(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6056577号
(P6056577)
(45)発行日　平成29年1月11日(2017.1.11)　(24)登録日　平成28年12月16日(2016.12.16)

(51)Int.Cl.　F I
G06F 21/32 (2013.01)　G06F 21/32

請求項の数 5　(全 23 頁)

(21)出願番号　特願2013-56093(P2013-56093)
(22)出願日　平成25年3月19日(2013.3.19)
(65)公開番号　特開2014-182552(P2014-182552A)
(43)公開日　平成26年9月29日(2014.9.29)
審査請求日　平成27年10月7日(2015.10.7)

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100099759
弁理士　青木　篤
(74)代理人　100119987
弁理士　伊坪　公一
(74)代理人　100081330
弁理士　樋口　外治
(74)代理人　100114177
弁理士　小林　龍
(72)発明者　松濤　智明
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

最終頁に続く

(54)【発明の名称】生体認証装置、生体認証方法及び生体認証用コンピュータプログラム

(57)【特許請求の範囲】
【請求項１】
利用者の生体情報に基づいて、当該利用者を登録利用者として認証するか否かを判定する生体認証装置であって、
過去の生体認証時において利用者の生体情報を表す過去データが取得された際の当該生体情報の取得環境の状態を表す過去状態情報を記憶する記憶部と、
利用者の生体情報を表すデータを取得する生体情報取得部と、
前記利用者の生体情報を表すデータから、当該データ取得時における利用者の生体情報の取得環境の状態を表す現状態情報を抽出する状態情報抽出部と、
前記現状態情報と前記過去状態情報の類似度合いを表す再現度を算出する再現度算出部と、
前記データが前記過去データそのものあるいは前記過去データの一部を改変したものであると推定される閾値と前記再現度を比較し、前記再現度が当該閾値以上である場合、利用者を認証しない不正アクセス判定部と、
を有する生体認証装置。
【請求項２】
前記利用者の生体情報が前記登録利用者の生体情報と一致するか否かを判定する認証判定部をさらに有し、
前記記憶部は、前記過去状態情報とともに、前記過去状態情報が得られた時の生体認証に成功したか否かを表すフラグを含み、

前記再現度算出部は、
前記認証判定部が、前記利用者の生体情報と前記登録利用者の生体情報が一致すると判定した場合、前記過去状態情報のうちの生体認証に成功したことを表すフラグが付された過去状態情報と前記現状態情報との間で前記再現度を算出し、
一方、前記認証判定部が、前記利用者の生体情報と前記登録利用者の生体情報が一致しないと判定した場合、前記過去状態情報のうちの生体認証に失敗したことを表すフラグが付され、かつ、前記利用者が生体認証の試行を開始してから前記現状態情報取得までの間に繰り返された生体認証時の過去状態情報と前記現状態情報との間で前記再現度を算出する、
請求項１に記載の生体認証装置。
【請求項３】
前記記憶部は、過去の生体認証時における利用者の生体情報の特徴を表す第１の過去情報と、過去の生体認証時における利用者の取得環境の状態を表す第２の過去情報とを前記過去状態情報として記憶し、
前記状態情報抽出部は、前記利用者の生体情報を表すデータから、当該データ取得時における利用者の生体情報の特徴を表す第１の現情報と、当該データ取得時における利用者の生体情報の取得環境を表す第２の現情報とを前記現状態情報として抽出し、
前記再現度算出部は、前記第１の現情報と前記第１の過去情報間の第１の類似度と前記第２の現情報と前記第２の過去情報間の第２の類似度とを算出し、前記第１の類似度と前記第２の類似度の何れもが高くなるほど前記再現度が高くなるように前記再現度を算出する、請求項１または２に記載の生体認証装置。
【請求項４】
コンピュータにより、利用者の生体情報を表すデータを取得し、
前記コンピュータにより、前記利用者の生体情報を表すデータから、当該データ取得時における利用者の生体情報の取得環境の状態を表す現状態情報を抽出し、
前記コンピュータにより、前記現状態情報と過去の生体認証時において利用者の生体情報を表す過去データが取得された際の当該生体情報の取得環境の状態を表す過去状態情報の類似度合いを表す再現度を算出し、
前記コンピュータにより、前記データが前記過去データそのものあるいは前記過去データの一部を改変したものであると推定される閾値と前記再現度を比較し、前記再現度が当該閾値以上である場合、利用者を認証せず、
前記再現度が前記閾値未満である場合、前記利用者を登録利用者として認証するか否かを判定する、
ことを含む生体認証方法。
【請求項５】
利用者の生体情報を表すデータを取得し、
前記利用者の生体情報を表すデータから、当該データ取得時における利用者の生体情報の取得環境の状態を表す現状態情報を抽出し、
前記現状態情報と過去の生体認証時において利用者の生体情報を表す過去データが取得された際の当該生体情報の取得環境の状態を表す過去状態情報の類似度合いを表す再現度を算出し、
前記データが前記過去データそのものあるいは前記過去データの一部を改変したものであると推定される閾値と前記再現度を比較し、前記再現度が当該閾値以上である場合、利用者を認証せず、
前記再現度が前記閾値未満である場合、前記利用者を登録利用者として認証するか否かを判定する、
ことをコンピュータに実行させるための生体認証用コンピュータプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】

本発明は、個人の生体情報を表すデータに基づいて個人を認証するか否かを判定する生体認証装置、生体認証方法及び生体認証用コンピュータプログラムに関する。

【背景技術】

【０００２】

近年、指紋、掌紋、静脈パターン、虹彩、顔、または声といった人の生体情報を利用して、個人を認証するか否か判定する生体認証技術が開発されている。生体認証技術は、入退室管理システム、ボーダーコントロール用システムまたは国民識別番号を用いたシステムといった登録された利用者の数が多い大規模なシステムから、コンピュータまたは携帯端末といった特定の個人が利用する装置まで、広く利用されている。

【０００３】

例えば、生体情報として何れかの指の指紋が利用される場合、生体認証装置は、指紋を表す生体画像を入力生体画像として取得する。そして生体認証装置は、入力生体画像に表された利用者の指紋である入力生体情報を、予め登録された登録利用者の生体画像に表された指紋である登録生体情報と照合する。生体認証装置は、照合処理の結果に基づいて、入力生体情報と登録生体情報が一致すると判定した場合、その利用者を正当な権限を有する登録利用者として認証する。そして生体認証装置は、生体認証装置が組み込まれた装置または生体認証装置と接続された他の装置を認証された利用者が使用することを許可する。

【０００４】

一般に、生体情報の登録時と、照合時とで、生体情報を含む部位の状態が変化していたり、生体情報を取得する際の環境が異なっていることがある。そのため、登録利用者本人が認証を受けようとする場合であっても、入力生体情報と登録生体情報は完全には一致しない。そのため、生体認証装置は、例えば、入力生体情報と登録生体情報間の類似度を算出し、その類似度が所定の認証閾値以上である場合に、入力生体情報と登録生体情報が一致すると判定する。認証閾値が高いほど、登録利用者でない人物を誤ってその登録利用者として認証してしまう、いわゆる他人受入れが発生する確率は低下するものの、登録利用者本人が利用者である場合に認証に失敗する、いわゆる本人拒否が生じる確率は高くなる。一方、認証閾値が低いほど、本人拒否が生じる確率は低下するものの、他人受入れが生じる確率は上昇する。そこで、認証閾値は、他人受入れが生じる確率と本人拒否が生じる確率の何れかが高くなり過ぎないように設定される。そのため、他人受入れが生じる可能性がわずかに残る。そこで、登録利用者でない不正利用者が、不正に認証されることを意図して、生体認証を複数回試みることがある。そのような不正な認証を防ぐために、例えば、生体認証装置は、所定回数以上連続して認証に失敗すると、その利用者の認証を拒否するように設定される。しかし、登録利用者本人が利用者である場合に、本人拒否が連続して生じると、その登録利用者が生体認証装置を利用できなくなってしまう。そこで、認証を失敗したときの生体情報と過去に認証に失敗したときの生体情報とが同一性を有しないときに認証処理の失敗回数のカウンタ値を加算して、カウンタ値が所定値以上になると利用者を認証しない技術が提案されている（例えば、特許文献１を参照）。

【先行技術文献】

【特許文献】

【０００５】

【特許文献１】特開２００６－７９５３７号公報

【発明の概要】

【発明が解決しようとする課題】

【０００６】

しかし、不正利用者が、何らかの方法により照合時に算出される類似度の値（以下では、便宜上照合スコアと呼ぶ）を取得できることがある。このような場合、不正利用者は、入力生体画像の何れかの画素の値、あるいは、特徴点の座標などを少しずつ変更して照合スコアを確認することで照合スコアの向上を図り、不正に認証を受けようとする。これはヒルクライミング攻撃と呼ばれる。

また、不正利用者が、何らかの方法により、過去に認証に成功した時の入力生体画像など、登録利用者の生体情報を表すデータを不正に取得し、そのデータを生体認証装置へ入力することで、不正に認証を受けようとすることがある。これはリプレイ攻撃と呼ばれる。

【０００７】

ヒルクライミング攻撃では、直前の照合時の入力生体画像と、次の照合時の入力生体画像とが同一性を有するように、入力生体画像を僅かに改変させつつ、生体認証装置に生体認証処理を繰り返させることができる。そのため、上記の技術では、失敗回数のカウント値が閾値に達さないうちに、生体認証装置は、不正利用者を誤って認証してしまうおそれがある。

また、リプレイ攻撃では、過去に認証に成功したデータが利用されるので、生体認証装置は、不正利用者を誤って認証してしまうおそれがある。

【０００８】

そこで、一つの側面では、本発明は、リプレイ攻撃またはヒルクライミング攻撃がなされても、不正利用者を誤って認証することを抑制可能な生体認証装置を提供することを目的とする。

【課題を解決するための手段】

【０００９】

一つの実施形態によれば、利用者の生体情報に基づいて、その利用者を登録利用者として認証するか否かを判定する生体認証装置が提供される。この生体認証装置は、過去の生体認証時において利用者の生体情報を表す過去データが取得された際の生体情報の特徴または取得環境の状態を表す過去状態情報を記憶する記憶部と、利用者の生体情報を表すデータを取得する生体情報取得部と、利用者の生体情報を表すデータから、そのデータ取得時における利用者の生体情報の特徴または取得環境の状態を表す現状態情報を抽出する状態情報抽出部と、現状態情報と過去状態情報の類似度合いを表す再現度を算出する再現度算出部と、利用者の生体情報を表すデータが過去データそのものあるいは過去データの一部を改変したものであると推定される閾値と再現度を比較し、再現度がその閾値以上である場合、利用者を認証しない不正アクセス判定部とを有する。

【００１０】

本発明の目的及び利点は、請求項において特に指摘されたエレメント及び組み合わせにより実現され、かつ達成される。

上記の一般的な記述及び下記の詳細な記述の何れも、例示的かつ説明的なものであり、請求項のように、本発明を限定するものではないことを理解されたい。

【発明の効果】

【００１１】

リプレイ攻撃またはヒルクライミング攻撃がなされても、不正利用者を誤って認証することを抑制できる。

【図面の簡単な説明】

【００１２】

【図１】第１の実施形態による生体認証装置の概略構成図である。

【図２】処理部の機能ブロック図である。

【図３】不正利用者によるヒルクライミング攻撃またはリプレイ攻撃が行われた時の再現度の頻度分布と、登録利用者本人が利用者である時の再現度の頻度分布を表す図である。

【図４】第１の実施形態による生体認証処理の動作フローチャートを示す図である。

【図５】一人の登録利用者について、記憶部に記憶されている過去特徴情報のリストの一例を表す図である。

【図６】第２の実施形態による生体認証処理の動作フローチャートを示す図である。

【図７】第３の実施形態による処理部の機能ブロック図である。

【図８】実施形態またはその変形例による、生体認証システムの一例の概略構成図である。

【発明を実施するための形態】
【００１３】
以下、図を参照しつつ、様々な実施形態による、生体認証装置について説明する。
上記のように、ヒルクライミング攻撃またはリプレイ攻撃が行われるときの生体画像に表された生体情報は、過去に同一人物の照合に利用された生体画像に表された生体情報と非常に類似している。一方、登録利用者本人が利用者として認証を求める場合でも、生体情報を表すデータが生成される度に、生体情報を含む部位の状態が異なったり、生体情報撮影時の生体情報を含む部位の姿勢など、撮影時の環境の状態が異なる。そのため、最新の照合時において取得された生体画像に表された生体情報は、過去に照合に利用された生体画像に表された生体情報とある程度異なる。
【００１４】
そこでこの生体認証装置は、利用者の生体情報を表すデータを取得すると、生体情報を表す生体画像からその生体情報の特徴を表す特徴情報を求める。そしてこの生体認証装置は、過去の照合時において取得された生体画像から抽出された特徴情報と今回の照合時における特徴情報の類似度合いである再現度を算出する。そしてこの生体認証装置は、再現度が予め設定された閾値よりも高い場合、ヒルクライミング攻撃またはリプレイ攻撃といった、不正に認証を受ける試みがなされていると判断し、利用者を認証しない。
【００１５】
本実施形態では、生体認証装置は、生体認証に利用する生体情報として何れかの指の指紋を利用する。
また、本明細書において、「照合処理」という用語は、利用者の生体情報と登録利用者の生体情報の相違度合いまたは類似度合いを表す指標を算出する処理を示すために使用される。また、「生体認証処理」という用語は、照合処理だけでなく、照合処理により求められた指標を用いて、利用者を認証するか否かを決定する処理を含む、認証処理全体を示すために使用される。
【００１６】
図１は、一つの実施形態である生体認証装置の概略構成図を示す。図１に示されるように、生体認証装置１は、表示部２と、入力部３と、生体情報取得部４と、記憶部５と、処理部６とを有する。表示部２、入力部３及び生体情報取得部４は、記憶部５と処理部６が収容された筐体とは別個に設けられてもよい。あるいは、表示部２、入力部３、生体情報取得部４、記憶部５及び処理部６は、いわゆるノート型パーソナルコンピュータまたはタブレット型端末のように、一つの筐体に収容されてもよい。また生体認証装置１は、磁気ディスク、半導体メモリカード及び光記憶媒体といった記憶媒体８にアクセスする記憶媒体アクセス装置７をさらに有する。そして生体認証装置１は、例えば、記憶媒体アクセス装置を介して、記憶媒体に記憶された、処理部６上で実行される生体認証処理用のコンピュータプログラムを読み込み、そのコンピュータプログラムに従って生体認証処理を実行してもよい。
【００１７】
生体認証装置１は、生体情報取得部４により生成された利用者の指紋を表す生体画像を用いて、その指紋を登録利用者の指紋と照合することにより、生体認証処理を実行する。そして生体認証装置１は、生体認証処理の結果、利用者を登録利用者の何れかとして認証した場合、生体認証装置１が実装された装置をその利用者が使用することを許可する。あるいは、生体認証装置１は、図示しない他の装置へ、利用者が認証された旨を表す信号を送信して、その利用者が他の装置を使用することを許可する。
【００１８】
表示部２は、例えば、液晶ディスプレイなどの表示装置を有する。そして表示部２は、例えば、照合に用いられる部位（何れかの指）を示すメッセージ、または生体情報取得部４が適正な生体画像を取得可能な位置へその部位を配置させるためのガイダンスメッセージを利用者に対して表示する。また表示部２は、処理部６により実行された生体認証処理の結果を表すメッセージ、あるいはアプリケーションに関連する各種情報などを表示する

。

【００１９】

入力部３は、例えば、キーボード、マウス、またはタッチパッドなどのユーザインターフェースを有する。そして入力部３を介して利用者により入力された利用者のユーザ名あるいはコマンド若しくはデータは、処理部６へ渡される。

【００２０】

生体情報取得部４は、例えば、エリアセンサを用いた指紋センサを有する。この指紋センサは、例えば、光学式、静電容量式、電界式または感熱式の何れかの方式を採用したセンサとすることができる。そして生体情報取得部４は、利用者が指紋センサのセンサ面に指を載置している間に、その指の表面を撮影することにより、指紋が表された生体画像を生成する。この生体画像は、生体情報を表すデータの一例である。

なお、生体情報取得部４は、スライド式の指紋センサを有してもよい。この場合、生体情報取得部４は、指紋センサに対して指をスライドさせている間に、所定の時間間隔で順次部分画像を生成する。部分画像には、その指の表面の指紋の一部が写されており、複数の部分画像を生成された時間順に連結することで、その指の指紋全体が写った生体画像が合成される。

【００２１】

生体情報取得部４は、生体画像を生成する度に、その生体画像を処理部６へ渡す。

【００２２】

記憶部５は、例えば、不揮発性の半導体メモリ及び揮発性の半導体メモリを有する。そして記憶部５は、生体認証装置１で使用されるアプリケーションプログラム、少なくとも一人の登録利用者のユーザ名、ユーザ識別番号及び個人設定情報、各種のデータ等を記憶する。また記憶部５は、生体認証処理を実行するためのプログラムを記憶する。さらに記憶部５は、登録利用者それぞれについて、登録利用者の生体情報である特定の指の指紋の特徴を表す登録特徴情報を、その登録利用者のユーザ名、ユーザ識別番号といった登録利用者の識別情報とともに記憶する。登録特徴情報は、例えば、登録利用者の生体画像そのもの、その生体画像の一部、あるいはその生体画像から抽出された、生体情報の特徴（例えば、隆線の分岐点及び端点の座標、隆線方向など）を含む。

【００２３】

また記憶部５は、登録利用者ごとに、その登録利用者について過去に行われた生体認証処理時に取得された生体画像から抽出された、その生体画像に写った生体情報の特徴を表す特徴情報を、登録利用者の識別情報及び生体画像の取得時刻とともに記憶する。なお、以下では、過去に行われた生体認証処理時に取得された生体画像から抽出された特徴情報を、便宜上、過去特徴情報と呼ぶ。過去特徴情報は、過去状態情報の一例である。

さらに記憶部５は、生体情報取得部４から受け取った生体画像を一時的に記憶してもよい。

【００２４】

処理部６は、１個または複数個のプロセッサ及びその周辺回路を有する。そして処理部６は、生体情報取得部４から取得した生体画像に基づいて、生体認証処理を実行する。

【００２５】

図２は、処理部６の機能ブロック図である。図２に示されるように、処理部６は、特徴情報抽出部１１と、再現度算出部１２と、不正アクセス判定部１３と、照合部１４と、認証判定部１５とを有する。処理部６が有するこれらの各部は、処理部６が有するプロセッサ上で実行されるコンピュータプログラムによって実装される機能モジュールである。あるいは、処理部６が有するこれらの各部は、ファームウェアとして生体認証装置１に実装されてもよい。

【００２６】

特徴情報抽出部１１は、状態情報抽出部の一例であり、生体画像から、生体情報の特徴を表す特徴情報を抽出する。本実施形態では、特徴情報は、上述した再現度の算出及び照合処理に利用される。

【００２７】
特徴情報抽出部１１は、特徴情報として、例えば、指紋の隆線の分岐点及び端点といった特徴的な指紋の構造であるマニューシャの位置を求める。そのために、特徴情報抽出部１１は、例えば、生体画像の各画素の輝度値を２値化して、隆線を表す画素と谷線を表す画素とを区別する。２値化のための閾値は、例えば、生体画像の輝度値の平均値とすることができる。次に特徴情報抽出部１１は、２値化された生体画像について、隆線に相当する輝度値を持つ画素に対して細線化処理を行うことにより、隆線を表す画素が連結した線を、例えば１画素幅を持つ線に細線化する。そして特徴情報抽出部１１は、隆線の分岐点または端点に対応する２値パターンを持つ複数のマスクパターンを用いて細線化された生体画像を走査することにより、何れかのマスクパターンと一致するときの、生体画像上の位置を検出する。そして特徴情報抽出部１１は、検出された位置の中心画素を、マニューシャとし、かつ一致したマスクパターンが表すマニューシャの種類（すなわち、分岐点または端点）を、検出されたマニューシャの種類とする。
【００２８】
なお、特徴情報抽出部１１は、隆線の端点または分岐点をマニューシャとして求める公知の他の方法を用いて、生体画像からマニューシャを抽出してもよい。特徴情報抽出部１１は、抽出されたマニューシャの総数、各マニューシャの種類及び生体画像上の位置座標を特徴情報とする。
あるいは、特徴情報抽出部１１は、生体画像そのもの、あるいは生体画像上の指紋が写った領域を含む一部の領域を生体画像から切り出して、特徴情報としてもよい。
【００２９】
特徴情報抽出部１１は、得られた特徴情報を、過去特徴情報として、入力部３を介して入力された利用者の識別情報、生体画像の取得時刻とともに記憶部５に記憶する。
なお、記憶部５は、再現度の算出に要する演算量を抑制するために、過去特徴情報と関連付けられた生体画像の取得時刻から一定期間が経過すると、その過去特徴情報を消去してもよい。その一定期間は、例えば、１か月、３か月、６か月あるいは１年に設定される。
【００３０】
再現度算出部１２は、最新の照合処理のために得られた生体画像から抽出された特徴情報と過去の照合時に得られた生体画像から抽出された過去特徴情報との間の再現度を算出する。なお、以下では、説明の便宜上、最新の照合処理のために得られた生体画像から抽出された特徴情報を、現特徴情報と呼ぶ。
【００３１】
再現度算出部１２は、入力部３を介して入力された識別情報と一致する登録利用者の識別情報と関連付けられた過去特徴情報を記憶部５から読み込む。そして再現度算出部１２は、現特徴情報と過去特徴情報とを照合することにより再現度を算出する。
【００３２】
特徴情報が生体画像から抽出されたマニューシャの位置を含む場合、再現度算出部１２は、マニューシャマッチングにより再現度を算出する。再現度算出部１２は、例えば、現特徴情報に含まれるマニューシャのうちの注目するマニューシャを、過去特徴情報に含まれるマニューシャの何れかと位置合わせする。そして再現度算出部１２は、現特徴情報に含まれるマニューシャのうち、過去特徴情報に含まれるマニューシャと一致するマニューシャの数を求める。なお、再現度算出部１２は、二つのマニューシャ間の距離が、例えば、隆線間隔以下であれば、その二つのマニューシャは一致すると判定する。また再現度算出部１２は、二つのマニューシャの種類が一致する場合に限り、その二つのマニューシャが一致すると判定してもよい。
【００３３】
再現度算出部１２は、位置合わせをするマニューシャの組を変えつつ、一致するマニューシャの数を求める。そして再現度算出部１２は、一致するマニューシャの数が最大となる時の、現特徴情報に含まれるマニューシャの総数に対する、一致するマニューシャの数

の比を再現度とする。この場合、再現度は、0～1の何れかの値をとる。

【００３４】

また、特徴情報が、生体画像そのもの、あるいは生体画像の一部を含む場合、再現度算出部１２は、パターンマッチングにより再現度を算出してもよい。この場合、再現度算出部１２は、現特徴情報に含まれる生体画像と過去特徴情報に含まれる生体画像間の相対的な位置を変えつつ、正規化相互相関値を算出する。そして再現度算出部１２は、その正規化相互相関値の最大値を再現度とする。正規化相互相関値は、-1～1の何れかの値をとるので、この場合、再現度も-1～1の何れかの値となる。しかし、再現度の値が0～1の範囲に含まれるように、再現度算出部１２は、再現度の値を正規化してもよい。

【００３５】

再現度算出部１２は、算出した再現度を不正アクセス判定部１３へ通知する。

なお、入力部３を介して入力された識別情報と一致する登録利用者の識別情報と関連付けられた過去特徴情報が複数存在する場合、再現度算出部１２は、過去特徴情報ごとに再現度を算出する。そして再現度算出部１２は、過去特徴情報ごとの再現度のうちの最大値を求め、再現度の最大値を不正アクセス判定部１３へ通知する。

【００３６】

不正アクセス判定部１３は、再現度算出部１２から通知された再現度を不正判定閾値と比較する。不正アクセス判定部１３は、再現度が不正判定閾値以上である場合、生体認証装置１に対して、ヒルクライミング攻撃またはリプレイ攻撃といった、不正なアクセスが試みられたと判定する。そして不正アクセス判定部１３は、生体認証処理の続行を拒否する。不正アクセス判定部１３は、生体認証処理の続行を拒否したことを処理部６へ通知する。この場合、処理部６は、利用者を認証せず、生体認証装置１が実装された装置あるいは生体認証装置１が接続された装置を利用者が使用することを拒否する。また処理部６は、表示部２に、不正アクセスが試みられたことを示す警告メッセージを表示させてもよい。さらに、処理部６は、生体認証装置１の管理者が許可するまで、あるいは、一定期間にわたって、入力部３を介して入力された識別情報で特定される登録利用者についての生体認証処理の実行を受け付けないようにしてもよい。一定期間は、例えば、１日、あるいは１週間とすることができる。

一方、再現度が不正判定閾値未満である場合、不正アクセス判定部１３は、不正なアクセスは行われていないと判定し、その判定結果を処理部６へ通知する。

【００３７】

図３は、不正利用者によるヒルクライミング攻撃またはリプレイ攻撃が行われた時の再現度の頻度分布と、登録利用者本人が利用者である時の再現度の頻度分布を表す図である。図３において、横軸は再現度を表し、縦軸は頻度を表す。グラフ３０１は、不正利用者によるヒルクライミング攻撃またはリプレイ攻撃が行われた時の再現度の頻度分布を表す。またグラフ３０２は、登録利用者本人が利用者である時の再現度の頻度分布を表す。リプレイ攻撃が行われた時の現特徴情報と過去特徴情報とは同一であるので、再現度は1となる。また、ヒルクライミング攻撃が行われた時の現特徴情報と過去特徴情報との差は非常に小さいので、再現度は1に近い値となる。そのため、グラフ３０１に示されるように、再現度は、その取り得る最大値（本実施形態では、１）の近くに分布する。一方、登録利用者本人が利用者である場合には、生体情報を含む部位の状態などのばらつきにより、グラフ３０２に示されるように、再現度は、ヒルクライミング攻撃などの不正アクセスがおこなわれたときよりも低い値、例えば、0.6～0.7を中心に分布する。そのため、不正判定閾値は、例えば、現特徴情報の抽出に利用された生体画像が過去特徴情報の抽出に利用された過去生体画像そのものあるいは過去生体画像の一部を改変したものであると推定されるときの再現度の下限値に設定される。すなわち、不正判定閾値は、例えば、上記の二つの分布の間、例えば、0.8に設定される。あるいは、不正判定閾値は、リプレイ攻撃などの不正アクセスが行われた時の再現度の平均値と不正判定閾値間のマハラノビス距離と、登録利用者本人が利用者である時の再現度の平均値と不正判定閾値間のマハラノビス距離が等しくなるように設定されてもよい。

【００３８】
不正アクセス判定部１３が不正なアクセスは行われていないと判定した場合、処理部６は、生体認証処理を続行する。そのために、処理部６は、入力部３を介して入力された識別情報により特定される登録利用者の生体情報の特徴を表す登録特徴情報を記憶部５から読み込む。なお、登録特徴情報は、現特徴情報と同様に、登録時において生体認証装置１が取得した、登録利用者の生体情報が表された生体画像から抽出される。
処理部６は、現特徴情報と登録特徴情報を照合部１４へ渡す。
【００３９】
照合部１４は、現特徴情報と登録特徴情報を照合することにより、利用者の生体情報と登録利用者の生体情報の類似度を算出する。
【００４０】
照合部１４は、例えば、現特徴情報及び登録特徴情報が、それぞれ、隆線の端点、分岐点などのマニューシャの座標を含む場合、マニューシャマッチングにより類似値を算出する。あるいは、現特徴情報及び登録特徴情報が、それぞれ、生体画像そのもの、あるいは生体画像の一部を含む場合には、照合部１４は、それら生体画像間のパターンマッチングによって類似度を算出してもよい。
なお、マニューシャマッチング及びパターンマッチングの手順は、再現度算出部１２にて説明した手順と同様である。
【００４１】
照合部１４は、類似度を、登録利用者の識別情報とともに、認証判定部１５へ渡す。
【００４２】
認証判定部１５は、類似度が認証判定閾値以上となるか否か判定する。類似度が認証判定閾値以上である場合、認証判定部１５は、利用者の生体情報は照合部１４から受け取った識別情報によって特定される登録利用者の生体情報と一致すると判定する。そして認証判定部１５は、利用者を、その登録利用者として認証する。認証判定部１５は、利用者を認証すると、その認証結果を処理部６へ通知する。そして処理部６は、生体認証装置１が実装された装置あるいは生体認証装置１が接続された装置を認証された利用者が利用することを許可する。
【００４３】
一方、類似度が認証判定閾値未満である場合、認証判定部１５は利用者の生体情報は登録利用者の生体情報と一致しないと判定する。そのため、認証判定部１５は利用者を認証しない。そして認証判定部１５は、認証に失敗したことを処理部６へ通知する。この場合、処理部６は、生体認証装置１が実装された装置あるいは生体認証装置１が接続された装置を認証されなかった利用者が使用することを拒否する。また処理部６は、表示部２に、認証に失敗したことを示すメッセージを表示させてもよい。なお、不正アクセスの検知によって生体認証処理の実行が拒否される場合と異なり、生体認証装置１は、認証に失敗した登録利用者についても、生体情報を読み取り直して再度生体認証処理を実行してもよい。
【００４４】
なお、認証判定閾値は、登録利用者本人が利用者である場合にのみ、認証判定部１５が認証に成功するような値に設定されることが好ましい。そして認証判定閾値は、登録利用者とは異なる他人が利用者である場合には、認証判定部１５が認証に失敗するような値に設定されることが好ましい。例えば、認証判定閾値は、類似度の取りうる最大値と最小値の差に0.6を乗じた値を、類似度の最小値に加えた値とすることができる。
【００４５】
また、再現度と類似度が同じ種類の特徴情報に基づいて算出される場合、本人拒否が生じる確率を低減するために、認証判定閾値は、不正判定閾値よりも低く設定されることが好ましい。再現度と類似度が同じ種類の特徴情報に基づいて算出される場合には、再現度の分布形状と類似度の分布形状は似たものとなる。そのため、認証判定閾値が不正判定閾値以上に設定されていると、再現度が不正判定閾値以下となるときには、類似度も認証判

定閾値以下となる可能性が高いためである。

【００４６】

図４は、本実施形態による、生体認証処理の動作フローチャートである。

処理部６は、入力部３を介して照合対象となる登録利用者の識別情報を取得する（ステップＳ１０１）。また処理部６は、生体情報取得部４から、利用者の生体画像を取得する（ステップＳ１０２）。

【００４７】

処理部６の特徴情報抽出部１１は、生体画像から現特徴情報を抽出し、記憶部５に記憶する（ステップＳ１０３）。また特徴情報抽出部１１は、現特徴情報を処理部６の再現度算出部１２へ通知する。再現度算出部１２は、現特徴情報と識別情報により特定される登録利用者の過去特徴情報間の再現度の最大値を算出する（ステップＳ１０４）。そして再現度算出部１２は、その最大値を処理部６の不正アクセス判定部１３へ通知する。

【００４８】

不正アクセス判定部１３は、再現度の最大値は不正判定閾値以上か否か判定する（ステップＳ１０５）。再現度の最大値が不正判定閾値以上である場合（ステップＳ１０５－Ｙｅｓ）、不正アクセス判定部１３は、リプレイ攻撃またはヒルクライミング攻撃といった不正アクセスが行われたと判定する。そして不正アクセス判定部１３は、利用者を認証せず、生体認証処理の続行を拒否する（ステップＳ１０６）。そして不正アクセス判定部１３は、その旨を処理部６に通知する。処理部６は、生体認証処理を中断する。

【００４９】

一方、再現度の最大値が不正判定閾値未満である場合（ステップＳ１０５－Ｎｏ）、不正アクセス判定部１３は、不正アクセスが行われていないと判定し、その判定結果を処理部６に通知する。この場合、処理部６の照合部１４は、現特徴情報と登録利用者の登録特徴情報間の類似度を算出する（ステップＳ１０７）。そして照合部１４は、類似度を処理部６の認証判定部１５に通知する。

認証判定部１５は、類似度が認証判定閾値以上か否か判定する（ステップＳ１０８）。類似度が認証判定閾値以上である場合（ステップＳ１０８－Ｙｅｓ）、認証判定部１５は、利用者の生体情報と登録利用者の生体情報は一致すると判定する。そして認証判定部１５は、利用者を認証する（ステップＳ１０９）。

一方、類似度が認証判定閾値未満である場合（ステップＳ１０８－Ｎｏ）、認証判定部１５は、利用者の生体情報と登録利用者の生体情報は一致しないと判定する。そして認証判定部１５は、利用者を認証しない（ステップＳ１１０）。

ステップＳ１０９またはＳ１１０の後、処理部６は、生体認証処理を終了する。

【００５０】

なお、ステップＳ１０１とＳ１０２の順序は入れ換わってもよい。あるいは、処理部６は、ステップＳ１０８にて類似度が認証判定閾値以上である場合に限り、ステップＳ１０４～Ｓ１０６の処理を実行してもよい。

【００５１】

以上に説明してきたように、この生体認証装置は、現特徴情報と登録特徴情報間の類似度とは別個に、現特徴情報と過去特徴情報間の再現度を算出し、その再現度に基づいて不正アクセスが行われたか否かを判定する。そのため、この生体認証装置は、認証用判定閾値を高くすることなく、すなわち、本人拒否が生じる確率が高くならないようにしつつ、ヒルクライミング攻撃などの不正アクセスによる他人受入れを抑制できる。

【００５２】

次に、第２の実施形態による生体認証装置について説明する。第２の実施形態による生体認証装置は、再現度算出部が、再現度の算出対象となる過去特徴情報を、ヒルクライミング攻撃を検知する場合とリプレイ攻撃を検知する場合とで異ならせる。

【００５３】

第２の実施形態による生体認証装置は、第１の実施形態による生体認証装置と比較して、処理部の一部の機能が異なる。そこで以下では、処理部の機能のうちの異なる点につい

て説明する。第２の実施形態による生体認証装置のその他の構成要素の詳細については、第１の実施形態による生体認証装置の対応する構成要素の説明を参照されたい。

【００５４】

本実施形態では、記憶部５は、過去特徴情報を、登録利用者の識別情報及び過去特徴情報が抽出された生体画像の取得時刻の他に、その過去特徴情報を用いた生体認証処理が成功したか否かを表すフラグとともに記憶する。

【００５５】

再現度算出部１２は、リプレイ攻撃がなされたか否かを判定するために、入力部３を介して取得された識別情報に対応する登録利用者の過去特徴情報のうち、生体認証処理が成功したことを表すフラグが付された過去特徴情報を記憶部５から読み込む。そして再現度算出部１２は、読み込んだ過去特徴情報のそれぞれと、現特徴情報間の再現度を算出する。そして再現度算出部１２は、それら再現度のうちの最大値を、リプレイ攻撃判定用再現度とする。

【００５６】

不正アクセス判定部１３は、リプレイ攻撃判定用再現度が不正判定閾値以上である場合、リプレイ攻撃による不正アクセスが行われたと判定する。そして不正アクセス判定部１３は、生体認証処理を中止する。

【００５７】

一方、リプレイ攻撃判定用再現度が不正判定閾値未満であり、かつ、認証に失敗した場合、再現度算出部１２は、現特徴情報と同じセッションに含まれる過去特徴情報のうち、認証に失敗した過去特徴情報のそれぞれと現特徴情報間の再現度を算出する。そして再現度算出部１２は、それら再現度のうちの最大値を、ヒルクライミング攻撃判定用再現度とする。

【００５８】

本実施形態において、「セッション」は、利用者が生体認証の試行を開始してから現特徴情報を取得するまでの間に繰り返された、一連の生体認証処理を表す。本実施形態では、再現度算出部１２は、連続して取得された二つの生体画像の取得時間の間隔が所定時間未満である場合、その二つの生体画像に対応する過去特徴情報は同一セッションに含まれると判定する。なお、所定時間は、例えば、１分に設定される。

【００５９】

ヒルクライミング攻撃では、生体情報が表された画像または特徴情報の一部の変更を繰り返しながら、認証に成功するまで、何度も生体認証処理が実行される。そのため、上記のように、現特徴情報と同じセッション内の、認証に失敗したときの過去特徴情報との間で再現度を算出することにより、処理部６は、ヒルクライミング攻撃が行われたか否かを正確に判定できる。

【００６０】

図５は、一人の登録利用者について、記憶部５に記憶されている過去特徴情報のリストの一例を表す図である。このリスト５００を用いて、過去特徴情報とセッションの関係について説明する。

リスト５００の各行には、記憶部５に記憶された順に、一つの過去特徴情報が格納されている。そしてリスト５００の左端の各欄には、過去特徴情報の番号が格納されている。またリスト５００の左から２番目の列の各欄には、過去特徴情報が抽出された生体画像の取得時刻が格納されている。またリスト５００の左から３番目の列の各欄には、生体認証に成功したか否かを表すフラグが格納されている。この例では、フラグが’１’であれば認証に成功したことを表し、フラグが’０’であれば認証に失敗したことを表す。そしてリスト５００の右端の列の各欄には、過去特徴情報が格納されている。以下では、過去特徴情報が抽出された生体画像の取得時刻を、単に取得時刻と呼ぶ。この例では、１番目の過去特徴情報の取得時刻と２番目の過去特徴情報の取得時刻の差は１分よりも長いので、１番目の過去特徴情報は、２番目以降の過去特徴情報とは別のセッションに属する。一方、２番目の過去特徴情報の取得時刻と３番目の過去特徴情報の取得時刻の差、及び、３番

目の過去特徴情報の取得時刻と４番目の過去特徴情報の取得時刻の差は、何れも１分未満であるため、２番目～４番目の過去特徴情報は、同一セッションに属する。そのため、例えば、４番目の過去特徴情報が得られたとき、再現度算出部１２は、リスト５００の２番目及び３番目の過去特徴情報について、ヒルクライミング攻撃判定のための再現度を算出する。

【００６１】

不正アクセス判定部１３は、ヒルクライミング攻撃判定用再現度が不正判定閾値以上である場合、ヒルクライミング攻撃による不正アクセスが行われたと判定する。そして不正アクセス判定部１３は、生体認証処理を中止する。

【００６２】

一方、ヒルクライミング攻撃判定用再現度が不正判定閾値未満であれば、不正アクセス判定部１３は、不正アクセスは行われていないと判定する。

【００６３】

なお、ヒルクライミング攻撃判定用再現度に対する不正判定閾値は、リプレイ攻撃判定用再現度に対する不正判定閾値よりも低く設定されてもよい。リプレイ攻撃では、その特性上、再現度が1になるので、不正判定閾値も1または非常に1に近い値、例えば、0.99に設定できる。一方、ヒルクライミング攻撃では、現特徴情報と過去特徴情報の一部が相違している可能性が高いので、再現度は1未満となる可能性が高い。そのため、ヒルクライミング攻撃判定用再現度に対する不正判定閾値を、リプレイ攻撃判定用再現度に対する不正判定閾値よりも低く設定することで、不正アクセス判定部１３は、それぞれの攻撃が行われたか否かをより適切に判定できる。

【００６４】

認証判定部１５は、リプレイ攻撃による不正アクセスが行われていないと判定した場合において、認証に成功すると、記憶部５に記憶されている現特徴情報に、認証に成功したことを表すフラグを付す。一方、認証判定部１５は、認証に失敗すると、記憶部５に記憶されている現特徴情報に、認証に失敗したことを表すフラグを付す。

【００６５】

図６は、第２の実施形態による、生体認証処理の動作フローチャートである。

処理部６は、入力部３を介して照合対象となる登録利用者の識別情報を取得する（ステップＳ２０１）。また処理部６は、生体情報取得部４から、利用者の生体画像を取得する（ステップＳ２０２）。

【００６６】

処理部６の特徴情報抽出部１１は、生体画像から現特徴情報を抽出し、生体画像の取得時刻とともに記憶部５に記憶する（ステップＳ２０３）。また特徴情報抽出部１１は、現特徴情報を処理部６の照合部１４及び再現度算出部１２へ通知する。

【００６７】

照合部１４は、現特徴情報と入力部３を介して入力された識別情報に対応する登録利用者の登録特徴情報間の類似度を算出する（ステップＳ２０４）。そして照合部１４は、類似度を処理部６の認証判定部１５に通知する。

認証判定部１５は、類似度が認証判定閾値以上か否か判定する（ステップＳ２０５）。類似度が認証判定閾値以上である場合（ステップＳ２０５－Ｙｅｓ）、認証判定部１５は、利用者の生体情報と登録利用者の生体情報は一致すると判定し、その旨を再現度算出部１２へ通知する。

【００６８】

再現度算出部１２は、識別情報により特定される登録利用者の過去特徴情報のうち、認証に成功したときの過去特徴情報と、現特徴情報との間の再現度の最大値を算出する（ステップＳ２０６）。そして再現度算出部１２は、その最大値をリプレイ攻撃判定用再現度として処理部６の不正アクセス判定部１３へ通知する。

【００６９】

不正アクセス判定部１３は、リプレイ攻撃判定用再現度は不正判定閾値以上か否か判定

する（ステップＳ２０７）。リプレイ攻撃判定用再現度が不正判定閾値以上である場合（ステップＳ２０７－Ｙｅｓ）、不正アクセス判定部１３は、リプレイ攻撃が行われたと判定する。そして不正アクセス判定部１３は、生体認証処理の続行を拒否する（ステップＳ２０８）。そして不正アクセス判定部１３は、その旨を処理部６に通知する。処理部６は、生体認証処理を中断し、利用者を認証しない。

【００７０】

一方、リプレイ攻撃判定用再現度が不正判定閾値未満である場合（ステップＳ２０７－Ｎｏ）、不正アクセス判定部１３は、不正アクセスが行われていないと判定し、その判定結果を認証判定部１５に通知する。そして認証判定部１５は、利用者を認証する（ステップＳ２０９）。また認証判定部１５は、記憶部５に記憶されている現特徴情報に、認証に成功したことを表すフラグを付す。

【００７１】

一方、ステップＳ２０５にて、類似度が認証判定閾値未満である場合（ステップＳ２０５－Ｎｏ）、認証判定部１５は、利用者の生体情報と登録利用者の生体情報は一致しないと判定し、その旨を再現度算出部１２へ通知する。この場合、再現度算出部１２は、識別情報により特定される登録利用者の過去特徴情報のうち、現特徴情報と同じセッションに含まれ、かつ、認証に失敗したときの過去特徴情報と現特徴情報間の再現度を算出する。そして再現度算出部１２は、その再現度のうちの最大値をヒルクライミング攻撃判定用再現度として算出する（ステップＳ２１０）。

【００７２】

不正アクセス判定部１３は、ヒルクライミング攻撃判定用再現度は不正判定閾値以上か否か判定する（ステップＳ２１１）。ヒルクライミング攻撃判定用再現度が不正判定閾値以上である場合（ステップＳ２１１－Ｙｅｓ）、不正アクセス判定部１３は、ヒルクライミング攻撃が行われたと判定する。そして不正アクセス判定部１３は、生体認証処理の続行を拒否する（ステップＳ２１２）。そして不正アクセス判定部１３は、その旨を処理部６に通知する。処理部６は、生体認証処理を中断し、利用者を認証しない。

【００７３】

一方、ヒルクライミング攻撃判定用再現度が不正判定閾値未満である場合（ステップＳ２１１－Ｎｏ）、不正アクセス判定部１３は、不正アクセスが行われていないと判定し、その判定結果を認証判定部１５に通知する。認証判定部１５は、記憶部５に記憶されている現特徴情報に、認証に失敗したことを表すフラグを付す。また処理部６は、認証に失敗した旨のメッセージを表示部２に表示させ、利用者に生体情報の再入力を促す（ステップＳ２１３）。その後、生体情報の再入力が行われれば、処理部６は、ステップＳ２０１以降の処理を繰り返す。

【００７４】

この実施形態によれば、生体認証装置は、リプレイ攻撃とヒルクライミング攻撃とを区別して検知することができる。またこの生体認証装置は、リプレイ攻撃を検知する際の不正判定閾値とヒルクライミング攻撃を検知する際の不正判定閾値とを個別に設定できるので、それぞれの攻撃が行われたか否かをより適切に判定できる。

【００７５】

次に、第３の実施形態について説明する。第３の実施形態では、生体認証装置は、最新の生体認証処理の実行時の生体情報と過去の生体認証処理の実行時の生体情報の類似性だけでなく、それぞれの生体情報取得時における環境条件の類似性も考慮して再現度を算出する。

【００７６】

第３の実施形態による生体認証装置は、第１の実施形態による生体認証装置と比較して、処理部の一部の機能が異なる。そこで以下では、処理部の機能のうちの異なる点について説明する。第３の実施形態による生体認証装置のその他の構成要素の詳細については、第１の実施形態による生体認証装置の対応する構成要素の説明を参照されたい。

【００７７】

図７は、第３の実施形態による処理部６１の機能ブロック図である。図７に示されるように、処理部６１は、特徴情報抽出部１１と、再現度算出部１２と、不正アクセス判定部１３と、照合部１４と、認証判定部１５と、環境情報抽出部１６とを有する。処理部６１が有するこれらの各部は、処理部６１が有するプロセッサ上で実行されるコンピュータプログラムによって実装される機能モジュールである。あるいは、処理部６１が有するこれらの各部は、ファームウェアとして生体認証装置１に実装されてもよい。

図７において、処理部６１の各部には、図２に示された処理部６の対応する構成要素と同じ参照番号を付した。第３の実施形態による処理部６１は、第１の実施形態による処理部６と比較して、環境情報抽出部１６を有する点で異なる。

【００７８】

環境情報抽出部１６は、状態情報抽出部の他の一例であり、処理部６１が生体情報取得部４から生体画像を受け取る度に、その生体情報読み取り時の環境状態を表す環境情報を求める。例えば、生体認証に利用される生体情報が指紋または掌紋である場合、生体画像に写った隆線の幅の平均値を環境情報とする。一般に、隆線の幅は、生体情報取得部４のセンサ面に対して指を押圧する力が強いほど広くなるので、隆線の幅は、指を押圧する力の度合いを表している。このように、隆線の幅は、生体情報読み取り時の環境状態を表している。

【００７９】

環境情報抽出部１６は、例えば、生体画像の各画素の輝度値を２値化して、隆線を表す画素と谷線を表す画素とを区別する。そして環境情報抽出部１６は、例えば、２値化された生体画像と、指紋の渦中心を表すテンプレートとのテンプレートマッチングにより、２値化された生体画像上で渦中心を検出する。そして環境情報抽出部１６は、渦中心から放射状に走査線を設定する。一般に、渦中心から指の先端側では、隆線は、渦中心を中心とする略同心円状となっている。そこで環境情報抽出部１６は、走査線に沿って、隆線に相当する輝度を持つ画素の連続数の平均値を算出し、その平均値を隆線の幅とする。

【００８０】

あるいは、環境情報抽出部１６は、生体画像において、生体情報を含む部位が写っている領域である被写体領域の面積、または被写体領域の重心位置を環境情報として求めてもよい。被写体領域の面積及び被写体領域の重心位置も、生体情報取得部４のセンサ面に対する指の置き方に関する情報を表している。

あるいは、環境情報抽出部１６は、隆線に相当する画素の輝度平均値と谷線に相当する画素の輝度平均値との差をコントラストとして算出し、そのコントラストを環境情報としてもよい。この差は、例えば、生体画像取得時における、指の表面の乾燥度合いに応じて変化する。

あるいまた、環境情報抽出部１６は、環境情報として、複数の特徴量、例えば、隆線の幅、被写体領域の重心の位置及びコントラストのうちの少なくとも二つを求めてもよい。

【００８１】

環境情報抽出部１６は、環境情報を、特徴情報抽出部１１により抽出された特徴情報、入力部３を介して入力された利用者の識別情報、生体画像の取得時刻とともに記憶部５に記憶する。

なお、記憶部５は、再現度の算出に要する演算量を抑制するために、特徴情報及び環境情報が記憶されてから一定期間が経過すると特徴情報及び環境情報を消去してもよい。その一定期間は、例えば、１か月、３か月、６か月あるいは１年に設定される。

【００８２】

再現度算出部１２は、最新の生体認証実行時の特徴情報である現特徴情報と過去の生体認証実行時の特徴情報である過去特徴情報とに基づいて算出される再現度（以下では、この再現度を生体再現度と呼ぶ）を算出する。また再現度算出部１２は、最新の生体認証実行時の環境情報である現環境情報と過去の生体認証実行時の環境情報である過去環境情報とに基づいて算出される再現度（以下では、この再現度を環境再現度と呼ぶ）を算出する。そして再現度算出部１２は、生体再現度に環境再現度を乗じて得られる値を、再現度と

して算出する。
あるいは、再現度算出部１２は、生体再現度と環境再現度の平均値を再現度としてもよい。
【００８３】
なお、再現度算出部１２は、例えば、環境再現度を次式に従って算出する。
【数１】

$$Cr = \frac{1}{1+\sum_{m}\left(\frac{x_m(n)-x_m(n-1)}{x_m(n)}\right)^2} \qquad (1)$$

ここでCrは環境再現度を表す。$x_m(n)$は、現環境条件に含まれる、m番目の要素の値を表し、$x_m(n-1)$は、過去環境条件に含まれる、m番目の要素の値を表す。
【００８４】
環境再現度Crは、現環境条件に含まれる全ての要素と過去環境条件に含まれる全ての要素が一致する場合に1となり、対応する要素間の値の差が大きくなるほど小さくなる。
【００８５】
一般に、生体情報の入力時、すなわち、生体画像の作成時の環境は、生体認証の実行時ごとに変動する。そのため、環境再現度は相対的に低い値、例えば、0.7となる。また上述したように、登録利用者本人が利用者であっても、生体再現度はばらつく。そのため、登録利用者本人が利用者であっても、生体再現度及び環境再現度の両方とも、それほど高くならず、その結果、再現度も相対的に低くなる。例えば、登録利用者本人が利用者であっても、生体再現度が0.7、環境再現度が0.7となり、再現度が0.49となる。
【００８６】
一方、ヒルクライミング攻撃では、過去の生体認証処理に利用された生体情報を表すデータ（例えば、生体画像）の一部または生体情報の一部が変更されたものが最新の生体認証処理で利用される。そのため、現特徴情報と過去特徴情報間の差が非常に小さいだけでなく、現環境情報と過去環境情報との差も非常に小さい。したがって、環境再現度及び生体再現度の両方が、1または1に近い値を持つ。その結果として、再現度も1または1に近い値となる。ヒルクライミング攻撃が行われている場合、例えば、生体再現度が0.9、環境再現度が0.9となり、再現度が0.81となる。
【００８７】
さらに、リプレイ攻撃では、過去の生体認証処理で成功したときの生体情報を表すデータが最新の生体認証処理においてそのまま利用されるので、そのようなデータから求められる特徴情報だけでなく、環境情報も変化しない。したがって、環境再現度及び生体再現度の両方が、1となる。その結果として、再現度も1となる。
【００８８】
このように、特徴情報だけでなく、環境情報も参照して再現度を算出することにより、ヒルクライミング攻撃またはリプレイ攻撃が行われた時の再現度と、登録利用者本人が利用者である場合の再現度との差が大きくなる。そのため、生体認証装置は、ヒルクライミング攻撃またはリプレイ攻撃といった不正アクセスの検出精度を向上できる。
【００８９】
なお、変形例によれば、再現度算出部は、環境再現度そのものを再現度としてもよい。上述したように、ヒルクライミング攻撃またはリプレイ攻撃が行われた時には、現環境条件と過去環境条件の差は比較的小さく、登録利用者本人が利用者である場合の現環境条件と過去環境条件の差は比較的大きいためである。
【００９０】

また、他の変形例によれば、第２の実施形態による再現度算出部が、第３の実施形態による再現度算出部のように、環境再現度と生体再現度に基づいて再現度を算出してもよい。

【００９１】

さらに他の変形例によれば、再現度の算出に利用される特徴情報と、照合処理に利用される特徴情報は異なっていてもよい。例えば、再現度が、現特徴情報に含まれるマニューシャと過去特徴情報に含まれるマニューシャとのマニューシャマッチングによって算出される場合、照合部は、利用者の生体画像と登録利用者の生体画像間のパターンマッチングによって類似度を算出してもよい。逆に、再現度が、現特徴情報及び過去特徴情報に含まれる生体画像間のパターンマッチングによって算出される場合、照合部は、マニューシャマッチングにより類似度を算出してもよい。

【００９２】

また、生体認証に利用される生体情報は、指紋に限られない。生体認証に利用される生体情報は、掌紋、静脈パターン、虹彩、顔または声紋であってもよい。例えば、生体認証に利用される生体情報が掌紋である場合には、生体認証装置は、上記と同様の処理によって再現度、生体再現度及び環境再現度を算出できる。また生体情報が静脈パターンである場合も、生体認証装置は、その静脈パターンが写った生体画像に対して、例えば、静脈パターンの特徴的な部分を表すテンプレートを用いたテンプレートマッチングにより、その部分の位置を特徴情報として求めればよい。なお、静脈パターンの特徴的な部分として、例えば、静脈の分岐点が利用できる。さらに、生体認証装置は、生体画像上での静脈パターンを含む部位（手のひら）の重心位置または面積などを環境情報として求めればよい。同様に、生体認証に利用される生体情報が顔である場合も、生体認証装置は、その顔が写った生体画像に対して、例えば、顔の特徴点を表すテンプレートを用いたテンプレートマッチングにより、その特徴点の位置を特徴情報として求めればよい。なお、顔の特徴点は、例えば、目頭、目尻、鼻尖点、口角など、顔上の特徴的な部位の一部とすることができる。さらに、生体認証装置は、生体画像上での顔が写っている領域の平均輝度値、あるいは顔の向きなどを環境情報として求めればよい。なお、顔の向きは、例えば、両目の目頭間の中点と口の中点とを結ぶ線に対する、鼻尖点の相対的な位置により推定される。

【００９３】

さらに、生体情報として声紋が利用される場合には、生体認証装置は、生体情報取得部としてマイクロホンを有してもよい。そして生体認証装置は、マイクロホンを介して利用者の音声を集音することにより生成された、生体情報を含むデータの一例である音声データを解析して、メル周波数ケプストラム係数などを特徴情報として算出してもよい。さらに、生体認証装置は、環境情報として、音声データに含まれるノイズ成分の強度などを算出してもよい。

【００９４】

図８は、上記の各実施形態またはその変形例による生体認証装置が実装された、生体認証システムの一例の概略構成図である。

例えば、生体認証システム１００は、少なくとも１台の端末１１０とサーバ１２０とを有する。そして端末１１０とサーバ１２０は、有線または無線の通信ネットワーク１３０を介して接続される。なお、図８において、生体認証システム１００が有する構成要素のうち、図１に示した生体認証装置１が有する構成要素の何れかと対応する構成要素には、生体認証装置１が有する構成要素の参照番号と同じ参照番号を付した。

【００９５】

このシステムでは、端末１１０は、例えば、携帯電話機またはタブレット型端末といった携帯端末、あるいは、固定的に設置される端末であり、表示部２、入力部３及び生体情報取得部４を有する。さらに、端末１１０は、記憶部２１と、画像取得制御部２２と、インターフェース部２３とを有する。

記憶部２１は、例えば、半導体メモリ回路を有し、生体情報取得部４により生成された生体画像を一時的に記憶する。また画像取得制御部２２は、一つまたは複数のプロセッサ

とその周辺回路とを有し、端末１１０の各部を制御し、かつ、端末１１０で動作する各種のプログラムを実行する。そして画像取得制御部２２は、生体情報取得部４により生成された生体画像を、端末１１０の識別情報とともに、端末１１０を通信ネットワーク１３０と接続するためのインターフェース回路を有するインターフェース部２３を介してサーバ１２０へ送信する。さらに画像取得制御部２２は、入力部３を介して入力されたユーザ識別情報もサーバ１２０へ送信してもよい。

【００９６】

サーバ１２０は、記憶部５と、処理部６と、サーバ１２０を通信ネットワーク１３０と接続するためのインターフェース回路を有するインターフェース部２４とを有する。サーバ１２０の処理部６は、インターフェース部２４を介して受信した生体画像を用いて、上記の各実施形態の何れかまたはその変形例による処理部が有する各部の機能を実現することにより、生体認証処理を実行する。そしてサーバ１２０は、認証に成功したか否かの判定結果を、インターフェース部２４を介して端末１１０へ返信する。

【００９７】

あるいは、端末１１０の画像取得制御部２２が、上記の各実施形態による処理部の機能のうち、特徴情報抽出部及び／または環境情報抽出部の処理を実行してもよい。この場合、端末１１０からサーバ１２０へ、利用者の生体画像から抽出された特徴情報及び／または環境情報と利用者の識別情報と端末１１０の識別情報がサーバ１２０へ送信されてもよい。一方、サーバ１２０の処理部６は、上記の各実施形態による処理部の機能のうち、再現度算出部、不正アクセス判定部、照合部及び認証判定部の処理のみを実行する。これにより、サーバ１２０の負荷が軽減されるので、同時に多数の生体認証処理が実行されても、生体認証システム１００は、利用者に対する待ち時間を抑制できる。

【００９８】

上記のシステムでは、サーバ１２０は、特徴情報とともに、その特徴情報が抽出された生体画像を生成した端末１１０の識別情報を記憶部５に記憶してもよい。この場合、サーバ１２０の処理部６は、不正アクセスが試みられたと判定したときに、その判定が行われた生体認証処理を要求した端末１１０について、一定期間の間、生体認証処理の要求を受け付けないようにしてもよい。

【００９９】

また、上記の各実施形態による処理部の機能をコンピュータに実現させる命令を有するコンピュータプログラムは、磁気記録媒体、光記録媒体あるいは不揮発性の半導体メモリといった、記録媒体に記録された形で提供されてもよい。なお、コンピュータ読取可能な記録媒体には、搬送波は含まれない。

【０１００】

ここに挙げられた全ての例及び特定の用語は、読者が、本発明及び当該技術の促進に対する本発明者により寄与された概念を理解することを助ける、教示的な目的において意図されたものであり、本発明の優位性及び劣等性を示すことに関する、本明細書の如何なる例の構成、そのような特定の挙げられた例及び条件に限定しないように解釈されるべきものである。本発明の実施形態は詳細に説明されているが、本発明の精神及び範囲から外れることなく、様々な変更、置換及び修正をこれに加えることが可能であることを理解されたい。

【０１０１】

以上説明した実施形態及びその変形例に関し、更に以下の付記を開示する。

（付記１）

利用者の生体情報に基づいて、当該利用者を登録利用者として認証するか否かを判定する生体認証装置であって、

過去の生体認証時において利用者の生体情報を表す過去データが取得された際の当該生体情報の特徴または取得環境の状態を表す過去状態情報を記憶する記憶部と、

利用者の生体情報を表すデータを取得する生体情報取得部と、

前記利用者の生体情報を表すデータから、当該データ取得時における利用者の生体情報

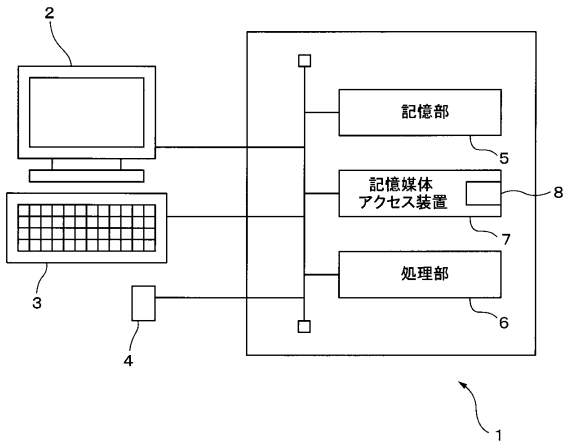
の特徴または取得環境の状態を表す現状態情報を抽出する状態情報抽出部と、
前記現状態情報と前記過去状態情報の類似度合いを表す再現度を算出する再現度算出部と、
前記データが前記過去データそのものあるいは前記過去データの一部を改変したものであると推定される閾値と前記再現度を比較し、前記再現度が当該閾値以上である場合、利用者を認証しない不正アクセス判定部と、
を有する生体認証装置。
（付記２）
前記利用者の生体情報が前記登録利用者の生体情報と一致するか否かを判定する認証判定部をさらに有し、
前記記憶部は、前記過去状態情報とともに、前記過去状態情報が得られた時の生体認証に成功したか否かを表すフラグを含み、
前記再現度算出部は、
前記認証判定部が、前記利用者の生体情報と前記登録利用者の生体情報が一致すると判定した場合、前記過去状態情報のうちの生体認証に成功したことを表すフラグが付された過去状態情報と前記現状態情報との間で前記再現度を算出し、
一方、前記認証判定部が、前記利用者の生体情報と前記登録利用者の生体情報が一致しないと判定した場合、前記過去状態情報のうちの生体認証に失敗したことを表すフラグが付され、かつ、前記利用者が生体認証の試行を開始してから前記現状態情報取得までの間に繰り返された生体認証時の過去状態情報と前記現状態情報との間で前記再現度を算出する、
付記１に記載の生体認証装置。
（付記３）
前記記憶部は、過去の生体認証時における利用者の生体情報の特徴を表す情報を前記過去状態情報として記憶し、
前記状態情報抽出部は、前記利用者の生体情報を表すデータから、当該データ取得時における利用者の生体情報の特徴を表す情報を前記現状態情報として抽出する、付記１または２に記載の生体認証装置。
（付記４）
前記記憶部は、過去の生体認証時における利用者の取得環境の状態を表す情報を前記過去状態情報として記憶し、
前記状態情報抽出部は、前記利用者の生体情報を表すデータから、当該データ取得時における利用者の生体情報の取得環境を表す情報を前記現状態情報として抽出する、付記１または２に記載の生体認証装置。
（付記５）
前記生体情報は指紋または掌紋であり、
前記利用者の生体情報を表すデータは、当該利用者の生体情報が写った生体画像であり、
前記状態情報抽出部は、前記生体画像に写った指紋または掌紋の隆線の幅の平均値を、当該生体画像取得時における利用者の生体情報の取得環境を表す情報を前記現状態情報として抽出する、付記４に記載の生体認証装置。
（付記６）
前記記憶部は、過去の生体認証時における利用者の生体情報の特徴を表す第１の過去情報と、過去の生体認証時における利用者の取得環境の状態を表す第２の過去情報とを前記過去状態情報として記憶し、
前記状態情報抽出部は、前記利用者の生体情報を表すデータから、当該データ取得時における利用者の生体情報の特徴を表す第１の現情報と、当該データ取得時における利用者の生体情報の取得環境を表す第２の現情報とを前記現状態情報として抽出し、
前記再現度算出部は、前記第１の現情報と前記第１の過去情報間の第１の類似度と前記第２の現情報と前記第２の過去情報間の第２の類似度とを算出し、前記第１の類似度と前

記第２の類似度の何れもが高くなるほど前記再現度が高くなるように前記再現度を算出する、付記１または２に記載の生体認証装置。
（付記７）
前記記憶部は、前記過去状態情報とともに、当該過去状態情報に対応する前記利用者の生体情報を表すデータの取得時刻を記憶し、かつ、当該取得時刻に基づいて、前記過去状態情報が記憶されてから所定期間が経過した前記過去状態情報を消去する、付記１～６の何れか一項に記載の生体認証装置。
（付記８）
前記生体情報取得部を有する端末と、
前記記憶部及び前記処理部を有するサーバとを有し、
前記端末と前記サーバとが通信ネットワークを介して接続される、付記１～７の何れか一項に記載の生体認証装置。
（付記９）
利用者の生体情報を表すデータを取得し、
前記利用者の生体情報を表すデータから、当該データ取得時における利用者の生体情報の特徴または取得環境の状態を表す現状態情報を抽出し、
前記現状態情報と過去の生体認証時において利用者の生体情報を表す過去データが取得された際の当該生体情報の特徴または取得環境の状態を表す過去状態情報の類似度合いを表す再現度を算出し、
前記データが前記過去データそのものあるいは前記過去データの一部を改変したものであると推定される閾値と前記再現度を比較し、前記再現度が当該閾値以上である場合、利用者を認証せず、
前記再現度が前記閾値未満である場合、前記利用者を登録利用者として認証するか否かを判定する、
ことを含む生体認証方法。
（付記１０）
利用者の生体情報を表すデータを取得し、
前記利用者の生体情報を表すデータから、当該データ取得時における利用者の生体情報の特徴または取得環境の状態を表す現状態情報を抽出し、
前記現状態情報と過去の生体認証時において利用者の生体情報を表す過去データが取得された際の当該生体情報の特徴または取得環境の状態を表す過去状態情報の類似度合いを表す再現度を算出し、
前記データが前記過去データそのものあるいは前記過去データの一部を改変したものであると推定される閾値と前記再現度を比較し、前記再現度が当該閾値以上である場合、利用者を認証せず、
前記再現度が前記閾値未満である場合、前記利用者を登録利用者として認証するか否かを判定する、
ことをコンピュータに実行させるための生体認証用コンピュータプログラム。
【符号の説明】
【０１０２】
１　生体認証装置
２　表示部
３　入力部
４　生体情報取得部
５　記憶部
６　処理部
７　記憶媒体アクセス装置
８　記憶媒体
１１　特徴情報抽出部
１２　再現度算出部

１３　　不正アクセス判定部
１４　　照合部
１５　　認証判定部
１６　　環境情報抽出部
１００　　生体認証システム
１１０　　端末
１２０　　サーバ
１３０　　通信ネットワーク
２１　　記憶部
２２　　画像取得制御部
２３、２４　　インターフェース部

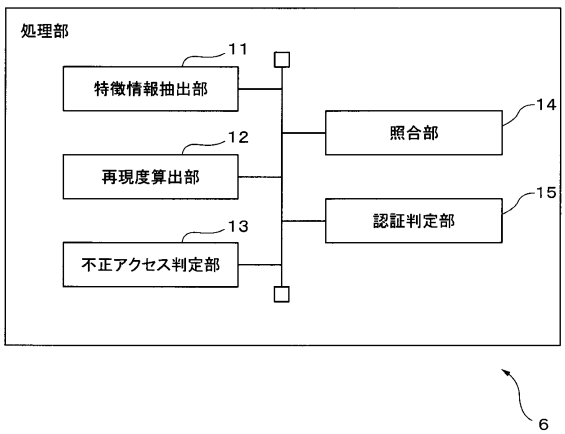
【図１】

図1



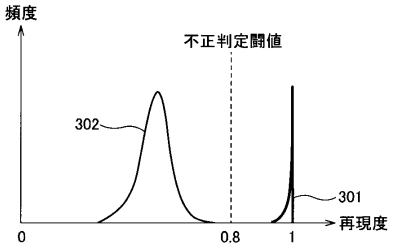
【図２】

図2



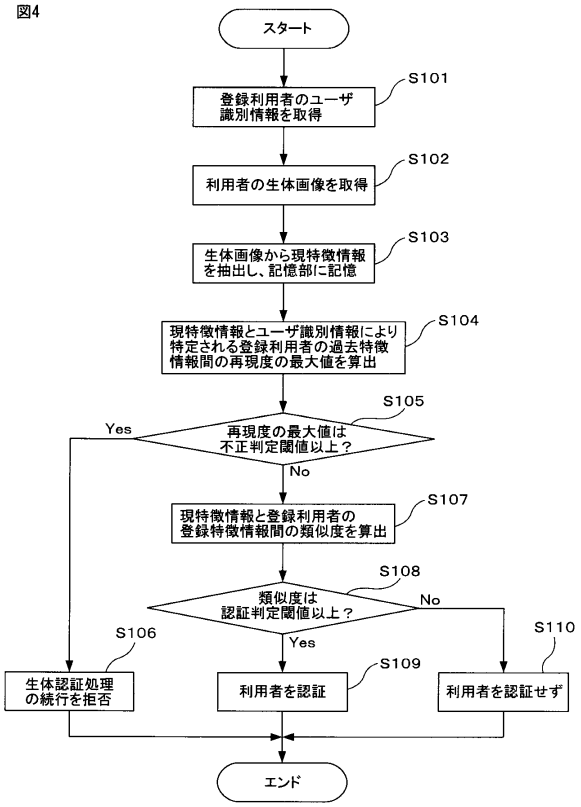
【図３】

図3



【図４】

図4



【図５】

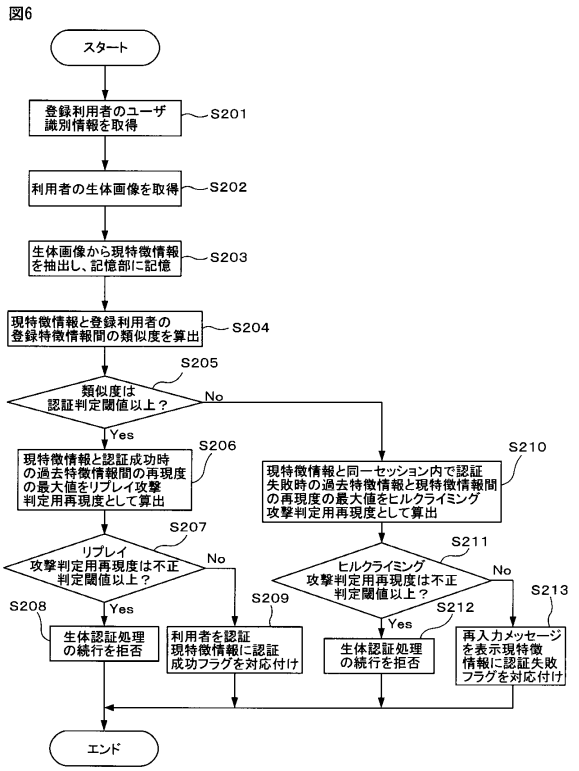
図5

番号	生成時刻	成功／失敗	特徴情報
1	08:00:00	1	0x78B12EA・・・
2	08:03:01	0	0xC6D903B・・・
3	08:03:10	0	0xC79903A・・・
4	08:03:16	0	0xB6D8008・・・
⋮	⋮	⋮	⋮

500

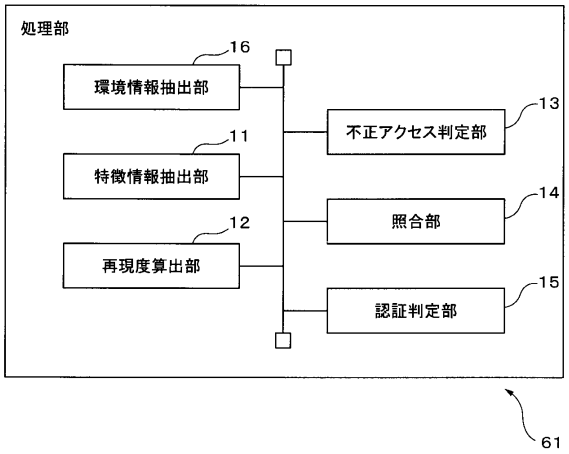
【図６】

図6



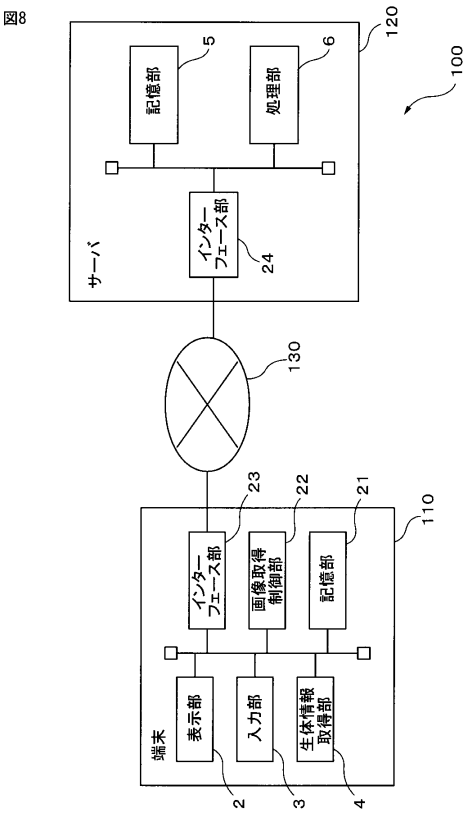
【図７】

図7


処理部
16
環境情報抽出部
11
特徴情報抽出部
12
再現度算出部
13
不正アクセス判定部
14
照合部
15
認証判定部
61

【図８】

図8


100
120
記憶部
5
処理部
6
インターフェース部
24
サーバ
130
110
23
22
21
インターフェース部
画像取得制御部
記憶部
表示部
入力部
生体情報取得部
端末
2
3
4

フロントページの続き

審査官　岸野　徹

(56)参考文献　特開２００２－３０４３７８（ＪＰ，Ａ）
特開２００２－２５９３４５（ＪＰ，Ａ）
特開２０１０－２４４２１８（ＪＰ，Ａ）
特開２０００－１３２５１５（ＪＰ，Ａ）
松濤　智明　Tomoaki　Matsunami，生体認証における「なりすまし攻撃」の検知　Spoofing detection in biometric authentication system，電子情報通信学会技術研究報告　Ｖｏｌ．１１２　Ｎｏ．１２６　IEICE Technical Report，日本，一般社団法人電子情報通信学会　The Institute of Electronics,Information and Communication Engineers，２０１２年　7月１２日，第112巻，pp.127-134
山崎　恭，４．脆弱性の解消に向けた最新対策技術の動向　１．安全性対策技術の動向，情報処理，日本，社団法人情報処理学会，２００６年　6月１５日，第４７巻　第6号，ｐ．６００～６０４

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／３２