(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5729302号
(P5729302)
(45)発行日　平成27年6月3日(2015.6.3)　(24)登録日　平成27年4月17日(2015.4.17)

(51)Int.Cl.　　F I
A61B 5/117 (2006.01)　　A61B 5/10 322
G06T 7/00 (2006.01)　　G06T 7/00 530
　　G06T 7/00 510B
　　A61B 5/10 320C

請求項の数 10　(全 22 頁)

(21)出願番号　特願2011-530803 (P2011-530803)
(86)(22)出願日　平成22年8月20日 (2010.8.20)
(86)国際出願番号　PCT/JP2010/064540
(87)国際公開番号　WO2011/030675
(87)国際公開日　平成23年3月17日 (2011.3.17)
審査請求日　平成25年7月16日 (2013.7.16)
(31)優先権主張番号　特願2009-208042 (P2009-208042)
(32)優先日　平成21年9月9日 (2009.9.9)
(33)優先権主張国　日本国(JP)

(73)特許権者　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100109313
弁理士　机　昌彦
(74)代理人　100124154
弁理士　下坂　直樹
(72)発明者　門田　啓
東京都港区芝五丁目７番１号
日本電気株式会社内

審査官　鹿野　博嗣

最終頁に続く

(54)【発明の名称】生体認証システム、方法およびプログラム

(57)【特許請求の範囲】
【請求項１】
生体情報に含まれる特徴量の生起分布を記憶する生起分布記憶手段と、
入力データが入力されたという条件下での、該入力データが任意のデータと偶然に一致する第１の条件付き確率を、前記生起分布記憶手段が記憶する生起分布に従い求められる特徴量と該入力データの特徴量との一致度合いが、該入力データと予め記憶している登録者の生体情報を示すテンプレートデータとの一致度合い以上となる確率として算出する条件付き確率算出手段と、
前記条件付き確率算出手段が算出した第１の条件付き確率を所定の閾値と比較することにより入力データがテンプレートとして記憶された登録者の生体情報であるか否かを同定する同定手段とを
含み、
前記同定手段は、閾値として、生体認証システムで許容される誤合致率の値、前記誤合致率に所定の１未満の値である安全係数を乗じた値、又は前記誤合致率を所定の式に代入して演算することにより定まる値のいずれかを用いる
生体認証システム。
【請求項２】
第１の条件付き確率に加え、テンプレートデータが入力されたという条件下での、任意のデータと偶然に一致する第２の条件付き確率を、生起分布に従い求められる特徴量とテンプレートデータの特徴量との一致度合いが、入力データとテンプレートデータとの一致

度合い以上となる確率として算出する第２の条件付き確率算出手段を含み、
前記同定手段は、第１の条件付き確率及び前記第２の条件付き確率算出手段が算出した第２の条件付き確率の両方を用いて同定を行う
請求項１記載の生体認証システム。
【請求項３】
テンプレートデータ登録時に、テンプレートが生体情報であることを検証する登録データ検証手段を含む
請求項１乃至２のいずれか１項に記載の生体認証システム。
【請求項４】
特徴量として特徴点の位置を用い、照会データとテンプレートデータとの特徴点のうち、所定の距離以内にある照会データとテンプレートデータとの特徴点の組を対応特徴点とし、対応特徴点の数を一致度合いとして求める対応特徴点数算出手段を含み、
第１の条件付き確率算出手段は、特徴点を生起分布に従って配置した場合に、照会データの特徴点と対応する特徴点の数が、前記対応特徴点数算出手段が算出した照会データとテンプレートデータとの間で対応する特徴点の数より多くなる確率を第１の条件付き確率として求める
請求項１乃至３のうちいずれか１項に記載の生体認証システム。
【請求項５】
生体情報として指紋を用い、特徴点として指紋隆線の途切れる点又は分岐する点を用いる
請求項４記載の生体認証システム。
【請求項６】
生体情報として静脈を用い、特徴点として静脈の途切れる点又は分岐する点を用いる請求項４記載の生体認証システム。
【請求項７】
生体情報として画像を用い、画像中の各画素をカテゴリに分類し、特徴量として各画素のカテゴリを用い、照会データとテンプレートデータとの画素のうち、カテゴリが所定の関係にある照会データとテンプレートデータとの画素の組を対応画素とし、対応画素の数を一致度合いとして求める対応画素数算出手段を含み、
第１の条件付き確率算出手段は、各画素のカテゴリを生起分布に従って配置した場合に、照会データの画素と対応する画素の数が、前記対応画素数算出手段が算出した照会データとテンプレートデータとの間で対応する画素の数より多くなる確率を第１の条件付き確率として求める
請求項１乃至３のうちいずれか１項に記載の生体認証システム。
【請求項８】
生体情報として静脈を用い、画素のカテゴリとして静脈領域、背景領域及びあいまい領域を用い、対応画素とするカテゴリの所定の関係として、静脈領域と背景領域との組み合わせではないことを条件として対応画素を求める
請求項７記載の生体認証システム。
【請求項９】
生体情報に含まれる特徴量の生起分布を生起分布記憶手段に記憶し、
入力データが入力されたという条件下での、該入力データが任意のデータと偶然に一致する第１の条件付き確率を、前記生起分布記憶手段が記憶する生起分布に従い求められる特徴量と該入力データの特徴量との一致度合いが、該入力データと予め記憶している登録者の生体情報を示すテンプレートデータとの一致度合い以上となる確率として算出し、
前記条件付き確率算出手段が算出した第１の条件付き確率を所定の閾値と比較することにより入力データがテンプレートとして記憶された登録者の生体情報であるか否かを、前記閾値として、生体認証システムで許容される誤合致率の値、前記誤合致率に所定の１未満の値である安全係数を乗じた値、又は前記誤合致率を所定の式に代入して演算することにより定まる値のいずれかを用いて同定する生体認証方法。

【請求項１０】
生体情報に含まれる特徴量の生起分布を記憶する生起分布記憶手段を備えるコンピュータに、
入力データが入力されたという条件下での、該入力データが任意のデータと偶然に一致する第１の条件付き確率を、前記生起分布記憶手段が記憶する生起分布に従い求められる特徴量と該入力データの特徴量との一致度合いが、該入力データと予め記憶している登録者の生体情報を示すテンプレートデータとの一致度合い以上となる確率として算出するステップと、
前記条件付き確率算出手段が算出した第１の条件付き確率を所定の閾値と比較することにより入力データがテンプレートとして記憶された登録者の生体情報であるか否かを、前記閾値として、生体認証システムで許容される誤合致率の値、前記誤合致率に所定の１未満の値である安全係数を乗じた値、又は前記誤合致率を所定の式に代入して演算することにより定まる値のいずれかを用いて同定するステップと、
を実行させる生体認証プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、入力された生体情報とデータベースに登録されている生体情報とを照合することで人物の認証を行う、生体認証システム、方法およびプログラムに関する。
【背景技術】
【０００２】
人物を認証する方法として個人の生体情報（身体的特徴）を利用した生体認証（バイオメトリクス認証）がある。これは、登録者の指紋や顔といった個人特有の生体情報を、データベースへ登録しておき、登録してある生体情報（テンプレート）と、認証を受けたい照会者が提示した生体情報（照会データ）とを照合して、テンプレートを登録した登録者と同一人物であるか否かを認証するものである。テンプレートと照会データとの照合においては、テンプレートと照会データとの類似度や距離等の照合評価値を求め、照合評価値を予め定められた閾値との大小関係から判定することが一般に行われる。
生体認証システムの誤りには、照会者と登録者とが同一人物であるにもかかわらず異なる人物であると判定する本人棄却と、登録者では無い照会者を登録者と判定してしまう他人受入との２種類がある。本人棄却が発生する確率を本人棄却率（ＦＲＲ（Ｆａｌｓｅ Ｒｅｊｅｃｔｉｏｎ Ｒａｔｅ））や誤非合致率（ＦＮＭＲ（Ｆａｌｓｅ Ｎｏｎ－Ｍａｔｃｈｉｎｇ Ｒａｔｅ））といい、他人受入が発生する確率を他人受入率（ＦＡＲ（Ｆａｌｓｅ Ａｃｃｅｐｔａｎｃｅ Ｒａｔｅ））や誤合致率（ＦＭＲ（Ｆａｌｓｅ Ｍａｔｃｈ Ｒａｔｅ））という。
誤非合致率・誤合致率は、照合評価値と閾値とを比較する照合アルゴリズムの誤りのことを指す。また、本人棄却率・他人受入率は、照合評価値と閾値とを比較した照合アルゴリズムの判定結果を元にした認証システムとしての判定結果の誤りのことを指すことが一般的である。この場合、本人棄却率・他人受入率は、誤非合致率・誤合致率から定まるものである。
本人棄却率（誤非合致率）と他人受入率（誤合致率）とは、共に低いほうが好ましい。これら２種類の誤りには強い関連がある。判定の閾値をゆるめると、誤って登録者を登録者ではないと判定してしまう誤りが減り、本人棄却率（誤非常合致率）を低くすることができるが、他人を誤って登録者と判定してしまう誤りが増え、他人受入率（誤合致率）が高くなってしまう。一方、判定の閾値を厳しくすると、他人を誤って登録者と判定してしまう誤りが減り、他人受入率（誤合致率）を低くすることができるが、誤って登録者を登録者ではないと判定してしまう誤りが増え、本人棄却率（誤非合致率）が高くなってしまう。
このように本人棄却率（誤非合致率）と他人受入率（誤合致率）とは、トレードオフの関係があるため、応用場面に応じた適切な閾値を設定することが求められる。例えば、業

務システムへのログオンや入退管理システム等、一定の安全性を確保する必要があるシステムでは、システムとして許容できる他人受入率の上限を定め、他人受入率（誤非合致率）が上限未満となるように、閾値を設定することが行われている。

一般に、閾値をどの値にすると他人受入率の値がどうなるかの閾値（照合評価値）と他人受入率（誤非合致率）との関係は、テストデータを用いた評価実験によって、テストデータの平均的な振舞いとして求められる。それは、多くの照合評価値と他人受入率（誤非合致率）とには理論的な関係が無いためである。

しかしながら、広く行われているテストデータを用いた平均的な評価方法には問題がある。それは、多くの場合、データ毎に他人受入しやすさが異なるが、平均的に評価しているため全体の平均としか評価できない点である。

非特許文献１の図１には、個々のデータに対して個別ＦＭＲ（誤合致率）を調べるとデータによって大きくばらつくことがあることが示されている。以下、広く行われている平均的な評価によるＦＭＲを平均ＦＭＲ、データ毎に調べた各データに対するＦＭＲを個別ＦＭＲと呼ぶこととする。

非特許文献１の図１に示されるように、データによって誤合致しやすさは異なるため、平均ＦＭＲを用いて平均的には所望のＦＭＲよりも低くなるように閾値を設定したとしても、誤合致しやすい個別ＦＭＲの高いデータが存在することにより、認証システムとして所望の安全性（ＦＭＲ）が確保されない危険がある。

また、非特許文献１には、広く行われている平均ＦＭＲによる評価ではなく、個別ＦＭＲの分布を評価することで統計的に認証システムのＦＭＲを保証できる精度評価方法が記載されている。

また、非特許文献２には、理論的に認証システムのＦＭＲを保証できる照合方法が記載されている。予め任意の生体情報の特徴量の生起分布を求めておき、任意の生体情報と偶然に特徴量が一致する確率を照合評価値とすることで理論的にＦＭＲを保証する方法である。

偶然に特徴量が一致する確率を照合評価値とする照合を行う装置としては、例えば、特許文献１に記載されたパターン照合装置がある。

ところで、生体認証システムに対する攻撃として、非特許文献３に記載されるようなウルフ攻撃がある。ウルフ攻撃とは、データ毎に誤合致しやすさが異なることを利用して、誤合致しやすいデータを攻撃者が選択的に用いることで、認証システムで想定されているＦＭＲよりも高い確率で、誤合致を起こさせる攻撃である。

更に攻撃者は、通常の生体情報と考えられる集合以外から選択して攻撃することもある。一般に、通常見られる生体情報の集合は、生体情報としての物理的制約等の制約があるため、システムへ入力可能なデータ集合の一部である。そこで、人工的に作成しなければできないようなデータも選択対象とすることで、生体情報の集合から選択するよりも、より高い確率で誤合致を起こすことのできる可能性がある。

例えば、非特許文献４には、一致した特徴点の数を用いて判定する指紋照合方法に対して、通常の指紋に見られる特徴点数よりもはるかに多い特徴点を持つデータを照会データとすることで、高い確率で誤合致を起こすことが可能であることが示されている。

また、非特許文献６には、非特許文献５記載の指静脈認証方法に対して、通常の指静脈としてはありえないデータを照会データとすることで、全てのテンプレートと誤合致させることが可能なことが示されている。

このようなウルフ攻撃に対して安全な認証方法が、非特許文献７に記載されている。この方法では、認証毎に多くのデータと照合を行うことで、誤合致しやすいかどうかを判断することにより、誤合致しやすいデータを用いた攻撃に強くしている。

【先行技術文献】

【特許文献】

【０００３】

【特許文献１】特開２００２－２８８６８７号公報

【非特許文献】

【０００４】
【非特許文献１】門田、黄、吉本：個別安全性を保証できる指紋の精度評価，Ｐｒｏｃ．ｏｆ Ｔｈｅ ２００５ Ｓｙｍｐｏｓｉｕｍ ｏｎ Ｃｒｙｐｔｏｇｒａｐｈｙ ａｎｄ Ｉｎｆｏｒｍａｔｉｏｎ Ｓｅｃｕｒｉｔｙ，ｐｐ．５４１－５４６，２００５
【非特許文献２】門田、黄、吉本：個別安全性を保証できる指紋照合，Ｐｒｏｃ．ｏｆ Ｔｈｅ ２００７ Ｓｙｍｐｏｓｉｕｍ ｏｎ Ｃｒｙｐｔｏｇｒａｐｈｙ ａｎｄ Ｉｎｆｏｒｍａｔｉｏｎ Ｓｅｃｕｒｉｔｙ，２００７
【非特許文献３】宇根、大塚、今井：生体認証システムにおける新しいセキュリティ評価尺度：ウルフ攻撃確率，Ｐｒｏｃ．ｏｆ Ｔｈｅ ２００７ Ｓｙｍｐｏｓｉｕｍ ｏｎ Ｃｒｙｐｔｏｇｒａｐｈｙ ａｎｄ Ｉｎｆｏｒｍａｔｉｏｎ Ｓｅｃｕｒｉｔｙ，２００７
【非特許文献４】河上、繁富、美添、宇根、大塚、今井：マニューシャマッチングのウルフに関する理論的考察，Ｐｒｏｃ．ｏｆ Ｔｈｅ ２００７ Ｓｙｍｐｏｓｉｕｍ ｏｎ Ｃｒｙｐｔｏｇｒａｐｈｙ ａｎｄ Ｉｎｆｏｒｍａｔｉｏｎ Ｓｅｃｕｒｉｔｙ，２００７
【非特許文献５】三浦、長坂、宮武：線追跡の反復試行に基づく指静脈パターンの抽出と個人認証への応用，電子情報通信学会論文誌，Ｊ８６－ＤＩＩ，Ｎｏ．５，ｐｐ．６７８－６８７，２００３
【非特許文献６】渡邉、繁富、宇根、大塚、今井：指静脈パターン照合アルゴリズムにおけるユニバーサル・ウルフ，Ｐｒｏｃ．ｏｆ Ｃｏｍｐｕｔｅｒ Ｓｅｃｕｒｉｔｙ Ｓｙｍｐｏｓｉｕｍ（ＣＳＳ２００６），２００６
【非特許文献７】小島、繁富、井沼、大塚、今井：ウルフ攻撃確率を考慮したマッチングアルゴリズムのフレームワークにおける安全で可用性の高い認証プロトコル，Ｐｒｏｃ．ｏｆ Ｔｈｅ ２００９ Ｓｙｍｐｏｓｉｕｍ ｏｎ Ｃｒｙｐｔｏｇｒａｐｈｙ ａｎｄ Ｉｎｆｏｒｍａｔｉｏｎ Ｓｅｃｕｒｉｔｙ，２００９
【発明の概要】
【発明が解決しようとする課題】
【０００５】
しかし、上記の各文献に記載された方法を用いても、攻撃者が照会データを選択的に用いて攻撃した場合に、実用的な処理時間で、ＦＭＲを保証できない。
例えば、非特許文献１に記載された方法は、他人が登録者と偽って自分の生体情報を提示することを前提としており、通常の生体情報の集合から無作為に選ばれた照会データとテンプレートデータとが誤合致する確率を統計的に保証するものである。よって、攻撃者が生体情報の集合から特に誤合致しやすいものを選択的に用いることや、攻撃者が生体情報の集合以外から特に誤合致しやすいものを選択的に用いることは、統計に含まれていない。そのため、このような場合にはＦＭＲを保証することはできない。
非特許文献２に記載された方法は、照合評価値とＦＭＲとの関係を理論的に求めているため、データ毎の個別ＦＭＲにばらつきがない。よって、生体情報の集合の中に、誤合致しやすいデータというものがない。そのため、攻撃者が生体情報の集合から、特に誤合致しやすいものを選択的に用いる攻撃ができない。よって、非特許文献１に記載された方法とは異なり、攻撃者が生体情報の集合から攻撃に用いるデータを選択できるとしても、ＦＭＲを保証することができる。
しかしながら、非特許文献２に記載された方法は、生体情報の特徴量の生起分布を元に計算した、任意パターンと比較する二つのパターンのうちの片方のパターン（指紋Ａ）が偶然に一致する確率を求めるものであり、生体情報の集合以外から比較するもう片方のパターン（指紋Ｂ）を選択して攻撃した場合に偶然一致する確率がどうなるかは不明である。なぜなら、生体情報の集合以外から選択されたデータの特徴量は、生体情報の特徴量の生起分布に従う保証がないためである。そのため、攻撃者が生体情報の集合以外から特に誤合致しやすいものを選択できる可能性があり、このような場合にはＦＭＲを保証することはできない。

同様に、特許文献１に記載された方法でも、生体情報の集合以外からデータを選択して攻撃される場合は想定されておらず、照会データの特徴量が生体情報の特徴量の生起分布に従う場合の確率を求めるか、照会データとテンプレートデータを区別せずに扱っている。

非特許文献７に記載された方法は、認証毎に多くのデータと照合を行うことで、誤合致しやすいかどうかを判断している。この方法では、誤合致しやすさを実験的に評価するため、精度に応じたデータ数が必要になる。例えば、誤って認証される確率を１０００万分の１にしたい場合には、照合毎に最低１０００万、統計的なばらつきを考慮すると、その数倍のデータとの照合を必要とする。１回の認証で数千万回の照合を行うと認証時間が長くかかり、応用上の利便性が著しく低下する。例えば１回の認証に１０００分の１秒かかるとすると、１０００万回照合すると１万秒、つまりおよそ２時間４７分かかることとなる。ドアの開錠に応用した場合、ドアを開けるのに２時間以上かかるのでは、実用性はない。

そこで、本発明は、攻撃者が、生体情報データ集合以外のデータも含めて、照会データを選択的に用いて生体認証システムを攻撃した場合でも、実用的な処理時間でＦＭＲを保証できる生体認証システム、生体認証方法および生体認証プログラム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】

【０００６】

本発明による生体認証システムは、入力されたデータが任意のデータと偶然に一致する確率を計算して評価値として求める評価値計算手段と、評価値計算手段が求めた評価値に基づいて、入力されたデータを予め記憶している生体情報を示すテンプレートデータと同定するか否かを判定する判定手段とを含むことを特徴とする。

本発明による生体認証方法は、入力されたデータが任意のデータと偶然に一致する確率を計算して評価値として求め、求めた評価値に基づいて、入力されたデータを予め記憶している生体情報を示すテンプレートデータと同定するか否かを判定することを特徴とする。

本発明による生体認証プログラムは、コンピュータに、入力されたデータが任意のデータと偶然に一致する確率を計算して評価値として求める評価値計算処理と、求めた評価値に基づいて、入力されたデータを予め記憶している生体情報を示すテンプレートデータと同定するか否かを判定する判定処理とを実行させることを特徴とする。

【発明の効果】

【０００７】

本発明によれば、攻撃者が、生体情報データ集合以外のデータも含めて、照会データを選択的に用いて生体認証システムを攻撃した場合でも、実用的な処理時間でＦＭＲを保証できる。

【図面の簡単な説明】

【０００８】

【図１】本発明による生体認証システムの構成例を示すブロック図である。

【図２】生体認証システムの動作例を示すフローチャートである。

【図３】第２の実施形態における生体認証システムの構成例を示すブロック図である。

【図４】第２の実施形態における生体認証システムの動作例を示すフローチャートである。

【図５】第３の実施形態における生体認証システムの構成例を示すブロック図である。

【図６Ａ】第３の実施形態における認証時の生体認証システムの動作例を示すフローチャートである。

【図６Ｂ】第３の実施形態における登録時の生体認証システムの動作例を示すフローチャートである。

【図７】指紋の特徴点の一例を示す説明図である。

【図８】対応特徴点と判定される特徴点の一例を示す説明図である。

【図９】非対応特徴点と判定される特徴点の一例を示す説明図である。
【図１０】指紋特徴点の一致度合いの判定の一例を示す説明図である。
【図１１】生起分布にしたがって特徴点が観測される一例を示す説明図である。
【図１２】任意の指紋データとの比較の一例を示す説明図である。
【図１３】静脈照会データの一例を示す説明図である。
【図１４】静脈テンプレートデータの一例を示す説明図である。
【図１５】各画素の一致・不一致のラベル付けの一例を示す説明図である。
【図１６】生体認証システムの最小の構成例を示すブロック図である。
【発明を実施するための形態】
【０００９】
実施形態１.
次に、本発明の第１の実施形態について図面を参照して説明する。図１は、本発明による生体認証システムの構成例を示すブロック図である。図１を参照すると、本発明による生体認証システムは、第１の実施形態において、入力手段１、テンプレート記憶手段２、一致度計算手段３、生起分布記憶手段４、評価値計算手段５、判定手段６および出力手段７を含む。なお、生体認証システムは、具体的には、パーソナルコンピュータ等の情報処理装置を用いて実現される。
入力手段１は、具体的には、指紋センサ等の入力装置及びプログラムに従って動作する情報処理装置のＣＰＵによって実現される。入力手段１は、生体認証システムにおいて、照会対象のデータを照会データとして入力する機能を備えている。入力手段１は、テンプレートとして登録されているデータによって特定される人物と同一の人物を特定するデータか否かを判定する照会対象の照会データを読みこむ機能を備えている。例えば、入力手段１は、ユーザによって指紋読取部に指などを当てる操作が行われると、指紋センサを用いて、指紋を含む照会データを入力する。
テンプレート記憶手段２は、具体的には、光ディスク装置や磁気ディスク装置などの記憶装置によって実現される。テンプレート記憶手段２は、生体認証システムの登録者の生体情報を予めテンプレートデータとして記録している。例えば、テンプレートデータは、予めシステム管理者などによってテンプレート記憶手段２に登録される。
一致度計算手段３は、具体的には、プログラムに従って動作する情報処理装置のＣＰＵによって実現される。一致度計算手段３は、入力された照会データと、テンプレート記憶手段２が記録するテンプレートデータとの一致度合いを示す一致度を計算する機能を備えている。
生起分布記憶手段４は、具体的には、光ディスク装置や磁気ディスク装置などの記憶装置によって実現される。生起分布記憶手段４は、生体情報の特徴量の生起分布を記憶する。生起分布については、例えば、システム管理者等が予め実験などによって分布データを作成し、生起分布記憶手段４に登録する。また、例えば、システム管理者が論理値を求めて生起分布記憶手段４に登録するようにしてもよい。なお、特徴量の生起分布とは、特徴量が、ある確率分布にしたがって出現する場合の、確率分布のことを示す。例えば、ある特徴量Ｘが、０～１の範囲で一様（どの値も同じ確率）に出現する場合、特徴量Ｘの生起分布は、０～１の一様分布である。また、例えば、ある特徴量Ｙが平均０、分散１の正規分布にしたがって出現する場合、特徴量Ｙの生起分布は、平均０、分散１の正規分布となる。
評価値計算手段５は、具体的には、プログラムに従って動作する情報処理装置のＣＰＵによって実現される。評価値計算手段５は、入力された照会データが観測された場合に（入力手段１によって照会データが入力された場合）、照会データと任意のデータとが、一致度以上に一致する条件付き確率を求める機能を備えている。すなわち、評価値計算手段５は、入力した照会データが任意のデータに一致する度合いが、一致度計算手段が求めた一致度以上となる確率（条件付き確率）を求める。具体的には、評価値計算手段５は、生起分布記憶手段４が記憶する生起分布に従って観測された（求めた）特徴量と照会データの特徴量との一致度合いを求め、求めた一致度合いが一致度以上となる確率を計算し、第

１の評価値とする。すなわち、評価値計算手段５は、照会データの特徴量と生起分布による特徴量との一致度合いが、一致度計算手段３が計算した照会データとテンプレートデータとの一致度以上となる確率を、照会データと任意のデータとが偶然に一致する確率として算出し、第１の評価値とする。

判定手段６は、具体的には、プログラムに従って動作する情報処理装置のＣＰＵによって実現される。判定手段６は、第１の評価値に基づいて、照会データが、テンプレートデータによって特定される人物と同一の人物を特定するものであるか否かを判定する機能を備えている。判定手段６は、例えば、第１の評価値が所定の閾値より小さい場合に、同一の人物を特定するものであると判定する。すなわち、判定手段６は、第１の評価値を所定の閾値と比較することにより、入力データがテンプレートとして記憶された登録者の生体情報であるか否かを同定する。

出力手段７は、判定手段６による判定結果を出力する機能を備えている。出力手段７は、例えば、ディスプレイ装置等の表示装置によって実現され、判定手段６の指示に従って、判定手段６の判定結果を表示する。

次に、図２のフローチャートおよび図１を参照して、本実施形態における生体認証システムの動作について説明する。図２は、生体認証システムの動作例を示すフローチャートである。

生体認証を行うために、ユーザは、指紋センサ等の入力装置によって実現される入力手段１を操作して、生体情報（例えば、指紋データ）を入力する。すると、入力手段１は、ユーザの操作に従って、生体情報を、テンプレートとして登録されているデータによって特定される人物と同一の人物を特定するデータか否かを判定する照会対象の照会データとして入力する（ステップＳ１１）。

次に、一致度計算手段３は、入力された照会データと、テンプレート記憶手段２に記録されているテンプレートデータとの一致度合いを示す一致度を計算する（ステップＳ１２）。

次に、評価値計算手段５は、入力された照会データが観測された場合に、照会データと任意のデータとが、一致度以上に一致する条件付き確率を、生起分布記憶手段４に記憶された生起分布に従って観測された特徴量と照会データの特徴量とが一致度以上に一致する確率として計算し、第１の評価値とする（ステップＳ１３）。すなわち、評価値計算手段５は、照会データの特徴量と生起分布による特徴量との一致度合いが、一致度計算手段３が計算した照会データとテンプレートデータとの一致度以上となる確率を、照会データと任意のデータとが偶然に一致する確率として算出し、第１の評価値とする。

次に、判定手段６は、第１の評価値に基づいて、照会データが、テンプレートデータによって特定される人物と同一の人物を特定するものであるか否かを判定する（ステップＳ１４）。判定手段６は、例えば、第１の評価値が所定の閾値より小さい場合に、同一の人物を特定するものであると判定する。

次に、出力手段７は、判定手段６による判定結果を出力する。例えば、出力手段７は、ディスプレイ装置等の表示装置によって実現され、判定手段６の指示に従って、判定手段６の判定結果を表示する。

以上のように、本実施形態では、攻撃者が照会データを、生体情報の集合以外からも含めて、選択的に用いて攻撃した場合でも、実用的な処理時間で、ＦＭＲを保証できる認証を行うことができる。

その理由は、本実施形態では、照会データが観測された場合の条件付き確率として、任意のデータの特徴量が生起分布記憶手段４が記憶する生起分布に従って生起したとした場合に、照会データと任意のデータとが、照会データとテンプレートデータとの一致度合い以上に偶然に一致する確率を求め、この偶然一致確率を照合評価値としているからである。

また、攻撃者が一致しやすい照会データを選択的に用いて攻撃した場合でも、その選択された照会データが観測された場合の条件付き確率として扱っているため、求めた条件付き確率には照会データの一致しやすさが織り込み済みであるためである。

更に、本実施形態では、照会データが観測された場合の条件付き確率を求める際に、照会データは観測されたデータをそのまま用いており、照会データについてなんら仮定を置いていない。そのため、生体情報の集合以外から照会データが選択されて入力されたとしても対応できる。

また、本実施形態では、一つの確率値を計算するだけでよく、非特許文献７に記載されているように多数の照合処理を行う必要がないため、実用的な処理時間で認証を行うことができる。

実施形態２．

次に、本発明による生体認証システムの第２の実施形態について図面を参照して説明する。図３は、第２の実施形態における生体認証システムの構成例を示すブロック図である。図４は、第２の実施形態における生体認証システムの動作例を示すフローチャートである。

図３および図４を参照すると、本発明の第２の実施形態における生体認証システムは、第１の実施形態の構成に加え、第２評価値計算手段８を含むことが第１の実施形態と異なる。また、第２の実施形態における生体認証システムは、判定手段６の動作が第１の実施形態と異なる。

第２評価値計算手段８は、具体的には、プログラムに従って動作する情報処理装置のＣＰＵによって実現される。第２評価値計算手段８は、テンプレートデータが観測された場合（照会データの入力に応じてテンプレートデータが入力された場合）に、テンプレートデータと任意のデータとが、第１の一致度以上に一致する条件付き確率を求める機能を備えている。すなわち、第２評価値計算手段８は、テンプレートデータが任意のデータに一致する度合いが、一致度計算手段が求めた一致度以上となる確率（条件付き確率）を求める。具体的には、第２評価値計算手段８は、生起分布記憶手段４に記憶された生起分布に従って観測された（求めた）特徴量とテンプレートデータの特徴量との一致度合いを求め、求めた一致度合いが、第１の一致度以上となる確率を計算し、第２の評価値とする。すなわち、第２評価値計算手段８は、テンプレートデータの特徴量と生起分布による特徴量との一致度合いが、一致度計算手段３が計算した照会データとテンプレートデータとの一致度以上となる確率を、テンプレートデータと任意のデータとが偶然に一致する確率として算出し、第２の評価値とする。

第２の実施形態において、判定手段６は、第１の評価値と第２の評価値との両方に基づいて、照会データが、テンプレートデータによって特定される人物と同一の人物を特定するものであるか否かを判定する機能を備えている。判定手段６は、例えば、第１の評価値および第２の評価値が所定の閾値より小さい場合に、同一の人物を特定するものであると判定する。

次に、本発明による生体認証システムの第２の実施形態の効果について説明する。本実施形態では、第２評価値計算手段８は、テンプレートデータと任意のデータとが偶然に一致する確率を第２の評価値として算出する。そして、判定手段６は、第１の評価値に加え、テンプレートデータと任意のデータとが偶然に一致する確率にも基づいて、照会データがテンプレートデータによって特定される人物と同一の人物を特定するものであるか否かを判定する。従って、本実施形態では、攻撃者によってテンプレートデータに一致しやすいデータをテンプレートとして登録する攻撃が行われたとしても、ＦＭＲを保証することができる。

実施形態３．

次に、本発明による生体認証システムの第３の実施形態について図面を参照して説明する。図５は、第３の実施形態における生体認証システムの構成例を示すブロック図である。図６Ａは、第３の実施形態における認証時の生体認証システムの動作例を示すフローチャートである。図６Ｂは、第３の実施形態における登録時の生体認証システムの動作例を示すフローチャートである。

図５および図６Ａ、Ｂを参照すると、本発明の第３の実施形態における生体認証システムは、第１の実施形態の構成に加えて、登録データ検証手段９を含むことが第１の実施形

態と異なる。

登録データ検証手段９は、具体的には、プログラムに従って動作する情報処理装置のＣＰＵによって実現される。登録データ検証手段９は、テンプレートを記録する際に、テンプレートとして登録するデータが正規なものか否かを検証し、正規なものと検証された場合のみ、テンプレート記憶手段２へ登録する機能を備えている。

次に、本発明による生体認証システムの第３の実施形態の効果について説明する。第１の実施形態では、テンプレート記憶手段２には正しく生体情報が登録されていることを前提とし、攻撃者が生体情報の集合以外から照会データを選択する攻撃を行っても、ＦＭＲを保証するようにしていた。本実施形態では、登録データ検証手段９は、テンプレートとして登録するデータを検証し、正規なものと検証された場合のみテンプレート記憶手段２に登録する。従って、本実施形態では、上記の前提が成り立つことを保証し、より確実にＦＭＲを保証することができる。なお、本実施形態においても、第２の実施形態で示した第２評価値計算手段８を含むようにしてもよい。

【実施例１】

【００１０】

次に、具体的な実施例を用いて、本発明による生体認証システムの動作を説明する。この実施例は本発明の第１の実施形態に対応する。

本実施例では、指紋を用いて登録者か否かを判定する生体認証システムに本発明を適用する場合を例に説明する。本実施例における生体認証システムは、指紋センサが検出した指紋データを入力し、入力した指紋データとテンプレートとして記録している指紋データとが、同一人物を特定するものか否かを判定することで、登録者か否かを判定する。

指紋とは、指先に見られる隆線と呼ばれる線状の皮膚の隆起パターンであり、万人不同、終生不変であることから個人の同定に用いられる。二つの指紋の一致度合いを調べる方法には、マニューシャと呼ばれる図７に示すような隆線の端点や分岐点といった特徴点を比較する方法がある。特徴点を用いた一致度計算方法の一例として、二つの指紋データの特徴点の位置を重ねた場合において、特徴点の位置が差Ｒ以内の場合を対応特徴点（図８）、特徴点の位置が差Ｒ以上の場合を非対応特徴点（図９）とし、対応特徴点の数を一致度合いとする方法がある。

本実施例では、入力手段１として、特徴点を検出する機能を備えた指紋センサを用いる。認証を行うために、ユーザが指紋センサに指を置くと、入力手段１は、指紋画像を読み込み、読み込んだ指紋画像から特徴点を抽出し、特徴点の位置を特徴量とする照会データを作成する。

ここで、テンプレート記憶手段２には、システム管理者等によって、予め登録者の指紋データが、特徴点の位置を特徴量とするテンプレートデータとして登録されているものとする。なお、テンプレート記憶手段２としては、例えば、ＩＣカードや不揮発性メモリ、ハードディスク等の任意の記憶媒体を用いることができる。

入力手段１が照会データを作成すると、図１０に示すように、一致度計算手段３は、照会データの特徴点とテンプレート記憶手段２が記憶するテンプレートデータの特徴点とを比較し、対応特徴点を調べ、対応特徴点の数を第１の一致度として求める。

例えば、照会データにはＮｓ個の特徴点、テンプレートデータにはＮｔ個の特徴点があり、そのうち位置の差がＲ以内であるものがＭ個であったとする。この場合、一致度計算手段３は、この照会データとテンプレートデータとの一致度合い（一致度）をＭとして求める。

ここで、非特許文献４で想定しているような一致度Ｍの値そのものと閾値とを比較して同一か否かを判定する認証システムの場合、非特許文献４で示されているように、特徴点の非常に多いデータを照会データとすることで、高い確率で同一と判定されてしまうことになる。そのため、非特許文献４で想定しているような認証システムでは、攻撃者は、特徴点の非常に多いデータを選択して攻撃を行うことで、ＦＭＲを高くすることができる。

そこで本実施例では、一致度計算手段３は、一致度Ｍの値そのものと閾値とを比較するのではなく、照会データと任意のデータとを比較とすると、一致度Ｍよりも偶然に高い一

致度が得られる確率を求め、その確率を評価値とする。

生起分布記憶手段４は、生体情報の特徴量の生起分布を記憶している。なお、生起分布記憶手段４としては、例えば、不揮発性メモリ、ハードディスク装置等の任意の記憶媒体を用いることができる。

本実施例では、特徴点の位置を特徴量としているため、生起分布記憶手段４は、特徴点の数の生起分布と特徴点の座標値（Ｘ座標値とＹ座標値）の生起分布とを記憶している。例えば、指紋の特徴点の個数が所定の平均値と分散とを持つ正規分布に従い、その位置が指の中に一様に分布している場合を想定する。この場合、生起分布記憶手段４は、特徴点の個数として、（１）式で示される平均μＮと分散σＮとを持つ正規分布ｐＮ（ｘ）を記憶する。また、生起分布記憶手段４は、Ｘ座標値として、（２）式で示される指幅（ＭｉｎＸ～ＭａｘＸ）に応じた一様分布ｕＸ（ｘ）を記憶する。また、生起分布記憶手段４は、Ｙ座標値として、（３）式で示される指高（ＭｉｎＹ～ＭａｘＹ）に応じた一様分布ｕＹ（ｘ）を記憶する。

【数１】

$$P_N(x)=\frac{1}{\sqrt{2\pi}\,\sigma_N}\exp\left(-\frac{(x-\mu_N)^2}{2\sigma^2{}_N}\right)\quad\cdots(1)$$

【数２】

$$u_X(x)=\frac{1}{Max_X-Min_X}\quad\cdots(2)$$

【数３】

$$u_Y(x)=\frac{1}{Max_Y-Min_Y}\quad\cdots(3)$$

次に、評価値計算手段５は、入力された照会データが観測された場合に、照会データと任意の指紋データとの一致度を調べた場合に、一致度Ｍよりも多くの特徴点が一致する確率を求める。

評価値計算手段５は、任意のデータとの比較については、生起分布記憶手段４が記憶する生起分布に従って特徴点が観測されたと仮定した場合に（図１１）、観測された特徴点と照会データの特徴点とを比較することで行う（図１２）。

指紋の面積をＳとすると、一つの特徴点と対応特徴点とされる位置の範囲はπＲ２である。そのため、評価値計算手段５は、Ｘ座標値、Ｙ座標値共に一様分布に従って観測された特徴点が、ある一つの特徴点と対応特徴点とされる確率ｐを、以下の（４）式に示すように求めることができる。

【数４】

$$p=\frac{\pi R^2}{S}\quad\cdots(4)$$

また、評価値計算手段５は、（５）式に示すように指紋全体の領域をπＲ２の領域に分割するとＮｃ個の部分領域に分割できる。

【数５】

$$N_C = \left[\frac{S}{\pi R^2} \right] \quad \cdots(5)$$

また、評価値計算手段５は、照会データの特徴点数ＮがＮｓ個の場合に、Ｘ座標値、Ｙ座標値を生起分布記憶手段４が記憶する一様分布に従って観測されたＮｔ個の点のうち、ちょうどｍ個が、Ｎｃ個の部分領域のうちのＮｓ個の照会データの特徴点を含む部分領域のどれかに入り、残りの（Ｎｔ－ｍ）個が照会データの特徴点を含まない（Ｎｃ－Ｎｓ）個の部分領域のどれかに入る確率Ｐ（Ｎｔ，ｍ｜Ｎ＝Ｎｓ）は、以下の（６）式に示すように求めることができる。

【数６】

$$P(N_t, m \mid N = N_S) = \frac{\binom{N_S}{m}\binom{N_C - N_S}{N_t - m}}{\binom{N_C}{N_t}} \quad \cdots(6)$$

また、評価値計算手段５は、ちょうどｍ個対応する確率がＰ（Ｎｔ，ｍ｜Ｎ＝Ｎｓ）であるので、Ｍ個以上偶然対応する確率ＰＡ（Ｎｔ，Ｍ｜Ｎ＝Ｎｓ）を、以下の（７）式に示すように求めることができる。

【数７】

$$P_A(N_t, M \mid N = N_S) = \sum_{m=M}^{N_S} P(N_t, m \mid N = N_S) \quad \cdots(7)$$

また、特徴点の個数については、生起分布記憶手段４が記憶する（１）式で示される分布に従って観測されるため、評価値計算手段５は、照会データの特徴点数ＮがＮｓ個の場合の、偶然対応特徴点がＭ個以上となる確率の期待値ＡＣＰ（Ｍ｜Ｎ＝Ｎｓ）を、以下の（８）式に示すように求めることができる。

【数８】

$$ACP(M \mid N = N_S) = \int P_A(x, M \mid N = N_S) p_N(x) dx \quad \cdots(8)$$

判定手段６は、この偶然に一致する確率ＡＣＰ（Ｍ｜Ｎ＝Ｎｓ）を所定の閾値と比較し、所定の閾値よりも小さければ偶然に一致したのではないとして、同じ人物の指紋であると判定する。また、判定手段６は、所定の閾値以上であれば偶然に一致した可能性が高いとして、同じ人物の指紋ではないと判定する。その後、出力手段７は、判定手段６による判定結果を出力する。例えば、出力手段７がディスプレイ装置等の表示装置によって実現される場合には、出力手段７は、判定手段６で求められた判定結果を表示する。

なお、この偶然に一致する確率ＡＣＰ（Ｍ｜Ｎ＝Ｎｓ）は、任意のデータと照合した場合に偶然に一致する確率であるので、ＦＭＲを直接示す値となる。そのため、所定の閾値としては、生体認証システムに許容されるＦＭＲや、生体認証システムに許容されるＦＭＲに１より小さい安全係数をかけた値を用いることができる。

例えば、非特許文献４で示されるような、対応する特徴点が多くなりやすい特徴点の非常に多いデータを攻撃者が選んで攻撃した場合、Ｎｓが非常に大きくなると、（６）式で

示される対応する特徴点がちょうどｍ個ある確率が大きくなるものがあったり、（７）式で示す数式において多くの項の和をとることになる。そのため、結果として、（８）式で示される偶然に一致する確率ＡＣＰ（Ｍ｜Ｎ＝Ｎｓ）が大きくなり、判定手段６は、登録者とは判定しない。

一方、特徴点が多い本人のデータを照会データとした場合、Ｎｓが大きくなるが、本人のデータ同士なのでＭもＮｓの増加に応じて大きくなる。そのため、（７）式で示す数式において和をとる項が少なくなり、（８）式で示される偶然に一致する確率ＡＣＰ（Ｍ｜Ｎ＝Ｎｓ）はそれほど大きくならない。そのため、本人の照会データを登録者ではないと判定する誤りは起こりにくい。

また、本実施例では、照会データに対しては生体情報の生起分布に従うことを仮定しておらず、入力された照会データが観測された場合の条件付き確率として偶然に一致する確率を計算している。そのため、本実施例における生体認証システムでは、攻撃者が生体情報の集合以外から照会データを選択した場合でも、偶然に一致する確率を正しく計算することができる。

また、本実施例では、入力された照会データが観測された場合の条件付き確率として、照会データと任意のデータとが、照会データとテンプレートデータとの一致度以上に偶然に一致する確率を計算している。ここで、照会データとテンプレートデータとを入れ換えて、テンプレートデータが観測された場合の条件付き確率として、テンプレートデータと任意のデータとが、照会データとテンプレートデータとの一致度以上に偶然に一致する確率として計算してはならない。それは、テンプレートデータについては、生体認証システムが管理するものであり、正しく生体情報がテンプレートデータとして登録されていることを念頭においているが、照会データについては、攻撃者が自由にデータを選んで入力できるため、生体情報の集合以外からデータを選択することも想定されるからである。そのため、入力された照会データが観測された場合の条件付き確率として求めることが重要である。

本実施例では、指紋の特徴点位置の座標値を特徴量として用いて説明したが、位置に加えて特徴点の接する隆線の方向や接する隆線の曲率、端点や分岐点等の特徴点の種別等他の特徴量も、事前に生起分布や生起確率を求めることができれば、同様に特徴量として用いることができる。

また、本実施例では、特徴点の位置を所定の距離以内にあるか否かによって一致度合いを計算しており、特徴点の位置が非常に近いのか、所定の距離以内ではあるが、ある程度離れているのかについては判定に用いていない。これらを考慮して、例えば、非特許文献２の４．２節に記載されているような計算方法を用いて、位置差の距離についても偶然に一致する確率を計算することもできる。

また、本実施例では、特徴点数の生起分布として、正規分布を用いたが、対象に応じてχ自乗分布やｔ分布等の一般の確率分布を用いることができる。また、連続分布だけではなく、２項分布等の非連続分布を用いることもできる。同様に、座標値の生起分布として一様分布を用いたが、対象に応じて、他の一般の確率分布を用いることができる。例えば、特徴点が指の中心に多く、周辺に少ない場合であれば、特徴点の位置は、指の中心を平均とし、所定の分散を持った２次元正規分布に従うとすることができる。また、指は正円より楕円に近いので、横方向と縦方向で異なった分散を持つ、２次元正規分布とすることもできる。

特徴量の生起分布としては、事前に対象生体情報の物理的制約等から理論的に分布を求めることもできるし、実際にデータを計測することで分布を推定して用いることもできる。また、数式として表される分布として扱うこともできるし、数式として表せなくても数表として特徴量と出現頻度の関係を定めることもできる。

また、本実施例では、一致度計算手段３が特徴点の位置（座標値）が対応した個数を一致度として計算したが、特徴量の生起分布を事前に求めることができ、特徴量の一致度合いを定めることができれば、任意の特徴量と任意の一致度とを用いることができる。

例えば、指紋画像の画素値を直接用いて、画素値の生起分布を予め求めておき、照会デ

ータとテンプレートデータとで同一画素の画素値が所定の差以内になると一致画素とする。そして、一致画素数を照会データとテンプレートデータとの一致度としたり、同一画素の画素値差の全画素での合計を照会データとテンプレートデータとの一致度としたりすることができる。

また、本実施例では、指紋の面積をＳで共通として計算したが、指紋の入力毎の位置ずれを考慮して、照会指紋およびテンプレート指紋の押捺されている領域をそれぞれ求め、共通に押捺されている部分に限って照合に用いることもできる。

また、本実施例では、テンプレートデータの指紋特徴点の数は、生起分布記憶手段４が記憶する特徴点数の生起分布に従って観測されるとして計算したが、実際にテンプレートデータの特徴点数を用いることもできる。その場合、（８）式に示すように特徴点数での期待値をとる必要が無く、（７）式を用いて求めた値を照合評価値として用いればよい。

また、本実施例では、特徴点を検出する機能を備えた指紋センサを入力装置として用いたが、カメラのような純粋に入力機能だけを備えた入力装置を用いて、入力装置から入力された画像から別途特徴を抽出する特徴抽出手段を含むように構成してもよい。また、生体認証システムを備えた情報処理装置がネットワークを介して他の機器と接続し、他の機器で入力したデータを、ネットワークを介して受信するようにしてもよい。

また、本実施例では、出力手段７としてディスプレイ装置に判定結果を表示するよう構成したが、例えば、ドアの電子錠に判定結果を含む信号を送るように構成し、ドアを用いた入退管理システムに適用することができる。また、クライアントＰＣから認証結果をアプリケーションサーバへネットワークを介して送信する等、本人認証が必要な任意の場面で出力結果を利用できるよう構成することができる。

また、本実施例では、認証に用いる生体情報として指紋を用いたが、個人で異なる特徴を持ち、特徴量の生起分布を事前に求めることができ、一致度を定めることができれば、例えば、顔画像や虹彩、静脈、掌形等の任意の生体情報を用いることができる。

【実施例２】

【００１１】

次に、第２の実施例について説明する。かかる実施例は、本発明の第２の実施形態に対応するものである。本実施例は、第１の実施形態の構成に加えて、第２評価値計算手段８を含むことが第１の実施形態と異なる。本実施例では、指静脈を用いて登録者か否かを判定する生体認証システムに本発明を適用する場合を例に説明する。また、本実施例で用いる指静脈の特徴量は、非特許文献５のように各画素を静脈画素（Ｖ）、背景領域（Ｂ）及びあいまい領域（Ｕ）の３種類に分類することとする（図１３、図１４）。以後、説明を簡単にするため、静脈パターンを３×３画素として扱う。

生起分布記憶手段４は、各画素が各領域（カテゴリ）に分類される確率を記録している。各画素に対して静脈画素と分類される確率（ＰＶ）、背景画素と分類される確率（ＰＢ）、あいまい画素と分類される確率（ＰＵ＝（１－ＰＶ－ＰＢ））と同じ確率とすることもできるし、各画素に違う値を割り振ることもできる。ここでは、説明を簡単にするため、全画素に対して共通の値ＰＶ＝ＰＢ＝ＰＵ＝１／３であるとする。

本実施例では、入力手段１として、指静脈を検出する機能を備えたセンサを用いる。認証を行うために、ユーザがセンサに指を置くと、入力手段１は、指静脈を検出して入力し、各画素を静脈画素（Ｖ）、背景領域（Ｂ）及びあいまい領域（Ｕ）の３種類に分類し、照会データＶＳとする（図１３）。

ここで、テンプレート記憶手段２は、各画素を静脈画素（Ｖ）、背景領域（Ｂ）及びあいまい領域（Ｕ）の３種類に分類されたテンプレートデータＶＴ（図１４）を記録しているものとする。これらのテンプレートデータＶＴは、例えば、予めシステム管理者等によって登録される。

次に、一致度計算手段３は、照会データＶＳとテンプレートデータＶＴとの一致度を計算する。一致度計算手段３は、一致度として、あいまい領域以外の静脈領域と背景領域とが同じ領域に分類されている画素数を用いる。一致度計算手段３は、照会データＶＳ（図１３）およびテンプレートデータＶＴ（図１４）の各画素で、両方が静脈領域又は両方が

背景領域で一致している画素を○、片方が静脈領域でもう片方が背景領域と不一致な画素を×、どちらかがあいまい領域のため比較対象とされない画素を△とラベルづけする（図１５）。具体的には、一致度計算手段３は、いずれの画像であるかを判定する処理を行う。そして、一致度計算手段３は、×とならなかった画素数Ｍを第１の一致度とする。

次に、第１の評価値計算手段５は、照会データＶＳが観測された場合に、照会データＶＳと任意のデータとが偶然に、照会データＶＳとテンプレートデータＶＴとの一致度Ｍ以上に一致する条件付き確率Ｐ１（ＶＴ，Ｍ｜ＶＳ）を求め、第１の評価値とする。

例えば、照会データＶＳの全ＮＡ＝９画素のうち、あいまい画素でない画素数がＮｓＲ、あいまい画素数がＮｓＵであったとする。この場合、照会データのあいまい画素でない画素が任意のデータと比較すると、不一致となる確率は１／３である。また、あいまい画素は不一致とならない。そのため、×（照会データのあいまい画素でない画素が不一致となる）となる画素数がちょうどｍ個となる確率Ｐ（ｍ｜ＮｓＲ）は、以下の（９）式に示すように求めることができる。

【数９】

$$P(m \mid N_S^R) = {}_{N_S^R}C_m \left(\frac{1}{3}\right)^m \left(\frac{2}{3}\right)^{(N_S^R - m)} \quad \cdots(9)$$

よって、照会データＶＳが観測された場合に、照会データＶＳと任意のデータとが偶然に、照会データＶＳとテンプレートデータＶＴとの一致度Ｍ以上に一致する条件付き確率Ｐ１（ＶＴ，Ｍ｜ＶＳ）は、ちょうどｋ個一致するということはｋ個×にならないということであり、（ＮＡ－ｋ）個×となるということであるので、以下の（１０）式に示すように求めることができる。

【数１０】

$$P_1(V_T, M \mid V_S) = \sum_{k=M}^{N_A} P(N_A - k \mid N_S^R) \quad \cdots(10)$$

非特許文献７には、非特許文献５に記載された静脈パターンの認証方法では、攻撃者が全ての画素があいまい領域である照会データを用いると、必ず登録者であると認証されることが指摘されている。非特許文献５に記載された静脈パターンの認証方法では、一致度として×とならない画素の割合を用いており、本実施例で用いている一致度とは計算式が異なるが、本実施例で用いている一致度でも、あいまい領域が多いと一致度が高くなり、全てがあいまい領域であると一致度が最も高くなることは同様である。

しかしながら、本実施例では、不一致でない画素数を直接用いるのではなく、任意のデータと比較した場合に偶然に一致する確率として扱っており、照会データのあいまい領域が多い場合、ＮｓＲが小さくなるため、（９）式で求められる確率が大きくなり、（１０）式で求められる確率が大きくなる。そのため、全てがあいまい領域な照会データを攻撃者が選択したとしても、登録者として判定することはない。

次に、第２の評価値計算手段は、テンプレートデータＶＴが観測された場合に、テンプレートデータＶＴと任意のデータとが、偶然に、照会データＶＳとテンプレートデータＶＴとの一致度Ｍ以上に一致する条件付き確率Ｐ２（ＶＳ，Ｍ｜ＶＴ）を求め、第２の評価値とする。なお、Ｐ２（ＶＳ，Ｍ｜ＶＴ）の計算方法は、Ｐ１（ＶＴ，Ｍ｜ＶＳ）の計算方法で、照会データとテンプレートデータとを入れ換えたものと等しいため、説明を省略する。

次に、判定手段６は、第１の評価値と第２の評価値との両方が、所定の閾値よりも小さい場合に、登録者と同じ人物であると判定し、どちらかが所定の閾値以上の場合には、登

録者と同じ人物ではないと判定する。
所定の閾値としては、第１の評価値の場合と第２の評価値の場合とで同じ値を用いることもできるし、異なる値にすることもできる。特に、テンプレート登録時よりも照会時のほうが攻撃者が攻撃しやすいため、第２の評価値と比較する閾値よりも第１の評価値と比較する閾値を厳しくしておくことが好ましい。また、判定手段６は、第１の評価値と第２の評価値とのそれぞれで判定し、判定結果を総合することもできる。また、判定手段６は、第１の評価値と第２の評価値とを、例えば所定の係数をかけて加えるといった所定の式に代入して得られた値を所定の閾値と比較して判定するようにすることもできる。
本実施例の第２評価値計算手段８は、本実施例に記載された静脈認証の場合のみでなく、第１の実施例に記載した顔画像や虹彩、静脈、掌形等の任意の生体情報に対して追加して構成できるものである。
次に、本実施例における生体認証システムの効果について説明する。第１の実施例では、テンプレートデータとしては正しく生体情報が登録されていると想定し、その想定の下では、攻撃者が生体情報の集合以外から照会データを選択して攻撃してもＦＭＲを保証することができた。しかし、第１の実施例における生体認証システムでは、攻撃者がテンプレートデータに生体情報以外を登録する場合を想定しておらず、その場合にはＦＭＲの保証ができない。
本実施例では、第１の実施例の構成に加えて、テンプレートと任意のデータとが偶然に一致する確率も用いて判定するように構成されている。そのため、攻撃者がテンプレートに一致しやすいデータを登録する攻撃に対しても、ＦＭＲを保証することができる。
【実施例３】
【００１２】
次に、第３の実施例について説明する。かかる実施例は本発明の第３の実施形態に対応するものである。本実施例における生体認証システムは、第１の実施形態の構成に加えて、登録データ検証手段９を含むことが第１の実施形態と異なる。
登録データ検証手段９は、テンプレートを記録する際に、テンプレートとして登録するデータが正規なものか否かを検証し、正規なものと検証した場合のみ、テンプレート記憶手段２へ登録する機能を備えている。
本実施例における生体認証システムでは、例えば、利用者が運転免許証のようなＩＤカードを入力する操作を行った場合に、登録データ検証手段９がＩＤ番号により正当な利用者であることを確認しないと登録を受けつけないようにすることができる。また、登録データ検証手段９は、例えば、光学的、電気的、磁気的な計測装置により、登録用の入力装置に入力されたのが本物の生体情報なのか否かを判定し、本物の生体情報と判定された場合のみテンプレートとして登録するようにすることもできる。
次に、本実施例における生体認証システムの効果について説明する。本実施例では、第１の実施例に加えて、登録データ検証手段９により正規なものと検証された場合のみ、テンプレートとしてテンプレート記憶手段２に登録する。第１の実施例では、テンプレート記憶手段２には正しく生体情報が登録されていることを前提とし、攻撃者が生体情報の集合以外から照会データを選択する攻撃を行っても、ＦＭＲを保証するようにしていた。本実施例では、登録データ検証手段９がテンプレートとして登録するデータを検証することで、上記の前提が成り立つことを保証し、より確実にＦＭＲを保証することができる。
以上のことから、本発明は、次のような特徴を有するといえる。本発明による生体認証システムは、照会データを入力する入力手段と、テンプレートデータを登録するテンプレート記憶手段と、生体情報の特徴量の生起分布を記憶する生起分布記憶手段と、照合データとテンプレートデータとを比較して、一致度合いを求める一致度計算手段と、任意の生体情報と照会データとが偶然に一致する偶然一致確率を、照会データが観測された場合に任意のデータと一致する条件付き確率として、任意のデータの特徴量が生起分布記憶手段が記憶する生起分布に従って生起した場合に、観測された照会データとの一致度合いが一致度以上になる確率として求める偶然一致確率計算手段と、偶然一致確率を照合評価値とし、照合評価値と予め定められた閾値とを比較することで照会データとテンプレートデー

タとが同一人物のものであるか否かを判定する判定手段とを含む。

次に、本発明による生体認証システムの最小構成について説明する。図１６は、生体認証システムの最小の構成例を示すブロック図である。図１６に示すように、生体認証システムは、評価値計算手段５と、判定手段６とを含む。

図１６に示す最小構成の生体認証システムでは、評価値計算手段５は、入力されたデータが任意のデータと偶然に一致する確率を計算して評価値として求める。そして、判定手段６は、評価値計算手段５が計算した評価値に基づいて、入力されたデータを予め記憶している登録者の生体情報を示すテンプレートデータと同定するか否かを判定する。

従って、最小構成の生体認証システムによれば、攻撃者が照会データを、生体情報の集合以外からも含めて、選択的に用いて攻撃した場合でも、実用的な処理時間で、ＦＭＲを保証できる認証を行うことができる。

なお、本実施形態では、以下の（１）～（１１）に示すような生体認証システムの特徴的構成が示されている。

（１）生体認証システムは、入力されたデータ（例えば、入力データ）が任意のデータと偶然に一致する確率を計算して評価値として求める評価値計算手段（例えば、評価値計算手段５によって実現される）と、評価値計算手段が求めた評価値に基づいて、入力されたデータを予め記憶している（例えば、テンプレート記憶手段２によって実現される）登録者の生体情報を示すテンプレートデータと同定するか否かを判定する判定手段（例えば、判定手段６によって実現される）とを含むことを特徴とする。

（２）生体認証システムにおいて、入力されたデータとテンプレートデータとの一致度合いを計算する一致度計算手段（例えば、一致度計算手段３によって実現される）を含み、評価値計算手段は、予め記憶している（例えば、生起分布記憶手段４によって実現される）生体情報に含まれる特徴量の生起分布に基づく特徴量と入力されたデータの特徴量との一致度合いが、一致度計算手段が計算した一致度合い以上となる確率を計算して評価値として求め、判定手段は、評価値計算手段が求めた評価値と所定の閾値とを比較することにより、入力されたデータをテンプレートデータと同定するか否かを判定するように構成されていてもよい。

（３）生体認証システムは、生体情報に含まれる特徴量の生起分布を記憶する生起分布記憶手段（例えば、生起分布記憶手段４によって実現される）と、入力データが入力されたという条件下での、入力データが任意のデータと偶然に一致する第１の条件付き確率（例えば、第１の評価値）を、生起分布記憶手段が記憶する生起分布に従い求められる特徴量と入力データの特徴量との一致度合いが、入力データと予め記憶している（例えば、テンプレート記憶手段２によって実現される）登録者の生体情報を示すテンプレートデータとの一致度合い以上となる確率として算出する条件付き確率算出手段（例えば、評価値計算手段５によって実現される）と、条件付き確率算出手段が算出した第１の条件付き確率を所定の閾値と比較することにより入力データがテンプレートとして記憶された登録者の生体情報であるか否かを同定する同定手段（例えば、判定手段６によって実現される）とを含むことを特徴とする。

（４）生体認証システムにおいて、同定手段は、閾値として、生体認証システムで許容される他人受入率の値、他人受入率に所定の１未満の値である安全係数を乗じた値、又は他人受入率を所定の式に代入して演算することにより定まる値のいずれかを用いるように構成されていてもよい。

（５）生体認証システムにおいて、第１の条件付き確率に加え、テンプレートデータが入力されたという条件下での、任意のデータと偶然に一致する第２の条件付き確率を、生起分布に従い観測される特徴量とテンプレートデータの特徴量との一致度合いが、入力データとテンプレートデータとの一致度合い以上となる確率として算出する第２の条件付き確率算出手段（例えば、第２評価値計算手段８によって実現される）を含み、同定手段は、第１の条件付き確率及び第２の条件付き確率算出手段が算出した第２の条件付き確率（例えば、第２の評価値）の両方を用いて同定を行うように構成されていてもよい。

（６）生体認証システムにおいて、テンプレートデータ登録時に、テンプレートが生体

情報であることを検証する登録データ検証手段（例えば、登録データ検証手段９によって実現される）を含むように構成されていてもよい。

（７）生体認証システムにおいて、特徴量として特徴点の位置を用い、照会データとテンプレートデータとの特徴点のうち、所定の距離以内にある照会データとテンプレートデータとの特徴点の組を対応特徴点とし、対応特徴点の数を一致度合いとして求める対応特徴点数算出手段（例えば、一致度計算手段３によって実現される）を含み、第１の条件付き確率算出手段は、特徴点を生起分布に従って配置した場合に、照会データの特徴点と対応する特徴点の数が、対応特徴点数算出手段が算出した照会データとテンプレートデータとの間で対応する特徴点の数より多くなる確率を第１の条件付き確率として求めるように構成されていてもよい。

（８）生体認証システムにおいて、生体情報として指紋を用い、特徴点として指紋隆線の途切れる点や分岐する点を用いるように構成されていてもよい。

（９）生体認証システムにおいて、生体情報として静脈を用い、特徴点として静脈の途切れる点や分岐する点を用いるように構成されていてもよい。

（１０）生体認証システムにおいて、生体情報として画像を用い、画像中の各画素をカテゴリに分類し、特徴量として各画素のカテゴリを用い、照会データとテンプレートデータとの画素のうち、カテゴリが所定の関係にある照会データとテンプレートデータとの画素の組を対応画素とし、対応画素の数を一致度合いとして求める対応画素数算出手段（例えば、一致度計算手段３によって実現される）を含み、第１の条件付き確率算出手段は、各画素のカテゴリを生起分布に従って配置した場合に、照会データの画素と対応する画素の数が、対応画素数算出手段が算出した照会データとテンプレートデータとの間で対応する画素の数より多くなる確率を第１の条件付き確率として求めるように構成されていてもよい。

（１１）生体認証システムにおいて、生体情報として静脈を用い、画素のカテゴリとして静脈領域、背景領域及びあいまい領域を用い、対応画素とするカテゴリの所定の関係として、静脈領域と背景領域との組み合わせではないことを条件として対応画素を求めるように構成されていてもよい。

以上、実施形態を参照して本願発明を説明したが、本願発明は上記実施形態に限定されるものではない。本願発明の構成や詳細には、本願発明のスコープ内で当業者が理解しうる様々な変更をすることができる。

この出願は、２００９年９月９日に出願された日本出願特願２００９－２０８０４２を基礎とする優先権を主張し、その開示の全てをここに取り込む。

【産業上の利用可能性】

【００１３】

本発明は、生体情報を用いて利用者の認証を行う生体認証システムの分野に適用できる。

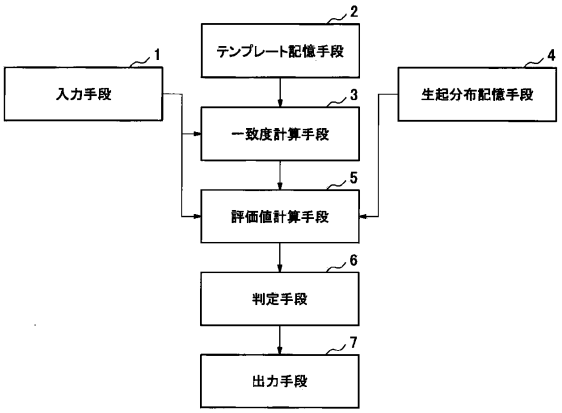
【符号の説明】

【００１４】

１　入力手段
２　テンプレート記憶手段
３　一致度計算手段
４　生起分布記憶手段
５　評価値計算手段
６　判定手段
７　出力手段
８　第２評価値計算手段
９　登録データ検証手段

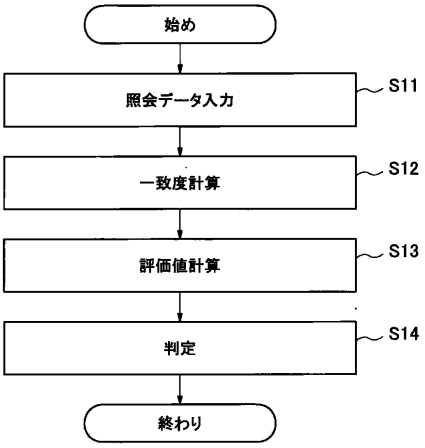
【図１】

図1



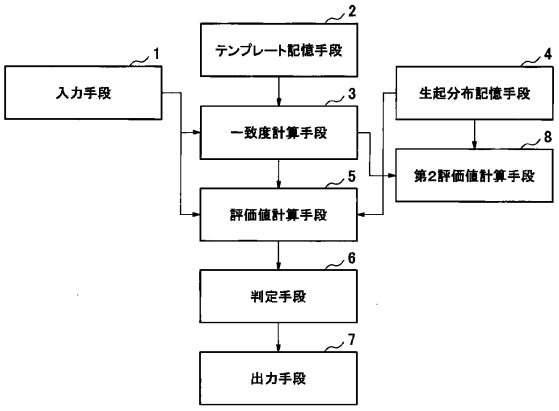
【図２】

図2



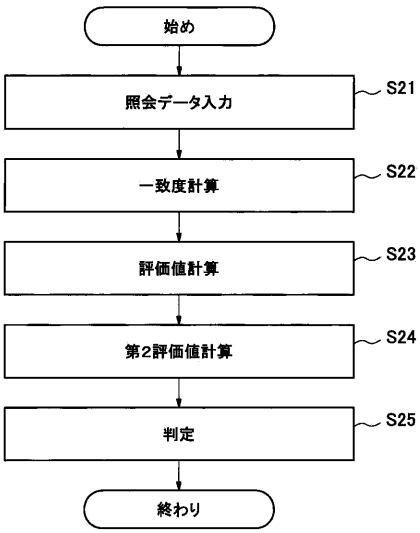
【図３】

図3



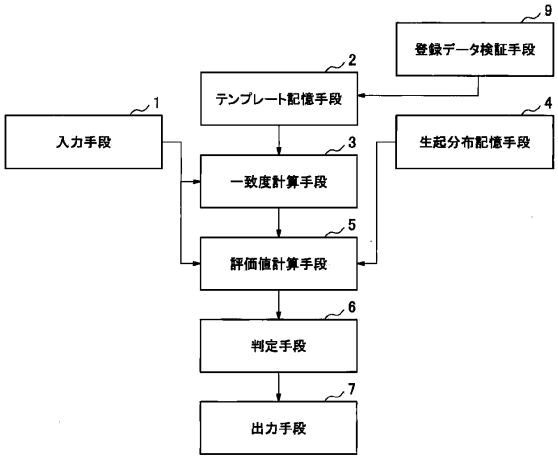
【図４】

図4



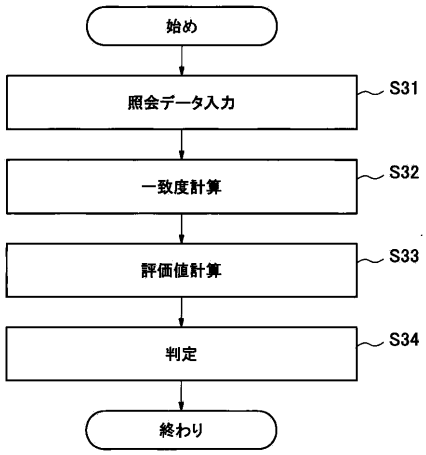
【図５】

図5



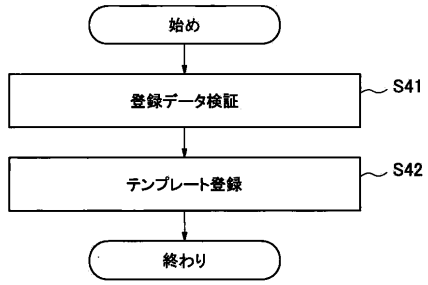
【図６Ａ】

図6A



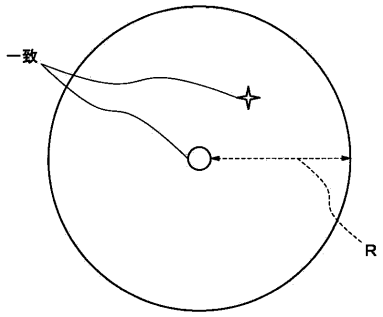
【図６Ｂ】

図6B



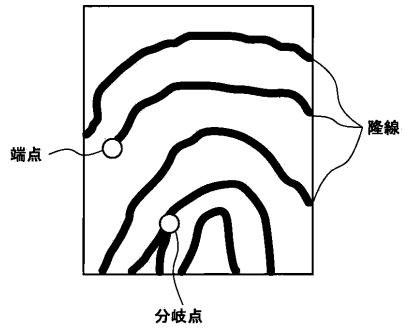
【図８】

図8



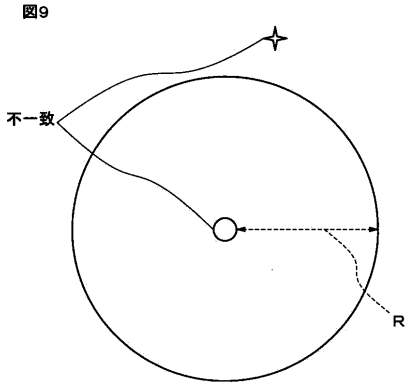
【図７】

図7



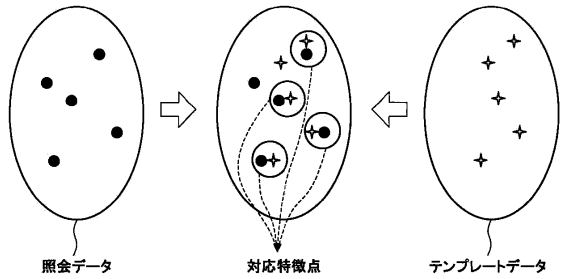
【図９】

図9



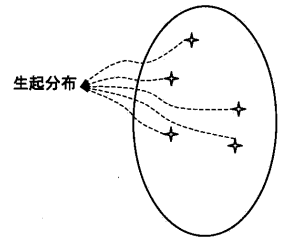
【図１０】

図10



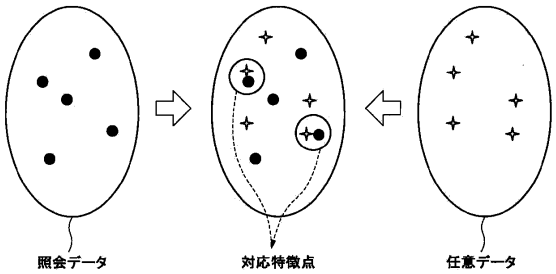
【図１１】

図11



【図１２】

図12



【図１３】

図13

V	B	V
V	U	B
B	U	B

【図１４】

図14

V	U	V
V	U	B
B	B	V

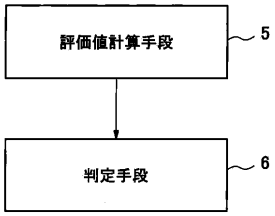
【図１５】

図15

○	△	○
○	△	○
○	△	×

【図１６】

図16



フロントページの続き

(56)参考文献 特開２００２－２８８６６７（ＪＰ，Ａ）
特開２００１－２２９３７９（ＪＰ，Ａ）
特開２００７－２５９９６４（ＪＰ，Ａ）
特開２００８－２４３０５４（ＪＰ，Ａ）
国際公開第２００７／０７３８５５（WO，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ａ６１Ｂ　　５／１１７
Ｇ０６Ｔ　　７／００