(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-293490
(P2005-293490A)
(43)公開日　平成17年10月20日(2005.10.20)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 15/00	G06F 15/00	330F	5B043
G06T 7/00	G06F 15/00	330G	5B085
H04L 9/32	G06T 7/00	530	5J104
	H04L 9/00	673D	

審査請求 未請求　請求項の数 17　ＯＬ　（全 13 頁）

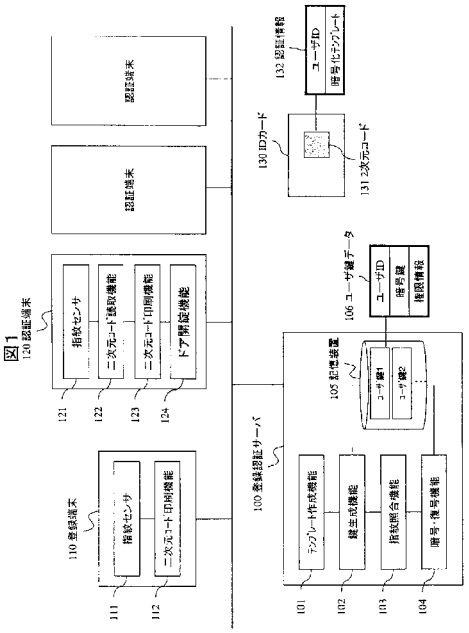
(21)出願番号　特願2004-111235 (P2004-111235)
(22)出願日　平成16年4月5日 (2004.4.5)

(71)出願人　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　100093492
弁理士　鈴木　市郎
(74)代理人　100078134
弁理士　武　顕次郎
(72)発明者　高橋　健太
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
(72)発明者　三村　昌弘
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内

最終頁に続く

(54)【発明の名称】生体認証システム

(57)【要約】
【課題】
プライバシを容易に保護することのできる生体認証システムを提供する
【解決手段】
利用者が入力した生体情報をもとに生成したテンプレートと、利用者の生体情報を表すテンプレートを暗号化して暗号化テンプレートとして記録媒体１３０に記録した暗号化テンプレートを復号化して生成したテンプレートとを比較し、該比較結果をもとに利用者を認証する登録認証サーバ１００を備え、登録認証サーバ１００により利用者の認証に成功したとき、前記記録媒体に記録した暗号化テンプレートを異なる暗号化キー用いた暗号化テンプレートに置換して記録する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
利用者が入力した生体情報をもとに生成した生体特徴量と、利用者の生体情報を表す生体特徴量を暗号化して暗号化生体特徴量として登録した暗号化生体特徴量を復号化して生成した生体特徴量とを比較し、該比較結果をもとに利用者を認証する認証手段を備え、
認証手段により利用者の認証に成功したとき、前記暗号化生体特徴量を異なる暗号化キーを用いた暗号化生体特徴量に置換して記録することを特徴とする生体認証システム。
【請求項２】
請求項１記載の生体認証システムにおいて、
認証手段は、利用者が入力した生体情報をもとに生成した生体特徴量と、利用者の生体情報を表す生体特徴量を暗号化して暗号化生体特徴量として記録媒体に登録した暗号化生体特徴量を復号化して生成した生体特徴量とを比較し、該比較結果をもとに利用者を認証する登録認証サーバであることを特徴とする生体認証システム。
【請求項３】
請求項２記載の生体認証システムにおいて、
前記記録媒体は表面に繰り返し印刷可能なリライトカードであることを特徴とする生体認証システム。
【請求項４】
請求項２記載の生体認証システムにおいて、
暗号化生体特徴量は生体情報を暗号化した２次元バーコードであることを特徴とする生体認証システム。
【請求項５】
請求項２記載の生体認証システムにおいて、
暗号化キーはランダムに生成し、生成した暗号化キーは生体情報の登録および利用者の認証を管理する登録認証サーバに格納することを特徴とする生体認証システム。
【請求項６】
請求項２記載の生体認証システムにおいて、
生体情報は利用者の指紋であることを特徴とする生体認証システム。
【請求項７】
請求項１記載の生体認証システムにおいて、
認証手段は、利用者が入力した生体情報をもとに生成した生体特徴量と、利用者の生体情報を含む生体特徴量を暗号化して暗号化生体特徴量として携帯端末に記録した暗号化生体特徴量を復号化して生成した生体特徴量とを比較し、該比較結果をもとに利用者を認証する認証端末であることを特徴とする生体認証システム。
【請求項８】
請求項７記載の生体認証システムにおいて、
暗号化生体特徴量は、生体情報を、生体情報自体をもとに生成した暗号化キーを用いて暗号化した情報であることを特徴とする生体認証システム。
【請求項９】
請求項７記載の生体認証システムにおいて、
暗号化キーは生体情報および生体情報の補助情報をもとに生成することを特徴とする生体認証システム。
【請求項１０】
請求項９記載の生体認証システムにおいて、
生体情報は利用者の指紋であり、生体情報の補助情報は指紋の隆線方向を表すコードであることを特徴とする生体認証システム。
【請求項１１】
請求項１記載の生体認証システムにおいて、
登録認証サーバによる利用者の認証に失敗したとき、利用者が入力した生体情報を保存することを特徴とする生体認証システム。

【請求項１２】
利用者の生体情報を表す生体特徴量を暗号化して登録した暗号化生体特徴量を復号化して読み取るステップと、
利用者が入力した生体情報をもとに生成した生体特徴量と前記復号化した生体特徴量とを比較し、該比較結果をもとに利用者を認証するステップと、
認証ステップにより利用者の認証に成功したとき、前記暗号化生体特徴量を異なる暗号化キーを用いた暗号化生体特徴量に置換して記録するステップを備えたことを特徴とする生体認証方法。
【請求項１３】
請求項１２記載の生体認証方法において
利用者を認証するステップは、
利用者が入力した生体情報をもとに生成した生体特徴量と、記録媒体に記録した暗号化生体特徴量を復号化して生成した生体特徴量とを比較するステップを含むことを特徴とする生体認証方法。
【請求項１４】
請求項１３記載の生体認証方法において、
前記記録媒体は表面に繰り返し印刷可能なリライトカードであることを特徴とする生体認証方法。
【請求項１５】
請求項１２記載の生体認証方法において、利用者を認証するステップは、
利用者が入力した生体情報をもとに生成した生体特徴量と、前記携帯端末に記録した暗号化生体特徴量を復号化して生成した生体特徴量とを比較するステップを含み、
前記暗号化に用いる暗号化キーおよび復号化キーは、利用者の生体情報をもとに生成することを特徴とする生体認証方法。
【請求項１６】
請求項１５記載の生体認証システムにおいて、
暗号化キーは生体情報および生体情報の補助情報をもとに生成することを特徴とする生体認証方法。
【請求項１７】
記録媒体から読み取った、利用者の生体情報を含む生体特徴量を暗号化した暗号化生体特徴量と、利用者が入力した生体情報をもとに生成した生体特徴量とを入力する入力手段と、
前記暗号化生体特徴量を予め格納してある復号キーを用いて復号化して復号化生体特徴量を生成する復号手段と、
復号化生体特徴量と、利用者が入力した生体情報をもとに生成した生体特徴量とを比較する照合手段と、
照合手段により利用者の認証に成功したとき、前記暗号化生体特徴量を異なる暗号化キー用いた暗号化生体特徴量に置換し、置換した暗号化生体特徴量を記録媒体側に送信することを特徴とする認証サーバ。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、生体認証システムに係り、特に、プライバシを容易に確保することのできる生体認証システムに関する。
【背景技術】
【０００２】
生体情報を用いたユーザ認証システムは、例えば、登録時にユーザから生体情報を取得し、特徴的な情報を抽出して記録する。この抽出した情報を生体特徴量（以下、テンプレートと称する）という。

【０００３】
認証時には、再びユーザから生体情報を取得してテンプレートを生成し、生成したテンプレートと前記登録したテンプレートと照合して本人か否かを確認する。この場合、プライバシ保護あるいは管理コストの点から、テンプレートは個人が所持、管理することが望ましい。
【０００４】
テンプレートを個人が管理する生体認証技術としては、特許文献１記載の技術がある。この技術では、ユーザが所持するカードなどの記録媒体にテンプレートを二次元コードとして記録する。
【０００５】
また、特定の管理区域内のコンピュータシステムの利用者を認証する技術として、例えば特許文献２記載の技術が知られている。この技術では、ユーザのテンプレートをＩＣカードに記録してユーザに発行し、ユーザが管理区域に入場する際、入場口に設置されたＩＣカードリーダでユーザのＩＣカードに記録されたテンプレートを読み取り、読み取ったテンプレートとコンピュータシステム利用時に入力したユーザの生体情報を照合してユーザを認証する。また、非特許文献１には、指紋から一意に暗号鍵を生成する方法が示されている。
【特許文献１】特開２００３－６７３４５号公報
【特許文献２】特開２００１－７６２７０号公報
【非特許文献１】柴田陽一 他，“指紋からのユニークＩＤの動的抽出”，SCIS2004，3B1-1，2004/1
【発明の開示】
【発明が解決しようとする課題】
【０００６】
特許文献１記載の技術のようにテンプレートを二次元コードとして記録した場合、二次元コードを写真撮影したり、複写機で複写することにより、容易にテンプレートを盗用することが可能であり、生体情報を偽造して本人になりすますことなどが可能となる。
【０００７】
一方、特許文献２の技術のように、ＩＣカードなどのアクセス制御可能な媒体にテンプレートを格納して発行する場合、媒体および該媒体に対するリーダ／ライタのコストが高くなる。このため不特定多数のユーザを認証する必要のあるアプリケーションへの適用は困難となる。
【０００８】
本発明は、これらの問題点に鑑みてなされたもので、生体情報を保護してプライバシを容易に保護することのできる生体認証システムを提供する。
【課題を解決するための手段】
【０００９】
本発明は上記課題を解決するため、次のような手段を採用した。
【００１０】
利用者が入力した生体情報をもとに生成したテンプレートと、利用者の生体情報を表すテンプレートを暗号化して暗号化テンプレートとして登録した暗号化テンプレートを復号化して生成したテンプレートとを比較し、該比較結果をもとに利用者を認証する認証手段を備え、認証手段により利用者の認証に成功したとき、前記暗号化テンプレートを異なる暗号化キーを用いた暗号化テンプレートに置換して記録する。
【発明の効果】
【００１１】
本発明は、以上の構成を備えるため、プライバシを容易に保護することのできる生体認証システムを提供することができる。
【発明を実施するための最良の形態】
【００１２】

以下、最良の実施形態を添付図面を参照しながら説明する。図１は、本発明の第１の実施形態を説明する図である。図を参照しながら、ビル内の各フロアあるいは各部屋に入る際に使用する認証システムについて説明する。この例の認証システムは、従業員や訪問者など不特定多数のユーザに対し、各フロアや各部屋のドアにおける入室権限を指紋を用いて認証するものである。

【００１３】

図１は、本実施形態にかかる認証システムの構成を説明する図である。図に示すように本認証システムは、ユーザを登録する際にオペレータが運用する登録端末１１０、各部屋のドアに設置され、ユーザの入室権限を認証しドアを開錠する認証端末１２０、テンプレート作成や指紋照合などの処理を行う登録認証サーバ１００、ユーザに対して発行しユーザが所持・管理するＩＤカード１３０を備える。ビル内にはＬＡＮが敷設され、登録認証サーバ１００、登録端末１１０、および認証端末１２０はＬＡＮで接続されている。

【００１４】

登録認証サーバ１００は、テンプレート作成機能１０１、鍵生成機能１０２、指紋照合機能１０３、暗号・復号化機能１０４、および記憶装置１０５を備える。記憶装置１０５は、各登録ユーザに割り当てたユーザ鍵データ１０６を記憶する。ユーザ鍵データ１０６は、ユーザＩＤ、暗号鍵、および権限情報を含む。権限情報は入室が許可されているフロアのリストなどを含む。

【００１５】

登録端末１１０は、指紋センサ１１１、および二次元コード印刷機能１１２を備える。

【００１６】

認証端末１２０は、指紋センサ１２１、二次元コード読取機能１２２、二次元コード印刷機能１２３、およびドア開錠機能１２４を備える。

【００１７】

ＩＤカード１３０は、表面に繰り返し印刷可能なカード（リライトカード）であり、認証情報１３２が二次元コード１３１として印刷される。認証情報１３２は、ユーザＩＤと暗号化されたテンプレートを含む。リライトカードは近年チェーン店や量販店などのポイントカードを中心に普及が進んでいるもので、ＩＣカードなどアクセス制御能力を持つチップ内蔵のカードと比較して価格が十分の一以下と安価であるため、不特定多数のビル利用者に対して発行する場合のコストを低く抑えられるという利点がある。テンプレートは暗号化された状態で二次元コード化し印刷されるため、第三者が複写などによって二次元コードを手に入れても、テンプレートを復号することができず、プライバシが保護されると同時に、テンプレートから指紋を偽造して行うなりすまし攻撃が困難となる。

【００１８】

図２は、ユーザ登録の処理手順およびデータの流れを説明する図である。ユーザ登録は、ユーザがビルを最初に訪問した際などに行う。

【００１９】

まず、登録端末１１０は、ユーザの指紋を読み取り、読み取った指紋情報を登録認証サーバ１００に送信する（ステップ２００）。登録認証サーバ１００は、指紋情報を受け取り、テンプレートを作成する（ステップ２０５）。次いで、登録認証サーバ１００は、暗号鍵をランダムに生成する（ステップ２１０）。

【００２０】

登録認証サーバ１００は、ユーザＩＤ、前記暗号鍵、およびユーザの権限情報を組にしてユーザ鍵データ１０６を作成し、作成したユーザ鍵データを記憶装置１０５に保存する（ステップ２１５）。なお、ユーザＩＤおよび権限情報はセキュリティポリシーや運用規則に従ってオペレータが入力するとよい。次いで、登録認証サーバ１００は前記暗号鍵を用いて前記テンプレートを暗号化し、ユーザＩＤと暗号化テンプレートを組にした認証情報を登録端末１１０に送信する（ステップ２２０）。

【００２１】

登録端末１１０は、認証情報を受け取り、これを二次元コード化してＩＤカード１３０

に印刷してユーザに発行する（ステップ２２５）。

【００２２】

図３は、ユーザ入室時におけるユーザ認証の処理手順およびデータの流れを説明する図である。

【００２３】

認証端末１２０は、ユーザが提示したＩＤカード１３０の二次元コードを読み取り、読み取った二次元コードの認証情報を登録認証サーバ１００へ送信する（ステップ３００）。また、認証端末１２０は、ユーザの指紋を読み取り、読み取った指紋情報を登録認証サーバ１００に送信する（ステップ３０５）。登録認証サーバ１００は、認証情報と指紋情報を受け取り、前記認証情報に含まれるユーザＩＤをキーとして、ユーザ鍵データ１０６を検索する（ステップ３１０）。

【００２４】

次いで、登録認証サーバ１００は、ユーザ鍵データ１０６に含まれる暗号鍵を用いて、前記認証情報に含まれる暗号化テンプレートを復号化する（ステップ３１５）。復号化に失敗した場合、認証端末１２０はユーザに対してエラーメッセージを表示し、認証端末１２０および登録認証サーバ１００はその処理を終了する（ステップ３２５）。復号化の失敗は、登録認証サーバ１００が保管する暗号鍵とＩＤカードに印刷された暗号化テンプレートに対応する暗号鍵が異なることを意味する。後述するように、暗号鍵は正規のユーザが使用して認証が成功する度に更新されるため、復号化に失敗した場合、ＩＤカードが不正に利用された可能性が高いことを意味する。従って、このとき、取得した指紋画像を監査ログとして記録したり、当該ユーザＩＤの利用を一時的にロックしたり、次回正規のユーザが利用して認証が成功した場合に警告メッセージを表示するなどの対策をとることができる。

【００２５】

復号化に成功した場合、登録認証サーバ１００は復号化したテンプレートと前記指紋情報をもとに生成したテンプレートを照合する（ステップ３３０）。照合に失敗した場合、認証端末１２０はユーザに対してエラーメッセージを表示し、認証端末１２０と登録認証サーバ１００はその処理を終了する（ステップ３４０）。照合に成功した場合、登録認証サーバ１００はランダムに新しい暗号鍵を生成し、ユーザ鍵データ１０６を生成した暗号鍵で書き換える（ステップ３４５）。

【００２６】

認証が成功した場合にのみ暗号鍵を書き換えることにより、正当なユーザは常に新しい暗号鍵で暗号化されたテンプレートを所持していることを期待することができ、過去に複写するなどして偽造したＩＤカードは無効となる。また、不正に偽造されたＩＤカードの利用を検出することができるため、高いセキュリティを実現することができる。更に攻撃者の利用により不正に暗号鍵を更新されて正当なユーザが利用できなくなる脅威も防ぐことができる。

【００２７】

登録認証サーバ１００は、新しい暗号鍵を用いてテンプレートを暗号化し、暗号化したテンプレートとユーザＩＤとを組みにした認証情報、およびユーザ鍵データ１０６に含まれる権限情報を認証端末１２０に送信する（ステップ３５０）。認証端末１２０は、ＩＤカード１３０に既に印刷してある二次元コードを消去し、受信した認証情報を二次元コード化してＩＤカード１３０に印刷する（ステップ３５５）。

【００２８】

認証端末１２０は、受信した権限情報を参照し、ユーザが当該認証端末の管理するフロアや部屋への入室権限を持たないならば、エラーメッセージを表示し、処理を終了する（ステップ３６０）。ユーザが入室権限を持つならば、認証端末１２０はドアを開錠する（ステップ３６５）。

【００２９】

図４は、本発明の第２の実施形態を説明する図である。本認証システムは、ユーザを登

録する際にオペレータが運用する登録端末４００、各室のドアに設置されてユーザの入室権限を認証しドアを開錠する認証端末４１０、およびユーザが所持する携帯端末４２０を備える。なお、登録端末４００と認証端末４１０はＬＡＮなどで接続されている必要はない。

【００３０】

登録端末４００は、指紋センサ４０１、補助情報作成機能４０２、鍵生成機能４０３、テンプレート作成機能４０４、暗号機能４０５、および通信機能４０６備える。鍵生成機能４０３は、指紋情報および補助情報をもとに暗号鍵を生成する。前記補助情報は補助情報作成機能４０２によりユーザ毎に作成する。

【００３１】

一般に、同一の指紋から取得した指紋情報であっても、センサに対する指の位置や歪みなどにより取得する毎にその情報は異なる。鍵生成機能４０３は、前記補助情報を用いて、同一の指紋から取得される指紋情報に対して一意のデジタルデータを作成し、これを暗号鍵として出力する。このように生体情報から一意のデジタルデータを作成する方法は非特許文献１などに開示されている。また、通信機能４０６は、赤外線などを用いて携帯端末４２０と通信する。

【００３２】

認証端末４１０は、通信機能４１１、指紋センサ４１２、鍵生成機能４１３、暗号・復号機能４１４、指紋照合機能４１５、ドア開錠機能４１６を備える。通信機能４１１は、赤外線などを用いて携帯端末４２０と通信する。鍵生成機能４１３は、指紋情報と補助情報から暗号鍵を生成する。

【００３３】

携帯端末４２０は、登録端末４００や認証端末４１０と通信するための通信機能４２１および記憶装置４２２を備える。記憶装置４２２は、携帯端末４２０の所有者の認証情報４２３を記憶する。認証情報４２３は、ユーザＩＤ、補助情報、暗号化テンプレートを含む。テンプレートは暗号化された状態で記憶されるため、携帯端末４２０は耐タンパ（改竄）性やアクセス制御機能といった特殊なセキュリティ機能は必要としない。このため携帯端末４２０として、例えばユーザが所有する携帯電話を利用して、その表示画面に暗号化テンプレートを２次元バーコードとして表示するすることできる。これによりユーザ一人当たりの登録コストを低く抑えることができる。

【００３４】

図５は、指紋から一意に暗号鍵を生成する方法を説明する図である。図５（ａ）に示すような採取した指紋画像５００を考える。指紋画像５００は、指紋のコアの位置などを基準に平行移動して補正を行ってあるものとする。

【００３５】

また、補助情報５０１は、図５（ｂ）に示すように隆線方向とコードを対応させた表である。なお、この表の作成に際しては、指紋取得時にある程度の歪みが生じても高い確率で同じ暗号鍵が生成されるよう、登録時に複数回指紋画像を取得して各ブロックの隆線方向のずれを解析し、補助情報５０１の隆線方向範囲を設定しておく。

【００３６】

鍵の生成時には、指紋画像５００を格子状のブロックに分割し、各ブロック内における指紋の隆線の方向を調べ、補助情報５０１を用いてコード化する。例えば、左上のブロックから順にコード化し、それらを連結することにより暗号鍵５０２を生成することができる。

【００３７】

図６は、ユーザ登録の処理手順およびデータの流れを説明する図である。ユーザ登録は、ユーザがビルを最初に訪問した際などに行う。

【００３８】

まず、登録端末４００は、ユーザの指紋から指紋情報を複数回読み取る（ステップ６００）。次いで、登録端末４００は、読み取った指紋情報をもとに補助情報を作成する（ス

テップ６０５）。次いで、前記指紋情報と前記補助情報をもとに暗号鍵を生成する（ステップ６１０）。

【００３９】

また、登録端末４００は、前記指紋情報をもとにテンプレートを生成する（ステップ６１５）。次いで、生成したテンプレートを前記暗号鍵を用いて暗号化する（ステップ６２０）。次いで、ユーザＩＤ、前記補助情報、前記暗号化テンプレートを含む認証情報を作成し、作成した認証情報を携帯端末４２０に送信する（ステップ６２５）。

【００４０】

携帯端末４２０は、前記認証情報を受信し、受信した認証情報を記憶装置４２２に保存する（ステップ６３０）。

【００４１】

補助情報と暗号化テンプレートからテンプレートを復号化することは困難であるため、携帯端末に格納した認証情報をコピーされた場合にもおいても、テンプレートの漏洩を防止することができる。

【００４２】

図７は、ユーザ入室時におけるユーザ認証の処理手順およびデータの流れを説明する図である。

【００４３】

まず、携帯端末４２０は、自身が保持する認証情報（ユーザＩＤ、補助情報、暗号化テンプレート）４２３を認証端末４１０へ送信する（ステップ７００）。

【００４４】

一方、認証端末４１０は、指紋センサ４１２を介してユーザの指紋から指紋情報を読み取る（ステップ７０５）。次いで、読み取った指紋情報および受信した認証情報４２３に含まれる補助情報をもとに暗号鍵を生成する（ステップ７１０）。次いで、この生成した暗号鍵を用いて、前記受信した認証情報４２３に含まれる暗号化テンプレートを復号化する（ステップ７１５）。

【００４５】

復号化に失敗した場合、携帯端末４２０はユーザに対してエラーメッセージを表示し、認証端末４１０と携帯端末４２０は処理を終了する（ステップ７２０）。復号化に成功した場合、認証端末４１０は復号化したテンプレートと、前記ユーザの指紋から読み取った指紋情報もとに生成したテンプレートとを照合する（ステップ７３０）。

【００４６】

照合が失敗した場合、携帯端末４２０はユーザに対してエラーメッセージを表示し、認証端末４１０と携帯端末４２０は処理を終了する（ステップ７３５）。照合に成功した場合、認証端末４１０はドアを開錠する（ステップ７４５）。

【００４７】

このように指紋情報から動的に暗号鍵を生成し、生成した暗号鍵を用いて暗号化テンプレートを復号化する。これにより登録端末４００および認証端末４１０は暗号鍵を管理する必要がなくなる。また登録端末４００と認証端末４１０をＬＡＮなどで接続する必要がない。このため低コストでシステムを構築・運用可能であるという利点がある。

【００４８】

以上説明したように、本発明の実施形態によれば、ユーザは自身のテンプレートを所持、管理することができる。また、テンプレートを暗号化することで、安価な媒体を用いながらテンプレートの盗用によるプライバシの侵害や生体情報の偽造などを防止することができる。このため、低コスト・高セキュリティの認証システムを実現することができる。

【００４９】

例えば、暗号鍵を登録認証端末内で管理し、照合が成功するたびに暗号鍵を更新してテンプレートを暗号化しなおすことにより、リライトカードに二次元コードで記録するといったような複製の容易な媒体を用いる場合においても、二次元コードで記録したテンプレートの盗用を困難とし、セキュリティを高めることができる。

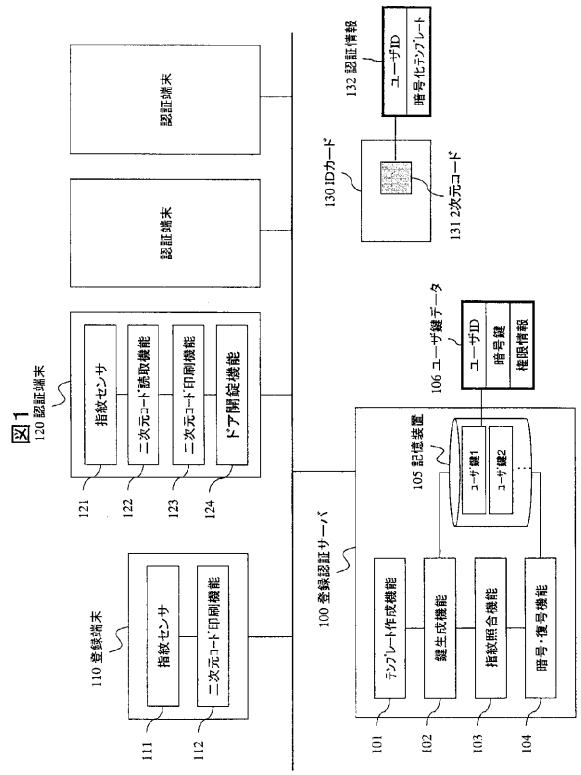
【００５０】
　また、ＩＣカードのような耐タンパ性やアクセス制御機能を持たない安価な媒体を利用することができる、不特定多数のユーザを認証する必要のあるアプリケーションに対しても低コストで適用可能という利点がある。
【００５１】
　また、ユーザの生体情報自体をもとに暗号鍵を生成し、テンプレートを暗号化する。これにより、複製の容易な媒体を用いる場合にもテンプレートの盗用を困難とし、安価でセキュリティの高い認証システムを実現することができる。更に登録認証端末内で暗号鍵を管理する必要がない。このため、運用コストが低く、また、端末からの暗号鍵の漏洩によるセキュリティが低下することがなくなる。

【図面の簡単な説明】
【００５２】
【図１】本実施形態にかかる認証システムの構成を説明する図である。
【図２】ユーザ登録の処理手順およびデータの流れを説明する図である。
【図３】ユーザ入室時におけるユーザ認証の処理手順およびデータの流れを説明する図である。
【図４】本発明の第２の実施形態を説明する図である。
【図５】指紋から一意に暗号鍵を生成する方法を説明するずである。
【図６】ユーザ登録の処理手順およびデータの流れを説明する図である。
【図７】ユーザ入室時におけるユーザ認証の処理手順およびデータの流れを説明する図である。

【符号の説明】
【００５３】
１００　登録認証サーバ
１０１　テンプレート作成機能
１０２　鍵生成機能
１０３　指紋照合機能
１０４　暗号・復号機能
１０５　記憶機能
１１０　登録端末
１１１　指紋センサ
１１２　２次元コード印刷機能
１２０　認証端末
１２１　指紋センサ
１２２　２次元コード読み取り機能
１２３　２次元コード印刷機能
１２４　ドア開錠機能
１３０　ＩＤカード
４００　登録端末
４０１　指紋センサ
４０２　補助情報作成機能
４０３　鍵生成機能
４０４　テンプレート作成機能
４０５　暗号機能
４０６　通信機能
４１０　認証端末
４１１　指紋センサ
４１３　鍵生成機能
４１４　暗号・復号機能
４１５　指紋照合機能

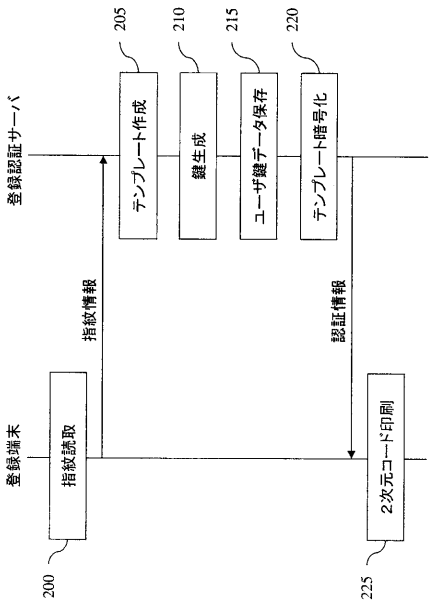
４１６　ドア開錠機能
４２０　携帯端末
４２１　通信機能
４２２　記憶装置

【図１】



【図２】

図2



【図３】

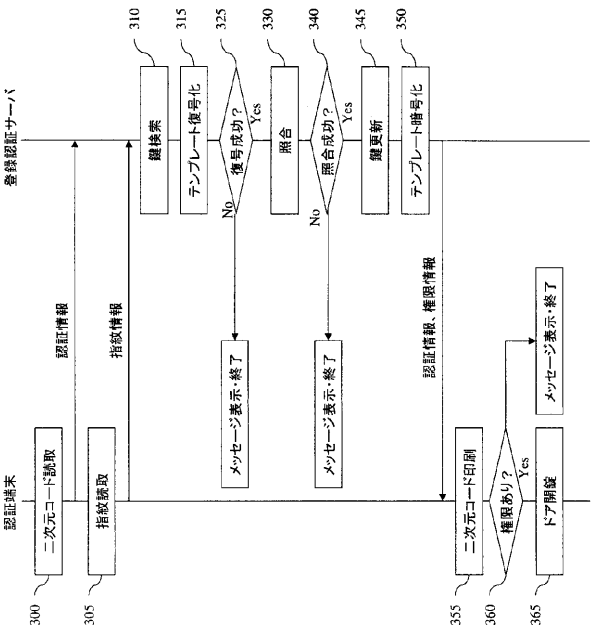


図3
登録認証サーバ
認証端末
二次元コード読取
指紋読取
認証情報
指紋情報
鍵検索
テンプレート復号化
復号成功？
No
Yes
照合
照合成功？
No
Yes
鍵更新
テンプレート暗号化
メッセージ表示・終了
メッセージ表示・終了
認証情報、権限情報
二次元コード印刷
権限あり？
Yes
ドア開錠
メッセージ表示・終了
300
305
310
315
325
330
340
345
350
355
360
365

【図４】

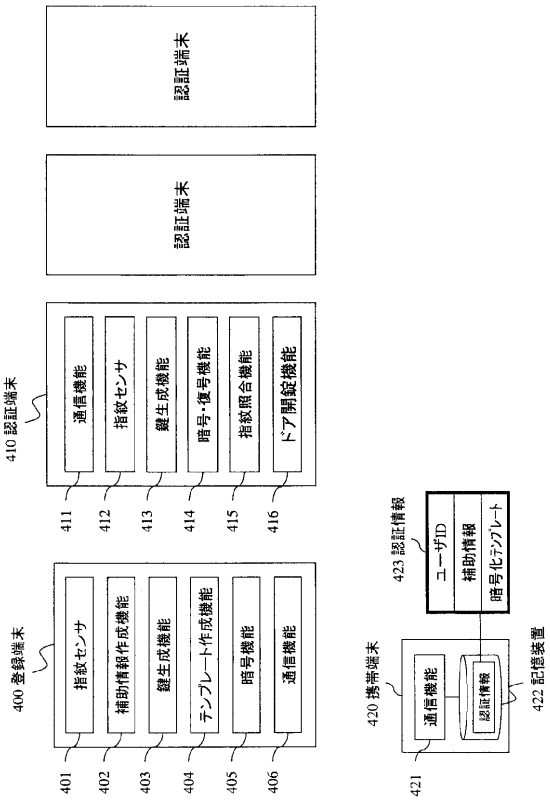


図4
認証端末
認証端末
410 認証端末
通信機能
指紋センサ
鍵生成機能
暗号・復号機能
指紋照合機能
ドア開錠機能
411
412
413
414
415
416
400 登録端末
指紋センサ
補助情報作成機能
鍵生成機能
テンプレート作成機能
暗号機能
通信機能
401
402
403
404
405
406
423 認証情報
ユーザID
補助情報
暗号化テンプレート
420 携帯端末
通信機能
認証情報
421
422 記憶装置

【図５】

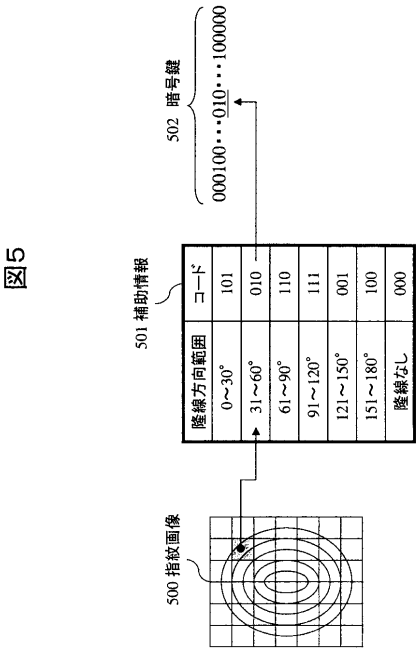


図5
502 暗号鍵
000100・・・010・・・100000
501 補助情報
隆線方向範囲
コード
0～30°
101
31～60°
010
61～90°
110
91～120°
111
121～150°
001
151～180°
100
隆線なし
000
500 指紋画像

【図６】

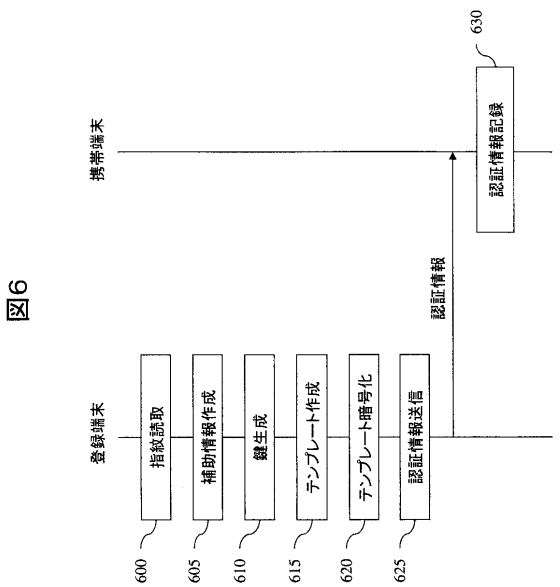
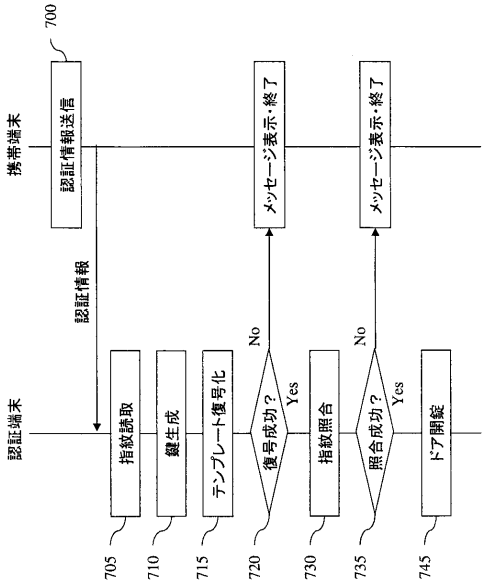


図6
携帯端末
630
認証情報記録
認証情報
登録端末
指紋読取
補助情報作成
鍵生成
テンプレート作成
テンプレート暗号化
認証情報送信
600
605
610
615
620
625

【図７】

図7


携帯端末
認証端末
700
認証情報送信
認証情報
指紋読取
鍵生成
テンプレート復号化
復号成功？
No
Yes
メッセージ表示・終了
指紋照合
照合成功？
No
Yes
メッセージ表示・終了
ドア開錠
705
710
715
720
730
735
745

フロントページの続き

Ｆターム(参考) 5B043 AA04 AA09 BA02 BA08 CA09 EA08 FA04 FA08 GA02 GA17
5B085 AE09 AE26
5J104 AA07 AA16 EA03 EA04 EA15 EA16 EA17 EA18 EA22 JA03
KA01 KA04 KA16 KA17 MA05 NA02 NA05 NA33 NA37 NA38