(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4221385号
(P4221385)

(45)発行日　平成21年2月12日(2009.2.12)　(24)登録日　平成20年11月21日(2008.11.21)

(51)Int.Cl.		F I		
G06F 21/20	(2006.01)	G06F	15/00	330F
G06K 17/00	(2006.01)	G06K	17/00	V
H04L 9/32	(2006.01)	H04L	9/00	673D
A61B 5/117	(2006.01)	H04L	9/00	673C
		H04L	9/00	673E

請求項の数 4　(全 14 頁)　最終頁に続く

(21)出願番号　特願2005-43371(P2005-43371)
(22)出願日　平成17年2月21日(2005.2.21)
(65)公開番号　特開2006-228080(P2006-228080A)
(43)公開日　平成18年8月31日(2006.8.31)
審査請求日　平成18年7月19日(2006.7.19)

早期審査対象出願

前置審査

(73)特許権者　504373093
日立オムロンターミナルソリューションズ株式会社
東京都品川区大崎一丁目６番３号
(74)代理人　100100310
弁理士　井上　学
(72)発明者　緒方　日佐男
東京都品川区大崎一丁目６番３号　日立オムロンターミナルソリューションズ株式会社内
(72)発明者　今泉　敦博
東京都品川区大崎一丁目６番３号　日立オムロンターミナルソリューションズ株式会社内

最終頁に続く

(54)【発明の名称】生体認証装置、端末装置及び自動取引装置

(57)【特許請求の範囲】

【請求項１】

個人の認証に用いられる端末装置において、

暗号鍵を記憶する記憶手段とＩＣカードに情報を書き込む書込手段と静脈情報を取得する取得手段とが一体となった生体認証装置を有し、

前記生体認証装置は、

前記取得手段によって取得した静脈情報と指の傾きに関する情報を含む特性データとを第１の記憶部へ記憶する第１の処理と、前記記憶手段から前記暗号鍵を読み出し前記第１の記憶部の静脈情報を暗号化して第２の記憶部へ記憶する第２の処理と、前記第１の記憶部の静脈情報を削除する第３の処理と、からなる一連の処理を所定の回数繰り返すことによって所定の個数の暗号化された静脈情報を第２の記憶部へ記憶させ、さらに、

前記特性データを用いて、前記所定の個数の暗号化された静脈情報の中から登録に適した情報を選択して前記書込手段によって該静脈情報をＩＣカードに登録することを特徴とする端末装置。

【請求項２】

請求項１記載の端末装置において、

前記生体認証装置は、静脈情報を認証する認証プログラムを暗号化して記憶する記憶部と、前記記憶手段から前記暗号鍵を読み出し、当該暗号鍵によって暗号化された前記認証プログラムを復号する復号部とを有することを特徴とする端末装置。

【請求項３】

請求項２記載の端末装置において、
前記復号部によって復号された前記認証プログラムによって、前記取得手段による静脈情報の抽出を制御することを特徴とする端末装置。
【請求項４】
請求項１記載の端末装置において、
前記生体認証装置は、前記取得手段を制御する暗号化された暗号化認証プログラムを記憶する不揮発性記憶部と、前記暗号化認証プログラムを暗号鍵によって復号化した認証プログラムを記憶する揮発性記憶部とを有し、
前記揮発性記憶部の前記認証プログラムによって前記取得手段によって静脈情報を取得することを特徴とする端末装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は生体情報、例えば、指紋や静脈パターン等を用いた本人確認のための生体認証装置、および、その生体認証に方法関わる。特に、認証装置で取得した生体情報が装置外に出て第三者に悪用されることを防止するために、生体情報の取得処理、並びに、認証処理を認証装置内部で実行する装置、方法に関するものである。
【背景技術】
【０００２】
金融機関における預金の引き出しやインターネットを用いた電子商取引においては、他人の成りすましを防ぐために本人確認のための生体認証が極めて重要である。一般的な認証方法として、磁気ストライプを有するカードと暗証番号入力による認証や、カード裏面の署名と商品購入時の署名を照合することによる認証が広く行われている。
【０００３】
しかし、このような従来の個人認証方法にはセキュリティに関する問題点が指摘されている。磁気ストライプを有するキャッシュカードと暗証番号入力の組合せの場合、磁気情報と暗証番号とが第三者に盗難されると容易に預金を引き出すことが可能になる。あるいは、署名の場合は第三者が署名を真似ることで登用されることもありうる。
【０００４】
そこの対策として、磁気ストライプを有するカードに代えてＩＣカードの導入が提案されている。ＩＣカードは、磁気ストライプカードと比較しカードの複製が困難になると共に、内部情報が容易に盗難されないという安全性も確保できるようになる。加えて、カード内部に格納できる情報量を飛躍的に増大できることに着目し、指紋や静脈パターン等の生体情報をＩＣカードに保持し、その照合による生体認証技術として、特許文献１，２がある。
【０００５】
【特許文献１】特開昭６１－１９９１６２号公報
【特許文献２】特開平１０－３１２４５９公報
【発明の開示】
【発明が解決しようとする課題】
【０００６】
上述の背景技術によると、例えば、認証する装置から生体情報が外部に出ると、悪意を持った第三者により盗難され悪用される可能性がある。生体情報による個人認証は、暗証番号や署名による認証に比べて安全性が高くなる一方、一度流出してしまうと容易には変更できないという負の側面もある。そのため、生体情報が第三者に容易に利用可能な形で外部に流出しないような仕掛けが特に重要となる。
【０００７】
加えて、生体情報となる生体特徴量の抽出、照合する生体認証プログラムに対するセキュリティ確保も不可欠である。プログラム内部を第三者による解析、改変を防止しなければ、生体認証装置としての効果が失われてしまう恐れがある。その意味で、生体認証装置

が接続されている制御装置、例えば、パソコン上に生体認証プログラムが解析可能な状態で存在すると、第三者に処理手順を解析、盗難される可能性が高まる。仮にパソコンではなく生体認証装置内に生体認証プログラムが存在したとしても、外部から容易に解析可能な状態で存在していれば、やはり悪意を持った第三者にその情報を盗難される可能性がある。

【０００８】

また、生体認証装置から出力される生体認証結果が第三者に漏れることも防止する必要がある。生体認証装置が認証受入れした信号を第三者が偽造すると、装置による認証拒絶の場合でも認証装置が接続された制御装置に認証受入れの信号が伝わり、不正な取引が行われる可能性がある。

【０００９】

本発明は上記課題の少なくとも一部を解決するためになされたものである。本発明の第一の目的は個人の生体情報が生体認証装置から第三者が容易に利用可能な形で外部に流出するのを防止することである。本発明の第二の目的は、生体特徴量を抽出したり照合したりする生体認証プログラムを第三者が盗難、改変することを防止することである。本発明の第三の目的は、生体認証装置が出力する生体認証結果の外部の漏れを防止することにある。

【課題を解決するための手段】

【００１０】

本発明は、個人の生体情報を用いて本人確認を行うための生体認証装置であって、生体情報を取り込むセンサと、取り込まれたセンサ情報から認証を行うための生体特徴量を抽出する特徴量抽出手段と、抽出された生体特徴量を暗号化するための暗号化手段と、暗号化された生体特徴量を本人確認のための認証用基準データとして生体認証装置外部に出力する手段と、を具備することを特徴とする生体認証装置である。

【００１１】

また、他の好ましい例では、個人の生体情報を用いて本人確認を行うための生体認証装置であって、生体情報を取り込むセンサと、取り込まれたセンサ情報から認証を行うための生体特徴量を抽出する特徴量抽出手段と、抽出された生体特徴量を暗号化するための暗号化手段と、本人確認のための認証用基準データとして暗号化された生体特徴量を、生体認証装置に接続された制御コンピュータを介さずに直接ＩＣカードに出力する手段と、を具備することを特徴とする生体認証装置である。

【００１２】

また、他の好ましい例では、個人の生体情報を用いて本人確認を行うための生体認証装置であって、生体情報を取り込むセンサと、取り込まれたセンサ情報から認証を行うための生体特徴量を抽出する特徴量抽出手段と、認証用基準データとなる生体特徴量を暗号化された形で生体認証装置外部から入力する手段と、前記認証用基準データとなる暗号化された生体特徴量を復号する復号手段と、前記特徴量抽出手段から出力された生体特徴量と、前記復号された認証用基準データとなる生体特徴量を照合する生体特徴量照合手段と、前記生体特徴量照合手段の出力を暗号化する暗号化手段と、前記暗号化された生体特徴量照合手段の出力を装置外部に出力する手段と、を具備することを特徴とする生体認証装置である。

【００１３】

また、他の好ましい例では、個人の生体情報を用いて本人確認を行うための生体認証装置であって、生体情報を取り込むセンサと、取り込まれたセンサ情報から認証を行うための生体特徴量を抽出する特徴量抽出手段と、ＩＣカードに格納された認証用基準データとなる暗号化された生体特徴量を、生体認証装置に接続された制御コンピュータを介さずに、直接ＩＣカードから入力する手段と、前記認証用基準データとなる暗号化された生体特徴量を復号する復号手段と、前記特徴量抽出手段から出力された生体特徴量と、前記復号された認証用基準データとなる生体特徴量を照合する生体特徴量照合手段と、前記生体特徴量照合手段の出力を暗号化する暗号化手段と、前記暗号化された生体特徴量照合手段の

出力を装置外部に出力する手段と、を具備することを特徴とする生体認証装置である。
また、他の好ましい例では、前記特徴量抽出手段と前記生体特徴量照合手段は、生体認証装置を起動する前は暗号化された形で装置内に格納され、装置が起動された後に復号されることを特徴とする生体認証装置である。
【００１４】
また、他の好ましい例では、前記特徴量抽出手段と前記生体特徴量照合手段は、生体認証装置が起動する前は、生体認証装置に接続された制御コンピュータと生体認証装置それぞれに分割して格納され、生体認証装置が起動された後に結合復号されて動作可能な状態になることを特徴とする生体認証装置である。
【発明の効果】
【００１５】
本発明によれば、悪意を持った第三者が生体情報又は生体特徴量を盗み出すことを防止できる。また、生体認証に関わる生体特徴量抽出処理、生体特徴量の照合処理を行うプログラムの解析、改ざん、取得等を防止できる。また、仮に装置を分解し、解析しても改ざんを防止できる。
【発明を実施するための最良の形態】
【００１６】
以下、図１～８を参照して本発明の実施形態について説明する。
【００１７】
本実施形態では、ＩＣカードを介した金融営業店における営業店窓口端末での生体情報登録処理とＡＴＭ（現金自動預払機）での生体情報認証処理について説明する。ここで生体情報とは、個人を特定するために有効な生体特徴量であると想定する。
【００１８】
営業店窓口端末における生体特徴量の登録処理では、窓口端末でＩＣカードに個人認証用の暗号化された生体特徴量を登録する。窓口端末にはＩＣカード装置付き生体認証装置が接続されており、登録用の生体特徴量が暗号化されて、窓口端末を経由せずに生体認証装置からＩＣカードに直接転送される。一方、ＡＴＭ（現金自動預払機）では、ＩＣカードから暗号化された生体特徴量が読み出されて、ＡＴＭに接続された生体認証装置に転送され装置内部で認証処理を行う。なお、ＩＣカードに限らずＲＦＩＤタグなど、携帯可能な電子的媒体であれば、任意の媒体で良い。
【００１９】
図１は全体システムの構成例である。１０１は金融営業店であり、勘定系ホストコンピュータ１０９が設置してあるデータセンタ１０３とは、広域ネットワーク１０２を介して接続されている。金融営業店１０１では、営業店窓口端末１０５やＡＴＭ１０７が営業店内のＬＡＮ１０８で接続されている。営業店窓口端末１０５にはＩＣカード装置付き生体認証装置１０４を接続する。同様にＡＴＭ１０７には生体認証装置１０６を接続し、ＩＣカード装置はＡＴＭ内部に組み込んでいる。
【００２０】
まず、図２、図３、図４を用いて営業店窓口端末１０５における生体特徴量の登録処理について説明する。図２はＩＣカード装置付生体認証装置１０４の構成例を示す図である。ＣＰＵ２０１は装置のデータ処理を担うプロセッサであり、後述する各種のプログラム、データの制御、処理を司る。周辺装置I/0デバイス２０２は、生体認証装置１０４と営業店窓口端末１０５を接続するためのインタフェースである。２０３は生体画像を取得するための照明ＬＥＤであり、例えば、指静脈認証であれば指の静脈パターンの取得に好適な近赤外光ＬＥＤを用いる。画像センサ２０４は生体画像を取得するためのセンサであり、ＣＣＤなどのデバイスが挙げられ、ＬＥＤ２０３によって照射された指の静脈パターンを取得する。ＩＣカード装置２０５は暗号化された登録用生体特徴量をＩＣカードに書き込むための装置である。
【００２１】
主記憶装置２０７は揮発性メモリ（ＤＲＡＭ等）で構成されており、認証装置の電源が

切断されると格納されているデータが消滅する。ここには装置を動作させるための各種プログラムやデータ領域が確保されている。主記憶装置２０７に記憶されるプログラム、データは後述のフラッシュメモリ２１７から読み出して記憶する記憶部、記憶手段である。装置全体制御プログラム２０８はＩＣカード装置２０５の制御も含めて認証装置１０４全体を制御するプログラムである。周辺装置I/0制御プログラム２０９は周辺装置I/0デバイス２０２を制御する。

暗号/復号プログラム２１０は２つの処理を行う。

一つはフラッシュメモリ（以下、不揮発性メモリと言う）２１７に格納された暗号化認証プログラム２１９を復号し、２１１の領域に認証プログラムとして格納することである。

もう一つは、認証プログラム２１１が生成した登録用の生体特徴量をＩＣカードに書き込む前に暗号化することである。ＩＣカード装置制御プログラム２１２はＩＣカード装置２０５を制御するプログラムである。

【００２２】

このように、プログラムは各種の機能を有し、また種々の処理を行い、上述の通り、ＣＰＵ２０１のハード構成によって制御される。本発明においてはプログラムを中心として説明するが、これら各プログラムの様々な機能、例えば、制御手段、暗号化手段、認証手段、登録手段、照合手段などとも言え、各手段を各部とも表現できることは言うまでもない。

【００２３】

画像バッファ２１３は画像センサ２０４で取得した生体画像データ（生データ）を格納するための領域である。生体特徴量２１４は、画像バッファ２１３に格納された生体画像データから認証プログラム２１１によって例えば、静脈パターンのみを抽出して生成された生体特徴量を格納するための領域である。暗号化生体特徴量２１５は、生体特徴量２１４のデータを暗号/復号プログラム２１０によって暗号化されたデータを格納する領域である。２１５のデータ（暗号化状態の生体特徴量）はＩＣカード装置２０５を介してＩＣカードに生体登録特徴量として格納される。なお、ＩＣカード装置２０５と認証装置との間に営業店窓口端末１０５を接続、介在させる場合でも、認証装置で取得した暗号化状態の生体特徴量を窓口端末１０５に記憶せずに（残さずに）、ＩＣカード装置２０５によってＩＣカード内に登録する。暗号鍵２１６は暗号/復号プログラム２１０がデータを暗号化したり、復号したりする際に必要な鍵データである。本鍵データは生体認証装置が接続されている営業店窓口端末１０５やＡＴＭ１０７から周辺I/0デバイスを介して取得することも特徴の一つである。２０６は認証装置内のプロセッサや各デバイスを接続するバスである。２１７は認証装置の電源を落としても内容が消去されない不揮発性メモリであり、その内部に暗号化された認証プログラム２１８が格納されている。認証装置が起動されると、暗号/復号プログラム２１０が暗号鍵２１６を用いて暗号化認証プログラム２１８を復号し、２１１の領域に格納する。

【００２４】

図３は営業店窓口端末１０５の構成例を示す図である。窓口端末１０５は金融機関のカウンタに設置され、オペレータが入金、出金、為替等の処理業務を行うコンピュータであり、加えて生体認証の登録処理も行う端末装置である。

ＣＰＵ３０１は端末のデータ処理、各種の制御を担うプロセッサである。ＬＡＮデバイス３０２は営業店内のＬＡＮ１０８と端末を接続するためのデバイスであり、ＬＡＮ１０８を介して勘定系ホストコンピュータ１０９に接続されている。周辺装置I/0デバイス３０３は、ＩＣカード装置付生体認証装置１０４とを接続するためのインタフェースである。表示装置３０４は生体特徴量の登録結果（成功か、失敗かのステータスであって、生体特徴量は含まず）や、顧客の取引情報、取引に必要な項目などを、窓口端末を操作するオペレータに表示するモニタであり、キー入力装置３０５はオペレータのキー入力装置である。現金処理装置３０６は端末における現金処理を行うための装置である。主記憶装置３０８には、各種プログラムやデータが格納されている。３０９は窓口端末全体を制御する

全体制御プログラムであり、３１０には窓口で行う業務に関する業務アプリケーションプログラムが格納されている。周辺装置I/0制御プログラム３１１は周辺装置I/0デバイス３０３を制御する。生体認証装置制御プログラム３１２は、周辺装置I/0デバイス３０３を介して接続されているＩＣカード装置付生体認証装置１０４を制御するプログラムである。暗号鍵３１３はＩＣカード装置付生体認証装置１０４を起動したり、ＩＣカードに登録する生体特徴量を暗号化するために使用される。３０７は端末内の各装置をつなぐバスである。

【００２５】

図４を用いてＩＣカード装置付生体認証装置１０４、ならびに、営業店窓口端末１０５の動作を説明する。ステップ４０１、４０６、４０７、４０８は、営業店窓口端末１０５が出力する指示に基づきＩＣカード装置付生体認証装置１０４が処理する内容である。

【００２６】

窓口端末１０５の表示装置３０４に表示する生体認証登録の項目を入力装置３０５で選択すると、全体制御プログラム３０９が生体認証に関する機能を生体認証装置１０４に展開する。ステップ４０１では、営業店窓口端末１０５に格納された生体認証装置制御プログラム３１２が生体特徴量登録処理の起動信号、ならびに、暗号鍵３１３をＩＣカード装置付生体認証装置１０４に送信する。生体認証装置１０４では、受信した起動信号によりＣＰＵ２０１を中心として起動し、受信した暗号鍵３１３を装置全体制御プログラム２０８が２１６の領域に格納する。その後、装置全体制御プログラム２０８は暗号/復号プログラム２１０を起動し、暗号鍵２１６を用いて不揮発性メモリ２１７内の暗号化認証プログラム２１８を復号し、２１１に格納してプログラムを起動する。そのため次のような耐タンパ性を有している。

【００２７】

上述の通り、不揮発性メモリ２１７内に暗号化された状態で認証プログラム２１８を格納し、起動時に主記憶装置２０７内の２１１に展開している。生体認証装置に電源が入って正常に動作している場合は、装置外部との通信は暗号鍵２１６を用いて暗号化されているので、正規に接続された端末でなければ生体認証装置の内部を参照することはできない。そのため、認証プログラム２１１が主記憶装置２０７に解析可能な状態で格納されていても、外部からの不正アクセスから保護されている。一方、生体認証装置に電源が入っていない状態では、不揮発性メモリ２１７にのみ暗号化された認証プログラム２１８が格納されている。このように、プログラムを暗号化することで第三者が装置を分解して不揮発性メモリ２１７を解析、その偽造、改ざんが困難になるとの効果がある。

【００２８】

上述の例では不揮発性メモリ２１７に暗号化認証プログラムを、揮発性メモリ２０７に復号して展開した認証プログラムを格納、記憶する方式１について説明した。

この他、暗号化認証プログラムを揮発性メモリ２１７に記憶する方式２と、不揮発性メモリ２１７内にて暗号化認証プログラム２１８を展開して認証プログラムを記憶する方式３とが考えられる。ただし、方式２では認証装置の電源断にて暗号化認証プログラムが消去されてしまうことから現実的ではない。また方式３では認証装置が不揮発メモリ２１７内の復号された認証プログラムを消去する前に認証装置の電源を切断されると、そのまま不揮発メモリ２１７内に復号されてしまった認証プログラムが残存してしまう。それゆえ、セキュリティの面で適切ではない。

【００２９】

以上から方式１は他の方式２，３に比較して現実的でもあり、安全性の高いものである。なお、本実施例では、認証装置が起動した時に不揮発メモリ２１７の暗号化認証プログラムが主記憶装置２０７に復号され、以降認証装置が電源を切断されるまで主記憶装置２０７に復号された認証プログラムが存在し続ける。更に望ましい例としては、生体特徴量を抽出／認証する度に、暗号化されたプログラムを復号して主記憶装置に展開し、処理が終わると主記憶装置上の認証プログラムを消去する例がある。この場合、装置内で認証プログラムが解析可能（実行可能）な状態で存在する時間がより短くなるので、安全性をさ

らに高められることが期待できる。

【００３０】

続いて、主記憶装置２０７に正しく認証プログラム２１１が復号されて起動すれば、営業店窓口端末１０５、ならびに、ＩＣカード装置付生体認証装置１０４は暗号鍵を通じて相互に機器認証を確立する。第三者が生体認証装置を盗難して不正な制御コンピュータに接続したとしても、認証プログラムが起動しないので認証装置を動作させることが不可能である。また、認証プログラムは上述の通り、不揮発性メモリ２１７にて暗号化されるので、第三者が認証装置を分解して解析したとしても認証プログラムの内容を知ることは極めて困難である。このように起動について説明したが、窓口端末１０５のシャットダウン、電源断等に基づく認証装置１０４の終了においては、２１１に格納した復号化された認証プログラムをクリア（又は不活性化）することでプログラムの解析を困難なものとすることができる。

【００３１】

認証プログラム２１１は、照明ＬＥＤ２０３、ならびに、画像センサ２０４を制御して生体画像の特徴量を取得して画像バッファ２１３に格納する（４０２）。その後、認証プログラム２１１は画像バッファ２１３に格納された生体画像を読み出し、画像からＩＣカードに登録するための生体特徴量、ならびに、登録特徴量を選択するための特性データを抽出して結果を生体特徴量２１４に格納する（４０３）。なお、登録特徴量の選択とは後述のステップ４０６にて繰り返し登録されるデータから選択することを言う。ここで、特性データとは例えば指静脈認証の場合、指の傾きなど登録に適した生体特徴量を選択するための基準となるデータである。なお、生体特徴量は単に生体情報とも言い、生体認証装置は生体情報を取得する取得手段、取得部を有している。

【００３２】

装置全体制御プログラム２０８は暗号/復号プログラム２１０を再度起動する。つまり、上述では認証プログラムの起動、復号化（活性化）の機能を有しているが、次の説明では取得した生体特徴量の暗号化の機能に用いるために再起動する。プログラム２１０の再起動によって、暗号鍵２１６により生体特徴量２１４を暗号化して、結果を暗号化生体特徴量２１５に格納する（４０４）。その後、データが流出するのを防ぐために、画像バッファ２１３、生体特徴量２１４の領域をメモリクリアする（４０５）。

【００３３】

営業店窓口端末１０５は規定回数に達するまでステップ４０２から４０５の処理をＩＣカード装置付生体認証装置１０４に繰り返し実行させ、結果を暗号化生体特徴量２１５に格納する（４０６）。そして、営業店窓口端末１０５からの指示で、認証プログラム２１１はステップ４０３で抽出した特性データ（基準データ）を基に、ＩＣカードに登録すべき暗号化登録特徴量を２１５のデータの中から選択する（４０７）。

【００３４】

装置全体制御プログラム２０８は、窓口端末１０５からの指示の下、ＩＣカード装置制御プログラム２１２を介して、選択された暗号化登録特徴量をＩＣカード装置２０５に書き込む（４０８）。その後、装置内に暗号化登録特徴量が残存するのを防止するため、暗号化生体特徴量２１５の領域をメモリクリアする（４０９）。なお、上述では窓口端末１０５の指示によって各種の処理が行われる例を説明したが、認証装置内部のみでこれらの処理を自動的に行っても良い。また、Ｓ４０９のクリア時にＳ４０５のクリアを同時にする例もあるが、上述の４０６の繰り返し処理前に行うのが良い。つまり、繰り返し実行によってそのデータサイズが大きくなり、結局、画像バッファ２１３のサイズも大きくする必要があるためである。またＳ４０９の暗号化データのクリアに比較して、Ｓ４０５のデータは暗号化されていないデータのため使用後はできるだけ早くクリアした方がセキュリティ向上になるためである。

【００３５】

以上のステップ４０１から４０９の処理により、営業店窓口端末１０５に生体特徴量が出力されることなく、生体認証装置内部で暗号化されてＩＣカードに格納される。

【００３６】
次に、図５、図６、図７、図８を用いてＩＣカード内に格納された生体特徴量を用いてＡＴＭにおける認証処理について説明する。ＡＴＭとは金融機関に設置され、エンドユーザによって入金、出金、振込処理等を自動的に行い、現金自動取引装置とも言う。ＡＴＭの例にて説明するが、利用者の個人認証に用いられる端末、コンピュータに応用可能であり、自動取引装置とも称す。
【００３７】
図５はＡＴＭ１０７の構成例を示す図である。ＣＰＵ５０１はＡＴＭのデータ処理を担い、各種のプログラムの制御やコマンドの発生など種々の処理、制御を行うプロセッサである。ＬＡＮデバイス５０２は営業店内のＬＡＮ１０８と端末を接続するためのデバイスであり、ＬＡＮ１０８を介して勘定系ホストコンピュータ１０９に接続されている。周辺装置I/0デバイス５０３は、生体認証装置１０６とを接続するためのインタフェースである。ＩＣカード装置５０４はＡＴＭのカード挿入口に組み込まれており、ＡＴＭでは本人確認に用いる生体認証装置１０６と分離されている。表示装置５０５は取引情報や生体認証結果を利用者に表示するモニタであり、キー入力装置５０６は利用者が取引メニューや暗証番号をキー入力するための装置である。現金処理装置５０７はＡＴＭにおける現金処理を行うための装置である。主記憶装置５０９には、各種プログラムやデータが格納されている。
【００３８】
５１０はＡＴＭ全体を制御する全体制御プログラムであり、５１１にはＡＴＭ取引で行う業務に関する業務アプリケーションプログラムが格納されている。周辺装置I/0制御プログラム５１２は周辺装置I/0デバイス５０３を制御する。生体認証装置制御プログラム５１３は、周辺装置I/0デバイス５０３を介して接続されている生体認証装置１０６を制御するプログラムである。暗号/復号プログラム５１５は暗号鍵５１６を用いて、生体認証装置１０６から送信される暗号化された認証結果（生体特徴量は含まない）を復号する。５１７は生体認証装置１０６から送信される暗号化された認証結果を格納する領域であり、５１８は暗号鍵５１６を用いてそれを復号した結果を格納する領域である。
【００３９】
ＡＴＭに接続されている認証用の生体認証装置１０６の構成例を図６に示す。６０１から６０４はそれぞれ図２における２０１から２０４と同様の機能を有するため説明を省略する。主記憶装置６０５には装置を動作させるための各種プログラムやデータ領域が確保されている。装置全体制御プログラム６０７は生体認証装置全体を制御するプログラムである。６０８から６１２は、それぞれ図２における２０９から２１１、ならびに、２１３から２１４と同様で説明を省略する。６１３は周辺装置I/0デバイス６０２を介して生体認証装置がＩＣカードに登録された暗号化生体登録特徴量をＡＴＭから受信して格納するための領域である。生体登録特徴量６１４は６１３の暗号化特徴量を暗号/復号プログラム６０９が暗号鍵６１７を用いて復号し格納する領域である。照合結果６１５は生体特徴量６１２と生体登録特徴量６１４を認証プログラム６１０が照合した結果を格納する領域である。暗号化照合結果６１６は、暗号/復号プログラム６０９が暗号鍵６１７を用いて照合結果６１５を暗号化して格納する領域である。暗号鍵６１７は生体認証装置が接続されているＡＴＭ１０７から取得する。６０６はプロセッサや各デバイスを接続するバスである。６１８、６１９はそれぞれ図２の２１７、２１８と同様である。
【００４０】
ここでは、ＡＴＭが電源ＯＮ、又は起動した時に生体認証装置１０６も同時に起動されたと仮定する。具体的には、認証装置１０６は起動時にＡＴＭ１０７から暗号鍵を受信して６１７に格納する。それと同時に、不揮発性メモリ６１８に格納された暗号化認証プログラム６１９を、暗号鍵６１７を用いて復号し主記憶装置６０５の６１０に格納されていることを想定している。更に、ＡＴＭの正常閉局又は異常時のシャットダウン、電源断によって認証装置１０６も終了するが、その終了と共に認証プログラム６１０はクリアされる。これらの認証プログラムの復号化によるＡＴＭの制御部と生体認証装置との確立処理

などや、不揮発メモリ６１８と主記憶装置（揮発メモリ）６０５との構成にした理由については上述の営業店システムの例において説明したので省略する。

【００４１】

図７を用いてＡＴＭ１０７ならびに生体認証装置１０６の動作について説明する。ＡＴＭはＣＰＵ（制御手段、部）５０１の指示で、表示装置５０５に初期画面として預入、支払、振込等の各種項目（メニュー）を表示する。ＡＴＭの利用者は表示装置５０５に表示されている取引メニューから、キー入力装置５０６を用いて取引項目を選択する（７０１）。なお、表示装置５０５とキー入力装置５０６はタッチパネルであり、単に表示装置（手段、部）とも言う。例えば、ここでは預金の支払取引を選択したと仮定する。その後、表示装置５０５に表示される「カードを挿入して下さい」とのガイダンスに従い、利用者はＩＣカードをＡＴＭのカード挿入口に挿入すると、挿入されたＩＣカードはＩＣカード装置５０４に取り込まれて内容を読取られる（７０２）。引き続き、表示部５０５にはテンキーと共に暗証番号入力のガイダンスを表示し、利用者はガイダンスに従いキー入力装置５０６を用いて暗証番号を入力する（７０３）。入力された暗証番号はホスト１０９に送信され、ホストで照合された結果（正否）を受信する。暗証番号の送信において、暗号鍵５１６にてデータを暗号化するのが望ましい。暗証番号入力による照合結果が間違いであれば、表示装置５０５に「もう一度入力してください」とのガイダンスを表示して、暗証番号の再入力を促す。一方、照合結果が正しければ、ＩＣカード内の登録された生体情報を読み出す又は「生体装置に指を置いて下さい」などのガイダンスを表示装置５０５に表示する。それと共に、ＡＴＭ内の生体認証装置制御プログラム５１３の制御、処理が生体認証装置１０６の装置全体制御プログラム６０７に移行され、生体認証処理を実行する（７０４）。このように、暗証認証処理はＡＴＭ側で実行され、生体認証処理は次に示す生体認証装置側で実行することもセキュリティ向上の一つの特徴でもある。

【００４２】

ステップ７０４の生体認証処理の詳細について図８、および、図６を用いて説明する。まず、ＡＴＭ１０７がＩＣカード内に格納されている暗号化された生体登録特徴量を、ＩＣカード装置５０４によって読み出して（読出処理）、ダイレクトに生体認証装置１０６に送信する。つまり、暗号化された生体情報の暗号状態を維持したまま、生体認証装置に送信する処理をＡＴＭ（制御部）が実行する。このように、ＡＴＭ１０７にも暗号鍵５１６を有しているが、ＩＣカードから読み出した暗号化生体登録特徴量を復号しない。認証装置１０６はその暗号化された特徴量を受信して、図６における暗号化生体登録特徴量６１３に格納する（８０１）。次に、装置全体制御プログラム６０７は暗号/復号プログラム６０９を起動し、暗号鍵６１７を用いて６１３に格納された暗号データを復号した（復号処理、復号部）後、その結果を生体登録特徴量６１４に格納する（８０２）。

【００４３】

ＡＴＭの表示装置５０５に表示されるガイダンスに従い、利用者は生体認証装置１０６の上に例えば指を置くと、装置１０６内の認証プログラム６１０は、照明ＬＥＤ６０３、ならびに、画像センサ６０４を制御して生体画像を取得して画像バッファ６１１に格納する（８０３）。認証プログラム６１０は画像バッファ６１１に格納された生体画像を読み出し、画像から認証用の生体特徴量を抽出して結果を生体特徴量６１２に格納する（８０４）。このように、利用者の生体画像、情報、特徴量を取得する機能を単に取得処理（手段、部）とも言う。

【００４４】

次に、認証プログラム６１０は生体特徴量６１２と生体登録特徴量６１４を読み出してそれらの間の距離値を計算し（マッチング、照合処理、部）、距離値が閾値未満であれば照合受入れ、閾値以上であれば照合拒絶として結果を６１５に格納する。さらに、６１５には受入れや拒絶といった照合結果に付随して状態コードを合わせて格納する（８０５）。例えば、照合拒絶の場合、生体を装置に置く位置が悪かったのか、生体を押し付ける力が極端に強くて生体情報が取得できなかったか、等を表すコードを添付する。認証装置はこのコードをＡＴＭ１０７に送信し、ＡＴＭ１０７が本コードを利用することで、例えば

照合拒絶の場合、コードに合わせた生体の置き方等のガイダンスをＡＴＭ利用者に対して表示することが可能になる。この結果、生体認証のやり方に関する的確なガイダンスができるので、利用者が必要以上に生体認証を繰り返すという煩わしさを低減することが可能になる。

暗号/復号プログラム６０９は、６１５に格納した照合結果に対して暗号鍵６１７を用いて暗号化し結果を６１６に格納する（８０６）。その後、外部にデータが流出する可能性を無くすために、装置全体制御プログラム６０７は６１１から６１７に格納されているデータをクリアする（８０７）。これにより、ＡＴＭは生体認証装置１０６内に残存している生体特徴量を削除する必要がなくなると共に、装置内に残存する生体特徴量が外部に漏洩するのを防止することが可能になる。最後に、２２０に格納された暗号化照合結果をＡＴＭに対して送信する（生体情報自身は含まず）と共に装置内に存在する暗号化照合結果を消去する（８０８）。もし、認証結果が拒絶の場合、ＡＴＭは規定回数に達するまでステップ８０１から８０８の処理を繰り返す。以上説明した図７の処理によりステップ７０４の生体認証処理が完了する。ここで、ステップ８０８にて照合結果を暗号化したものをＡＴＭに送信しているが、その理由は以下の通りである。

【００４５】

認証装置は基本的にＡＴＭに対して認証受入れか、認証拒絶かのデータを送信すればよい。しかし、そのデータフォーマットが第三者に漏れると、正規の生体認証装置を外して、認証受入れのデータを常に送信する不正な機器を、ＡＴＭに接続する可能性が出てくる。この場合、生体認証を行わずとも認証受入れのデータをＡＴＭは受け取るので、生体認証装置の不正防止効果が失われる恐れがあるためである。

【００４６】

ステップ７０４の生体認証の結果、認証受入れでＯＫであればステップ７０６に進み、ＮＧであればステップ７１０の取引中止に進む（７０５）。

【００４７】

利用者はキー入力装置５０６を用いて払戻し金額をＡＴＭ１０７に入力し（７０６）、ＡＴＭ１０７は入力された金額に基づき勘定系ホストコンピュータ１０９と通信して勘定処理を行う（７０７）。その後、ＡＴＭはＩＣカードをＩＣカード挿入口から排出すると共に、取引結果を記載した明細書を印刷する（７０８）。最後にＡＴＭは現金処理装置５０７から入力された金額分の紙幣が出金され、現金取出口から現金を排出して一連の処理を終了する（７０９）。

【００４８】

以上のステップ７０１から７０９の処理により、生体認証装置１０６から生体特徴量が外部に出力されることなく認証処理が完了する。なお、ＩＣカード装置５０４と生体認証装置１０６とを別体で構成する例を説明したが、図２のように一体と形成されたものであっても良い。この場合、ＩＣカードから読み出す登録、暗号化された生体情報はＡＴＭ内を一切通ることはなく、更にセキュリティの安全を確保できる。

【００４９】

上記実施例では営業店窓口端末で生体特徴量をＩＣカードに登録し、ＡＴＭで生体認証を行う方式について説明したが、生体特徴量の登録もＡＴＭに接続されている生体認証装置で行ってもよいし、営業店端末で生体認証を行っても良く、上述と同様に登録生体情報は営業店端末を介する必要がない。なお、登録と認証を１台の生体認証装置で兼用する場合は、図６における６１３から６１６のデータを図２の主記憶装置２０７に追加すれば可能となる。

【００５０】

また、上記実施例では暗号化のための暗号鍵を１種類しか持たせなかったが、認証プログラムを復号するための暗号鍵と認証結果を暗号化／復号するための暗号鍵を分けてもよく、暗号化方式は任意の方法を用いてもよい。

【００５１】

さらに、上記実施例では生体認証装置内の認証プログラムは装置が起動していない時は

暗号化された状態で不揮発性メモリに格納されて、装置の起動時に復号される方式について説明した。この暗号化による認証プログラムのセキュリティ確保以外にも、認証プログラムを分割し、プログラムの一部を装置外に格納し、残りを生体認証装置内の不揮発性メモリに格納する方法も有効である。すなわち、認証装置の起動時に装置外部に格納された認証プログラムの一部と、装置内の不揮発性メモリに格納された認証プログラムの一部を結合し、元の認証プログラムに復元することができる。あるいは、認証プログラムの暗号化と分割を組み合わせることも可能である。

【００５２】

また、ＡＴＭにおける認証において、暗証番号による認証処理の後に、生体認証処理を実行する例で説明した。暗証番号を先に入力する方式の利点として以下の点が挙げられる。生体認証を用いない取引では「取引メニュー選択」、「キャッシュカード挿入」、「暗証番号入力」の形で処理が進む。そのため、ＡＴＭ利用者はこのような順番の手順に慣れており、生体認証が後であればその手順は変わらないために操作の戸惑いがない。一方、生体認証処理後に暗証番号認証処理を行う例は、暗証番号入力後のホストとの電文タイミング、表示する画面の遷移など一切変更する必要がない点で有利である。このとき、生体認証装置から送信される照合結果がＯＫのときに初めて暗証番号の入力画面を表示し、暗証番号認証処理に移行することで利用者に対して２重のセキュリティを確保できる。

【００５３】

上記実施例では、窓口端末やＡＴＭに暗号鍵が存在し、その鍵を用いて生体特徴量を暗号化してＩＣカードに登録した。生体特徴量を暗号化する鍵は必ずしも窓口端末やＡＴＭに存在する必要はなく、生体認証装置内のみに存在してもよい。この場合、窓口端末やＡＴＭ経由でＩＣカード生体認証装置の間で暗号化された生体特徴量を読み書きする際には、鍵が窓口端末やＡＴＭに存在しないので暗号化生体特徴量を解読することが原理的に困難になり、セキュリティを向上させることが可能になる。

【図面の簡単な説明】

【００５４】

【図１】生体認証を用いた金融営業店システムの全体構成例を示す図。

【図２】営業店窓口端末に接続されるＩＣカード装置付生体認証装置の構成例を示す図。

【図３】営業店窓口端末の構成例を示す図。

【図４】営業店窓口端末とＩＣカード装置付生体認証装置を用いて生体認証用の特徴量をＩＣカードに登録する処理フローを示す図。

【図５】ＡＴＭ（自動現金預払機）の構成例を示す。

【図６】ＡＴＭに接続される生体認証装置の構成例を示す図。

【図７】ＡＴＭにおいて生体認証処理を含む取引業務フローを示す図。

【図８】ＡＴＭに接続される生体認証装置の処理フローを示す図。

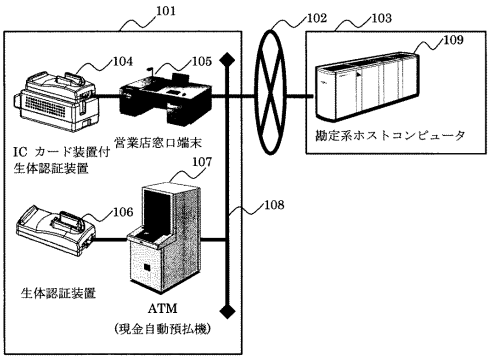
【符号の説明】

【００５５】

１０１…金融営業店、１０２…広域ネットワーク、１０３…データセンタ、１０４…ＩＣカード装置付生体認証装置、１０５…営業店窓口端末、１０６…生体認証装置、１０７…ＡＴＭ（現金自動預払機）、１０８…営業店内ＬＡＮ、１０９…勘定系ホストコンピュータ

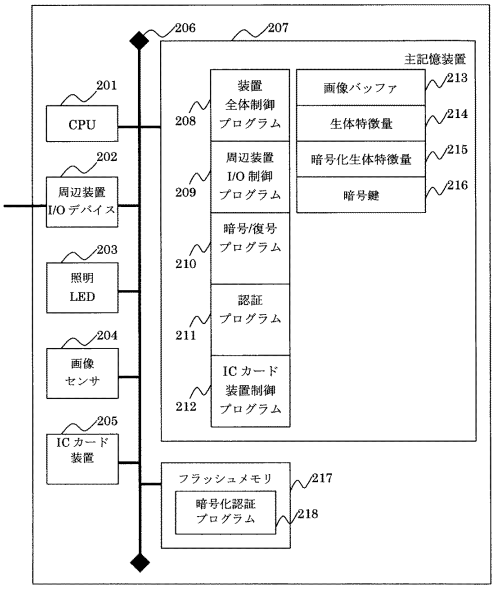
【図１】

【図１】



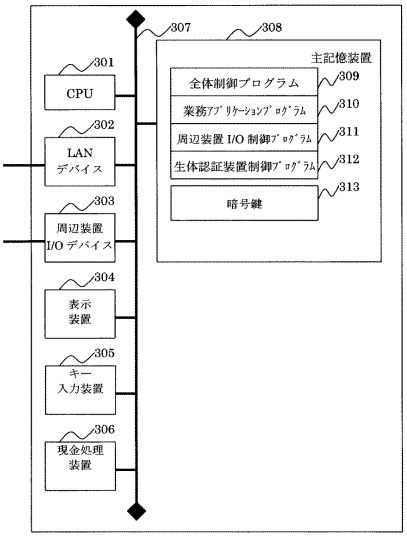
【図２】

【図２】



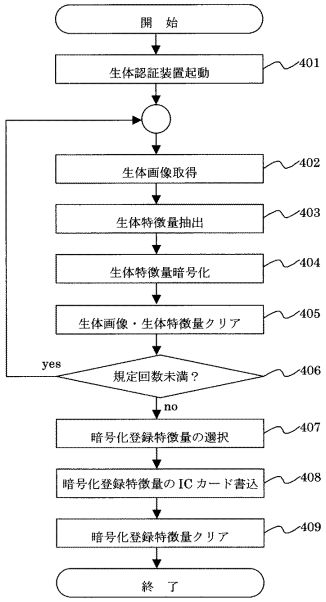
【図３】

【図３】



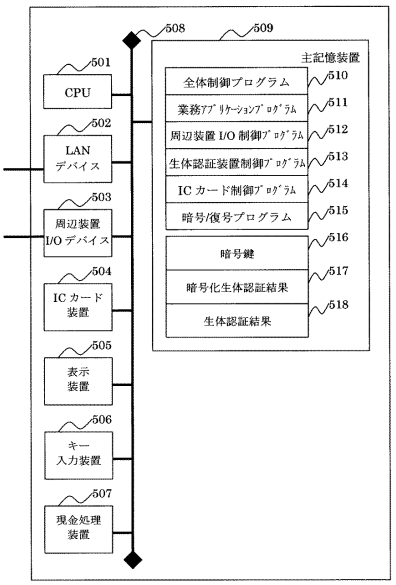
【図４】

【図４】



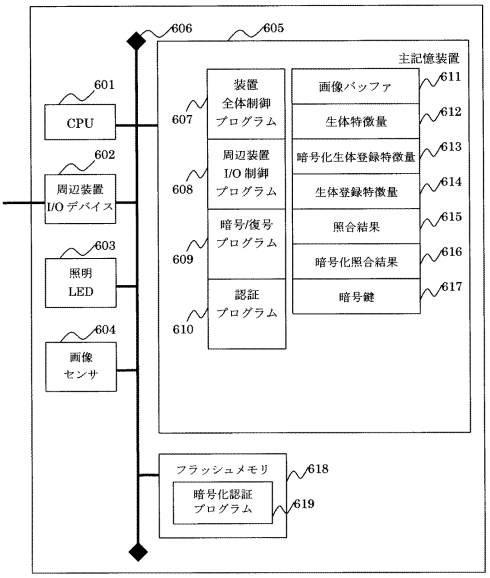
【図５】

【図５】



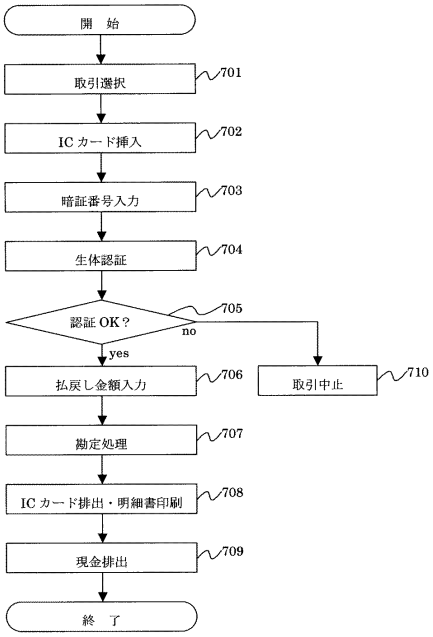
【図６】

【図６】



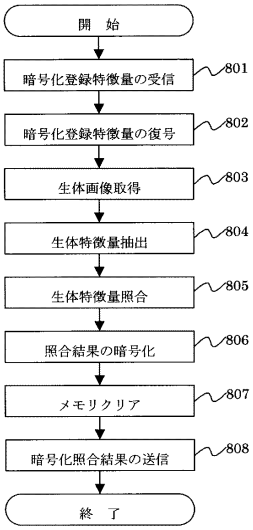
【図７】

【図７】



【図８】

【図８】



フロントページの続き

(51)Int.Cl. FI
Ａ６１Ｂ 5/10 ３２０Ｚ
Ａ６１Ｂ 5/10 ３２０Ｃ

(72)発明者 巻本 英二
東京都品川区大崎一丁目６番３号 日立オムロンターミナルソリューションズ株式会社内
(72)発明者 永田 幸平
東京都品川区大崎一丁目６番３号 日立オムロンターミナルソリューションズ株式会社内

審査官 小林 秀和

(56)参考文献 特開平１０－１６１８６４（ＪＰ，Ａ）
特開２００５－０３８２５７（ＪＰ，Ａ）
特開２００２－２２９８６１（ＪＰ，Ａ）
田中 一廣，指紋認証付きＩＣカードリーダライター ＩＣカードと指紋認証の融合により安全性と運用性を向上，月刊バーコード，日本，日本工業出版株式会社，２００３年 5月 2日，第16巻 第6号，p.43-p.46，国内技術雑誌2004-00491-011

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／２０
Ｇ０６Ｋ １７／００
Ｈ０４Ｌ ９／３２
Ａ６１Ｂ ５／１１７