセスできないように、データを物理的に保護する。
【０１０６】
前述の場合のように、特に従来型アルゴリズムによる生体計測データの系統的比較と比べて、処理の複雑性はなお限定される。
【０１０７】
特に図2および3を参照して上述した処理全ては、この種のシステムに適用できる。
【０１０８】
こうした種類の生体計測システムは、例えば、1つもしくは複数のHSMの1つもしくは複数のサブセクション、1つもしくは複数の中央データベースサーバ、1つもしくは複数のセンサー、1つもしくは複数のデジタル化サーバおよびこれらの各種エンティティ間の通信を可能にするネットワークリンクを備えることができる。HSMは2つのサブセクションに分けることができ、そのうちの少なくとも1つはc_iの順位付けに特化し、少なくともう1つ

は確認(照合)に特化し、これらのHSMのサブセクションは、物理的に別個であってよく、安全な方法で互いに通信できるよう設定される。当業者には明らかなように、他のアーキテクチャも考えられる。

【０１０９】

また、こうした処理方式が複雑な生体計測システムに限定されていないことが注目される。図2を参照して説明したような端末は、いくつかのサブセクションに分かれた安全モジュールを実際に使用することができる。これは、それぞれが一定のタスクに特化し、安全な方法で互いに通信できるいくつかの別個のマイクロチップのように、物理的に分かれていてよい。

【０１１０】

図4は、集中データベース13ならびに分散端末14および15を含む分散システムの一例である。1つの分散端末または3つより多い分散端末も変形として使用できることが注目される。

【０１１１】

この例では、データベース13は、好ましくは符号化された数組の生体計測データを含む。また、前述の方法の実施を可能にするデジタル化アルゴリズムも含むことができる。

【０１１２】

図4に示されている例では、データベース13は、2つの分散端末14および15のそれぞれにつき、デジタル化アルゴリズム(Φおよびφ)と共に1組の生体計測データ($E_K(b_1),\cdots,E_K(b_N)$および$E_K(d_1),\cdots,E_K(d_N)$)を保存する。

【０１１３】

有利なことに、データベース13は、登録が実行される、すなわち生体計測データの登録が確認前に実行される中央ワークステーションの一部を形成することができる。

【０１１４】

端末14および15の各々は、識別または許可の目的で処理に必要な生体計測データを符号化などの安全な方法でデータベース13から取得した後に、上述の端末1として機能することができる。

【０１１５】

有利なことに、登録システムはさらに、端末に保存されたデータc_iまたはe_iの送信または更新を管理する。

【０１１６】

この種のアーキテクチャは、例えば、登録が実行される中央ワークステーション、およびアクセスが各端末によって制御されている複数の空間を含むサイトで使用できる。この場合、登録された個人の同一性が、データベース13内で当該個人の生体計測データを符号化することによって、また端末14および15の各々の安全モジュールが提供する物理的保護によって、保護される。

【０１１７】

また、端末14および15は、生体計測データに比べて縮小されたサイズのデジタルデータに対して処理をするため、複雑性を軽減することができる。

【０１１８】

一般的に言って、システムはローカルなものであってよい。そのためシステムは、センサーを含む、安全モジュールが(例えば、組み込みまたは外部通信により)結び付いた端末を備える。安全モジュールは、例えば端末に含めることができるマイクロチップの形をとることができる。

【０１１９】

変形として、システムは分散型であってよい。その場合、システムは、生体計測データの少なくとも一部を保存する集中データベースおよびセンサーを含む少なくとも1つの分散端末を含むことができる。この場合、使用される各安全モジュールは集中データベースと結び付くことができ、分散端末の少なくとも1つと結び付くことができ、またはある部分が集中データベースと結び付き、別の部分が分散端末の少なくとも1つと結び付くこと

ができる。また、生体計測データの一部は分散端末の少なくとも1つの中に保存できる。

【０１２０】

最後に、上述の処理の全部または一部は、適切なコード命令を含む、少なくとも1つの安全モジュールと協働するコンピュータプログラムによって実施できることが注目される。

【符号の説明】

【０１２１】

1　端末
2　センサー
3　メモリ
4　安全モジュール、マイクロチップ
5　処理装置
7　リスト
13　集中データベース
14，15　分散端末

【図１】

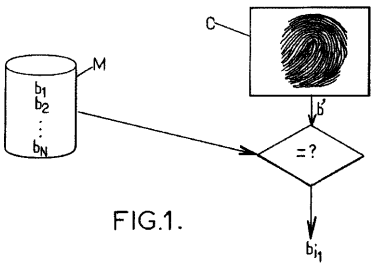


FIG.1.

【図２】

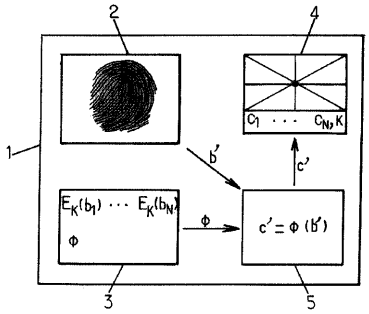


FIG.2.

【図３】

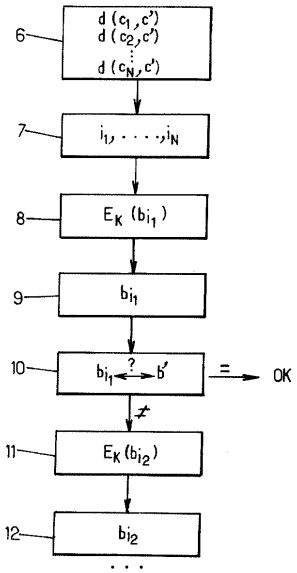
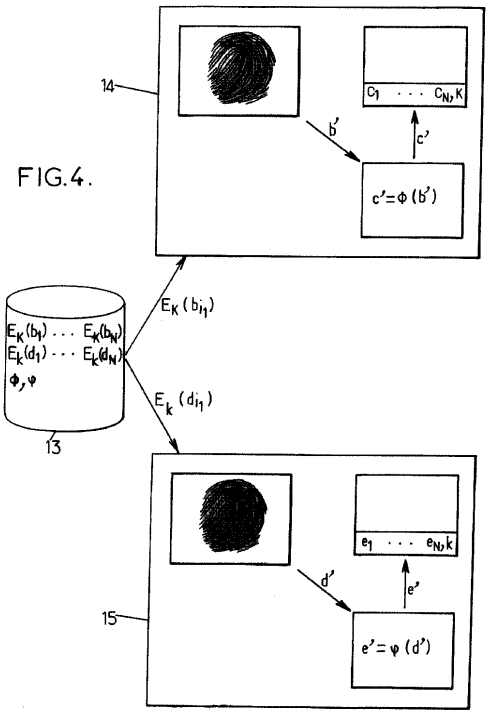


FIG.3.

【図４】

FIG.4.


14
$C_1 \cdots C_N, K$
b'
c'
c'=φ(b')
$E_K(b_{i_1})$
$E_K(b_1) \cdots E_K(b_N)$
$E_k(d_1) \cdots E_k(d_N)$
φ, ψ
$E_k(d_{i_1})$
13
$e_1 \cdots e_N, k$
d'
e'
15
e'=ψ(d')

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2009/052420

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/32 G06K9/00
ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L G06K

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, WPI Data, PAJ, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,P	WO 2009/083528 A (THALES SA [FR]; DELARUE ARNAUD [FR]; MARCELLO SANDRA [FR]; GIMENEZ JON) 9 July 2009 (2009-07-09) page 1 - page 14 figures 1-3 & FR 2 925 729 A (THALES SA [FR]) 26 June 2009 (2009-06-26) abstract page 1 - page 11 figures 1-3	1,2,5,8, 9,12,13, 15,16

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general 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" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

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

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with 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 documents, 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
12 April 2010	19/04/2010

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	Bec, Thierry

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

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2009/052420

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
T	BRINGER J ET AL: "The best of both worlds: Applying secure sketches to cancelable biometrics" SCIENCE OF COMPUTER PROGRAMMING, ELSEVIER SCIENCE PUBLISHERS BV., AMSTERDAM, NL, vol. 74, no. 1-2, 1 December 2008 (2008-12-01), pages 43-51, XP025686323 ISSN: 0167-6423 [retrieved on 2008-10-11] the whole document	1-16
A	WO 2007/029529 A (MITSUBISHI ELECTRIC CORP [JP]; MARTINIAN EMIN [US]; VETRO ANTHONY [US]) 15 March 2007 (2007-03-15) abstract page 3, line 15 - page 4, line 6 page 13, line 16 - page 21, line 22 figures 1-7	1-16
A	WO 02/095657 A (IRIDIAN TECHNOLOGIES INC [US]; BRAITHWAITE MICHAEL [US]; VON SEELEN UL) 28 November 2002 (2002-11-28) page 4, line 15 - page 5, line 20 page 6, line 14 - page 7, line 3 page 8, line 4 - page 15, line 15	1-16
A	US 2008/298642 A1 (MEENEN PETER M [US]) 4 December 2008 (2008-12-04) abstract paragraph [0061] - paragraph [0106]	1-16

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2009/052420

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2009083528 A	09-07-2009	FR 2925729 A1	26-06-2009
WO 2007029529 A	15-03-2007	CN 101253726 A	27-08-2008
		EP 1920554 A1	14-05-2008
		JP 2009507267 T	19-02-2009
		US 2006123241 A1	08-06-2006
WO 02095657 A	28-11-2002	CA 2447578 A1	28-11-2002
		EP 1402681 A2	31-03-2004
		JP 2004537103 T	09-12-2004
		US 2006235729 A1	19-10-2006
		US 2004193893 A1	30-09-2004
US 2008298642 A1	04-12-2008	NONE	

Form PCT/ISA/210 (patent family annex) (April 2005)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2009/052420

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. H04L9/32 G06K9/00
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)
H04L G06K

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, WPI Data, PAJ, IBM-TDB

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X,P	WO 2009/083528 A (THALES SA [FR]; DELARUE ARNAUD [FR]; MARCELLO SANDRA [FR]; GIMENEZ JON) 9 juillet 2009 (2009-07-09) page 1 - page 14 figures 1-3 & FR 2 925 729 A (THALES SA [FR]) 26 juin 2009 (2009-06-26) abrégé page 1 - page 11 figures 1-3	1,2,5,8, 9,12,13, 15,16

-/—

[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
12 avril 2010	19/04/2010

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	Bec, Thierry

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

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2009/052420

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
T	BRINGER J ET AL: "The best of both worlds: Applying secure sketches to cancelable biometrics" SCIENCE OF COMPUTER PROGRAMMING, ELSEVIER SCIENCE PUBLISHERS BV., AMSTERDAM, NL, vol. 74, no. 1-2, 1 décembre 2008 (2008-12-01), pages 43-51, XP025686323 ISSN: 0167-6423 [extrait le 2008-10-11] le document en entier	1-16
A	WO 2007/029529 A (MITSUBISHI ELECTRIC CORP [JP]; MARTINIAN EMIN [US]; VETRO ANTHONY [US]) 15 mars 2007 (2007-03-15) abrégé page 3, ligne 15 - page 4, ligne 6 page 13, ligne 16 - page 21, ligne 22 figures 1-7	1-16
A	WO 02/095657 A (IRIDIAN TECHNOLOGIES INC [US]; BRAITHWAITE MICHAEL [US]; VON SEELEN UL) 28 novembre 2002 (2002-11-28) page 4, ligne 15 - page 5, ligne 20 page 6, ligne 14 - page 7, ligne 3 page 8, ligne 4 - page 15, ligne 15	1-16
A	US 2008/298642 A1 (MEENEN PETER M [US]) 4 décembre 2008 (2008-12-04) abrégé alinéa [0061] - alinéa [0106]	1-16

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2009/052420

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
WO 2009083528	A	09-07-2009	FR	2925729 A1	26-06-2009
WO 2007029529	A	15-03-2007	CN	101253726 A	27-08-2008
			EP	1920554 A1	14-05-2008
			JP	2009507267 T	19-02-2009
			US	2006123241 A1	08-06-2006
WO 02095657	A	28-11-2002	CA	2447578 A1	28-11-2002
			EP	1402681 A2	31-03-2004
			JP	2004537103 T	09-12-2004
			US	2006235729 A1	19-10-2006
			US	2004193893 A1	30-09-2004
US 2008298642	A1	04-12-2008	AUCUN		

Formulaire PCT/ISA/210 (annexe familles de brevets) (avril 2005)

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(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,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),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,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,ZA,ZM,ZW

(72)発明者 エルヴェ・シャバンヌ
フランス・Ｆ－７５０１５・パリ・リュ・ルブラン・２７・サジェム・セキュリテ内
(72)発明者 ジュリアン・ブリンガー
フランス・Ｆ－７５０１５・パリ・リュ・ルブラン・２７・サジェム・セキュリテ内

Ｆターム(参考) 5B043 AA04 AA09 BA02 BA03 BA04 CA10 EA05 FA04 FA09 GA03
GA04
5B285 AA01 AA04 BA01 BA08 CA42 CA43 CA52 CB12 CB14 CB15
CB16 CB17 CB62 CB63 CB73 CB74