

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第6238867号

(P6238867)

(45) 発行日 平成29年11月29日 (2017.11.29)

(24) 登録日 平成29年11月10日 (2017.11.10)

(51) Int. Cl. F I
H04L 9/32 (2006.01) H04L 9/00 673D
G06F 21/32 (2013.01) G06F 21/32

請求項の数 2 (全 19 頁)

(21) 出願番号	特願2014-201055 (P2014-201055)	(73) 特許権者	000005108
(22) 出願日	平成26年9月30日 (2014. 9. 30)		株式会社日立製作所
(65) 公開番号	特開2016-72836 (P2016-72836A)		東京都千代田区丸の内一丁目6番6号
(43) 公開日	平成28年5月9日 (2016. 5. 9)	(74) 代理人	110000176
審査請求日	平成29年1月26日 (2017. 1. 26)		一色国際特許業務法人
		(72) 発明者	高橋 健太
			東京都千代田区丸の内一丁目6番6号 株
			式会社日立製作所内
		審査官	中里 裕正

最終頁に続く

(54) 【発明の名称】 逐次バイOMETリック暗号システムおよび逐次バイOMETリック暗号処理方法

(57) 【特許請求の範囲】

【請求項 1】

ユーザごとに複数種類の生体部位それぞれに関して取得された予め定めた所定数の生体情報の各々から特徴データを抽出し、当該抽出した複数個の特徴データから、予めユーザ毎に決められた前記複数種類の生体部位の間での入力順序に従って、前記生体部位ごとの生体情報に基づく前記特徴データの個数内で取り得る全ての特徴データの組合せを選択し、当該選択した各特徴データを前記入力順序に応じて組み合わせた組ごとに保護テンプレートを作成して記憶装置に格納する登録処理と、

所定ユーザの複数種類の生体部位それぞれについて前記入力順序に従ってセンサを介して取得した、該当ユーザの該当生体部位それぞれの前記所定数の生体情報の組合せについて特徴データを抽出し、当該抽出した特徴データの前記入力順序に応じた組合せに対し、所定属性が同じ生体情報に由来する前記保護テンプレートを照合し、当該照合に成功した場合に前記ユーザに関する所定処理を実行する照合処理と、

を実行する演算装置を含むことを特徴とする逐次バイOMETリック暗号システム。

【請求項 2】

情報処理装置が、

ユーザごとに複数種類の生体部位それぞれに関して取得された予め定めた所定数の生体情報の各々から特徴データを抽出し、当該抽出した複数個の特徴データから、予めユーザ毎に決められた前記複数種類の生体部位の間での入力順序に従って、前記生体部位ごとの生体情報に基づく前記特徴データの個数内で取り得る全ての特徴データの組合せを選択し

10

20

、当該選択した各特徴データを前記入力順序に応じて組み合わせる組ごとに保護テンプレートを作成して記憶装置に格納する登録処理と、

所定ユーザの複数種類の生体部位それぞれについて前記入力順序に従ってセンサを介して取得した、該当ユーザの該当生体部位それぞれの前記所定数の生体情報の組合せについて特徴データを抽出し、当該抽出した特徴データの前記入力順序に応じた組合せに対し、所定属性が同じ生体情報に由来する前記保護テンプレートを照合し、当該照合に成功した場合に前記ユーザに関する所定処理を実行する照合処理と、

を実行することを特徴とする逐次バイオメトリック暗号処理方法。

【発明の詳細な説明】

【技術分野】

10

【0001】

本発明は、逐次バイオメトリック暗号システムおよび逐次バイオメトリック暗号処理方法に関するものであり、具体的には、バイオメトリック暗号において、高い精度向上効果を持つ逐次マルチモーダル判定を実現し、暗号処理に関する安全性、精度、利便性を共に良好なものとする技術に関する。

【背景技術】

【0002】

指紋や静脈、顔、虹彩などの生体情報に基づいて個人を認証する生体認証技術が広く利用されている。従来の生体認証技術は、ユーザ登録時にユーザの生体情報から抽出した特徴データ（テンプレート）をシステムに登録しておき、ユーザ認証時に再びユーザの生体情報から抽出した特徴データをテンプレートと比較して、両者の類似度が十分大きい（距離が十分近い）ならば認証成功、そうでなければ認証失敗と判定する。

20

【0003】

しかし、生体情報は取り替えることのできない情報であるため、その漏洩の発生は大きな問題となる。こうした問題に対し、生体情報を秘匿したまま認証する、テンプレート保護型生体認証技術が研究開発されている。その中で、生体情報から鍵データを生成し、暗号学的な認証、暗号化、署名生成などの処理を行う、バイオメトリック暗号と呼ばれる技術が注目されている。

【0004】

上述のバイオメトリック暗号では、登録時に生体情報の特徴データ X を変換することで、保護テンプレート T を作成する。その後、新たに取得した生体情報の特徴データ X' と保護テンプレート T を照合する。この照合に成功した場合、認証、暗号、署名などの処理を行うことができる。こうしたバイオメトリック暗号において、 T から X を復元または推定することは十分困難でなくてはならない（安全性の要件）。また X' が X に十分類似している（距離が近い）ならば、その場合に限り認証、暗号、署名などの処理に成功しなくてはならない（完全性・健全性の要件）。更に、 X と X' が、本人の同一の生体情報から抽出された特徴データであるなら、その場合に限り、十分高い確率で X と X' が十分類似しなくては（距離が十分近くなくては）ならない（精度の要件）。

30

【0005】

以上のバイオメトリック暗号の具体的な実現方法として、例えば、登録時に秘密鍵 K をランダムに生成し、そのハッシュ値 $h = \text{Hash}(K)$ を計算するとともに、生体情報 X に対して K を不可分な形で埋め込み、補助情報 $H = F(X, K)$ を作成し、 H と h の組を保護テンプレート T とする（ $T = (H, h)$ ）、技術が提案されている（非特許文献1参照）。この技術において、鍵復元時には、再び生体情報 X' を取得し、補助情報 H を用いて秘密鍵 $K' = G(X', H)$ を復元する。 X' が X に十分近いならば、 $K' = K$ となるよう、埋め込み関数 F 、復元関数 G には誤り訂正符号技術などを利用する。また、 $\text{Hash}(K') = h$ が成立すれば照合成功とする。またこのとき、復元された $K (= K')$ を用いて認証、暗号化、署名生成などの処理を行うこともできる。

40

【0006】

一般に、生体認証システムの精度は、他人受入率（FAR: False Accept

50

tance Rate)と本人拒否率(FRR: False Rejection Rate)で評価される。FARが大きいと他人によるなりすましの危険が高まり、FRRが大きいと真正な本人が認証できず可用性の低下につながる。一般にFARとFRRは、認証しきい値 t によってコントロールすることができるが、一方を小さくすると他方が大きくなるというトレードオフの関係にあり、両者をともに小さくすることは難しい。

【0007】

一般的な生体認証技術においては、この問題に対する解決策として、複数の生体情報、例えば両手の指10本や、指紋・静脈・虹彩などを組み合わせて、FARを十分小さくしつつFRRも小さく抑える、マルチモーダル生体認証技術が提案されている。マルチモーダル生体認証においては、各生体情報をそれぞれテンプレートとして登録しておく。例えば両手の指10本を使う場合は、10本分のテンプレートを登録しておく。認証時にも各生体情報を取得して、対応するテンプレートと照合し、個々の照合結果を総合して最終的に認証成功とするか失敗とするかを判定する。

【0008】

しかし、認証時に全ての生体情報の入力を要求すると、利用者の操作が煩雑なものとなり、利便性の低下につながる。このため一つの生体情報を入力する度に照合・判定を行い、認証成功と判定された時点で処理を終了する、逐次判定技術も提案されている。

【0009】

例えば、単純に一つの生体情報を入力・照合し、それが十分類似していれば認証成功と判定する、OR判定方式がある。しかしながらOR判定方式は、個々の生体情報の照合・判定を独立に行っているだけであり、各判定におけるFARを十分小さなものとするためには、各判定におけるしきい値を十分厳しくせざるをえず、結果として各判定におけるFRRは大きくなってしまう。照合・判定を複数回繰り返すことでトータルとしてのFRRはある程度下げられるものの、複数の生体情報の組み合わせが持つ情報を有効活用できず、トータルでの認証精度の向上効果は限定的なものとなる。

【0010】

一方、より高度な逐次判定方式として、逐次確率比検定を用いる方法（非特許文献2参照）も提案されている。この技術は、生体情報 X_k ($k=1, 2, \dots, n$)を照合する度に、照合スコア（類似度または距離） S_k を、それらが従う統計的分布を用いて尤度比 L_k に正規化し、 $M_k = L_1 \times L_2 \times \dots \times L_k$ を、しきい値 t と比較する手法である。この方法は、認証精度と平均照合回数の観点から最適な逐次判定方式であることが証明されている。逐次確率比検定は、照合スコア S_k として連続的、あるいは多値の類似度または距離が計算できる場合に有効な方法である。

【先行技術文献】

【非特許文献】

【0011】

【非特許文献1】Y. Dodis, et. al., "Fuzzy extractors: How to generate strong keys", In Eurocrypt 2004, Vol. 3027 of LNCS, pp. 523-540, 2004.

【非特許文献2】K. Takahashi, et. al., "A Secure and User-Friendly Multi Modal Biometric System", International Symposium on Defence and Security 2004, 2014.

【発明の概要】

【発明が解決しようとする課題】

【0012】

上述の通り、バイオメトリック暗号において、保護テンプレート T から特徴データ X を復元または推定することは十分困難でなくてはならない（安全性の要件）。しかし、仮に保護テンプレート T と特徴データ X' を照合する際に、何らかの照合スコア（類似度や距

10

20

30

40

50

離値)が計算できてしまうとすると、攻撃者は適当な初期値X 0に対して様々な微小な摂動を加えつつ照合し、類似度がより大きくなる(距離がより小さくなる)方向の摂動を採用する、といった処理を繰り返すことで、最終的に類似度がしきい値tを超える特徴データX'を見つける可能性がある。こうした事態を防ぐためには、バイオメトリック暗号において、その照合結果は1(一致)、0(不一致)の2値でなければならない。更に同様の理由により、バイオメトリック暗号におけるしきい値は、認証時に変更できてはならない。実際、バイオメトリック暗号は、保護テンプレートTを作成する際にしきい値tが設定され、以降はtを変更できない仕組みとなっている。例えば非特許文献1の技術においては、補助情報を作成する際に誤り訂正符号を用いた符号化処理を行うが、その際に設定する訂正能力(何ビットまでのエラーを許容するか等)がしきい値tに相当する。

10

【0013】

以上の理由から、逐次マルチモーダル生体認証の手法を適用して精度と利便性を向上しようとした場合、照合スコアを利用する精度向上効果の高い手法(例えば逐次確率比検定)は適用することができない。OR判定は適用可能であるが、精度向上の効果は限定的なものとなる。

【0014】

そこで本発明の目的は、バイオメトリック暗号において、高い精度向上効果を持つ逐次マルチモーダル判定を実現し、暗号処理に関する安全性、精度、利便性を共に良好なものとする技術を提供することにある。

【課題を解決するための手段】

20

【0015】

上記課題を解決する本発明の逐次バイオメトリック暗号システムは、ユーザごとに複数種類の生体部位それぞれに関して取得された予め定めた所定数の生体情報の各々から特徴データを抽出し、当該抽出した複数個の特徴データから、予めユーザ毎に決められた前記複数種類の生体部位の間での入力順序に従って、前記生体部位ごとの生体情報に基づく前記特徴データの個数内で取り得る全ての特徴データの組合せを選択し、当該選択した各特徴データを前記入力順序に応じて組み合わせた組ごとに保護テンプレートを作成して記憶装置に格納する登録処理と、所定ユーザの複数種類の生体部位それぞれについて前記入力順序に従ってセンサを介して取得した、該当ユーザの該当生体部位それぞれの前記所定数の生体情報の組合せについて特徴データを抽出し、当該抽出した特徴データの前記入力順序に応じた組合せに対し、所定属性が同じ生体情報に由来する前記保護テンプレートを照合し、当該照合に成功した場合に前記ユーザに関する所定処理を実行する照合処理と、を実行する演算装置を含むことを特徴とする。

30

【0016】

また、本発明の逐次バイオメトリック暗号処理方法は、情報処理装置が、ユーザごとに複数種類の生体部位それぞれに関して取得された予め定めた所定数の生体情報の各々から特徴データを抽出し、当該抽出した複数個の特徴データから、予めユーザ毎に決められた前記複数種類の生体部位の間での入力順序に従って、前記生体部位ごとの生体情報に基づく前記特徴データの個数内で取り得る全ての特徴データの組合せを選択し、当該選択した各特徴データを前記入力順序に応じて組み合わせた組ごとに保護テンプレートを作成して記憶装置に格納する登録処理と、所定ユーザの複数種類の生体部位それぞれについて前記入力順序に従ってセンサを介して取得した、該当ユーザの該当生体部位それぞれの前記所定数の生体情報の組合せについて特徴データを抽出し、当該抽出した特徴データの前記入力順序に応じた組合せに対し、所定属性が同じ生体情報に由来する前記保護テンプレートを照合し、当該照合に成功した場合に前記ユーザに関する所定処理を実行する照合処理と、を実行することを特徴とする。

40

【発明の効果】

【0017】

本発明によれば、バイオメトリック暗号において、高い精度向上効果を持つ逐次マルチモーダル判定を実現し、暗号処理に関する安全性、精度、利便性を共に良好なものとして出来

50

る。

【図面の簡単な説明】

【0018】

【図1】本実施形態の逐次バイOMETリック暗号システムを含むネットワーク構成図である。

【図2】本実施形態の逐次バイOMETリック暗号システムを構成する登録端末のハードウェア構成例を示す図である。

【図3】本実施形態の逐次バイOMETリック暗号システムを構成する認証端末のハードウェア構成例を示す図である。

【図4】本実施形態のテンプレートデータベースの構成例を示す図である。

10

【図5】本実施形態の逐次バイOMETリック暗号処理方法の処理手順例1を示すフロー図である。

【図6】本実施形態の逐次バイOMETリック暗号処理方法の処理手順例2を示すフロー図である。

【発明を実施するための形態】

【0019】

——システム構成——

【0020】

以下に本発明の実施形態について図面を用いて詳細に説明する。図1は、本実施形態の逐次バイOMETリック暗号システム10を含むネットワーク構成図である。図1に示す逐次バイOMETリック暗号システム10は、バイOMETリック暗号において、高い精度向上効果を持つ逐次マルチモーダル判定を実現し、暗号処理に関する安全性、精度、利便性を共に良好なものとするコンピュータシステムである。

20

【0021】

本実施形態における逐次バイOMETリック暗号システム10は、登録端末100、認証端末150、およびテンプレートデータベース120をネットワーク140で接続した構成を想定する。このうち、登録端末100は、ユーザの生体情報から保護テンプレートを作成して登録する端末であり、認証端末150は、認証処理等の実行時にユーザの生体情報を複数取得して所定の特徴データを抽出し、これをテンプレートデータベース120における保護テンプレートと照合して、ユーザ認証、データの暗号化、復号化、および電子署名の作成といった所定の処理を行う端末である。また、テンプレートデータベース120は、上述の登録端末100が生成した保護テンプレートをユーザIDと紐づけて保存するデータベースである。

30

【0022】

なお、テンプレートデータベース120は、独立したサーバマシン上に実装してもよいが、登録端末100または認証端末150に実装する構成を採用してもよい。また、こうしたテンプレートデータベース120は、ユーザ毎に異なる実装形態を採用する状況を想定するとしてもよい。例えば、各ユーザが所持するカード、USBメモリ、携帯端末などの可搬媒体や個人管理の装置にテンプレートデータベース120が保持されとしてもよい。また、登録端末100、認証端末150、およびテンプレートデータベース120の少なくとも2つ以上が同じ装置に実装される構成であってもよい。登録端末100、認証端末150、およびテンプレートデータベース120の全てが同じ装置内に実装される構成とした場合、ネットワーク140は無くてもよい。

40

——ハードウェア構成の例——

【0023】

続いて、本実施形態の逐次バイOMETリック暗号システム10を構成する上述の装置類について、そのハードウェア構成の例について説明する。図2は本実施形態の逐次バイOMETリック暗号システム10を構成する登録端末100のハードウェア構成例を示す図である。

【0024】

50

本実施形態の登録端末100は、SSD (Solid State Drive) やハードディスクドライブなど適宜な不揮発性記憶素子で構成される記憶装置101、RAMなど揮発性記憶素子で構成されるメモリ103、記憶装置101に保持されるプログラム102をメモリ103に読み出すなどして実行し装置自体の統括制御を行なうとともに各種判定、演算及び制御処理を行なうCPU104、生体情報のセンサ1051を含む入力装置105、処理データの表示を行うディスプレイ等の出力装置106、ネットワーク140と接続し他装置との通信処理を担う通信装置107、を備える。

【0025】

なお、プログラム102の実行によって当該登録端末100に実装される機能部としては、センサ部110、特徴抽出部111、ID入力部112、および保護テンプレート作成部113が含まれている。これら機能部110～113の詳細については後述する。

10

【0026】

一方、上述の登録端末100と共に本実施形態の逐次バイOMETリック暗号システム10を構成する認証端末150は、図3にて例示するように、SSD (Solid State Drive) やハードディスクドライブなど適宜な不揮発性記憶素子で構成される記憶装置151、RAMなど揮発性記憶素子で構成されるメモリ153、記憶装置151に保持されるプログラム152をメモリ153に読み出すなどして実行し装置自体の統括制御を行なうとともに各種判定、演算及び制御処理を行なうCPU154、生体情報のセンサ1551を含む入力装置155、処理データの表示を行うディスプレイ等の出力装置156、ネットワーク140と接続し他装置との通信処理を担う通信装置157、を備える。

20

【0027】

なお、プログラム152の実行によって当該認証端末150に実装される機能部としては、ID入力部160、保護テンプレート取得部161、センサ部162、特徴抽出部163、および認証・暗号・署名部164から構成される。これら機能部160～164の詳細については後述する。

——機能の例——

【0028】

続いて、本実施形態の逐次バイOMETリック暗号システム10を構成する各装置が備える機能について説明する。上述したように、以下に説明する機能は、例えば逐次バイOMETリック暗号システム10を構成する各装置がプログラムを実行することで実装される機能と言える。ここでは上述の登録端末100および認証端末150の備える各機能部について説明するものとする。

30

【0029】

まず、本実施形態の登録端末100におけるセンサ部110は、入力装置105に備わるセンサ1051を介し、このセンサ1051に身体の所定部位を提示したユーザ（以下、登録対象ユーザ）から、指紋や静脈などの複数の登録用生体情報を取得する機能を備えている。センサ1051は、指紋、静脈、虹彩など生体情報の種類ごとに入力装置105に備わっているとしてもよい。また、手指の指紋など同一種類の異なる生体情報を処理対象とする場合、センサ1051は一つのみであってもよい。

40

【0030】

また、登録端末100における特徴抽出部111は、上述のセンサ部110が登録対象ユーザについて得た複数の登録用生体情報から、複数の登録用特徴データを抽出する機能を備えている。

【0031】

また、登録端末100におけるID入力部112は、入力装置105におけるタッチパネルやキーボード等のインターフェイスを介して、上述の登録対象ユーザによるユーザIDの入力を受け付ける機能を備えている。

【0032】

また、登録端末100における保護テンプレート作成部113は、上述の特徴抽出部1

50

11が抽出した、登録対象ユーザごとの複数の登録用特徴データをから、組合せ個数を通増させて複数の特徴データの組を順次選択し、当該選択した各特徴データの組ごとに、所定の他人受入率を達成する保護テンプレートを作成し、これを該当登録対象ユーザのユーザIDと少なくとも対応付けてテンプレートデータベース120に格納する機能を備えている。

【0033】

なお、この保護テンプレート作成部113は、保護テンプレートの作成に際し、上述の複数の登録用特徴データから、予め登録対象ユーザ毎に決められた生体情報の入力順序に従って、組合せ個数を通増させて複数の登録用特徴データの組を順次選択し、当該選択した各登録用特徴データの組ごとに、所定の他人受入率を達成する保護テンプレートを作成する機能も備えている。

10

【0034】

更に、この保護テンプレート作成部113は、保護テンプレートの作成に際し、上述の複数の登録用特徴データから、上述の組合せ個数の登録用特徴データの組を選択するにあたり、該当組合せ個数内で取り得る全ての登録用特徴データの組合せを選択し、当該選択した各登録用特徴データの組ごとに、所定の他人受入率を達成する保護テンプレートを作成する機能も備えている。

【0035】

一方、認証端末150におけるID入力部160は、入力装置155におけるタッチパネルやキーボード等のインターフェイスを介して、本人認証等の所定処理を行う希望のあるユーザ（以下、認証対象ユーザ）によるユーザIDの入力を受け付ける機能を備えている。

20

【0036】

また、認証端末150における保護テンプレート取得部161は、上述のID入力部160が得たユーザIDをキーにして、テンプレートデータベース120で検索を実行し、該当ユーザIDに紐づいた保護テンプレートを取得する機能を備えている。

【0037】

また、認証端末150におけるセンサ部162は、入力装置155に備わるセンサ1551を介し、このセンサ1551に身体の所定部位を提示した上述の認証対象ユーザから、指紋や静脈などの、1つまたは複数の生体情報を取得する機能を備えている。なお、このセンサ部162は、上述の認証対象ユーザに対する処理の開始以降、センサ1551に対する、該当認証対象ユーザによる身体部位（例：各手指のいずれか）の読み取らせ動作の毎に、異なる部位の生体情報を取得する。つまり、センサ部162は、認証対象ユーザに対する処理の開始以降、該当ユーザにおける互いに異なる身体部位の生体情報を、（ユーザの動作に伴って）逐次的に取得することとなる。

30

【0038】

また、認証端末150における特徴抽出部163は、上述のセンサ部162が得た、認証対象ユーザの1つ以上の生体情報の組合せについて特徴データを抽出する機能を備えている。

【0039】

また、認証端末150における認証・暗号・署名部164は、上述の特徴抽出部163が抽出した特徴データを、テンプレートデータベース120の保護テンプレートのうち該当ユーザID（ID入力部160が得たもの）と紐付いたもので、所定属性が同じ、すなわち同じ身体部位の生体情報に由来する前記保護テンプレートと照合し、その結果に応じて、上述の認証対象ユーザに関する認証、データの暗号化・復号化、電子署名の作成など所定処理を行う機能を備えている。

40

【0040】

なお、本実施形態の認証・暗号・署名部164は、センサ部162による生体情報取得開始から或る時点までに得た全ての生体情報（例：人差し指と中指の各生体情報）から特徴データを抽出して組合せ、当該特徴データの組合せに対し、該当ユーザIDと紐付いて

50

おり、所定属性が同じ生体情報（例：人差し指と中指の各生体情報）に由来する保護テンプレートを照合し、当該照合に成功した場合に、上述の認証対象ユーザに関する上述の所定処理を実行するものとする。

【0041】

この場合、認証・暗号・署名部164は、上述の特徴データと保護テンプレートとの照合に失敗した場合、上述の生体情報取得開始からの生体情報の取得数が規定数に達しているか判定し、この判定の結果、生体情報の取得数が規定数に達していないならば、センサ部162による、互いに異なる生体情報の逐次的な取得の処理と、特徴データの組合せに対する保護テンプレートの照合以降の処理を繰り返し実行する機能を備えている。また、認証・暗号・署名部164は、上述の判定の結果、生体情報の取得数が規定数に達してい

10

——データ構造例——

【0042】

次に、本実施形態の逐次バイOMETリック暗号システム10が用いるテンプレートデータベース120におけるデータ構造例について説明する。図4は本実施形態のテンプレートデータベース120の構成例を示す図である。本実施形態におけるテンプレートデータベース120は、図4にて例示するように、ユーザID毎に、部位の識別情報をキーとして保護テンプレートのデータを対応付けたレコードの集合体となっている。図4のテンプレートデータベース120の例では、ユーザID：00001なるユーザについて、その身体部位のうち「A」の生体情報から生成した保護テンプレート、「A」および「B」の生体情報から生成した保護テンプレート、「A」、「B」、「C」の生体情報から生成した保護テンプレート、「A」、「B」、「C」、「D」の生体情報から生成した保護テンプレート、が含まれるデータベースとなっている。

20

【0043】

このテンプレートデータベース120における部位に関する識別情報は、ユーザが登録動作の対象とする身体部位の登録順序に対応した文字列であるとしてもよい。従ってこの場合、当該テンプレートデータベース120における或るレコードにて、部位の識別情報が「A、B、C」であれば、該当ユーザは、登録端末100における生体情報の登録動作を、部位「A」→部位「B」→部位「C」の順で行ったことを示すことになる。また、該当ユーザが後に照合処理の対象となる場合にも、この文字列が示す身体部位の順序にて、自身の該当部位を認証端末150のセンサ1551に順次読み取らせることになる。

30

——処理手順例1——

【0044】

以下、本実施形態における逐次バイOMETリック暗号処理方法の実際手順について図に基づき説明する。以下で説明する逐次バイOMETリック暗号処理方法に対応する各種動作は、逐次バイOMETリック暗号システム10を構成する登録端末100、認証端末150らがメモリ等に読み出して実行するプログラムによって実現される。そして、このプログラムは、以下に説明される各種の動作を行うためのコードから構成されている。

【0045】

図5は、本実施形態における逐次バイOMETリック暗号処理方法の処理手順例1を示すフロー図であり、具体的には逐次バイOMETリック暗号処理方法における登録処理を示すフロー図である。例えば、或る金融機関のユーザが、該当金融機関でのサービスを受けるべく、自身の生体情報登録を行おうと、この金融機関に設置された登録端末100を操作する状況を想定する。

40

【0046】

ここではまず、登録端末100のID入力部112が、タッチパネル等の入力装置105において、上述のユーザ、すなわち登録対象ユーザによるユーザIDの入力を受け付けて、このユーザIDをメモリ103に一旦格納する（S200）。この登録対象ユーザは、ユーザIDの入力に引き続き、登録端末100が出力装置106に表示する所定の誘導メッセージ等に応じて、自身の手指をセンサ1051にかざしたとする。

50

【0047】

この時、登録端末100のセンサ部110は、入力装置105のセンサ1051を通して、この登録対象ユーザが逐次かざした手指、例えば人差し指、中指、薬指、小指、のそれぞれから指静脈等の生体情報を取得し、例えばメモリ103に一旦格納する（S201）。この場合、4本の手指からそれぞれ生体情報を取得することになるため、得られる登録用生体情報の総数Nは、4個となる。

【0048】

なお本実施形態では、登録対象ユーザに関してN個（ $N > 1$ ）の異なる生体情報を取得するものとする。例えば、片手の人差し指、中指、薬指、小指の静脈を取得するならば $N = 4$ 、両手の人差し指、中指、薬指の静脈を取得するならば $N = 6$ 、更に同じ指の指紋を

10

あわせて取得するならば $N = 12$ 、更に両目の虹彩をあわせて取得するならば $N = 14$ となる。このように登録対象ユーザの登録時には、N個全ての生体情報を取得して、保護テンプレート作成に用いるものとする。

【0049】

また、登録対象ユーザが、センサ1051にて自身の身体部位をかざす順序、すなわち入力順序は、予め決められたものを出力装置106で該当ユーザに指示するケースや、或いは、該当ユーザが任意に決めて入力装置105で入力するケースが想定出来る。この場合、いずれにしても、登録時と認証時とで上述の入力順序は同一ユーザである限りは固定されるため、これを「順序固定」と呼ぶことにする。いずれの場合でも、入力順序が規定する身体部位と登録用特徴データとは対応付くことになり、登録端末100は、センサ1051より得た生体情報を、入力順序が規定する身体部位の識別情報と対応付けてメモリ103に格納することとなる。

20

【0050】

なお、登録時の入力順序は固定である一方、認証時には、認証対象ユーザが自由に入力順序を選択するとしてもよく、これを「順序選択」と呼ぶことにする。また他の順序決定方法、例えば指紋6つ、静脈6つ、虹彩2つの順で入力することは固定されているが、指紋の6つの中では順序を選択することができる、など「順序固定」と「順序選択」を組み合わせ採用するとしてもよい。

【0051】

次に、登録端末100の特徴抽出部111が、上述のN個の登録用生体情報からN個の登録用特徴データ X_1 , X_2 , ..., X_N を抽出し、一旦メモリ103に格納する（S202）。ここで、登録端末100の保護テンプレート作成部113は、メモリ103に設けた適宜なワーク領域にて、以降の手順で用いる変数 k 、 j について、 $k = 1$ 、 $j = 1$ の各値を格納する（S203）。

30

【0052】

続いて登録端末100の保護テンプレート作成部113は、メモリ103に保持している上述のN個の登録用特徴データから、 k 個の登録用特徴データの組み合わせ $S_j = (X_i_1, X_i_2, \dots, X_i_k)$ を選択する（S204）。ここで、上述した順序固定の場合、 S_j は入力順序の先頭から k 個の登録用特徴データとする。一方、上述した順序選択の場合、保護テンプレート作成部113は、N個から k 個を選択する全ての組み合わせについて、以降のステップS204～S207を繰り返すものとする。

40

【0053】

続いて保護テンプレート作成部113は、上述で選択した k 個の登録用特徴データの組 S_j から、合成特徴データを作成する（S205）。 k 個の登録用特徴データを合成する方法は任意であるが、例えば各登録用特徴データ X_i_1 （ $i = 1, 2, \dots, k$ ）がベクトル形式（ビット列を含む）で表現されている場合、それぞれを適宜な定数倍して連結したベクトル形式のデータを合成特徴データとして求めるとしてもよい。また、各登録用特徴データ X_i_1 それぞれを適宜な定数倍して互いに加減算などの演算を施したものを合成特徴データとしてもよい。

50

【0054】

次に、保護テンプレート作成部113は、上述のステップS205で得た合成特徴データから、保護テンプレート T_j を作成し、これをテンプレートデータベース120に格納する（S206）。図4に関して既に例示したように、保護テンプレート作成部113が作成、格納する保護テンプレートは、合成特徴データの起源となっている登録用特徴データに紐付いている身体部位の識別情報と対応付けられている。

【0055】

なお、本実施例においては、認証・暗号・署名の際に逐次的に判定を行うが、このとき各判定において許容できるFAR値（許容FAR値）をあらかじめ定めておき、登録端末100はこれを保持するものとする。こうした保護テンプレート作成部113は、この許容FAR値を達成するように、しきい値 t （例えば誤り訂正符号の訂正能力）を設定して保護テンプレートの作成を行う。

10

【0056】

上述の k が所定値より小さい場合、例えば $k=1$ のときは、上述の許容FAR値を達成する保護テンプレートは、FRRが相対的に大きくなるが、 k が大きくなるに従って、同じ許容FAR値を達成する保護テンプレートであってもFRRは相対的に小さくなる。これは生体情報を複数組み合わせることで情報量が増えるため、より良い精度での照合が可能となり、同じFARに対してFRRを小さくすることができるためである。

【0057】

続いて、保護テンプレート作成部113は、上述の変数 $j=j+1$ とし（S207）、この段階にて、（上述の順序選択の場合） N 個から k 個の登録用特徴データを選択する全ての組み合わせについて保護テンプレートを作成し終えているか判定し（S208）、作成し終えていない場合（S208：n）、処理をステップS204へ戻す。

20

【0058】

他方、 N 個から k 個の登録用特徴データを選択する全ての組み合わせについて保護テンプレートを作成し終えていた場合（S208：y）、保護テンプレート作成部113は、上述の変数 $k=k+1$ とする（S209）。ここで、 $k=N$ なら（S210：y）、保護テンプレート作成部113は、 $m=j$ として、作成した m 個全ての保護テンプレートの組 $T=(T_1, \dots, T_m)$ を、上述のユーザIDとともにテンプレートデータベース120に送信する（S211）。一方、 $k<N$ ならば（S210：n）、保護テンプレート作成部113は、所定りをステップS204に戻す。ここで、上述の順序固定ならば $m=N$ 、順序選択ならば $m=2^N-1$ （ 2^N は、2の N 乗）である。

30

【0059】

一方、テンプレートDB120は、ネットワーク140を介して登録端末100の保護テンプレート作成部113から送信されてきた、上述の m 個の保護テンプレートを該当ユーザIDと紐づけて保存し（S212）、処理を終了する。こうした一連の処理によりテンプレートデータベース120が生成されることとなる。

【0060】

以上のように、登録処理の際、認証・暗号・署名の際に逐次的に入力されるであろう生体情報の全ての組み合わせに対して保護テンプレートを作成しつつ、各保護テンプレートの要求FAR値を一定に保つことで、総当たり攻撃による生体情報の復元や推定、なりすましを防止することができる。

40

——処理手順例2——

【0061】

次に、ユーザの生体情報に関する照合処理について図に基づき説明する。図6は、本実施形態の逐次バイオメトリック暗号処理方法の処理手順例2を示すフロー図であり、具体的には本実施形態の逐次バイオメトリック暗号処理方法における照合処理を示すフロー図である。ここでの「照合処理」とは、認証対象ユーザから読み取って取得した生体情報に由来する特徴データと、テンプレートデータベース120にて該当ユーザについて予め登録済みの保護テンプレートとを照合する処理と、その結果に応じて行う認証、データの暗

50

号化、復号化、電子署名といった処理も含む一連のものとする。

【0062】

また、上述の図5で例示した登録端末100での処理を受けた登録対象ユーザが、その後、該当金融機関でのサービスを実際に受けるべく、ATM等の認証端末150を操作する状況を想定する。ここでは、上述の登録対象ユーザが、認証対象ユーザとなったものとする。

【0063】

ここ場合まず、認証端末150のID入力部160が、タッチパネル等の入力装置155において、上述のユーザ、すなわち認証対象ユーザのID入力を受け付ける(S300)。次に、認証端末150の保護テンプレート取得部161は、上述のステップS300で受けたユーザIDをキーにテンプレートデータベース120で検索を実行し、該当ユーザIDに紐づいた保護テンプレートの集合、 $T_1, \dots, T_m$ を取得する(S301、S302)。

10

【0064】

ここで認証端末150のセンサ部162は、メモリ103に設けた適宜なワーク領域にて、以降の手順で用いる変数 k 、 S について、 $k=1$ 、 $S=\{\}$ ($\{\}$ は空集合)の各値を格納する(S303)。このうち「 S 」を取得済み特徴データ集合とする。

【0065】

続いて認証端末150のセンサ部162は、センサ1551に認証対象ユーザがかざした部位について生体情報を取得する(S304)。なお、認証対象ユーザは、後述する照合結果が失敗であった場合、その時点までに当該ステップS304で生体情報を取得させた部位とは異なる身体部位を、センサ1551にかざす動作を行うことになる。

20

【0066】

このように、当該ステップS304の繰り返しを踏まえて、本実施形態では、上述の変数 k の値を、ステップS304すなわち生体情報取得動作の回数としてカウントする。よって、センサ部162は、認証対象ユーザから i_k 番目の生体情報を取得したとする。今の時点では、当該ステップS304の初回実行に該当しており、上述のステップS303で示したように、 $k=1$ すなわち1番目の生体情報を取得したことになる。例えば、ユーザによる入力順序が、右手人差し指→右手中指→左手人差し指→左手中指→右手薬指→左手薬指としたならば、まずは入力順序1番目すなわち i_1 の生体情報として右手人差し指の生体情報を取得することとなる。

30

【0067】

次に、認証端末150の特徴抽出部163は、上述のステップS304で得た i_k 番目の生体情報から特徴データ X'_i_k を抽出する(S305)。上述の例では、入力順序1番目すなわち i_1 の生体情報である右手人差し指の生体情報から特徴データを抽出することとなる。生体情報からの特徴データの抽出手法自体は既存技術を適宜採用すればよい。

【0068】

また、認証端末150の特徴抽出部163は、上述のステップS305で得た特徴データ X'_i_k を、上述の取得済み特徴データ集合 S に加える(S306)。この時点における取得済み特徴データ集合 S は、 $S=S\cup\{X'_i_k\}$ となっている。

40

【0069】

続いて認証端末150の特徴抽出部163は、上述の取得済み特徴データ集合 S から、合成特徴データ U を作成する(S307)。ここでの合成の方法は、登録処理時のステップS205と同様とする。上述してきた具体例において、現時点までで認証対象ユーザから得た生体情報は、入力順序1番目すなわち i_1 の生体情報である右手人差し指の生体情報のみであるから、取得済み特徴データ集合 S が含む特徴データも特徴データ X'_i_1 のみで、合成特徴データ U もこの特徴データ X'_i_1 にのみ基づくものとなる。

【0070】

次に、認証端末150の認証・暗号・署名部164は、上述のステップS307で得た

50

合成特徴データUに対応する保護テンプレート T_j を、上述の保護テンプレートの組T（ステップS301、S302で得ているもの）の中から選択する（S308）。ここで「Uに対応する保護テンプレート」とは、合成特徴データUと、同じ身体部位の生体情報の組から生成された保護テンプレートのことを指している。従って、上述の場合、今のkの値すなわち $k=1$ に対応する入力順序で得ている「右手人差し指」に関して登録済みの保護テンプレートを選択することとなる。図4で例示するテンプレートデータベース120の場合、例えば、最初のレコード、すなわち入力順序1番であり、1つの部位「A」のみに関する保護テンプレートが該当する。

【0071】

次に認証端末150の認証・暗号・署名部164は、上述の合成特徴データUと、ステップS308で選択した保護テンプレート T_j とを照合する（S309）。ここでの照合処理は、例えば非特許文献1の方法を適用する場合、補助情報から秘密鍵を復元し、その秘密鍵のハッシュ値を照合する処理などに相当する。

【0072】

上述の照合に成功した場合（S310：y）、認証端末150の認証・暗号・署名部164は、予め定めた認証、データの暗号化、復号化、電子署名等の処理を上述の認証対象ユーザに関して実行する（S311）。例えば、ステップS309において秘密鍵を復元した場合は、当該ステップS311における認証・暗号・署名部164は、該当秘密鍵に基づいて所定の認証サーバとの間でチャレンジレスポンス認証を実行してもよいし、何らかの電子データに対して秘密鍵を用いて暗号化や署名処理を施してもよいし、暗号化されたデータを秘密鍵で復号化するなどしてもよい。

【0073】

他方、上述の照合に失敗した場合（S310：n）、認証端末150の認証・暗号・署名部164は、所定の上限入力回数nに対して $k < n$ であるか判定する（S312）。この判定の結果、 $k < n$ であれば（S312：n）、更に追加的な生体情報読み取りと以降の判定を同様に実行出来ると認識し、kを逡増すすなわち $k = k + 1$ として（S313）、上述のステップS304に処理を戻す。ただし $n \leq N$ 、つまり、上限入力回数nは、登録用生体情報の総数Nを越えない。なお $n < N$ の場合、上述の登録処理時のステップS204～S205の処理は、 $k = 1, 2, \dots, n$ のみで繰り返せばよい。

【0074】

上述のように、更に追加的な生体情報読み取りと以降の判定を同様に実行出来ると認識し、ステップS304に処理を戻した場合、当該ステップS304における認証端末150のセンサ部162は、変数 $k = 2$ 、 $S = \{\text{特徴データ } X' _i _1\}$ の状態において、センサ1551に認証対象ユーザが次にかざした部位、すなわち入力順序2番目 i_2 の生体情報として、例えば「右手中指」について生体情報を取得する。

【0075】

また続くステップS305における特徴抽出部163は、上述のステップS304で得た i_2 番目の生体情報たる、右手中指の生体情報から特徴データ $X' _i _2$ を抽出する。

【0076】

また同様に、ステップS306における特徴抽出部163は、上述のステップS305で得た特徴データ $X' _i _2$ を、上述の取得済み特徴データ集合Sに加える。この時点における取得済み特徴データ集合Sは、 $S = S \cup \{X' _i _1, X' _i _2\}$ となっている。

【0077】

続いてステップS307における特徴抽出部163は、上述の取得済み特徴データ集合Sから、合成特徴データUを作成する。ここまでの時点で上述の認証対象ユーザから得ている生体情報は、入力順序1番目および2番目、すなわち i_1 、 i_2 、の生体情報である右手人差し指、右手中指の各生体情報であるから、これらから合成特徴データUを作成することとなる。

10

20

30

40

50

【0078】

次にステップS308における認証・暗号・署名部164は、上述のステップS307で得た合成特徴データUに対応する保護テンプレートT_jを、上述の保護テンプレートの組T（ステップS301、S302で得ているもの）の中から選択する。上述の場合、今のkの値すなわちk=2に対応する入力順序で得ている「右手人差し指」、「右手中指」の組に関して登録済みの保護テンプレートを選択することとなる。図4で例示するテンプレートデータベース120の場合、例えば、2番目のレコード、すなわち入力順序2番であり、2つの部位「A」、「B」に関する保護テンプレートが該当する。

【0079】

続いてステップS309における認証・暗号・署名部164は、上述の合成特徴データUと、ステップS308で選択した保護テンプレートT_jとを照合し、以降、この照合結果に応じて、上述のステップS310～S311、或いはステップS310～S313を同様に実行する。

【0080】

ここで上述のステップS312に関する説明に戻る。照合に失敗し（S310：n）、かつk=nの場合（S312：y）、認証・暗号・署名部164は、認証失敗のメッセージを出力装置156に表示させるなどの所定処理を実行し（S314）、以降のフローを終了する。

【0081】

以上のように、本実施例ではユーザに逐次的に生体情報を入力させながら、逐次バイOMETリック暗号システム10の認証端末150は、これまでに入力された生体情報を組み合わせ、合成特徴データを作成した上で、これに対応する保護テンプレートと照合を行う。逐次処理が進むごとに生体情報が増えるため、合成特徴データの情報は増え、より確実に本人を認証することができるようになる、つまり本人が受理される確率が高まっていく。このようにして、照合スコアが計算できないバイOMETリック暗号においても、照合スコアを用いる逐次判定手法と同等の精度向上効果を達成することができる。更に本実施形態では、他人が誤って受理される確率は各逐次判定処理において常にFAR以下に制御されているため、総当たり攻撃による生体情報の復元や推定、なりすましを防止することもできる。

【0082】

なお、上述した図6のフローすなわち照合処理において、ユーザIDの取得（S300）のステップを実行しない形態を採用してもよい。この場合、認証端末150においてID入力部160は不要となる。ユーザIDの取得を行わない場合は、該当ユーザの存在認識の処理を行う状況に対応しており、ステップS301において、可能性のある全てのユーザIDに対する保護テンプレートの組Tを取得することになる。

【0083】

またステップS308において、認証・暗号・署名部164は、上述の可能性のある全てのユーザIDに対する保護テンプレートの組Tのそれぞれに対し、その中から、合成特徴データUに対応する保護テンプレートT_jを選択し、ステップS309において合成特徴データUと保護テンプレートT_jとを照合する。

【0084】

またステップS310で、可能性のある全てのユーザIDに対する保護テンプレートの組Tのいずれかと、合成特徴データUとの間で照合成功したならば、ステップS311において該当ユーザIDを出力装置156に出力したり、ステップS309において秘密鍵を復元した場合は、該当ユーザIDと秘密鍵とに基づいて所定の認証サーバとの間でチャレンジレスポンス認証を実行してもよいし、何らかの電子データに対して秘密鍵を用いて暗号化や署名処理を施してもよいし、暗号化されたデータを秘密鍵で復号化してもよい。

【0085】

以上、本発明を実施するための最良の形態などについて具体的に説明したが、本発明はこれに限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能である。

10

20

30

40

50

【0086】

こうした本実施形態によれば、生体情報を秘匿しつつ認証や暗号、署名などの処理を行うバイOMETリック暗号において、複数の生体情報を組み合わせることで高い認証精度を達成しつつ、認証、暗号、署名などの処理の際に、ユーザが入力する必要のある生体情報の数を最低限に抑え、利便性を高めることができる。ひいては、バイOMETリック暗号において、高い精度向上効果を持つ逐次マルチモーダル判定を実現し、暗号処理に関する安全性、精度、利便性を共に良好なものと出来る。

【0087】

本明細書の記載により、少なくとも次のことが明らかにされる。すなわち、本実施形態の逐次バイOMETリック暗号システムにおいて、前記演算装置は、前記照合処理における前記ユーザに関する所定処理として、ユーザ認証成功、所定データの暗号化、所定データの復号化、および、電子署名生成、の少なくともいずれかを実行するものである、としてもよい。

10

【0088】

これによれば、バイOMETリック暗号処理に伴うユーザ認証、データの暗号化、復号化、電子署名の各処理を、良好な安全性、精度、および利便性の下で実行できることになる。

【0089】

また、本実施形態の逐次バイOMETリック暗号システムにおいて、前記演算装置は、前記照合処理に際し、当該照合処理の開始から、前記所定ユーザについてセンサを介し、互いに異なる生体情報を逐次的に取得し、照合処理開始時点から現時点までに得ている全ての生体情報から特徴データを抽出して組合せ、当該特徴データの組合せに対し、所定属性が同じ生体情報に由来する前記保護テンプレートを照合し、当該照合に成功した場合に前記ユーザに関する所定処理を実行するものである、としてもよい。

20

【0090】

これによれば、照合処理開始時にユーザがセンサに読み取らせた部位、例えば人差し指に関して上述の照合に失敗した場合でも、続いて読み取らせた中指と既に読み取っている人差し指の各生体情報から特徴データを抽出して組合せ、これに対して、該当ユーザの人差し指と中指に関して保持する保護テンプレートを照合するといった処理が行われることとなり、逐次的な生体情報取得の処理が進むごとに生体情報が増えることで特徴データの

30

【0091】

また、本実施形態の逐次バイOMETリック暗号システムにおいて、前記演算装置は、前記照合処理に際し、前記照合に失敗した場合、前記照合処理開始時点からの生体情報の取得数が規定数に達しているか判定し、前記判定の結果、前記取得数が前記規定数に達していないならば、前記互いに異なる生体情報の逐次的な取得の処理と、前記特徴データの組合せに対する前記保護テンプレートの照合以降の処理を繰り返し実行し、前記判定の結果、前記取得数が前記規定数に達しているならば、前記照合処理に失敗したと判断し以降の処理を終了するものである、としてもよい。

40

【0092】

これによれば、上述した逐次的な生体情報取得の処理が進むに従って、真正な本人の認証に成功する確率が高まっていく効果と共に、例えば、単にセンサに対するユーザの体勢等に応じた照合失敗の事態から（上述の規定数到達までの）早期に脱し、あらためて照合処理を再実行させて全体の処理効率を高めることが可能となる。

【0093】

また、本実施形態の逐次バイOMETリック暗号システムにおいて、前記演算装置は、前記登録処理に際し、所定の他人受入率を達成する保護テンプレートを作成するものである、としてもよい。

50

【0094】

これによれば、上述のごとき本人拒否率（FRR）低下と併せて、他人受入率（FAR）を所定基準以下として、他人によるなりすましの発生を回避する効果が更に高まる。

【0095】

また、本実施形態の逐次バイオメトリック暗号システムにおいて、前記演算装置は、前記登録処理に際し、前記抽出した複数個の特徴データから、予めユーザ毎に決められた生体情報の入力順序に従って、組合せ個数を通増させて複数の特徴データの組を順次選択し、当該選択した各特徴データの組ごとに保護テンプレートを作成するものである、としてもよい。

【0096】

これによれば、ユーザがセンサに各部位を読み取らせた順番、例えば人差し指、中指、薬指、小指、といった順番に従って、組合せ個数を1からインクリメントさせた複数の特徴データの組を、例えば、人差し指のみの組み、人差し指と中指の組み、人差し指と中指と薬指の組み、人差し指と中指と薬指と小指の組み、などと順次選択し、当該選択した各特徴データの組ごとに保護テンプレートを作成することになる。この場合、予め定められた順番での生体情報読み取りと、これに応じた保護テンプレートとの照合が効率的に実行されることとなり、全体の処理効率も更に向上する。

【0097】

また、本実施形態の逐次バイオメトリック暗号システムにおいて、前記演算装置は、前記登録処理に際し、前記抽出した複数個の特徴データから前記組合せ個数の特徴データの組を選択するにあたり、該当組合せ個数内で取り得る全ての特徴データの組合せを選択し、当該選択した各特徴データの組ごとに保護テンプレートを作成するものである、としてもよい。

【0098】

これによれば、ユーザがセンサに各部位を読み取らせる順番に規定が無い状況にも対応した、保護テンプレートを作成することになる。この場合、ユーザの随意の順番での生体情報読み取りと、これに応じた保護テンプレートとの照合が確実に実行可能となる。

【0099】

また、本実施形態の逐次バイオメトリック暗号システムが、前記登録処理を実行する登録端末と、前記照合処理を実行する認証端末から構成されるとしてもよい。

【0100】

これによれば、例えば金融機関における窓口端末など、ユーザの生体情報登録を行う端末と、金融機関におけるATM端末など、ユーザの生体情報に基づく認証を行う端末とが別の装置構成となっている状況に対応して、逐次バイオメトリック暗号の処理を行うことが可能となる。

【0101】

また、本実施形態の逐次バイオメトリック暗号処理方法において、前記情報処理装置が、前記照合処理における前記ユーザに関する所定処理として、ユーザ認証成功、所定データの暗号化、所定データの復号化、および、電子署名生成、の少なくともいずれかを実行するとしてもよい。

【0102】

また、本実施形態の逐次バイオメトリック暗号処理方法において、前記情報処理装置が、前記照合処理に際し、当該照合処理の開始から、前記所定ユーザについてセンサを介し、互いに異なる生体情報を逐次的に取得し、照合処理開始時点から現時点までに得ている全ての生体情報から特徴データを抽出して組合せ、当該特徴データの組合せに対し、所定属性が同じ生体情報に由来する前記保護テンプレートを照合し、当該照合に成功した場合に前記ユーザに関する所定処理を実行するとしてもよい。

【0103】

また、本実施形態の逐次バイオメトリック暗号処理方法において、前記情報処理装置が、前記照合処理に際し、前記照合に失敗した場合、前記照合処理開始時点からの生体情報

10

20

30

40

50

の取得数が規定数に達しているか判定し、前記判定の結果、前記取得数が前記規定数に達していないならば、前記互いに異なる生体情報の逐次的な取得の処理と、前記特徴データの組合せに対する前記保護テンプレートの照合以降の処理を繰り返し実行し、前記判定の結果、前記取得数が前記規定数に達しているならば、前記照合処理に失敗したと判断し以降の処理を終了する、としてもよい。

【0104】

また、本実施形態の逐次バイOMETリック暗号処理方法において、前記情報処理装置が、前記登録処理に際し、所定の他人受入率を達成する保護テンプレートを作成するとしてもよい。

【0105】

10

また、本実施形態の逐次バイOMETリック暗号処理方法において、前記情報処理装置が、前記登録処理に際し、前記抽出した複数個の特徴データから、予めユーザ毎に決められた生体情報の入力順序に従って、組合せ個数を増進させて複数の特徴データの組を順次選択し、当該選択した各特徴データの組ごとに保護テンプレートを作成するとしてもよい。

【0106】

また、本実施形態の逐次バイOMETリック暗号処理方法において、前記情報処理装置が、前記登録処理に際し、前記抽出した複数個の特徴データから前記組合せ個数の特徴データの組を選択するにあたり、該当組合せ個数内で取り得る全ての特徴データの組合せを選択し、当該選択した各特徴データの組ごとに保護テンプレートを作成するとしてもよい。

20

【符号の説明】

【0107】

10 逐次バイOMETリック暗号システム

100 登録端末

101、151 記憶装置

102、152 プログラム

103、153 メモリ

104、154 CPU

105、155 入力装置

106、156 出力装置

30

107、157 通信装置

110 センサ部

111 特徴量抽出部

112 ID入力部

113 保護テンプレート作成部

120 テンプレートDB

140 ネットワーク

150 認証端末

160 ID入力部

161 保護テンプレート取得部

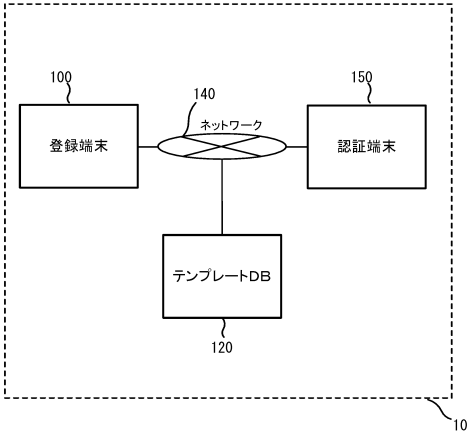
40

162 センサ部

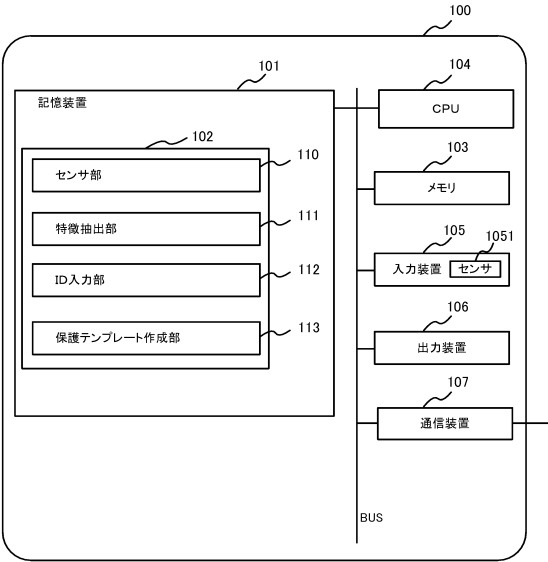
163 特徴抽出部

164 認証・暗号・署名部

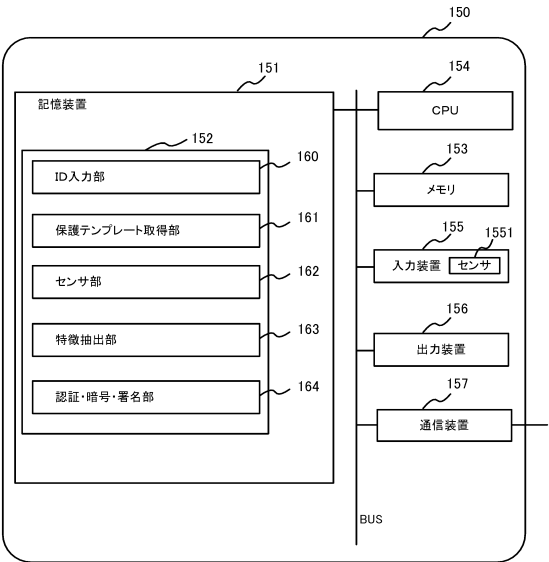
【図 1】



【図 2】



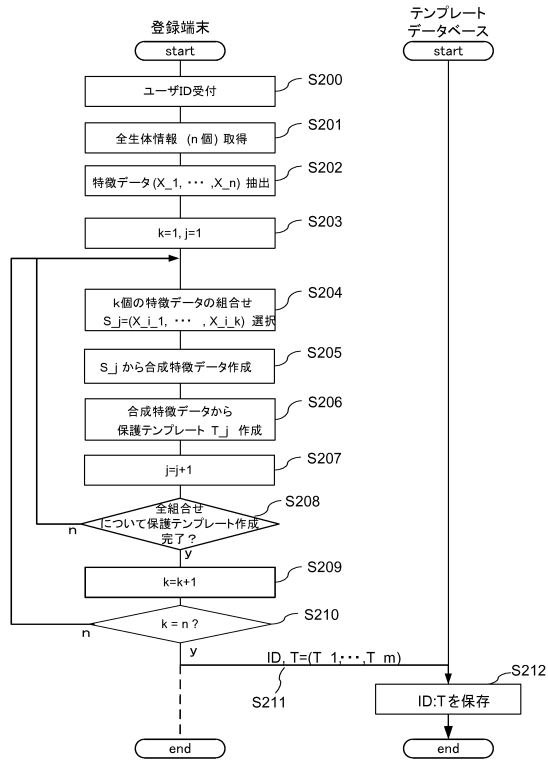
【図 3】



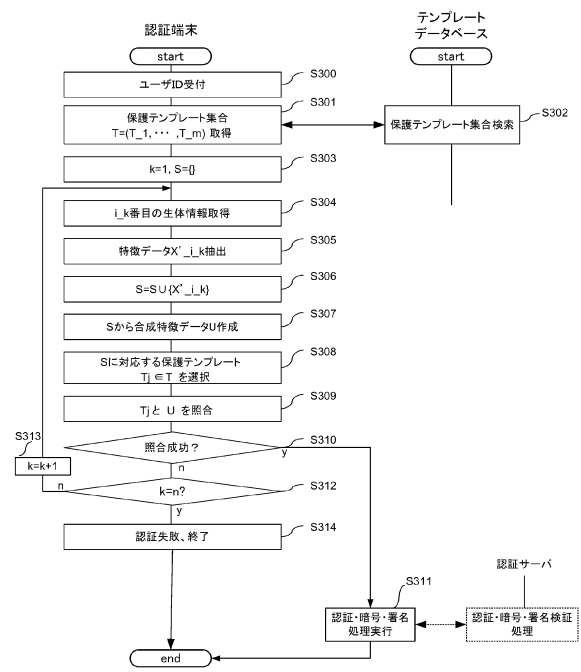
【図 4】

ユーザID:00001 ザID:00002 ...	
部位	保護テンプレート
A	*****
A, B	*****
A, B, C	*****
A, B, C, D	*****
...	...

【図 5】



【図 6】



フロントページの続き

- (56)参考文献 特開2003-030154 (JP, A)
特開2003-186836 (JP, A)
特表2001-525960 (JP, A)
特表2002-538504 (JP, A)
米国特許出願公開第2002/0120592 (US, A1)
米国特許出願公開第2003/0219121 (US, A1)
Geetika, M. K., Multimodal Based Fuzzy Vault Using Iris Retinaand Fingervein, 2013 Fourth International Conference on Computing, Communications and Networking Technologies, 2013年 7月, p.1-5

- (58)調査した分野(Int.Cl., DB名)

H04L 9/32

G06F 21/32

JSTPlus/JMEDPlus/JST7580 (JDreamIII)

IEEE Explore