

(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2005-18129
(P2005-18129A)

(43) 公開日 平成17年1月20日(2005.1.20)

(51) Int.Cl.⁷
G06T 7/00

F I
G O 6 T 7/00 5 3 0

テーマコード (参考)
5 B O 4 3

審査請求 未請求 請求項の数 7 O L (全 10 頁)

(21) 出願番号	特願2003-177994 (P2003-177994)	(71) 出願人	000005821
(22) 出願日	平成15年6月23日 (2003. 6. 23)		松下電器産業株式会社
			大阪府門真市大字門真1006番地
		(74) 代理人	100097445
			弁理士 岩橋 文雄
		(74) 代理人	100103355
			弁理士 坂口 智康
		(74) 代理人	100109667
			弁理士 内藤 浩樹
		(72) 発明者	西澤 真人
			大阪府門真市大字門真1006番地 松下電器産業株式会社内
		Fターム(参考)	5B043 AA09 BA02 BA04 DA05 EA04 EA06 EA10 FA07 FA08 GA02 GA05 GA13

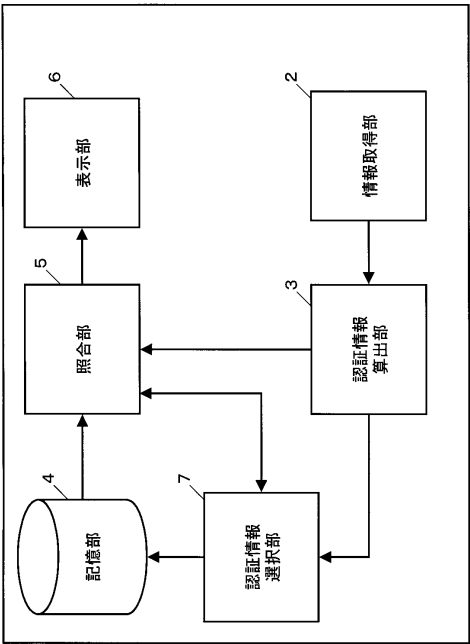
(54) 【発明の名称】 認証装置および認証情報選択方法

(57) 【要約】

【課題】 指に傷があったり、かすれやつぶれ等があるような指紋パターンが取得されたような場合にも、より高い認証率を有することのできる、外乱に強い認証装置を提供する。

【解決手段】 複数の認証情報の中から所定数の認証情報を選択する認証情報選択部7を備え、認証情報選択部7は、所定数の認証情報から任意に2つの認証情報を照合する際に算出される評価値が互いに一致するとみなされる閾値範囲内にあり、かつ、所定数の認証情報から任意の2つの認証情報を選択して算出した評価値間の距離値が最大となるように所定数の認証情報を選択する。

【選択図】 図1



1 認証装置

【特許請求の範囲】**【請求項 1】**

複数の認証情報から所定数の認証情報を選択する認証情報選択部を備え、
前記認証情報選択部は、それぞれの認証情報の差が所定の閾値範囲内にあり、前記それぞれの認証情報の差の総和が最大となるような前記所定数の認証情報を選択することを特徴とする認証装置。

【請求項 2】

被認証者から前記複数の認証情報を取得する認証情報取得部と、
前記認証情報選択部が選択した前記所定数の認証情報を記憶する認証情報記憶部とを備えたことを特徴とする請求項 1 に記載の認証装置。

10

【請求項 3】

被認証者から認証情報を取得する認証情報取得部と、
前記被認証者に対応した複数の認証情報を記憶する認証情報記憶部と、
前記認証情報取得部が取得した認証情報と前記被認証者に対応した複数の認証情報のそれぞれとを比較照合して一致するか否かを判定する判定部とを備え、
前記認証情報取得部が取得した認証情報と前記被認証者に対応した複数の認証情報のいずれかと一致すると前記判定部が判定した場合に、前記認証情報選択部は、前記被認証者に対応した複数の認証情報および前記認証情報取得部が取得した認証情報から前記所定数の認証情報を選択して、前記認証情報記憶部に記憶させることを特徴とする請求項 1 に記載の認証装置。

20

【請求項 4】

複数の認証情報から所定の関係を有する認証情報の組み合わせを選択する認証情報選択方法であって、
複数の認証情報から所定数の認証情報を選択する第 1 のステップと、
前記所定数の認証情報の各認証情報間の評価値を算出する第 2 のステップと、
前記第 2 のステップで算出された前記評価値から距離値を算出する第 3 のステップと、
前記複数の認証情報から、前記評価値が所定の閾値範囲内であり、前記距離値が最大となる前記認証情報の組み合わせを選択する第 4 のステップとを備えたことを特徴とする認証情報選択方法。

【請求項 5】

前記距離値は前記所定数の認証情報から算出される前記評価値の総和であることを特徴とする請求項 4 に記載の認証情報選択方法。

30

【請求項 6】

複数の認証情報から所定数の認証情報を選択して登録認証情報として登録する認証情報登録方法であって、
前記複数の認証情報から所定数の認証情報を選択する第 1 のステップと、
前記所定数の認証情報の各認証情報間の評価値を算出する第 2 のステップと、
前記第 2 のステップで算出された前記評価値から距離値を算出する第 3 のステップと、
前記複数の認証情報から、前記評価値が所定の閾値範囲内であり、前記距離値が最大となる前記認証情報の組み合わせを選択する第 4 のステップと、
前記第 4 のステップで選択された前記認証情報の組み合わせを登録認証情報として登録する第 5 のステップとを備えたことを特徴とする認証情報登録方法。

40

【請求項 7】

コンピュータに、
複数の認証情報から所定数の認証情報を選択する第 1 のステップと、
前記所定数の認証情報の各認証情報間の評価値を算出する第 2 のステップと、
前記第 2 のステップで算出された前記評価値から距離値を算出する第 3 のステップと、
前記複数の認証情報から、前記評価値が所定の閾値範囲内であり、前記距離値が最大となる前記認証情報の組み合わせを選択する第 4 のステップとを実行させることを特徴とするプログラム。

50

【発明の詳細な説明】**【0001】****【発明の属する技術分野】**

本発明は、虹彩パターンや指紋パターン等の生体固有の情報から作成された認証情報を用いて本人認証を行う認証装置および認証情報選択方法に関する。

【0002】**【従来の技術】**

近年、指紋パターンや虹彩パターン等の生体固有の情報（いわゆるバイオメトリクス情報）から作成された認証情報を利用して、あらかじめ登録された認証情報（以下、登録認証情報と記す）と被認証者から取得した認証情報とを比較照合し、その結果、被認証者から取得した認証情報が登録認証情報と一致するとみなされた場合には、その被認証者があらかじめ登録された者であると認証する認証装置が広く普及している。 10

【0003】

特に、指紋パターンを用いて被認証者の本人認証を行う指紋認証装置においては、その認証率を向上させるために、認証可能な者毎にあらかじめ認証情報を複数登録しておく技術が提案されている。このような技術においては、被認証者から取得された指紋パターンが、あらかじめ登録された複数の指紋パターンのうちのいずれか1つと一致するとみなされた場合には、被認証者をあらかじめ登録された者であると認証する。さらに、学習機能により、あらかじめ登録された者毎に複数個登録された指紋パターンのうち、一致率の低い指紋パターンを、より一致率の高い新しい指紋パターンで置換して更新記憶する構成により、高い認証率が得られる旨の提案がなされている（例えば、特許文献1を参照。）。 20

【0004】**【特許文献1】**

特許第2886575号公報

【0005】**【発明が解決しようとする課題】**

しかしながら、前述したような従来の指紋認証装置においては、指紋パターンの登録時に、複数取得された指紋パターンのうち、より高い一致率の指紋パターンが登録認証情報として記憶される。さらに、その学習機能によって、登録された指紋パターンが、より一致率の高いもの、すなわちより完全に近い指紋パターンと順次置換されていくので、例えば、照合を行う際に、指に傷があったり、かすれやつぶれ等のあるような指紋パターンが被 30
認証者から取得された場合には、このような登録認証情報では認証を行うことができない、すなわち、外乱に弱いという課題があった。

【0006】

本発明はこのような課題を解決するためになされたもので、被認証者から、指に傷があったり、かすれやつぶれ等があるような指紋パターンが取得されたような場合にも、高い認証率を実現することのできる、外乱に強い認証装置および認証情報選択方法を提供することを目的とする。

【0007】**【課題を解決するための手段】**

本発明の認証装置は、複数の認証情報から所定数の認証情報を選択する認証情報選択部を備え、認証情報選択部は、それぞれの認証情報の差が所定の閾値範囲内にあり、それぞれの認証情報の差の総和が最大となるような所定数の認証情報を選択することを特徴としている。このような構成により、登録認証情報の登録や更新を行う際、例えば被認証者から指紋パターン等の認証情報を複数回取得して、そのうち所定数の認証情報を登録認証情報として記憶、登録するような場合に、それぞれの認証情報の差が所定の閾値範囲内にあるので、信頼性の高い、さらに、認証情報の差の総和が最大となるような組み合わせを選択することにより、例えば指紋パターンを認証情報として用いた場合に、被認証者の指の濡れや乾き、傷等の影響を受けにくい、外乱に強い認証装置を実現できる。また、簡易に演算が行えるので、装置の小型化を実現できる。 40 50

【 0 0 0 8 】

また、被認証者から複数の認証情報を取得する認証情報取得部と、認証情報選択部が選択した所定数の認証情報を記憶する認証情報記憶部とを備えた構成であってもよい。このような構成により、被認証者から取得した複数の認証情報から信頼性の高い、かつ外乱に強い所定数の認証情報を選択して登録認証情報として登録することのできる、外乱に強い認証装置を実現できる。

【 0 0 0 9 】

さらに、被認証者から認証情報を取得する認証情報取得部と、被認証者に対応した複数の認証情報を記憶する認証情報記憶部と、認証情報取得部が取得した認証情報と被認証者に対応した複数の認証情報のそれぞれとを比較照合して一致するか否かを判定する判定部とを備え、認証情報取得部が取得した認証情報と被認証者に対応した複数の認証情報のいずれかと一致すると判定部が判定した場合に、認証情報選択部は、被認証者に対応した複数の認証情報および認証情報取得部が取得した認証情報から所定数の認証情報を選択して、認証情報記憶部に記憶させることを特徴とする構成であってもよい。このような構成によれば、被認証者から取得した認証情報と、あらかじめ登録された登録認証情報との比較照合を行った結果、被認証者から取得した認証情報が登録認証情報と一致すると判定された場合に、被認証者から取得した認証情報および登録認証情報から、所定の関係を満たす認証情報を選択して登録認証情報として更新して記憶、登録することにより、例えば指紋パターンを認証情報として用いた場合に、指の濡れや乾き、傷等の影響を受けにくい、外乱に強い認証装置を実現できる。

10

20

【 0 0 1 0 】

次に、本発明の認証情報選択方法は、複数の認証情報から所定の関係を有する認証情報の組み合わせを選択する認証情報選択方法であって、複数の認証情報から所定数の認証情報を選択する第1のステップと、所定数の認証情報の各認証情報間の評価値を算出する第2のステップと、第2のステップで算出された評価値から距離値を算出する第3のステップと、複数の認証情報から、評価値が所定の閾値範囲内であり、距離値が最大となる認証情報の組み合わせを選択する第4のステップとを備えたことを特徴としている。このような方法により、複数の認証情報の中から、各々の認証情報が互いに認証可能であるので、信頼性の高い、さらに、評価値からそのばらつきの度合いを示す距離値を算出してその距離値が最大となるような組み合わせを選択するので、例えば指紋パターンを認証情報として用いた場合に、指の濡れや乾き、傷等の影響を受けにくい、外乱に強い認証情報を選択することができる。これにより、認証装置にあらかじめ登録された登録認証情報を更新する際に好適な認証情報選択方法を提供できる。

30

【 0 0 1 1 】

また、距離値は所定数の認証情報から算出される評価値の総和である方法であってもよい。このような方法により、簡易に演算を行うことが可能であるので、装置の小型化等を実現できる。

【 0 0 1 2 】

次に本発明の認証情報登録方法は、複数の認証情報から所定数の認証情報を選択して登録認証情報として登録する認証情報登録方法であって、複数の認証情報から所定数の認証情報を選択する第1のステップと、所定数の認証情報の各認証情報間の評価値を算出する第2のステップと、第2のステップで算出された評価値から距離値を算出する第3のステップと、複数の認証情報から、評価値が所定の閾値範囲内であり、距離値が最大となる認証情報の組み合わせを選択する第4のステップと、第4のステップで選択された認証情報の組み合わせを登録認証情報として登録する第5のステップとを備えたことを特徴としている。このような方法により、複数の認証情報の中から、各々の認証情報が互いに認証可能であるので、信頼性の高い、さらに、評価値からそのばらつきの度合いを示す距離値を算出してその距離値が最大となるような組み合わせを選択して登録認証情報として登録するので、例えば指紋パターンを認証情報として用いた場合に、指の濡れや乾き、傷等の影響を受けにくい、高い認証率を実現できる認証情報を登録認証情報として登録することがで

40

50

きる。これにより、認証装置において被認証者から取得した複数の認証情報から登録認証情報を初期登録する際に好適な認証情報登録方法を実現できる。

【0013】

次に本発明のプログラムは、コンピュータに、複数の認証情報から所定数の認証情報を選択する第1のステップと、所定数の認証情報の各認証情報間の評価値を算出する第2のステップと、第2のステップで算出された評価値から距離値を算出する第3のステップと、複数の認証情報から、評価値が所定の閾値範囲内であり、距離値が最大となる認証情報の組み合わせを選択する第4のステップとを実行させることを特徴としている。このようなプログラムをコンピュータに実行させることにより、複数の認証情報の中から、各々の認証情報が互いに認証可能であるので、信頼性の高い、さらに、評価値からそのばらつきの度合いを示す距離値を算出してその距離値が最大となるような組み合わせを選択するので、例えば指紋パターンを認証情報として用いた場合に、指の濡れや乾き、傷等の影響を受けにくい、登録認証情報の選択が可能となる。これにより、認証装置にあらかじめ登録された登録認証情報を更新する際に好適なプログラムを提供できる。

【0014】

【発明の実施の形態】

まず、本発明の実施の形態における認証装置について、図面を用いて詳細に説明する。図1は、本発明の実施の形態における認証装置の構成を示すブロック図である。

【0015】

なお、本発明の実施の形態においては、認証装置の例として、被認証者の指紋パターンを用いて作成した認証情報と、登録された認証情報とを比較照合することによって本人認証を行う指紋認証装置について説明する。

【0016】

本発明の実施の形態における認証装置1は、被認証者から指紋パターンを取得する情報取得部2、情報取得部2と接続され、情報取得部2で取得された指紋パターンから特徴点等の認証に必要な認証情報を算出する認証情報算出部3、あらかじめ認証可能な者毎に複数の登録認証情報を格納する記憶部4、記憶部4、認証情報算出部3および後述する認証情報選択部7に接続され、記憶部4に格納された複数の登録認証情報と認証情報算出部3から出力された認証情報とを比較照合する照合部5、照合部5に接続され、照合部5での照合結果を被認証者等に表示する表示部6、ならびに、認証情報算出部3、記憶部4および照合部5に接続され、照合部5で用いられた複数の登録認証情報および認証情報算出部3から出力された認証情報のうち、後述するような関係を満たす組み合わせの認証情報を選択し、登録認証情報として記憶部4に記憶させる認証情報選択部7を備える。

【0017】

情報取得部2としては、被認証者の指紋パターンを取得できるものであれば、光学デバイスや静電容量式のデバイス等、公知の各種デバイスを用いることができる。

【0018】

また、認証情報算出部3で算出される認証情報としては、特徴点（マニューシャ）、周波数解析スペクトル、パターンマッチングにおける指紋パターンの画像等、公知の認証情報を適宜用いることができる。

【0019】

さらに、記憶部4は、記憶媒体を用いたものであれば、特にその種類を限定されるものではなく、RAM（ランダムアクセスメモリ）やHDD（ハードディスクドライブ）等、公知の記憶媒体を用いて構成することができる。

【0020】

さらに、認証情報算出部3、照合部5および認証情報選択部7は、所定の動作を行うものであれば、必ずしもハードウェアで構成されていなくても、ソフトウェアで構成され、図示しない演算装置等で実行されるものであってもよい。

【0021】

次に、本発明の実施の形態における認証装置1の動作について説明する。図2は、本発明

の実施の形態における認証装置 1 の動作ステップを説明するフローチャートである。ここでは、記憶部 4 に記憶された複数の登録認証情報を更新する場合を例として説明する。

【0022】

図 2 に示すように、まず認証装置 1 において、被認証者の指紋パターンが情報取得部 2 から取得される。前述の通り、本発明はこの指紋パターンを取得する方法を限定するものではないが、例えば、プリズム等の光学素子や静電容量式のデバイスを用い、被認証者の指をデバイスの表面に押しあてることにより被認証者の指紋パターンを取得することができる (S1)。

【0023】

次に、情報取得部 2 で取得された指紋パターンから、照合に用いるべき、例えば、特徴量等の認証情報が認証情報算出部 3 において算出される (S2)。

【0024】

認証情報算出部 3 で算出された認証情報は照合部 5 に送られて、照合部 5 は、記憶部 4 にあらかじめ記憶された登録認証情報と認証情報算出部 3 で算出された認証情報とを比較照合する (S3)。なお、記憶部 4 には、あらかじめ照合可能な者毎に、複数の登録認証情報が記憶されており、照合した結果、いずれか 1 つの登録認証情報と一致するとみなされた場合に、被認証者が記憶部 4 に記憶された認証可能な者であるとみなす構成が認証率向上の観点から望ましい。

【0025】

なお、本発明の認証装置 1 においては、照合部 5 における認証情報同士を比較照合する方法を限定するものではないが、本発明の実施の形態においては、一の認証情報と他の認証情報との間で所定の評価値を算出し、その評価値が所定の範囲内にある場合に、一致するとみなして認証可能であるとする。なお、この評価値の算出については、例えば、パターンマッチング法を用いた場合には、一の指紋パターン画像と他の指紋パターン画像 (ともに 2 値画像) とを画素毎に比較して、画素毎の両パターンの差分の絶対値を算出し、それを全画素について足し合わせたものを評価値とすることができる。この場合、一の指紋パターン画像と他の指紋パターン画像とが完全一致した場合には、評価値は「0」となる。その他、特徴点 (マニューシャ) を用いた方法や、周波数解析スペクトルを用いた方法等、公知の各種認証アルゴリズムを用いてこのような評価値を算出することができる。

【0026】

次に、ステップ S3 において、照合部 5 で照合された結果は、照合部 5 から表示部 6 に送られて、被認証者に対して表示される (S4)。

【0027】

ステップ S3 における照合の結果、照合部 5 で被認証者があらかじめ記憶部 4 に記憶された、あらかじめ登録された者 (以下、登録者と記す) であると判定された場合には、被認証者から取得された認証情報、および、照合の結果、被認証者とみなされた登録者に対応した複数の登録認証情報が認証情報選択部である認証情報選択部 7 へ送られる。

【0028】

認証情報選択部 7 では、送られてきた被認証者から取得された認証情報、および、照合の結果、被認証者とみなされた登録者に対応する複数の登録認証情報において各認証情報間の評価値を算出するとともに、算出された評価値から後述する方法で組み合わせ毎にそのばらつき度合いを示す距離値を算出し (S5)、距離値にもとづいて被認証者から取得された認証情報および照合の結果、被認証者とみなされた登録者についてあらかじめ登録された複数の登録認証情報から、所定の関係にある認証情報の組み合わせを選択して新たな登録認証情報として、記憶部 4 に更新記憶させる (S6)。

【0029】

この認証情報選択部 7 での認証情報の選択および更新記憶動作 (S5 および S6) について、さらに詳細に説明する。図 3 は本発明の実施の形態における認証装置 1 の認証情報選択部 7 の動作ステップを示すフローチャートである。なお、ここでは説明を簡単にするために、登録者毎に 3 つの登録認証情報があらかじめ記憶部 4 に記憶されているものとして

説明を行う。

【0030】

図3において、まず、認証情報選択部7は、照合部5において照合に用いられた被認証者から取得された認証情報と、比較照合の結果、被認証者であるとみなされた登録者の3つの登録認証情報との計4つの認証情報を、照合部5から取得する(S10)。

【0031】

次に、認証情報選択部7では、取得された4つの認証情報から、任意の3つの認証情報を選択する(S11)。この選択には、 ${}_4C_3 = 4$ 通りの方法があるが、順次、すべての選択を行う。

【0032】

次に、認証情報選択部7では、選択された3つの認証情報について、それぞれの各認証情報間の評価値および距離値を算出する(S12)。評価値の算出方法は、前述の通りであり、ステップS11で選択された各認証情報間の評価値すべてを算出する。例えば、3つの認証情報が選択された場合には、3つの評価値が算出される。なお、この評価値の演算は、認証情報選択部7で行ってもよいし、前述の選択された3つの認証情報を一端照合部5に送り、評価値の算出を照合部5に行わせてから、その結果を認証情報選択部7が受け取る構成であってもよい。

【0033】

次に、認証情報選択部7は選択された認証情報の距離値を算出する。距離値の算出について詳細に説明する。距離値とは、前述したように、選択された各認証情報間の評価値のばらつき度合いを示す値であり、実用的には、評価値をそれぞれ足し合わせた値を用いることができる。例えば3つの認証情報が選択された場合には、算出された3つの評価値の和を距離値とする。すなわち、距離値はステップS11で選択された認証情報の組み合わせ毎に1つ算出される。

【0034】

次に、認証情報選択部7は、すべての認証情報の組み合わせについて、評価値および距離値の演算を行ったか否かを判定する(S13)。すべての認証情報の組み合わせについて評価値および距離値が演算された場合には、ステップS14に進み、演算されていない場合には、再度ステップS11に戻って新たな認証情報の組み合わせを選択する。

【0035】

次に、認証情報選択部7は、後述する要件1および要件2の、2つの要件を満たす認証情報の組み合わせを選択して、記憶部4に登録認証情報として登録する(S14)。図4は、これらの要件を説明するための概念図である。

【0036】

まず、要件1について説明する。前述のように、4つの認証情報の中から3つの認証情報を登録認証情報として選択する場合、4通りの選択方法があるが、例えば、ステップS11においてA、BおよびCの3つの認証情報が選択されたとき、認証情報Aと認証情報Bとから算出される評価値をABと記し、同様に、認証情報Bと認証情報Cとから算出される評価値をBC、認証情報Cと認証情報Aとから算出された評価値をCAと記すと、 $AB + BC + CA$ の値、すなわち距離値が4通りの組み合わせの中で最大になることである。すなわち、評価値間のばらつきが大きいことが要件であるということもできる。

【0037】

次に、要件2は、認証情報A、認証情報Bおよび認証情報Cが互いに一致して認証可能とみなされること、いいかえれば、評価値AB、BCおよびCAのそれぞれが、すべて認証可能とみなされる閾値THの範囲内にあることである。

【0038】

これらの要件1および要件2の2つの要件を満たす認証情報の組み合わせを選択して、2つの要件を満たす場合に、その3つの認証情報を、新たな登録認証情報として、記憶部4に記憶させ、認証情報選択部7の動作は終了する(S14)。なお、実用的には、要件2における評価値を先に算出して、要件2を満たさない認証情報の組み合わせについては、

10

20

30

40

50

要件１の判定を行わずに、ステップＳ１１に戻って、異なる組み合わせの認証情報についての要件判定を行う構成とすれば、より処理の迅速化を図ることができるので望ましい。

【００３９】

このような構成とすることにより、常に互いの評価値の和（距離値）がもっとも大きくなる、すなわちばらつき度合いの高い組み合わせで、かつ相互に認証が可能な組み合わせの認証情報が選択されるので、情報取得部２から取得される指紋パターンに、多少かすれ等があったり、傷があったような場合でも、登録認証情報として記憶部４に登録され得るので、被認証者から取得した指紋に、かすれ、つぶれ等があるような場合でも、より高い認証率を実現できる、すなわち、外乱に強くロバストな認証装置を実現できる。また、このような構成とすることにより、被認証者から取得される指紋パターンの経年変化等にも強い認証装置を実現することができる。

【００４０】

また、上述の例では、記憶部４に記憶された指紋パターンを更新登録する際を例として示したが、本発明の実施の形態の認証装置１によれば、認証可能な者の指紋パターンを複数回取得して、記憶部４に登録認証情報として新規登録する際にも、同様の処理を行うことで、より高い認証率を実現できる登録認証情報を登録することが可能である。次に本発明の実施の形態における認証装置１における登録認証情報の新規登録時の動作について説明する。

【００４１】

登録認証情報の新規登録を行う際には、図１に戻って、登録されるべき被認証者の指紋パターンが情報取得部２で複数回取得され、取得された指紋パターンのそれぞれから対応する認証情報が認証情報算出部３で算出されると、算出されたすべての認証情報は認証情報選択部７に送られる。認証情報選択部７では、前述の図３のステップＳ１０～Ｓ１４に示したような処理を行って、所定の数選択された認証情報を、記憶部４に登録認証情報として登録させる。

【００４２】

このような構成とすることにより、被認証者から取得された認証情報のうち、互いの評価値の和（距離値）がもっとも大きな、すなわちばらつきの大きな組み合わせで、かつ相互に一致すると認証が可能な組み合わせの認証情報を選択して登録認証情報として登録するので、以降の処理において比較照合を行う際に、多少の指の濡れによるつぶれや乾きによるかすれ、傷等の影響に強い、認証率の高い外乱に強い認証装置を実現できる。

【００４３】

なお、本発明の実施の形態においては、認証装置の例として、人の指紋パターンを用いた認証装置を示したが、本発明の認証装置はこれに限定されない。例えば、目の虹彩パターンや、顔のパターン等、様々な生体情報から作成した認証情報を用いた認証装置に適用可能であることはいうまでもない。

【００４４】

【発明の効果】

以上のように本発明の認証装置は、認証情報のうち、互いの評価値のばらつきの大きな組み合わせで、かつ相互に一致すると認証が可能な組み合わせの認証情報を選択して登録認証情報として登録するので、指に傷があったり、かすれやつぶれ等があるような指紋パターンが取得されたような場合にも、より高い認証率を有することのできる、外乱に強い認証装置および認証情報選択方法を提供することができる。

【図面の簡単な説明】

【図１】本発明の実施の形態における認証装置の構成を示すブロック図

【図２】本発明の実施の形態における認証装置の動作を示すフローチャート

【図３】本発明の実施の形態における認証装置の認証情報選択部の動作を示すフローチャート

【図４】本発明の実施の形態における認証装置の認証情報選択部での処理を説明するための概念図

10

20

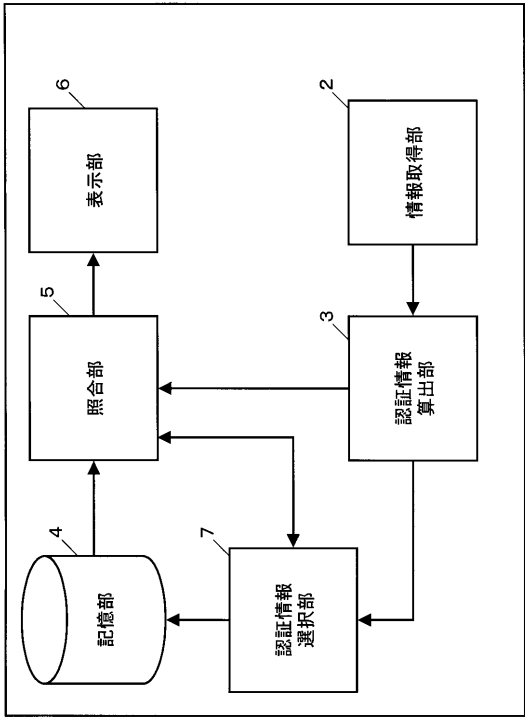
30

40

50

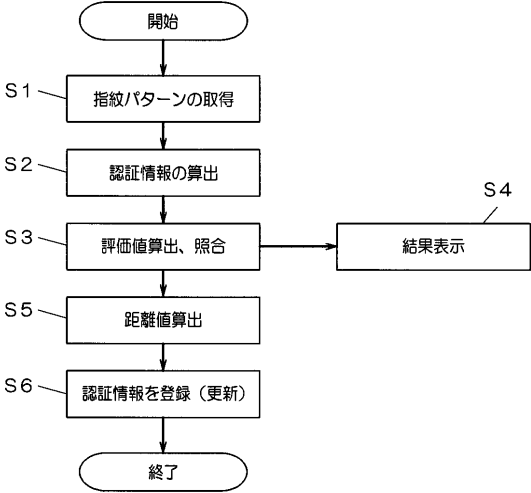
- 【符号の説明】
- 1 認証装置
 - 2 情報取得部
 - 3 認証情報算出部
 - 4 記憶部
 - 5 照合部
 - 6 表示部
 - 7 認証情報選択部

【図 1】

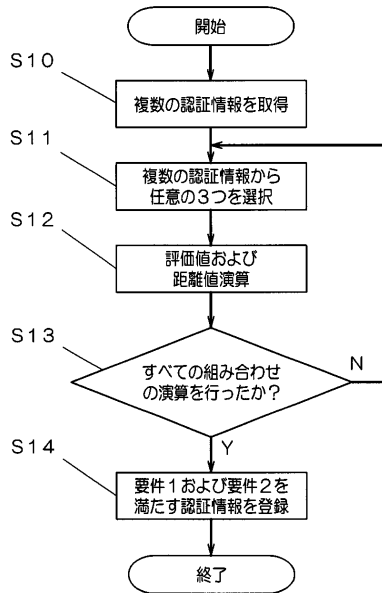


1 認証装置

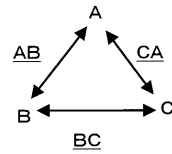
【図 2】



【 図 3 】



【 図 4 】



例:

A, B, C: 同一者の認証情報

AB: 認証情報AとBから算出した評価値要件1. 距離値 = $AB + BC + CA$ が最大要件2. $\underline{AB} < TH$ $\underline{BC} < TH$ $\underline{CA} < TH$ (TH: 認証閾値)