(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2004-164181
(P2004-164181A)
(43)公開日　平成16年6月10日(2004.6.10)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06T 7/00	G06T	7/00　530	5B043

審査請求 未請求　請求項の数 9　ＯＬ　（全 31 頁）

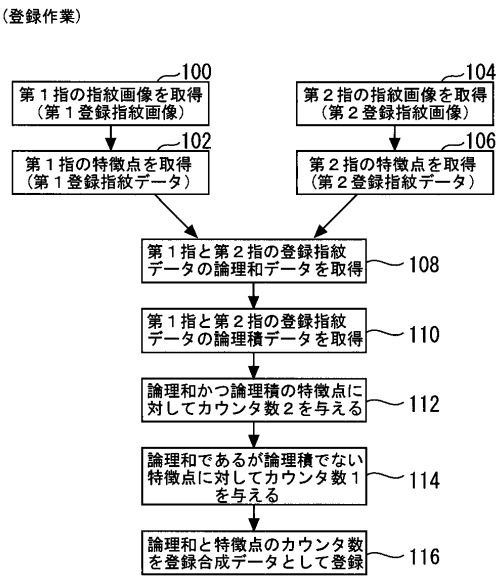
(21)出願番号　特願2002-328093(P2002-328093)
(22)出願日　平成14年11月12日(2002.11.12)

(71)出願人　591230295
エヌティティエレクトロニクス株式会社
東京都渋谷区道玄坂１丁目１２番１号
(74)代理人　100082175
弁理士　高田　守
(74)代理人　100106150
弁理士　高橋　英樹
(72)発明者　徳永　慶一郎
東京都渋谷区道玄坂一丁目１２番１号　エヌティティエレクトロニクス株式会社内

Ｆターム(参考)　5B043 AA09　BA02　EA06　EA08　EA15
FA03　FA07　GA02

(54)【発明の名称】指紋データ登録装置、および指紋データ認証装置

(57)【要約】
【課題】本発明は本人認証システムを構築するうえで有用な指紋データ登録装置に関し、ユーザーの指紋データが単独で流出或いは盗用されるのを確実に防ぐことを目的とする。
【解決手段】指紋を読み取るための指紋センサを設ける。指紋センサの出力に基づいて、第１指の登録指紋データ、および第２指の登録指紋データをそれぞれ生成する（ステップ１００～１０６）。第１指と第２指の登録指紋データを合成して登録合成データを生成する（ステップ１０８～１１４）。記憶部には、登録合成データを登録する（ステップ１１６）。
【選択図】　図２



【特許請求の範囲】
【請求項１】
指紋を読み取るための指紋センサと、
前記指紋センサの出力に基づいて登録指紋データを生成する登録指紋データ生成手段と、
複数の登録指紋データを合成して登録合成データを生成する登録合成データ生成手段と、
前記登録合成データを記憶する登録合成データ記憶手段と、
を備えることを特徴とする指紋データ登録装置。
【請求項２】
前記登録合成データ生成手段は、前記複数の登録指紋データの論理和データを演算する論理和データ演算手段を備え、当該論理和データが前記登録合成データであることを特徴とする請求項１記載の指紋データ登録装置。
【請求項３】
前記登録合成データ生成手段は、
前記複数の登録指紋データの論理和データを取得する論理和データ取得手段と、
前記複数の登録指紋データの論理積データを取得する論理積データ取得手段とを備え、
前記論理和データと共に、前記論理積データ、或いは、前記論理和データに含まれる個々のデータの、前記複数の登録指紋データ内での重複数を含む登録合成データを生成することを特徴とする請求項１記載の指紋データ取得手段。
【請求項４】
前記登録合成データ生成手段は、
前記複数の登録指紋データの相対位置関係を変更する相対位置関係変更手段と、
複数の相対位置関係について、前記複数の登録指紋データの論理積データを取得する特定用論理積データ取得手段と、
前記複数の相対位置関係のうち、論理積データのデータ数を最大とする相対位置関係を特定する相対位置関係特定手段とを備え、
前記特定された相対位置関係において前記複数の登録指紋データを合成して登録合成データを生成することを特徴とする請求項１乃至３の何れか１項記載の指紋データ登録装置。
【請求項５】
複数の登録指紋データを合成することで構成されている登録合成データを記憶する登録合成データ記憶手段と、
指紋を読み取るための指紋センサと、
前記指紋センサの出力に基づいて認証指紋データを生成する認証指紋データ生成手段と、
前記登録合成データ記憶手段から、対照用登録合成データを取得する対照用登録合成データ取得手段と、
前記対照用登録合成データを複数の認証指紋データと対照させることにより、当該複数の認証指紋データによる認証の可否を決定する認証可否決定手段と、
を備えることを特徴とする指紋データ認証装置。
【請求項６】
前記対照用登録合成データは、複数の登録指紋データの論理和データであり、
前記認証可否決定手段は、
第１指の認証指紋データに含まれるデータのうち、前記対照用登録合成データに含まれるものの数を第１一致数とする第１一致数取得手段と、
前記第１指の認証指紋データに含まれるデータのうち、前記対照用登録合成データに含まれないものの数を第１不一致数とする第１不一致数取得手段と、
前記対照用登録合成データに含まれるデータのうち、当該対照用登録合成データと対照されるべき前記複数の認証指紋データのいずれにも含まれないものの数を登録合成データ不一致数として取得する登録合成データ不一致数取得手段とを備え、
前記第１一致数、前記第１不一致数、および前記登録合成データ不一致数の少なくとも一つに基づいて、当該複数の認証指紋データによる認証の可否を決定することを特徴とする請求項５記載の指紋データ認証装置。

【請求項７】
前記対照用登録合成データは、複数の登録指紋データの論理和データと共に、前記論理和データに含まれる個々のデータの、前記複数の登録指紋データ内での重複数を含むデータであり、
前記認証可否決定手段は、
前記対照用登録合成データが有する論理和データに含まれる個々のデータのうち、第１指の認証指紋データに含まれるデータの重複数を減ずると共に、重複数１以上のデータのみを残すことにより第１認証後データを生成する第１認証後データ生成手段と、
前記第１指の認証指紋データに含まれるデータのうち、前記対照用登録合成データが有する論理和データに含まれるものの数を第１一致数とする第１一致数取得手段と、
前記第１指の認証指紋データに含まれるデータのうち、前記対照用登録合成データが有する前記論理和データに含まれないものの数を第１不一致数とする第１不一致数取得手段と、
第ｎ認証後データが有する論理和データに含まれる個々のデータのうち、第ｎ＋１指の認証指紋データに含まれるデータの重複数を減ずると共に、重複数１以上のデータのみを残すことにより第ｎ＋１認証後データを生成する第ｎ＋１認証後データ生成手段と、
前記第ｎ＋１指の認証指紋データに含まれるデータのうち、前記第ｎ認証後データが有する論理和データに含まれるものの数を第ｎ＋１一致数とする第ｎ＋１一致数取得手段と、
前記第ｎ＋１指の認証指紋データに含まれるデータのうち、前記第ｎ認証後データが有する前記論理和データに含まれないものの数を第ｎ＋１不一致数とする第ｎ＋１不一致数取得手段とを備え、
前記対照用登録合成データと対照されるべき前記複数の認証指紋データの数をＮとした場合に、前記ｎは、１≦ｎ≦Ｎ－１を満たす全ての整数であり、更に、第Ｎ認証後データに含まれるデータの数を登録合成データ不一致数として取得する登録合成データ不一致数取得手段を備え、
前記第１一致数、前記第１不一致数、前記第ｎ＋１一致数、前記第ｎ＋１不一致数、および前記登録合成データ不一致数の少なくとも一つに基づいて、当該複数の認証指紋データによる認証の可否を決定することを特徴とする請求項５記載の指紋データ認証装置。
【請求項８】
前記対照用登録合成データは、複数の登録指紋データの論理和データであり、
前記認証可否決定手段は、
第ｎ指の認証指紋データに含まれるデータのうち、前記対照用登録合成データに含まれるものの数を第ｎ一致数とする第ｎ一致数取得手段と、
前記第ｎ指の認証指紋データに含まれるデータのうち、前記対照用登録合成データに含まれないものの数を第ｎ不一致数とする第ｎ不一致数取得手段と、
前記対照用登録合成データに含まれるデータのうち、当該対照用登録合成データと対照されるべき前記複数の認証指紋データのいずれにも含まれないものの数を登録合成データ不一致数として取得する登録合成データ不一致数取得手段とを備え、
前記対照用登録合成データと対照されるべき前記複数の認証指紋データの数をＮとした場合に、前記ｎは、１≦ｎ≦Ｎを満たす全ての整数であり、更に、
前記第ｎ一致数、前記第ｎ不一致数、および前記登録合成データ不一致数の少なくとも一つに基づいて、当該複数の認証指紋データによる認証の可否を決定することを特徴とする請求項５記載の指紋データ認証装置。
【請求項９】
前記対照用登録合成データは、複数の登録指紋データの論理和データと共に、前記論理和データに含まれる個々のデータの、前記複数の登録指紋データ内での重複数を含むデータであり、
前記認証可否決定手段は、
前記対照用登録合成データに含まれる論理和データと第ｎ指の認証指紋データとの相対位置関係を変更する相対位置関係変更手段と、

前記論理和データに含まれる個々のデータのうち、第ｎ指の認証指紋データに含まれるデータの重複数を減ずると共に、重複数１以上のデータのみを残すことにより第ｎ認証後データを生成する処理を、複数の相対位置関係について実行する第ｎ認証後データ生成手段と、
個々の相対位置関係に対して生成された前記第ｎ認証後データのそれぞれにつき、当該第ｎ認証後データに含まれる個々のデータの重複数の総和を求めるカウンタ数和演算手段と、
前記重複数の和を最少とする相対位置関係を特定する相対位置関係特定手段と、
特定された前記相対位置関係を前提として、前記第ｎ指の認証指紋データに含まれるデータのうち、前記対照用登録合成データが有する論理和データに含まれるものの数を第ｎ一致数とする第ｎ一致数取得手段と、
特定された前記相対位置関係を前提として、前記第ｎ指の認証指紋データに含まれるデータのうち、前記対照用登録合成データが有する前記論理和データに含まれないものの数を第ｎ不一致数とする第ｎ不一致数取得手段と、
特定された前記相対位置関係を前提として、前記対照用登録合成データが有する論理和データに含まれるデータのうち、当該対照用登録合成データと対照されるべき前記複数の認証指紋データのいずれにも含まれないものの数を登録合成データ不一致数として取得する登録合成データ不一致数取得手段とを備え、
前記対照用登録合成データと対照されるべき前記複数の認証指紋データの数をＮとした場合に、前記ｎは、１≦ｎ≦Ｎを満たす全ての整数であり、更に、
前記第ｎ一致数、前記第ｎ不一致数、および前記登録合成データ不一致数の少なくとも一つに基づいて、当該複数の認証指紋データによる認証の可否を決定することを特徴とする請求項５記載の指紋データ認証装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、指紋データ登録装置、および指紋データ認証装置に係り、特に、本人認証システムを構築するうえで有用な指紋データ登録装置、および指紋データ認証装置に関する。

【０００２】

【従来の技術】

従来、例えば特開２００２－４１１６９号公報に開示されるように、指紋を利用した認証システムが知られている。この装置は、複数の指の指紋を登録しておくことにより、個々の指に対応させて異なるアプリケーションプログラムを起動させようとするものである。また、この装置は、上記の機能を実現するために、ユーザーの複数の指に対応する個々の指紋データを、データベース中に記憶している。

【０００３】

【特許文献１】

特開２００２－４１１６９号公報

【０００４】

【発明が解決しようとする課題】

指紋を用いた認証システムは、一般に、本人認証など、高いセキュリティレベルの要求される場面で使用される。このため、指紋データが、仮に流出したり、或いは盗用されたりした場合は、その指紋データの登録を抹消して、流出或いは盗用された指紋データを用いた認証の通過、すなわち、いわゆる「成りすまし」行為を防ぐ必要が生ずる。

【０００５】

上述した従来の装置は、データベース中に、個々の指紋データが、それぞれ独立したデータとして記憶されている。このため、そのデータが流出或いは盗用され、登録済みの指紋データを無効とする必要が生じた場合は、以後、今まで認証に用いていた指の指紋は、一切使用することができなくなってしまう。

【０００６】

指の数は両手合わせて１０本、つまり、さほど大きくない有限数である。このため、流出または盗用等が生ずることにより、自己の指紋が一つずつ認証に使用できないものになるとすれば、ユーザーは、そのシステムの使用に抵抗を覚え易い。このような事情は、手軽な本人認証を実現し得る指紋認証システムが普及し難い原因の一つとなっている。

【０００７】

本発明は、上記のような課題を解決するためになされたもので、ユーザーの指紋データが単独で流出或いは盗用されるのを確実に防ぐことのできる指紋データ登録装置を提供することを第１の目的とする。

また、本発明は、ユーザーの指紋データが単独で流出或いは盗用されるのを確実に防ぐことのできる指紋データ認証装置を提供することを第２の目的とする。

【０００８】

【課題を解決するための手段】

第１の発明は、指紋データ登録装置であって、

指紋を読み取るための指紋センサと、

前記指紋センサの出力に基づいて登録指紋データを生成する登録指紋データ生成手段と、

複数の登録指紋データを合成して登録合成データを生成する登録合成データ生成手段と、

前記登録合成データを記憶する登録合成データ記憶手段と、

を備えることを特徴とする。

【０００９】

第２の発明は、第１の発明において、前記登録合成データ生成手段は、前記複数の登録指紋データの論理和データを演算する論理和データ演算手段を備え、当該論理和データが前記登録合成データであることを特徴とする。

【００１０】

第３の発明は、第１の発明において、

前記登録合成データ生成手段は、

前記複数の登録指紋データの論理和データを取得する論理和データ取得手段と、

前記複数の登録指紋データの論理積データを取得する論理積データ取得手段とを備え、

前記論理和データと共に、前記論理積データ、或いは、前記論理和データに含まれる個々のデータの、前記複数の登録指紋データ内での重複数を含む登録合成データを生成することを特徴とする。

【００１１】

第４の発明は、第１乃至第３の発明の何れかにおいて、

前記登録合成データ生成手段は、

前記複数の登録指紋データの相対位置関係を変更する相対位置関係変更手段と、

複数の相対位置関係について、前記複数の登録指紋データの論理積データを取得する特定用論理積データ取得手段と、

前記複数の相対位置関係のうち、論理積データのデータ数を最大とする相対位置関係を特定する相対位置関係特定手段とを備え、

前記特定された相対位置関係において前記複数の登録指紋データを合成して登録合成データを生成することを特徴とする。

【００１２】

第５の発明は、指紋データ認証装置であって、

複数の登録指紋データを合成することで構成されている登録合成データを記憶する登録合成データ記憶手段と、

指紋を読み取るための指紋センサと、

前記指紋センサの出力に基づいて認証指紋データを生成する認証指紋データ生成手段と、

前記登録合成データ記憶手段から、対照用登録合成データを取得する対照用登録合成データ取得手段と、

前記対照用登録合成データを複数の認証指紋データと対照させることにより、当該複数の認証指紋データによる認証の可否を決定する認証可否決定手段と、

を備えることを特徴とする。
【００１３】
第６の発明は、第５の発明において、
前記対照用登録合成データは、複数の登録指紋データの論理和データであり、
前記認証可否決定手段は、
第１指の認証指紋データに含まれるデータのうち、前記対照用登録合成データに含まれるものの数を第１一致数とする第１一致数取得手段と、
前記第１指の認証指紋データに含まれるデータのうち、前記対照用登録合成データに含まれないものの数を第１不一致数とする第１不一致数取得手段と、
前記対照用登録合成データに含まれるデータのうち、当該対照用登録合成データと対照されるべき前記複数の認証指紋データのいずれにも含まれないものの数を登録合成データ不一致数として取得する登録合成データ不一致数取得手段とを備え、
前記第１一致数、前記第１不一致数、および前記登録合成データ不一致数の少なくとも一つに基づいて、当該複数の認証指紋データによる認証の可否を決定することを特徴とする。
【００１４】
第７の発明は、第５の発明において、
前記対照用登録合成データは、複数の登録指紋データの論理和データと共に、前記論理和データに含まれる個々のデータの、前記複数の登録指紋データ内での重複数を含むデータであり、
前記認証可否決定手段は、
前記対照用登録合成データが有する論理和データに含まれる個々のデータのうち、第１指の認証指紋データに含まれるデータの重複数を減ずると共に、重複数１以上のデータのみを残すことにより第１認証後データを生成する第１認証後データ生成手段と、
前記第１指の認証指紋データに含まれるデータのうち、前記対照用登録合成データが有する論理和データに含まれるものの数を第１一致数とする第１一致数取得手段と、
前記第１指の認証指紋データに含まれるデータのうち、前記対照用登録合成データが有する前記論理和データに含まれないものの数を第１不一致数とする第１不一致数取得手段と、
第ｎ認証後データが有する論理和データに含まれる個々のデータのうち、第ｎ＋１指の認証指紋データに含まれるデータの重複数を減ずると共に、重複数１以上のデータのみを残すことにより第ｎ＋１認証後データを生成する第ｎ＋１認証後データ生成手段と、
前記第ｎ＋１指の認証指紋データに含まれるデータのうち、前記第ｎ認証後データが有する論理和データに含まれるものの数を第ｎ＋１一致数とする第ｎ＋１一致数取得手段と、
前記第ｎ＋１指の認証指紋データに含まれるデータのうち、前記第ｎ認証後データが有する前記論理和データに含まれないものの数を第ｎ＋１不一致数とする第ｎ＋１不一致数取得手段とを備え、
前記対照用登録合成データと対照されるべき前記複数の認証指紋データの数をＮとした場合に、前記ｎは、１≦ｎ≦Ｎ－１を満たす全ての整数であり、更に、
第Ｎ認証後データに含まれるデータの数を登録合成データ不一致数として取得する登録合成データ不一致数取得手段を備え、
前記第１一致数、前記第１不一致数、前記第ｎ＋１一致数、前記第ｎ＋１不一致数、および前記登録合成データ不一致数の少なくとも一つに基づいて、当該複数の認証指紋データによる認証の可否を決定することを特徴とする。
【００１５】
第８の発明は、第５の発明において、
前記対照用登録合成データは、複数の登録指紋データの論理和データであり、
前記認証可否決定手段は、
第ｎ指の認証指紋データに含まれるデータのうち、前記対照用登録合成データに含まれるものの数を第ｎ一致数とする第ｎ一致数取得手段と、

前記第ｎ指の認証指紋データに含まれるデータのうち、前記対照用登録合成データに含まれないものの数を第ｎ不一致数とする第ｎ不一致数取得手段と、
前記対照用登録合成データに含まれるデータのうち、当該対照用登録合成データと対照されるべき前記複数の認証指紋データのいずれにも含まれないものの数を登録合成データ不一致数として取得する登録合成データ不一致数取得手段とを備え、
前記対照用登録合成データと対照されるべき前記複数の認証指紋データの数をＮとした場合に、前記ｎは、１≦ｎ≦Ｎを満たす全ての整数であり、更に、
前記第ｎ一致数、前記第ｎ不一致数、および前記登録合成データ不一致数の少なくとも一つに基づいて、当該複数の認証指紋データによる認証の可否を決定することを特徴とする。

【００１６】
第９の発明は、第５の発明において、
前記対照用登録合成データは、複数の登録指紋データの論理和データと共に、前記論理和データに含まれる個々のデータの、前記複数の登録指紋データ内での重複数を含むデータであり、
前記認証可否決定手段は、
前記対照用登録合成データに含まれる論理和データと第ｎ指の認証指紋データとの相対位置関係を変更する相対位置関係変更手段と、
前記論理和データに含まれる個々のデータのうち、第ｎ指の認証指紋データに含まれるデータの重複数を減ずると共に、重複数１以上のデータのみを残すことにより第ｎ認証後データを生成する処理を、複数の相対位置関係について実行する第ｎ認証後データ生成手段と、
個々の相対位置関係に対して生成された前記第ｎ認証後データのそれぞれにつき、当該第ｎ認証後データに含まれる個々のデータの重複数の総和を求めるカウンタ数和演算手段と、
前記重複数の和を最少とする相対位置関係を特定する相対位置関係特定手段と、
特定された前記相対位置関係を前提として、前記第ｎ指の認証指紋データに含まれるデータのうち、前記対照用登録合成データが有する論理和データに含まれるものの数を第ｎ一致数とする第ｎ一致数取得手段と、
特定された前記相対位置関係を前提として、前記第ｎ指の認証指紋データに含まれるデータのうち、前記対照用登録合成データが有する前記論理和データに含まれないものの数を第ｎ不一致数とする第ｎ不一致数取得手段と、
特定された前記相対位置関係を前提として、前記対照用登録合成データが有する論理和データに含まれるデータのうち、当該対照用登録合成データと対照されるべき前記複数の認証指紋データのいずれにも含まれないものの数を登録合成データ不一致数として取得する登録合成データ不一致数取得手段とを備え、
前記対照用登録合成データと対照されるべき前記複数の認証指紋データの数をＮとした場合に、前記ｎは、１≦ｎ≦Ｎを満たす全ての整数であり、更に、
前記第ｎ一致数、前記第ｎ不一致数、および前記登録合成データ不一致数の少なくとも一つに基づいて、当該複数の認証指紋データによる認証の可否を決定することを特徴とする。

【００１７】
【発明の実施の形態】
以下、図面を参照してこの発明の実施の形態について説明する。尚、各図において共通する要素には、同一の符号を付して重複する説明を省略する。
【００１８】
実施の形態１．
［システムのハードウェア構成］
図１は、本発明の実施の形態１の構成を説明するためのブロック図である。より詳細には、図１（Ａ）は、実施の形態１における指紋データ登録装置のブロック図であり、また、

図１（Ｂ）は、実施の形態１における指紋データ認証装置のブロック図である。

【００１９】

図１（Ａ）に示すように、本実施形態における指紋データ登録装置は、指紋センサ１０、処理部１２、記憶部１４および表示部１６により構成されている。処理部１２、記憶部１４、および表示部１６は、汎用のコンピュータシステムにより実現することができる。

【００２０】

指紋センサ１０は、ユーザーの指紋を読み取るためのセンサであり、例えば、半導体容量センサ、或いはＣＣＤカメラなどにより実現することができる。処理部１２は、指紋センサ１０により取得された指紋を記憶部１４に登録するために後述する種々の処理を実行する部分である。ここで、記憶部１４は、後述する登録合成データを恒常的に保存しておくための恒常記憶部の他、データを一時的に記憶しておくための一時記憶部を含むものとする。また、表示部１６は、データ処理の過程で生成される種々の情報を表示するための装置である。

【００２１】

図１（Ｂ）に示すように、本実施形態における指紋データ認証装置は、指紋センサ２０、処理部２２、記憶部２４および表示部２６により構成されている。これらのハードウェア構成は、図１（Ａ）に示す指紋データ登録装置が備えるものと実質的に同様である。但し、処理部２２は、記憶部２４に恒常的に記憶されている登録合成データを用いて、指紋の認証に必要な種々の処理を実行するものとする。尚、図１には、指紋データ登録装置と、指紋データ認証装置とを別個独立した装置として示しているが、それらは単一のコンピュータシステム上に共存させることとしてもよい。

【００２２】

［登録作業の説明］

次に、図２および図３を参照して、本実施形態における指紋データ登録装置の動作、および、その装置を用いた指紋データの登録作業について説明する。

図２は、図１（Ａ）に示す指紋データ登録装置を用いた指紋データの登録作業の流れを説明するためのフローチャートである。このフローチャートでは、２本の指の指紋を合成して登録合成データを生成し、その登録合成データを指紋登録装置の記憶部１４に恒常的に記憶させることとしている。但し、登録合成データを生成するために合成すべき指紋の数は、２つに限定されるものではなく、３つ以上の指紋データを合成して登録合成データを生成することとしてもよい。

【００２３】

図２に示す登録作業では、先ず、指紋センサ１０により第１指の指紋画像、すなわち、第１登録指紋画像が取得される（ステップ１００）。

図３（Ａ）は、本ステップ１００で取得される第１登録指紋画像の一例を示す。このようにして取得された第１登録指紋画像は、データ処理のため、記憶部１４のＲＡＭに一時的に記憶される。

【００２４】

第１登録指紋画像が取得されると、次に、その画像を処理することにより、第１指の特徴点データが取得され、更に、その特徴点データの集合である第１登録指紋データが生成される（ステップ１０２）。

図３（Ｂ）は、本ステップ１０２で生成された第１登録指紋データを模式的に表したイメージ図である。処理部１２は、本ステップ１０２において、具体的には、第１登録指紋画像の中から、個々の指紋線の端点および分岐点を検出し、それらの点の座標を特徴点の始点座標として認識する。処理部１２は、更に、個々の特徴点について、指紋線の延在方向を特定し（特徴点が分岐点の場合は分岐角を基礎として所定の規則に則って一の方向を特定する）、その方向の情報と始点座標とを結びつけて、図３（Ｂ）に示すようなベクトル量の特徴点データを生成する。そして、処理部１２は、第１登録指紋画像に基づいて生成される全ての特徴点データ（始点座標と方向情報を含むデータ）の集合を、第１登録指紋データとして記憶部１４のＲＡＭに一時的に記憶させる。

【００２５】
図２に示す登録作業では、また、指紋センサ１０により第２指の指紋画像、すなわち、第２登録指紋画像が取得される（ステップ１０４）。
図３（Ｃ）は、本ステップ１０４で取得された第２登録指紋画像の一例を示す。このようにして取得された第２登録指紋画像は、第１登録指紋画像と同様に、記憶部１４のＲＡＭに一時的に記憶される。
【００２６】
第２登録指紋画像が取得されると、次に、その画像を処理することにより、第２指の特徴点データ（始点座標と方向情報を含むデータ）が取得され、更に、その特徴点データの集合である第２登録指紋データが生成される（ステップ１０６）。
図３（Ｄ）は、本ステップ１０６で生成された第２登録指紋データを模式的に表したイメージ図である。第２登録指紋データは、第１登録指紋データと同様に、記憶部１４のＲＡＭに一時的に記憶される。
【００２７】
図２に示す登録作業では、上述した一連の処理に続いて、第１登録指紋データと、第２登録指紋データとの論理和データが取得される（ステップ１０８）。
本ステップ１０８において、処理部１２は、具体的には、第１および第２登録指紋データを記憶部１４から読み出し、何れかの登録指紋データに含まれている特徴点データの集合を論理和データとする。このようにして生成された論理和データは、記憶部１４のＲＡＭに一時的に記憶される。
【００２８】
次に、第１登録指紋データと、第２登録指紋データとの論理積データが取得される（ステップ１１０）。
本ステップ１１０において、処理部１２は、具体的には、第１および第２登録指紋データを記憶部１４から読み出し、双方の登録指紋データに重複して含まれている特徴点データ（始点座標および方向情報が共に一致するデータ）の集合を、論理積データとして生成する。生成された論理積データは、記憶部１４のＲＡＭに一時的に記憶される。
【００２９】
次に、論理和データと論理積データの双方に含まれている特徴点データが抽出され、それらのデータに対してカウンタ数２が与えられる（ステップ１１２）。
次いで、論理和データには含まれているが、論理積データにはふくまれていない特徴点データに対してカウンタ数１が与えられる（ステップ１１４）。
【００３０】
論理積データに含まれている特徴点データは、２つの登録指紋データ内に重複して存在しているデータである。一般に、異なる２つの指紋については、このように重複する特徴点データが２０％程度存在している。上記ステップ１１２では、２つの登録指紋データ内に重複して存在していた特徴点データに対して、その重複の履歴を示すべくカウンタ数２が与えられる。
【００３１】
一方、論理和データにのみ含まれている特徴点データは、２つの登録指紋データの一方のみに存在しているデータである。上記ステップ１１４では、重複することなく一方の登録指紋データにのみ存在していた特徴点データに対して、その非重複の履歴を示すべくカウンタ数１が与えられる。
【００３２】
図２に示す登録作業では、次に、論理和データに含まれていた全ての特徴点データと、個々の特徴点データに与えられたカウンタ数とが、登録合成データとして登録される（ステップ１１６）。
図３（Ｅ）は、本ステップ１１６で生成された登録合成データを模式的に表したイメージ図である。この図において、太線で記した矢印は、カウンタ数２が与えられた特徴点データのベクトルを示しており、一方、細線で記した矢印は、カウンタ数１が付与された特徴

点データのベクトルを示している。このようにして生成された登録合成データは、記憶部１４がデータを恒常的に保存しておくために有している記録媒体、例えば、ハードディスクなどに記憶される。その一方で、第１登録指紋データや、第２登録指紋データは、登録合成データの登録が終了すると同時に、以後読み出しができなくなるように記憶部１４上から消去される。

【００３３】

［認証作業の説明］

次に、図４を参照して本実施形態における指紋データ認証装置の動作、および、その装置を用いた指紋データの認証作業について説明する。

図４は、図１（Ｂ）に示す指紋データ認証装置を用いた指紋データの認証作業の流れを説明するためのフローチャートである。尚、認証作業が開始される前提として、指紋データ認証装置の記憶部２４には、図２に示す手順で登録された登録合成データが記憶されているものとする。

【００３４】

図４に示す認証作業では、先ず、指紋センサ２０により第１指の指紋画像、すなわち、第１認証指紋画像が取得される（ステップ１２０）。

次に、第１認証指紋画像を処理することにより、第１指の特徴点データが取得され、更に、その特徴点データの集合である第１認証指紋データが生成される（ステップ１２２）。

そして、上記の処理により生成された第１認証指紋データは、データ処理のため、記憶部１４のＲＡＭに一時的に記憶される。尚、上述した一連の処理は、実質的に、上記ステップ１００および１０２で実行される処理と同様である。

【００３５】

図４に示す認証作業では、次に、登録合成データと第１認証指紋データとの照合処理が実行される（ステップ１２４）。

本ステップ１２４において、処理部１２は、先ず、記憶部２４から登録合成データを読み出すと共に、その登録合成データと、第１認証指紋データとの相対位置合わせを実行する。

【００３６】

既述した通り、登録合成データを構成する個々の特徴点データは、特徴点の始点座標と指紋線の方向情報とで構成されている。同様に、第１認証指紋データを構成する個々の特徴点データも、特徴点の始点座標と指紋線の方向情報とで構成されている。そして、それらのデータにおける始点座標は、それぞれ絶対座標である。このため、登録合成データと第１認証指紋データとが、共に同じ指紋を基礎としている場合であっても、両者の相対位置がずれていたのでは、特徴点の始点座標にずれが生じ、両者の一致は認められない。そこで、本実施形態では、登録合成データを正しく照合するため、両者の一致を判断するに先立って、上記の如く両者の相対位置合わせを行うこととしている。

【００３７】

登録合成データと第１認証指紋データとの相対位置合わせは、具体的には、登録合成データの位置（座標軸）を固定したうえで、第１認証指紋データの位置を適当に移動、或いは回転させつつ、両者が最も整合する位置を探す手法で行われる。ここで、ある相対位置関係における両者の整合度合いは、その位置関係において、両者の論理積データを求めたうえで、そのデータ数により判断する。このため、登録合成データと第１認証指紋データとの相対位置は、両者の論理積データ数が最大となる位置、つまり、両者間での重複データ数が最大となるような位置に特定される。

【００３８】

本ステップ１２４では、上記の相対位置合わせが終了した後、その相対位置関係を前提として、登録合成データの特徴点データと、第１認証指紋データの特徴点データとが照合される。その結果、第１認証指紋データに含まれる特徴点データのうち、登録合成データ中の特徴点データと一致するものの数が「第１一致数」として算出される。また、第１認証指紋データに含まれる特徴点データのうち、登録合成データ中の特徴点データと一致しな

いものの数が「第１不一致数」として算出される。
【００３９】
更に、本ステップ１２４では、登録合成データに含まれている特徴点データのうち、第１認証指紋データに含まれている特徴点データと一致するものにつき、カウンタ数を１だけ減算する処理、および、上記減算の後になお、１以上のカウンタ数を有する特徴点データだけを登録合成データ中から抽出して、「第１認証後データ」を生成する処理が実行される。上記の処理によれば、登録合成データ中に存在しており、かつ、第１認証指紋データ中に存在していなかった特徴点データと、第１認証指紋データ中に存在していたが、登録合成データ中にカウンタ数２を伴って存在していた特徴点データとの集合が、第１認証後データとして抽出される。
【００４０】
図４に示す認証作業では、次に、指紋センサ２０により第２指の指紋画像、すなわち、第２認証指紋画像が取得される（ステップ１２６）。
次いで、第２認証指紋画像を処理することにより、第２指の特徴点データが取得され、更に、その特徴点データの集合である第２認証指紋データが生成される（ステップ１２８）。
そして、上記の処理により生成された第２認証指紋データは、データ処理のため、記憶部１４のＲＡＭに一時的に記憶される。尚、これらの処理は、実質的に、上記ステップ１２０および１２２で実行される処理と同様である。
【００４１】
図４に示す認証作業では、次に、第１認証後データと第２認証指紋データとの照合処理が実行される（ステップ１３０）。
本ステップ１３０では、上記ステップ１２４の場合と同様に、先ず、第１認証後データと第２認証指紋データとの相対位置合わせが実行する。そして、その相対位置合わせの終了後に、第１認証後データと第２認証指紋データとの照合が行われる。その結果、第２認証指紋データに含まれる特徴点データのうち、第１認証後データ中の特徴点データと一致するものの数が「第２一致数」として算出される。また、第２認証指紋データに含まれる特徴点データのうち、第１認証後データ中の特徴点データと一致しないものの数が「第２不一致数」として算出される。更に、第１認証後データから第２認証指紋データ中に含まれている特徴点データを消去することで「第２認証後データ」が生成される。
【００４２】
以上の処理において、上記ステップ１３０において生成される「第２認証後データ」は、実質的には、登録合成データに含まれる特徴点データのうち、第１認証指紋データにも、第２認証指紋データにも含まれていなかった特徴点の集合である。図４に示す認証作業では、上記ステップ１３０に次いで、そのような意味を有する第２認証後データの数が、「登録合成データ不一致数」として算出される（ステップ１３２）。
【００４３】
第１認証指紋データが、登録合成データの基礎とされた２つの指紋データの一方（例えば、第１登録指紋データ）と完全に一致している場合は、「第１一致数」が第１認証指紋データに含まれる特徴点データの数と等しくなり、かつ、「第１不一致数」は０となる。そして、この場合、「第１認証後データ」は、登録合成データの基礎とされた２つの指紋データの他方（例えば、第２登録指紋データ）と一致するものとなる。
【００４４】
更に、このような状況の下、第２認証指紋データが、登録合成データの基礎とされた２つの指紋データの他方（例えば第２登録指紋データ）と完全に一致していると、「第２一致数」は第２認証指紋データに含まれる特徴点データの数と等しくなり、かつ、「第２不一致数」は０となる。そして、この場合、「第２認証後データ」の数、つまり、「登録合成データ不一致数」は０となる。
【００４５】
以上説明した通り、上述した「第１一致数」および「第２一致数」は、何れも、第１およ

び第２認証指紋データが、第１および第２登録指紋データと近似するほど大きな値となる変数である。また、「第１不一致数」、「第２不一致数」、および「登録合成データ不一致数」は、第１および第２認証指紋データが第１および第２登録指紋データと近似するほど小さな値となる変数である。このため、処理部１４は、「第１一致数」、「第１不一致数」、「第２一致数」、「第２不一致数」、および「登録合成データ不一致数」の少なくとも１つに基づいて、認証の対象である使用者が登録された本人であるか否かを判断する（ステップ１３４）。

【００４６】

ここでは、具体的には、上述した５つの基準の全てが、それぞれ以下に示す条件を満たすか否かにより、本人であるかか否かが判断される。

・第１一致数が、第１一致閾値＝６より大きいか（６以下で他人判定）。
・第１不一致数が、第１不一致閾値＝３より小さいか（３以上で他人判定）。
・第２一致数が、第２一致閾値＝６より大きいか（６以下で他人判定）。
・第２不一致数が、第２不一致閾値＝３より小さいか（３以上で他人判定）。
・登録合成データ不一致数が、登録合成データ不一致閾値＝５より小さいか（５以上で他人判定）。

【００４７】

上記の判別の結果、上記の基準が満たされていると判断された場合は、認証の対象であるユーザーが本人と認められ、その判断に対応する処理が実行される（ステップ１３６）。一方、上記の基準が満たされていないと判断された場合は、認証の対象であるユーザーが他人であると判断され、その判断に対応する処理が実行される（ステップ１３８）。

【００４８】

［登録・認証作業の具体例］

次に、図５を参照して、上述した登録作業および認証作業の具体例を説明する。

既述した通り、本実施形態において登録および認証の対象とされる指紋データは、ベクトル量の特徴点データにより構成されている。これに対して、ここでは、特徴点データをスカラー量で置き換えて説明の簡単化を図ることとする。つまり、図５において、登録指紋データや認証指紋データの構成要素として記されている個々のスカラー量は、始点座標および方向に関する情報を含むベクトル量の特徴点データを簡易的に表したデータである。以下、それらのスカラー量についても、便宜上「特徴点データ」との呼称を用いるものとする。

【００４９】

図５は、登録作業の際に、上記ステップ１００～１０６の処理により、以下に示す第１登録指紋データおよび第２登録指紋データが取得された例を示している。

第１登録指紋データ：（１，８，１１，１２，１５，２３，２８，３０，３９，４４）
第２登録指紋データ：（３，８，１０，１５，１９，２８，３０，３３，４０，４７）

尚、図５中に斜体文字で記されている特徴点データ、すなわち、８，１５，２８，３０は、双方の登録指紋データに重複して存在しているデータである。

【００５０】

第１登録指紋データ、および第２登録指紋データが、それぞれ上記の特徴点データで構成されている場合、上記ステップ１０８および１１０の処理によれば、論理和データおよび論理積データは、それぞれ以下のように取得される。

論理積データ：（８，１５，２８，３０）
論理和データ：（１，３，８，１０，１１，１２，１５，１９，２３，２８，３０，３３，３９，４０，４４，４７）

【００５１】

上記ステップ１１２の処理によれば、論理積データに含まれる以下の特徴点データに対してはカウンタ数２が与えられる。また、上記ステップ１１４の処理によれば、論理和データにのみ含まれる以下のデータに対してカウンタ数１が与えられる。

カウンタ数２：８，１５，２８，３０

カウンタ数１：１，３，１０，１１，１２，１９，２３，３３，３９，４０，４４，４７
【００５２】
そして、上記ステップ１１６において、論理和データと、そこに含まれる個々の特徴点データのカウンタ数とを含む情報が、登録合成データとして記憶部１４のハードディスクなどに登録される。尚、図５に示す「登録合成データ」は、カウンタ数１の特徴点データを通常文字で表し、カウンタ数２の特徴点データを斜体文字で表したものである。
【００５３】
図５に示す例では、認証作業の際に、上記ステップ１２０および１２２の処理、並びに上記ステップ１２６および１２８の処理により、以下に示す第１認証指紋データおよび第２認証指紋データが取得されている。
第１認証指紋データ：（１，８，１１，１５，２３，２８，３０，３９，４４）
第２認証指紋データ：（３，８，１０，１５，２０，２３，２８，３０，３３，４０，４７）
これらの認証指紋データは、登録作業時に用いられたのと同じ指紋から得られたデータである。この例に示すように、登録作業時に生成される登録指紋データと、認証作業時に生成される認証指紋データとは、用いられる指紋が同じであっても、指紋センサ１０，２０の精度や指の状態などに起因して必ずしも同じにはならない。尚、図５中に斜体文字で記されている特徴点データ、すなわち、８，１５，２３，２８，３０は、双方の認証指紋データに重複して存在しているデータである。
【００５４】
上述した登録合成データに対して、上記の第１認証指紋データが取得された場合、上記ステップ１２４では、第１一致数、第１不一致数、および第１認証後データがそれぞれ以下のように取得される。
第１一致数＝９　（１，８，１１，１５，２３，２８，３０，３９，４４）
第１不一致数＝０
第１認証後データ：（３，８，１０，１２，１５，１９，２８，３０，３３，４０，４７）
但し、第１認証後データに含まれる特徴点データのカウンタ数は全て１である。
【００５５】
また、上記の如く取得された第１認証後データに対して、上記の第２認証指紋データが取得された場合、上記ステップ１３０では、第２一致数、第２不一致数、および第２認証後データがそれぞれ以下のように取得される。
第２一致数＝９　（３，８，１０，１５，２８，３０，３３，４０，４７）
第２不一致数＝２　（２０，２３）
第２認証後データ：（１２，１９）
【００５６】
そして、上記ステップ１３２の処理によれば、登録合成データ不一致数は、以下に示すように、第２認証データのデータ数と等しい「２」と算出される。
登録合成データ不一致数＝２　（１２，１９）
【００５７】
既述した通り、本実施形態における指紋データ認証装置は、第１一致数が６より大きく、第１不一致数が３より小さく、第２一致数が６より大きく、第２不一致数が３より小さく、かつ、登録合成データ不一致数が５より小さい場合に、認証の対象であるユーザーを本人として認証する（上記ステップ１３４参照）。図５に示す例では、これらの基準が全て満たされているため、認証の対象であるユーザーは、この場合、本人として認められる。
【００５８】
以上説明した通り、本実施形態における指紋データ登録装置、および指紋データ認証装置は、記憶部１４，２４内に、登録合成データのみを記憶しつつ、指紋を用いた認証処理を実現することができる。つまり、本実施形態のシステムによれば、記憶部１４，２４内に、単体の指紋に対応するデータを記憶しておくことなく、所望の認証処理を実現すること

ができる。更に、本実施形態において用いられる登録合成データには、それらを単体の指紋に対応するデータに分解する手がかりとなるような情報が何ら含まれていない。

【００５９】

このため、本実施形態のシステムによれば、ユーザーの指紋情報が、単体で流出し、或いは盗用されるのを確実に防ぐことができる。そして、登録合成データは、合成する指紋の組み合わせや、指紋の重ね合わせ角度を変えることにより、無限に生成することができるため、仮に登録合成データが流出、或いは盗用された場合には、その登録合成データの登録を抹消して、事実上無限に新たな登録合成データを登録することができる。このように、本実施形態のシステムは、個々の指紋データが単体で記憶されるシステムに比して、指紋データの流出や盗用に関してユーザーが感ずる危惧を和らげることができ、その点において、指紋認証の普及を図るうえで有用である。

【００６０】

ところで、上述した実施の形態１においては、論理和データとカウンタ数を登録合成データに含ませることとしているが、登録合成データの構成はこれに限定されるものではない。すなわち、登録合成データには、論理和データと共に、その論理和データに含まれる個々の特徴点データの、複数の登録指紋データ内での重複数に関する情報が含まれていればよく、例えば、上記のカウンタ数に代えて、論理積データそのものを登録合成データに含ませることとしてもよい。

【００６１】

尚、上述した実施の形態１においては、図１（Ａ）に示す指紋センサ１０および記憶部１４が、前記第１の発明における「指紋センサ」および「登録合成データ記憶手段」に、それぞれ相当している。また、実施の形態１においては、処理部１２が、上記ステップ１００～１０６の処理を実行することにより前記第１の発明における「登録指紋データ生成手段」が、上記ステップ１０８～１１４の処理を実行することにより前記第１の発明における「登録合成データ生成手段」が、それぞれ実現されている。

【００６２】

また、上述した実施の形態１においては、登録合成データに含まれる個々の特徴点に対して与えられたカウンタ数が、前記第３の発明における「重複数」に相当していると共に、処理部１２が、上記ステップ１０８の処理を実行することにより前記第３の発明における「論理和データ取得手段」が、上記ステップ１１０の処理を実行することにより前記第３の発明における「論理積データ取得手段」が、それぞれ実現されている。

【００６３】

また、上述した実施の形態１においては、図１（Ｂ）に示す指紋センサ２０および記憶部２４が、前記第５の発明における「指紋センサ」および「登録合成データ記憶手段」に、それぞれ相当している。また、実施の形態１においては、処理部２２が、上記ステップ１２０，１２２，１２６，１２８の処理を実行することにより前記第５の発明における「認証指紋データ生成手段」が、上記ステップ１２４および１２８において、論理和データとカウンタ数とを含む登録合成データを取得することにより前記第５の発明における「対照用登録合成データ取得手段」が、上記ステップ１３４の処理を実行することにより前記第５の発明における「認証可否決定手段」が、それぞれ実現されている。

【００６４】

また、上述した実施の形態１においては、処理部２２が、上記ステップ１２４において、第１認証後データを生成することにより前記第７の発明における「第１認証後データ生成手段」が、第１一致数を求めることにより前記第７の発明における「第１一致数取得手段」が、第１不一致数を求めることにより前記第７の発明における「第１不一致数取得手段」が、それぞれ実現されている。また、処理部２２が、上記ステップ１２８において、第２認証後データを生成することにより前記第７の発明における「第ｎ＋１認証後データ生成手段」が、第ｎ＋１一致数を求めることにより前記第７の発明における「第ｎ＋１一致数取得手段」が、第ｎ＋１不一致数を求めることにより前記第７の発明における「第ｎ＋１不一致数取得手段」が、それぞれ実現されている。更に、処理部２２が、上記ステップ

１３２の処理を実行することにより前記第７の発明における「登録合成データ不一致数取得手段」が実現されている。

【００６５】

実施の形態２．

次に、図６乃至図８を参照して、本発明の実施の形態２について説明する。

［登録作業の説明］

図６は、実施の形態２における指紋データ登録装置において実現される登録作業の流れを説明するためのフローチャートである。本実施形態において、指紋データ登録装置は、図１（Ａ）に示すハードウェア構成を用いて、図６に示すフローチャートに沿って登録作業を進行させることにより実現することができる。尚、図６において、上記図２に示すステップと同一のステップについては、同一の符号を付してその説明を省略または簡略する。

【００６６】

図６に示す登録作業では、ステップ１００～１０８の処理により、第１登録指紋データと、第２登録指紋データとの論理和データが求められると、その論理和データが、登録合成データとして記憶部１４に登録される（ステップ１４０）。

上述した実施の形態１の装置は、論理和データとカウンタ数とを登録合成データに含めることとしていた。また、そのために、実施の形態１の装置では、登録作業の際に複数の登録指紋データの論理積データが求められていた。これに対して、実施の形態２の指紋データ登録装置は、登録合成データに論理和データのみを含ませることとし、処理の簡単化を図っている。

【００６７】

［認証作業の説明］

図７は、実施の形態２における指紋データ認証装置において実現される認証作業の流れを説明するためのフローチャートである。本実施形態において、指紋データ認証装置は、図１（Ｂ）に示すハードウェア構成を用いて、図７に示すフローチャートに沿って認証作業を進行させることにより実現することができる。尚、図７において、上記図４に示すステップと同一のステップについては、同一の符号を付してその説明を省略または簡略する。

【００６８】

図７に示す認証作業では、ステップ１２０および１２２の処理により第１認証指紋データが取得された後、登録合成データと第１認証指紋データとの照合処理が実行される（ステップ１５０）。

本ステップ１５０では、図４に示すステップ１２４の場合と同様に、以下の処理が実行される。

▲１▼登録合成データと、第１認証指紋データとの相対位置合わせ。

▲２▼第１一致数（第１認証指紋データに含まれる特徴点データのうち、登録合成データ中の特徴点データと一致するものの数）の算出。

▲３▼第１不一致数（第１認証指紋データに含まれる特徴点データのうち、登録合成データ中の特徴点データと一致しないものの数）の算出。

▲４▼第１認証後データの生成。

【００６９】

上記▲１▼～▲４▼の処理のうち、▲１▼～▲３▼の処理については、図４に示すステップ１２４において実行される処理と何ら異なるところがない。このため、ここでは、それらについての詳細な説明は省略する。これに対して、▲４▼の処理は、上記ステップ１２４で実行される処理とその内容が異なっている。

【００７０】

すなわち、図４に示すステップ１２４は、登録合成データに論理和データおよびカウンタ数が含まれていることを前提として実行される。具体的には、上記ステップ１２４では、先ず、登録合成データに含まれている特徴点データのうち、第１認証指紋データに含まれている特徴点データと一致するものにつき、カウンタ数を１だけ減算する処理が実行される。そして、上記の減算の後、１以上のカウンタ数を有する特徴点データだけを抽出する

ことで「第１認証後データ」が生成される。この場合、複数の登録指紋データ中に重複して存在していた特徴点データは、第１認証指紋データにその特徴点データが含まれていても、第１認証後データ中に残存することになる。

【００７１】

これに対して、本ステップ１５０の処理は、登録合成データに論理和データのみが含まれていることを前提として実行される。具体的には、本ステップ１５０では、論理和データから、第１認証指紋データに含まれている特徴点データを単純に削除することにより「第１認証後データ」が生成される。この場合、複数の登録指紋データ中に重複して存在していた特徴点データは、第１認証指紋データに含まれている場合は、第１認証後データ中には残存しないことになる。

【００７２】

図７に示す認証作業では、次に、ステップ１２６および１２８の処理により、第２認証指紋データが生成される。その後、更に、第１認証後データと第２認証指紋データとの照合処理が実行される（ステップ１５２）。

本ステップ１５０では、具体的には、以下の処理が実行される。

▲１▼第１認証後データと、第２認証指紋データとの相対位置合わせ。

▲２▼第２認証後データの生成。

【００７３】

図４に示すステップ１３０では、上記▲１▼および▲２▼の処理の他、以下の２つの処理が実行されている。

▲３▼第２一致数（第２認証指紋データに含まれる特徴点データのうち、第１認証後データ中の特徴点データと一致するものの数）の算出。

▲４▼第２不一致数（第２認証指紋データに含まれる特徴点データのうち、第１認証後データ中の特徴点データと一致しないものの数）の算出。

そして、実施の形態１においては、このようにして算出される「第２一致数」および「第２不一致数」も、本人認証の判断の基礎として用いられている。

【００７４】

しかし、実施の形態２では、既述した通り、複数の登録認証データに重複して存在していた特徴点データは、第１認証指紋データ内に存在する限り第１認証後データには残存しない。このため、登録合成データの基礎とされた２つの登録指紋データと、認証に用いられた２つの認証指紋データとが仮に完全に一致していたとしても、第１認証後データは、第２認証指紋データと同じにはならない。従って、本実施形態においては、第２一致数、および第２不一致数が、本人認証のための有効な判断材料にはならない。このため、本ステップ１５２では、敢えてそれらを算出することなく、処理の簡単化を図ることとした。

【００７５】

図７に示す認証作業では、以後、ステップ１３２において、第２認証後データの数が「登録合成データ不一致数」として算出され、次いで、第１一致数、第１不一致数、および登録合成データ不一致数の少なくとも１つに基づいて、認証の対象である使用者が登録された本人であるか否かが判断される（ステップ１５４）。

ここでは、具体的には、上述した３つの基準の全てが、それぞれ以下に示す条件を満たすか否かにより、本人であるかか否かが判断される。

・第１一致数が、第１一致閾値＝６より大きいか（６以下で他人判定）。

・第１不一致数が、第１不一致閾値＝３より小さいか（３以上で他人判定）。

・登録合成データ不一致数が、登録合成データ不一致閾値＝５より小さいか（５以上で他人判定）。

【００７６】

そして、上記の判別の結果に従い、本人認証を肯定するためのステップ１３６の処理、或いは、本人認証を否定するためのステップ１３８の処理の何れかが実行される。

【００７７】

［登録・認証作業の具体例］

次に、図８を参照して、上述した登録作業および認証作業の具体例を説明する。尚、図８において、個々の特徴点データは、上記図５に示す場合と同様に、簡単化のためスカラー量で表している。

【００７８】

図８は、登録作業の際に、上記ステップ１００～１０６の処理により、以下に示す第１登録指紋データおよび第２登録指紋データが取得された例を示している。

第１登録指紋データ：（１，８，１１，１２，１５，２３，２８，３０，３９，４４）

第２登録指紋データ：（３，８，１０，１５，１９，２８，３０，３３，４０，４７）

【００７９】

第１登録指紋データ、および第２登録指紋データが、それぞれ上記の特徴点データで構成されている場合、上記ステップ１０８の処理によれば、論理和データは以下のように取得される。

論理和データ：（１，３，８，１０，１１，１２，１５，１９，２３，２８，３０，３３，３９，４０，４４，４７）

【００８０】

そして、上記ステップ１４０の処理によれば、上記の如く取得された論理和データが、登録合成データとして記憶部１４のハードディスクなどに登録される。

【００８１】

図８に示す例では、認証作業の際に、上記ステップ１２０および１２２の処理、並びに上記ステップ１２６および１２８の処理により、以下に示す第１認証指紋データおよび第２認証指紋データが取得されている。

第１認証指紋データ：（１，８，１１，１５，２３，２８，３０，３９，４４）

第２認証指紋データ：（３，８，１０，１５，２０，２３，２８，３０，３３，４０，４７）

【００８２】

上述した登録合成データに対して、上記の第１認証指紋データが取得された場合、上記ステップ１５０では、第１一致数、第１不一致数、および第１認証後データがそれぞれ以下のように取得される。

第１一致数＝９　（１，８，１１，１５，２３，２８，３０，３９，４４）

第１不一致数＝０

第１認証後データ：（３，１０，１２，１９，３３，４０，４７）

【００８３】

また、上記の如く取得された第１認証後データに対して、上記の第２認証指紋データが取得された場合、上記ステップ１５２では、第２認証後データが以下のように取得される。

第２認証後データ：（１２，１９）

【００８４】

そして、上記ステップ１３２の処理によれば、登録合成データ不一致数は、以下に示すように、第２認証データのデータ数と等しい「２」と算出される。

登録合成データ不一致数＝２　（１２，１９）

【００８５】

既述した通り、本実施形態における指紋データ認証装置は、第１一致数が６より大きく、第１不一致数が３より小さく、かつ、登録合成データ不一致数が５より小さい場合に、認証の対象であるユーザーを本人として認証する（上記ステップ１５４参照）。図８に示す例では、これらの基準が全て満たされているため、認証の対象であるユーザーは、この場合、本人として認められる。

【００８６】

以上説明した通り、本実施形態における指紋データ登録装置、および指紋データ認証装置は、複数の登録指紋データの論理和データのみを登録合成データとすることで、指紋データの登録および認証に要する処理を簡単化しつつ、高精度な指紋認証処理を実現することができる。このため、本実施形態の構成によれば、実施の形態１のシステムと同様の効果

を奏するシステムを、より安価に実現することができる。
【００８７】
尚、上述した実施の形態２においては、処理部１２が、上記ステップ１０８の処理を実行することにより前記第２の発明における「論理和データ演算手段」が実現されている。
【００８８】
また、上述した実施の形態２においては、処理部２２が、上記ステップ１５０において、第１一致数を求めることにより前記第６の発明における「第１一致数取得手段」が、第１不一致数を求めることにより前記第６の発明における「第１不一致数取得手段」が、それぞれ実現されている。また、処理部２２が、上記ステップ１３２の処理を実行することにより前記第６の発明における「登録合成データ不一致数取得手段」が実現されている。
【００８９】
実施の形態３．
次に、実施の形態２の説明において参照した図６と共に、図９および図１０を参照して、本発明の実施の形態３について説明する。
［登録作業の説明］
実施の形態３において、指紋データ登録装置は、実施の形態２の装置と同様の構成により実現することができる。すなわち、本実施形態における指紋データ登録装置は、図１（Ａ）に示すハードウェア構成を用いて、図６に示すフローチャートに沿って登録作業を進行させることにより実現することができる。この装置によれば、複数の登録指紋データの論理和データを登録合成データとして記憶部１４に登録することができる。
【００９０】
［認証作業の説明］
図９は、実施の形態３における指紋データ認証装置において実現される認証作業の流れを説明するためのフローチャートである。本実施形態において、指紋データ認証装置は、図１（Ｂ）に示すハードウェア構成を用いて、図９に示すフローチャートに沿って認証作業を進行させることにより実現することができる。尚、図９において、上記図４または図７に示すステップと同一のステップについては、同一の符号を付してその説明を省略または簡略する。
【００９１】
図９に示す認証作業では、ステップ１２０および１２２の処理により第１認証指紋データが取得された後、ステップ１５０において、登録合成データと第１認証指紋データとの照合処理が実行され、▲１▼第１一致数、▲２▼第１不一致数、および▲３▼第１認証後データが算出される。
【００９２】
次いで、ステップ１２６および１２８の処理により第２認証指紋データが取得された後、登録合成データと第２認証指紋データとの照合処理が実行され、その結果、▲１▼第２一致数、▲２▼第２不一致数、および▲３▼第２認証後データが算出される（ステップ１６０）。
【００９３】
以上説明した通り、図９に示す認証作業では、第１認証指紋データ、および第２認証指紋データが、何れも登録合成データと照合される。そして、上記ステップ１６０では、上記ステップ１５０において用いられるのと同様の手順で、第２一致数、第２不一致数、および第２認証後データが算出される。この場合、第２一致数は、第１一致数と同様に、認証に用いられた指紋と登録に用いられた指紋の一致度が増すほど大きくなる傾向を示す。また、第２不一致数は、第１不一致数と同様に、認証に用いられた指紋と登録に用いられた指紋の一致度が増すほど小さくなる傾向を示す。従って、本実施形態においては、第１一致数および第２一致数と同様に、第２一致数および第２不一致数も、本人認証のための有効な判断材料として用いることができる。
【００９４】
図９に示す認証作業では、次に、第１認証後データ、および第２認証後データの論理積を

とることにより、登録合成データ不一致数が求められる（ステップ１６２）。
既述した通り、第１認証後データは、登録合成データのうち、第１認証指紋データに含まれていなかった特徴点データの集合である。また、第２認証後データは、登録合成データのうち、第２認証指紋データに含まれていなかった特徴点データの集合である。従って、第１認証後データと第２認証後データの論理積は、登録合成データのうち、第１認証指紋データにも、第２認証指紋データにも含まれていなかった特徴点データの集合となる。本ステップ１６２では、その集合に含まれる特徴点データの数が、登録合成データ不一致数として算出される。
【００９５】
上記の手法によれば、実施の形態１または２の場合と一致する登録合成データ不一致数を得ることができる。そして、その登録合成データ不一致数は、認証に用いられた指紋と登録に用いられた指紋の一致度が増すほど小さくなる傾向を示す。このため、本実施形態において算出される登録合成データ不一致数も、実施の形態１または２の場合と同様に、本人認証のための有効な判断材料として用いることができる。
【００９６】
図９に示す認証作業では、以後、上記の如く算出された第１一致数、第１不一致数、第２一致数、第２不一致数、および登録合成データ不一致数の少なくとも１つに基づいて、認証の対象である使用者が登録された本人であるか否かが判断される（ステップ１６４）。ここでは、具体的には、上述した５つの基準の全てが、それぞれ以下に示す条件を満たすか否かにより、本人であるかか否かが判断される。
・第１一致数が、第１一致閾値＝６より大きいか（６以下で他人判定）。
・第１不一致数が、第１不一致閾値＝３より小さいか（３以上で他人判定）。
・第２一致数が、第２一致閾値＝６より大きいか（６以下で他人判定）。
・第２不一致数が、第２不一致閾値＝３より小さいか（３以上で他人判定）。
・登録合成データ不一致数が、登録合成データ不一致閾値＝５より小さいか（５以上で他人判定）。
【００９７】
そして、上記の判別の結果に従い、本人認証を肯定するためのステップ１３６の処理、或いは、本人認証を否定するためのステップ１３８の処理の何れかが実行される。
【００９８】
［登録・認証作業の具体例］
次に、図１０を参照して、上述した登録作業および認証作業の具体例を説明する。尚、図１０において、個々の特徴点データは、上記図５または図８に示す場合と同様に、簡単化のためスカラー量で表している。
【００９９】
図１０は、登録作業の際に、図６に示す登録作業により、以下に示す第１登録指紋データおよび第２登録指紋データが取得され、更に、以下に示す論理和データが登録合成データとして登録された例を示している。
第１登録指紋データ：（１，８，１１，１２，１５，２３，２８，３０，３９，４４）
第２登録指紋データ：（３，８，１０，１５，１９，２８，３０，３３，４０，４７）
論理和データ：（１，３，８，１０，１１，１２，１５，１９，２３，２８，３０，３３，３９，４０，４４，４７）
【０１００】
図１０に示す例では、認証作業の際に、上記ステップ１２０および１２２の処理、並びに上記ステップ１２６および１２８の処理により、以下に示す第１認証指紋データおよび第２認証指紋データが取得されている。
第１認証指紋データ：（１，８，１１，１５，２３，２８，３０，３９，４４）
第２認証指紋データ：（３，８，１０，１５，２０，２３，２８，３０，３３，４０，４７）
【０１０１】

上述した登録合成データに対して、上記の第１認証指紋データが取得された場合、図９に示すステップ１５０では、第１一致数、第１不一致数、および第１認証後データがそれぞれ以下のように取得される。
第１一致数＝９　（１，８，１１，１５，２３，２８，３０，３９，４４）
第１不一致数＝０
第１認証後データ：（３，１０，１２，１９，３３，４０，４７）
【０１０２】
また、上述した登録合成データに対して、上記の第２認証指紋データが取得された場合、上記ステップ１６０では、第２一致数、第２不一致数、および第２認証後データがそれぞれ以下のように取得される。
第２一致数＝１０　（３，８，１０，１５，２３，２８，３０，３３，４０，４７）
第２不一致数＝１　（２０）
第２認証後データ：（１，１１，１２，１９，３９，４４）
【０１０３】
そして、上記ステップ１６２の処理によれば、上記の第１認証後データ、および第２認証後データに基づいて、登録合成データ不一致数が以下に示すように算出される。
登録合成データ不一致数＝２　（１２，１９）
【０１０４】
既述した通り、本実施形態における指紋データ認証装置は、第１一致数が６より大きく、第１不一致数が３より小さく、第２一致数が６より大きく、第２不一致数が３より小さく、かつ、登録合成データ不一致数が５より小さい場合に、認証の対象であるユーザーを本人として認証する（上記ステップ１６４参照）。図１０に示す例では、これらの基準が全て満たされているため、認証の対象であるユーザーは、この場合、本人として認められる。
【０１０５】
以上説明した通り、本実施形態における指紋データ登録装置、および指紋データ認証装置は、複数の登録指紋データの論理和データのみを登録合成データとすることで、指紋データの登録および認証に要する処理を簡単化しつつ、高精度な指紋認証処理を実現することができる。このため、本実施形態の構成によれば、実施の形態１のシステムと同様の効果を奏するシステムを、より安価に実現することができる。
【０１０６】
尚、上述した実施の形態３においては、処理部１２が、上記ステップ１５０において第１一致数を求め、上記ステップ１６０において第２一致数を求めることにより前記第８の発明における「第ｎ一致数取得手段」が、上記ステップ１５０において第１不一致数を求め、上記ステップ１６０において第２不一致数を求めることにより前記第８の発明における「第ｎ不一致数取得手段」が、それぞれ実現されている。また、処理部２２が、上記ステップ１６２の処理を実行することにより前記第８の発明における「登録合成データ不一致数取得手段」が実現されている。
【０１０７】
実施の形態４．
次に、図１１を参照して、本発明の実施の形態４について説明する。
［登録作業の説明］
図１１は、実施の形態４における指紋データ登録装置において実現される登録作業の流れを説明するためのフローチャートである。本実施形態において、指紋データ登録装置は、図１（Ａ）に示すハードウェア構成を用いて、図１１に示すフローチャートに沿って登録作業を進行させることにより実現することができる。また、本実施形態における指紋データ登録装置は、実施の形態１における指紋データ認証装置と組み合わせて用いることができる。尚、図１１において、上記図２に示すステップと同一のステップについては、同一の符号を付してその説明を省略または簡略する。
【０１０８】

図１１に示す登録作業は、ステップ１００～１０６の処理に次いで、ステップ１７０の処理が実行される点を除き、図２に示す登録作業と同様である。すなわち、図１１に示す登録作業では、ステップ１００～１０６の処理により、第１登録指紋データと、第２登録指紋データとが取得された後、それら２つの登録指紋データの相対位置関係が、両者の論理積データのデータ数が最大となる位置に特定される（ステップ１７０）。

【０１０９】

本ステップ１７０における相対位置の特定は、具体的には、第１登録指紋データの位置（座標軸）を固定したうえで、第２登録指紋データの位置を所定の範囲内で適当に移動、或いは回転させつつ、両者が最も整合する位置を探す手法で行われる。ここで、ある相対位置関係における両者の整合度合いは、その位置関係において、両者の論理積データを求めたうえで、そのデータ数により判断する。その結果、本ステップ１７０の処理によれば、第１登録指紋データと第２登録指紋データとの相対位置が、両者の論理積データ数が最大となる位置、つまり、両者間での重複データ数が最大となるような位置に特定される。

【０１１０】

［認証作業の説明］

本実施形態において、認証作業は、実施の形態１の場合と同様に行われる（図４および図５参照）。つまり、本実施形態における認証作業では、登録合成データと第１認証指紋データとの照合処理（上記ステップ１２０～１２４参照）、および第１認証後データと第２認証指紋データとの照合処理（上記ステップ１２６～１３０参照）が実行される。また、それぞれの照合処理（ステップ１２４および１３０）は、照合すべき２つの指紋データの相対位置を適当に整合させるための処理を含んでいる。

【０１１１】

登録合成データに含まれている第１指の指紋データ（ここでは、第１登録指紋データと仮定する）の相対位置と、その指に対応する認証指紋データ（ここでは、第１認証指紋データと仮定する）の相対位置とを正確に整合させるためには、登録合成データに、第１登録指紋データ以外の余計な特徴点データが含まれていないことが望ましい。

【０１１２】

本実施形態における登録作業では、既述した通り、第１登録指紋データと第２登録指紋データの双方に重複して含まれる特徴点データが最大となるように、それら２つのデータが合成される。登録合成データがこのようにして生成される場合、登録合成データに含まれる特徴点データのうち、何れか一方の登録指紋データにしか含まれないものの数は最少となる。つまり、本実施形態における登録作業によれば、認証作業の際に、登録合成データの相対位置と第１認証指紋データの相対位置とを整合させるうえで余計な特徴点データとなるデータの数を最少とすることができる。

【０１１３】

このため、本実施形態のシステムによれば、認証作業の際に、登録合成データと第１認証指紋データとを精度よく相対位置合わせしたうえで両者を適正に照合することができる。ひいては、第２指の登録指紋データと精度良く一致する第１認証後データを生成することができ、その第１認証後データと第２認証指紋データとを精度良く照合させることができる。このため、本実施形態のシステムによれば、実施の形態１のシステムに比して、本人認証の精度をより一層高めることができる。

【０１１４】

ところで、上述した実施の形態４においては、第１登録指紋データと第２登録指紋データとを最適な相対位置関係で合成するという機能を、実施の形態１のシステムに組み込むこととしているが、この機能の適用はこれに限定されるものではない。すなわち、第１登録指紋データと第２登録指紋データとを最適な相対位置関係で合成するという機能は、実施の形態２または３の装置に組み込むこととしてもよい。

【０１１５】

尚、上述した実施の形態４においては、処理部１２が、上記ステップ１７０において、第１登録指紋データと第２登録指紋データの相対位置を変化させることにより前記第４の発

明における「相対位置関係変更手段」が、変更された個々の相対位置関係において両者の論理積データを取得することにより前記第４の発明における「特定用論理積データ取得手段」が、そのようにして取得された論理積データのデータ数が最大となるように２つの登録指紋データの相対位置を特定することにより前記第４の発明における「相対位置関係特定手段」が、それぞれ実現されている。

【０１１６】

実施の形態５．

次に、図１２を参照して、本発明の実施の形態５について説明する。

［登録作業の説明］

実施の形態５において、指紋データ登録装置は、実施の形態１の装置と同様の構成により実現することができる。すなわち、本実施形態における指紋データ登録装置は、図１（Ａ）に示すハードウェア構成を用いて、図２に示すフローチャートに沿って登録作業を進行させることにより実現することができる。この装置によれば、複数の登録指紋データの論理和データと、個々の特徴点データの、複数の登録指紋データ内での重複数を意味するカウンタ数とを登録合成データとして記憶部１４に登録することができる。

【０１１７】

［認証作業の説明］

図１２は、実施の形態５における指紋データ認証装置において実現される認証作業の流れを説明するためのフローチャートである。本実施形態の装置は、図１（Ｂ）に示すハードウェア構成を用いて、図１２に示すフローチャートに沿って認証作業を進行させることにより実現することができる。尚、図１２において、上記図４、図７、または図９に示すステップと同一のステップについては、同一の符号を付してその説明を省略または簡略する。

【０１１８】

図１２に示す認証作業では、ステップ１２０および１２２の処理により第１認証指紋データが取得された後、所定の規則に従って初期設定された相対位置関係において、登録合成データと第１認証指紋データとの照合処理が実行される（ステップ１８０）。

【０１１９】

次に、上記の照合の結果、登録合成データと第１認証指紋データの双方において一致している特徴点データの数が、所定閾値（例えば６）を超えているか否かが判別される（ステップ１８２）。

【０１２０】

特徴点データの一致数が所定閾値を超えていないと判別された場合は、今回の処理サイクルで採用された相対位置関係が適正なものではないと判断される。そして、この場合は、以後、ステップ１８４がジャンプされ、速やかにステップ１８６の処理が実行される。

【０１２１】

一方、上記ステップ１８２において、特徴点データの一致数が所定閾値を超えていると判別された場合は、今回の処理サイクルで採用された相対位置関係が、適正なものである可能性があると判断される。この場合は、以後、以下の処理が実行される（ステップ１８４）。

▲１▼特徴点データの一致数を第１一致数（第１認証指紋データに含まれる特徴点データのうち、登録合成データ中の特徴点データと一致するものの数）として記録。

▲２▼第１不一致数（第１認証指紋データに含まれる特徴点データのうち、登録合成データ中の特徴点データと一致しないものの数）の算出。

▲３▼第１認証後データの生成。

【０１２２】

上記▲１▼～▲３▼の処理のうち、▲１▼および▲２▼の処理は、図４に示すステップ１２４や、図９に示すステップ１５０において実行される処理と実質的に同様である。このため、ここでは、それらについての詳細な説明は省略する。これに対して、▲３▼の処理は、上記ステップ１２４、或いは上記ステップ１５０で実行される処理とその内容が異な

っている。

【０１２３】

すなわち、図４に示すステップ１２４では、登録合成データにカウンタ数が含まれていることを前提として、カウンタ数の減算後になお１以上のカウンタ数を有する特徴点データのみを残存させることで第１認証後データを生成している。また、図９に示すステップ１５０では、登録合成データにカウンタ数が含まれていないことを前提として、登録合成データに含まれている特徴点データのうち、第１認証指紋データに含まれている特徴点データを単純に削除することにより第１認証後データを生成している。

【０１２４】

これに対して、本ステップ１８４では、登録合成データにカウンタ数が含まれていることを前提とし、個々の特徴点データについてのカウンタ数を維持しつつ、登録合成データに含まれている特徴点データのうち、第１認証指紋データに含まれている特徴点データを削除することにより第１認証後データを生成している。つまり、本ステップ１８４の処理によれば、登録合成データに含まれており、かつ、第１認証指紋データに含まれていなかった特徴点データと、登録作業の際にそれらの特徴点データに付与されていたカウンタ数とを含む情報が、第１認証後データとして生成される。

【０１２５】

図１２に示す認証作業では、次に、処理部２２によって、予め設定された範囲（移動範囲、および移動角度）に属する全ての相対位置関係につき、照合処理が終了したか否かが判別される（ステップ１８６）。

【０１２６】

その結果、未だ全ての相対位置関係につき、照合処理が終了していないと判別された場合は、登録合成データと第１認証指紋データの相対位置関係を変化させたうえで、再び上記ステップ１８０以降の処理が繰り返される。一方、全ての相対位置関係につき照合処理が終了していると判別された場合は、有効な照合が存在していたか、つまり、上記ステップ１８２において、一致数が所定閾値を超えていると判断された照合が存在するか否かが判断される（ステップ１８８）。

【０１２７】

上記ステップ１８８において、有効な照合が存在しないと判断された場合は、今回の認証に用いられた指紋は、登録されたユーザーの指紋ではないと判断される。この場合、以後、本人認証を否定すべくステップ１３６の処理が実行される。一方、上記ステップ１８８において、有効な照合が存在すると判別された場合は、次に、ステップ１２６および１２８の処理により第２認証指紋データが取得される。

【０１２８】

ステップ１２８の処理が終了すると、今度は、登録合成データと第２認証指紋データとを対象として、上述したステップ１８０～１８８の処理と同様の処理が実行される（ステップ１９０～１９８）。

【０１２９】

そして、ステップ１９８において、登録合成データと第２認証指紋データとの関係では、有効な照合が存在しなかったと判断された場合は、本人認証を否定すべくステップ１３６の処理が実行される。一方、上記ステップ１９８において、有効な照合が存在すると判別された場合は、次に、有効な照合と判断された全ての照合の中から、第１認証指紋データ、および第２認証指紋データのそれぞれにつき、最適な照合（相対位置関係）が特定される（ステップ２００）。

【０１３０】

本ステップ２００では、具体的には、以下の処理が実行される。

▲１▼上記ステップ１８４で生成された全ての第１認証後データについて、カウンタ数の総和を算出。

▲２▼カウンタ数の総和が最少である第１認証後データを特定。

▲３▼上記の処理で特定された第１認証後データを生成させた照合（相対位置関係）を、

登録合成データと第１認証指紋データとについての最適な照合（相対位置関係）として特定。
▲４▼上記ステップ１９４で生成された全ての第２認証後データについて、カウンタ数の総和を算出。
▲５▼カウンタ数の総和が最少である第２認証後データを特定。
▲６▼上記の処理で特定された第２認証後データを生成させた照合（相対位置関係）を、登録合成データと第２認証指紋データとについての最適な照合（相対位置関係）として特定。
【０１３１】
第１認証後データのカウンタ数の総和、および第２認証後データのカウンタ数の総和は、何れも、それらのデータに含まれている特徴点データの数が少ないほど小さな値となる。そして、特徴点データの数が同数である場合は、カウンタ数２を有する特徴点データ数が少ないほどカウンタ数の総和は小さな値となる。従って、上記ステップ２００の処理によれば、第１認証後データ中の特徴点データ数を最少とし、かつ、そこに含まれるカウンタ数２の特徴点データ数を最少とする照合を、第１認証後データに関する最適な照合として特定することができる。同様に、第２認証後データ中の特徴点データ数を最少とし、かつ、そこに含まれるカウンタ数２の特徴点データ数を最少とする照合を第２認証指紋データに関する最適な照合として特定することができる。
【０１３２】
第１認証後データに含まれている特徴点データ数が最少であるということは、登録合成データと第１認証指紋データとが最も良く整合していることを意味する。また、第１認証後データに含まれているカウンタ数２の特徴点データ数が最少であるということは、その照合（相対位置関係）において、第１認証後データ中の特徴点データが、登録合成データ中の重複データ（２つの登録指紋データに含まれる特徴点データ）と、最も数多く整合していることを意味している。
【０１３３】
本実施形態において、登録合成データの中には、２つの登録指紋データのうち一方にしか含まれていない特徴点データ（非重複データ）と、何れの登録指紋データにも重複して含まれている特徴点データ（重複データ）とが含まれている。登録に用いられた２本の指で認証作業が行われる場合、登録合成データ中の非重複データについては、何れの指に対応するデータであるかが不確かである。これに対して、登録合成データ中の重複データは、何れの指の照合時にも、その指に対応していることが確かなデータである。
【０１３４】
従って、カウンタ数２の特徴点データが最少となる照合（相対位置関係）では、第１指についても、第２指についても、その指に対応することが確かなデータ同士が最も数多く整合していることになる。第１指を用いた照合処理において、第１認証指紋データが、その指に対応することが不確かな特徴点データと数多く整合している場合と、その指に対応することが確かな特徴点データと数多く整合している場合とでは、正しい認証結果を得るうえで後者の方が望ましいことは明らかである。上述したステップ２００の処理によれば、第１認証指紋データについても、第２認証指紋データについても、上記の観点から最適と判断できる照合（相対位置関係）を、最適な照合（相対位置関係）として特定することができる。
【０１３５】
図１２に示す認証作業では、以後、最適な照合（相対位置関係）において所得されていた第１一致数、第１不一致数、第１認証後データ、第２一致数、第２不一致数、および第２認証後データに基づいて、本人認証のための処理、すなわち、ステップ１６２および１６４の処理が実行される。
【０１３６】
［登録・認証作業の具体例］
次に、図１３を参照して、上述した登録作業および認証作業の具体例を説明する。尚、図

８において、個々の特徴点データは、上記図５に示す場合と同様に、簡単化のためスカラー量で表している。

【０１３７】

図１３は、登録作業の際に、上記ステップ１００～１０６の処理により、以下に示す第１登録指紋データおよび第２登録指紋データが取得された例を示している。

第１登録指紋データ：（１，８，１１，１２，１５，２３，２８，３０，３９，４４）

第２登録指紋データ：（３，８，１０，１５，１９，２８，３０，３３，４０，４７）

【０１３８】

本実施形態の指紋登録装置によれば、実施の形態１の場合と同様に、この場合、以下に示す論理和データ、およびカウンタ数の情報が、登録合成データとして登録される。

論理和データ：（１，３，８，１０，１１，１２，１５，１９，２３，２８，３０，３３，３９，４０，４４，４７）

カウンタ数２：８，１５，２８，３０

カウンタ数１：１，３，１０，１１，１２，１９，２３，３３，３９，４０，４４，４７

【０１３９】

図１３に示す例では、認証作業の際に、上記ステップ１２０および１２２の処理、並びに上記ステップ１２６および１２８の処理により、以下に示す第１認証指紋データおよび第２認証指紋データが取得されている。

第１認証指紋データ：（１，８，１１，１５，２３，２８，３０，３９，４４）

第２認証指紋データ：（３，８，１０，１５，２０，２３，２８，３０，３３，４０，４７）

【０１４０】

また、図１３は、上記の第１認証指紋データ、および第２認証指紋データが、そのままの状態で最適な照合を実現し得るものであった場合を示している。このため、図１３に示す例では、上述した登録合成データと、上記の第１認証指紋データとに基づいて、最適照合における第１一致数、第１不一致数、および第１認証後データが、それぞれ以下のように取得されている（上記ステップ１８４および２００参照）。

第１一致数＝９　（１，８，１１，１５，２３，２８，３０，３９，４４）

第１不一致数＝０

第１認証後データ：（３，１０，１２，１９，３３，４０，４７）

【０１４１】

また、図１３に示す例では、上述した登録合成データと、上記の第２認証指紋データとに基づいて、最適照合における第２一致数、第２不一致数、および第２認証後データが、それぞれ以下のように取得されている（上記ステップ１９４および２００参照）。

第２一致数＝１０　（３，８，１０，１５，２３，２８，３０，３３，４０，４７）

第２不一致数＝１　（２０）

第２認証後データ：（１，１１，１２，１９，３９，４４）

【０１４２】

この場合、ステップ１６２では、上記の第１認証後データ、および第２認証後データに基づいて、登録合成データ不一致数が以下に示すように算出される。

登録合成データ不一致数＝２　（１２，１９）

【０１４３】

そして、ステップ１６４では、第１一致数、第１不一致数、第２一致数、第２不一致数、および登録合成データ不一致数が何れも認証基準を満たしていることから、本人認証が肯定される。

【０１４４】

以上説明した通り、本実施形態における指紋データ登録装置、および指紋データ認証装置は、単体での指紋データを用いることなく、登録合成データのみを恒常的に記憶しつつ、最適な照合を探して認証作業を進めることができる。このため、本実施形態の構成によれば、単体の指紋データの流出や盗用を確実に防止しつつ、極めて高い精度での認証処理を

実現し得る指紋認証システムを提供することができる。

【０１４５】

ところで、上述した実施の形態５においては、指紋データの登録を、実施の形態１の場合と同様に実行することとしているが、その登録の手法はこれに限定されるものではない。すなわち、本実施形態では、複数の登録指紋データの論理和データと、個々の特徴点データの、複数の登録指紋データ内での重複数とが登録合成データに含まれていればよく、例えば、実施の形態４における方法でその登録を行うこととしてもよい。

【０１４６】

尚、上述した実施の形態５においては、処理部２２が、上記ステップ１８０および１９０の処理を実行することにより前記第９の発明における「相対位置関係変更手段」が、上記ステップ１８４において第１認証後データを生成し、上記ステップ１９４において第２認証後データを生成することにより前記第９の発明における「第ｎ認証後データ生成手段」が、上記ステップ２００において、第１認証後データのカウンタ数の総和、および第２認証後データのカウンタ数の総和を求めることにより前記第９の発明における「カウンタ数総和演算手段」が、上記ステップ２００において最適な相対位置関係を特定することにより前記第９の発明における「相対位置関係特定手段」が、特定された相対位置関係に対して上記ステップ１８４において第１一致数を算出し、かつ、上記ステップ１９４において第２一致数を算出することにより前記第９の発明における「第ｎ一致数取得手段」が、特定された相対位置関係に対して上記ステップ１８４において第１不一致数を算出し、かつ、上記ステップ１９４において第２不一致数を算出することにより前記第９の発明における「第ｎ不一致数取得手段」が、それぞれ実現されている。

【０１４７】

【発明の効果】

この発明は以上説明したように構成されているので、以下に示すような効果を奏する。

請求項１記載の発明によれば、単独の登録指紋データを記憶するのを避けて、恒常的には、複数の登録指紋データを合成することで生成された登録合成データだけを記憶させておくことができる。このため、本発明によれば、ユーザーの指紋データが単独で流出または盗用されるのを確実に防ぐことができる。

【０１４８】

請求項２記載の発明によれば、複数の登録指紋データの論理和データを求めることにより、登録合成データを簡単に生成することができる。

【０１４９】

請求項３記載の発明によれば、複数の登録指紋データの論理和データを求めると共に、それらの登録指紋データの論理積データを求めることにより、個々の登録指紋データに含まれる全てのデータと、それらのデータの、複数の登録指紋データ内での重複数とに関する情報を含む登録合成データを簡単に生成することができる。

【０１５０】

請求項４記載の発明によれば、複数の登録指紋データを、論理積データのデータ数を最大とする相対位置関係で合成することができる。この場合、登録合成データ中に、複数の登録指紋データにおいて重複するデータを数多く含ませることができるため、後の認証の際に、高い認証レベルを得ることができる。

【０１５１】

請求項５記載の発明によれば、複数の登録指紋データに関する情報を含む対照用登録合成データを用いて認証の可否を決定することができる。このため、本発明によれば、指紋データの単独での流出乃至盗用を確実に防ぐことができる。

【０１５２】

請求項６記載の発明によれば、複数の登録指紋データの論理和データで構成される対照用登録合成データを、第１指の認証指紋データと対照させることにより、第１一致数、および第１不一致数を求めることができる。更に、この発明によれば、対照用登録合成データに含まれるデータのうち、何れの認証指紋データにも含まれないものの数を登録合成デー

タ不一致数として求めることができる。そのうえで、少なくともそれらの一つに基づいて、認証の可否を決定することができる。

【０１５３】

請求項７記載の発明によれば、複数の登録指紋データの論理和データと、その論理和データに含まれる個々のデータの、上記複数の登録指紋データ内での重複数とに関する情報を含む登録合成データを、複数の認証指紋データと対照させることにより、第ｎ一致数、第ｎ不一致数（１≦ｎ≦Ｎ）、および登録合成データ不一致数を求めることができる。そのうえで、少なくともそれらの一つに基づいて、認証の可否を決定することができる。

【０１５４】

請求項８記載の発明によれば、複数の登録指紋データの論理和データで構成される対照用登録合成データを、複数の認証指紋データのそれぞれと対照させることにより、第ｎ一致数、第ｎ不一致数、および登録合成データ不一致数を求めることができる。そのうえで、少なくともそれらの一つに基づいて、認証の可否を決定することができる。

【０１５５】

請求項９記載の発明によれば、対照用登録合成データを、第ｎ指の認証指紋データと対照させる際に、第ｎ認証後データに含まれる個々のデータの重複数の和が最少となるように両者の相対位置関係を特定することができる。この場合、複数の登録指紋データにおいて重複しているものとして対照用登録合成データ中に記憶されているデータ、つまり、第ｎ指の指紋データである確率の高いデータが優先的に一致するように相対位置関係が決定される。そのうえで、第ｎ一致数、第ｎ不一致数、および登録合成データ不一致数の少なくとも１つに基づいて、認証の可否を決定することができるため、高い認証レベルを実現することができる。

【図面の簡単な説明】

【図１】本発明の実施の形態１のシステムの構成を説明するためのブロック図である。

【図２】本発明の実施の形態１における登録作業を説明するためのフローチャートである。

【図３】図２に示す登録作業において扱われるデータのイメージを説明するための図である。

【図４】本発明の実施の形態１における認証作業を説明するためのフローチャートである。

【図５】本発明の実施の形態１における登録・認証作業の具体例を説明するための図である。

【図６】本発明の実施の形態２における登録作業を説明するためのフローチャートである。

【図７】本発明の実施の形態２における認証作業を説明するためのフローチャートである。

【図８】本発明の実施の形態２における登録・認証作業の具体例を説明するための図である。

【図９】本発明の実施の形態３における認証作業を説明するためのフローチャートである。

【図１０】本発明の実施の形態３における登録・認証作業の具体例を説明するための図である。

【図１１】本発明の実施の形態４における登録作業を説明するためのフローチャートである。

【図１２】本発明の実施の形態５における認証作業を説明するためのフローチャートである。

【図１３】本発明の実施の形態５における登録・認証作業の具体例を説明するための図である。

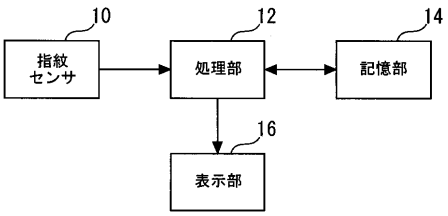
【符号の説明】

１０，２０　指紋センサ

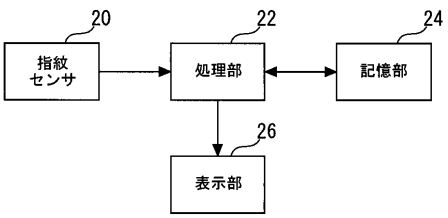
１２，２２　処理部
１４，２４　記憶部

【図１】

（Ａ）

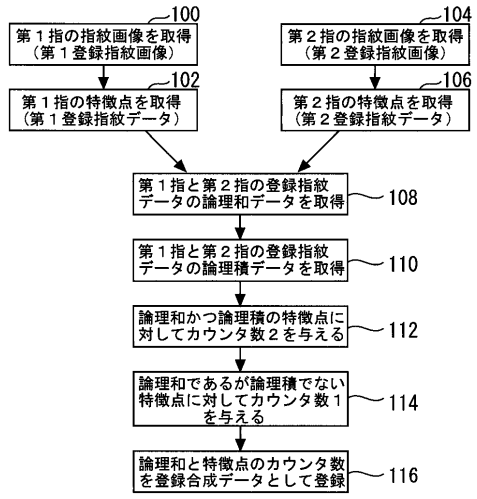


（Ｂ）

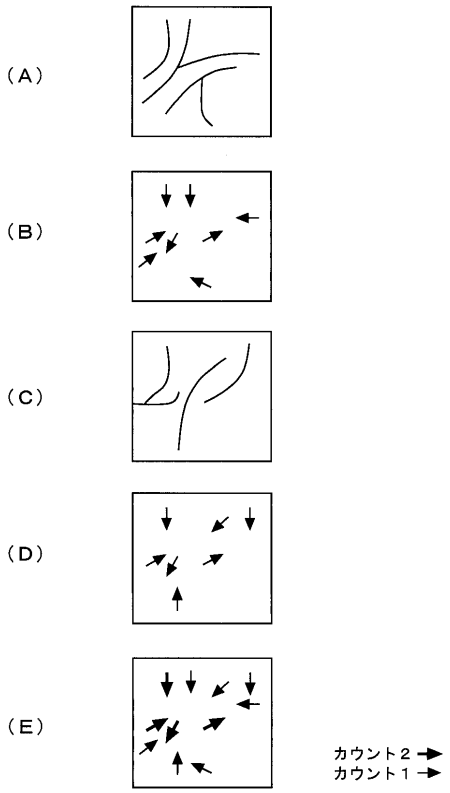


【図２】

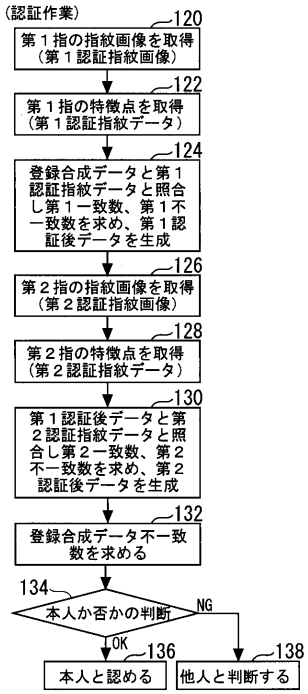
（登録作業）



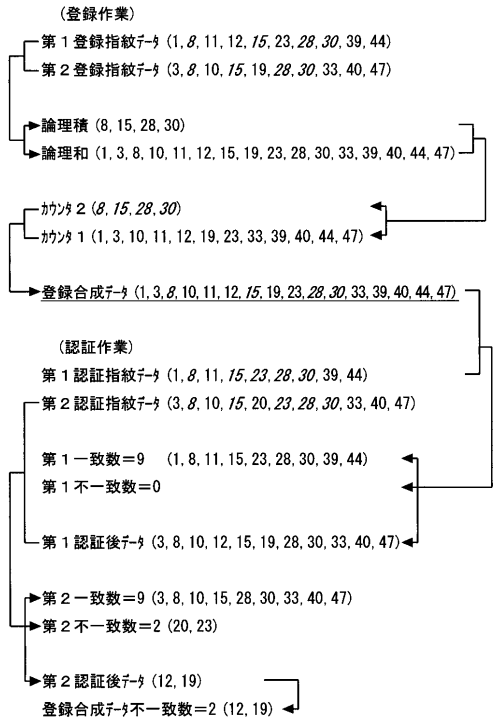
【図３】


（A）
（B）
（C）
（D）
（E）
カウント２
カウント１

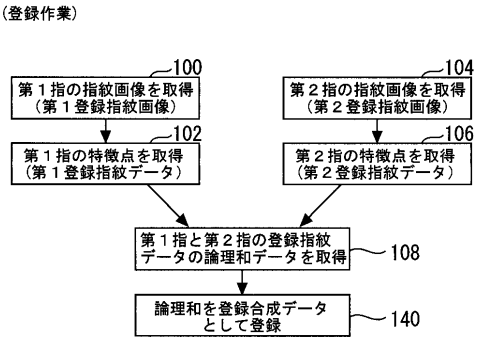
【図４】


（認証作業）
120
第１指の指紋画像を取得（第１認証指紋画像）
122
第１指の特徴点を取得（第１認証指紋データ）
124
登録合成データと第１認証指紋データと照合し第１一致数、第１不一致数を求め、第１認証後データを生成
126
第２指の指紋画像を取得（第２認証指紋画像）
128
第２指の特徴点を取得（第２認証指紋データ）
130
第１認証後データと第２認証指紋データと照合し第２一致数、第２不一致数を求め、第２認証後データを生成
132
登録合成データ不一致数を求める
134
本人か否かの判断
NG
OK
136
本人と認める
138
他人と判断する

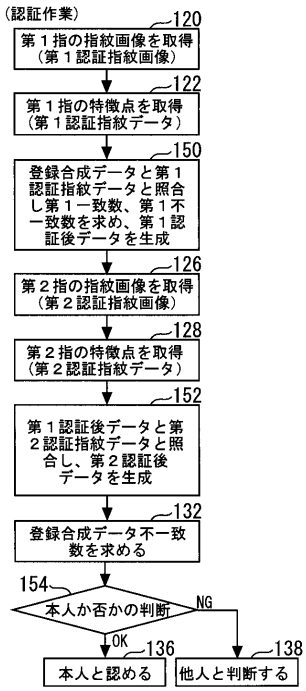
【図５】


（登録作業）
第１登録指紋データ (1, 8, 11, 12, 15, 23, 28, 30, 39, 44)
第２登録指紋データ (3, 8, 10, 15, 19, 28, 30, 33, 40, 47)
論理積 (8, 15, 28, 30)
論理和 (1, 3, 8, 10, 11, 12, 15, 19, 23, 28, 30, 33, 39, 40, 44, 47)
カウンタ２ (8, 15, 28, 30)
カウンタ１ (1, 3, 10, 11, 12, 19, 23, 33, 39, 40, 44, 47)
登録合成データ (1, 3, 8, 10, 11, 12, 15, 19, 23, 28, 30, 33, 39, 40, 44, 47)
（認証作業）
第１認証指紋データ (1, 8, 11, 15, 23, 28, 30, 39, 44)
第２認証指紋データ (3, 8, 10, 15, 20, 23, 28, 30, 33, 40, 47)
第１一致数＝9 (1, 8, 11, 15, 23, 28, 30, 39, 44)
第１不一致数＝0
第１認証後データ (3, 8, 10, 12, 15, 19, 28, 30, 33, 40, 47)
第２一致数＝9 (3, 8, 10, 15, 28, 30, 33, 40, 47)
第２不一致数＝2 (20, 23)
第２認証後データ (12, 19)
登録合成データ不一致数＝2 (12, 19)

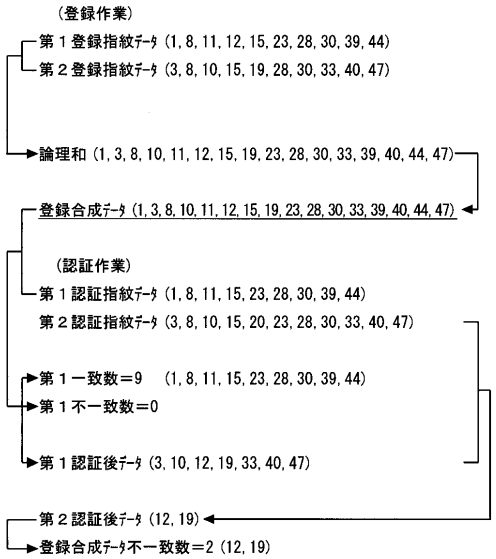
【図６】


（登録作業）
100
第１指の指紋画像を取得（第１登録指紋画像）
102
第１指の特徴点を取得（第１登録指紋データ）
104
第２指の指紋画像を取得（第２登録指紋画像）
106
第２指の特徴点を取得（第２登録指紋データ）
第１指と第２指の登録指紋データの論理和データを取得
108
論理和を登録合成データとして登録
140

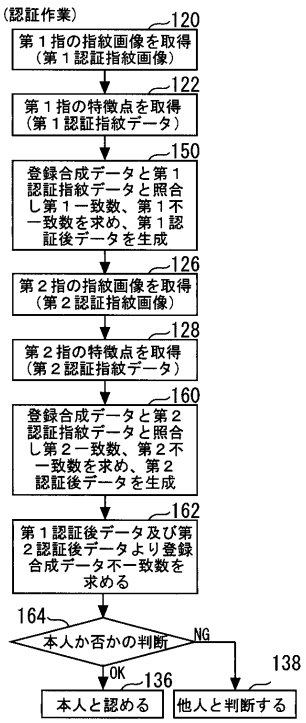
【図７】


(認証作業)
120
第１指の指紋画像を取得
（第１認証指紋画像）
122
第１指の特徴点を取得
（第１認証指紋データ）
150
登録合成データと第１認証指紋データと照合し第１一致数、第１不一致数を求め、第１認証後データを生成
126
第２指の指紋画像を取得
（第２認証指紋画像）
128
第２指の特徴点を取得
（第２認証指紋データ）
152
第１認証後データと第２認証指紋データと照合し、第２認証後データを生成
132
登録合成データ不一致数を求める
154
本人か否かの判断
NG
OK
136
本人と認める
138
他人と判断する

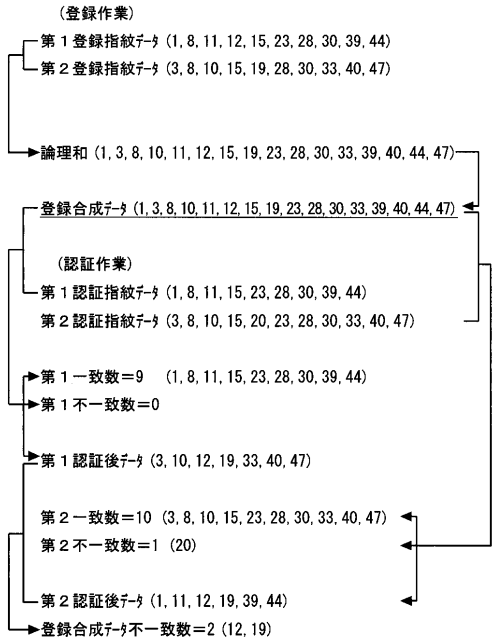
【図８】


（登録作業）
第１登録指紋ﾃﾞｰﾀ (1, 8, 11, 12, 15, 23, 28, 30, 39, 44)
第２登録指紋ﾃﾞｰﾀ (3, 8, 10, 15, 19, 28, 30, 33, 40, 47)
論理和 (1, 3, 8, 10, 11, 12, 15, 19, 23, 28, 30, 33, 39, 40, 44, 47)
登録合成ﾃﾞｰﾀ (1, 3, 8, 10, 11, 12, 15, 19, 23, 28, 30, 33, 39, 40, 44, 47)
（認証作業）
第１認証指紋ﾃﾞｰﾀ (1, 8, 11, 15, 23, 28, 30, 39, 44)
第２認証指紋ﾃﾞｰﾀ (3, 8, 10, 15, 20, 23, 28, 30, 33, 40, 47)
第１一致数＝9 (1, 8, 11, 15, 23, 28, 30, 39, 44)
第１不一致数＝0
第１認証後ﾃﾞｰﾀ (3, 10, 12, 19, 33, 40, 47)
第２認証後ﾃﾞｰﾀ (12, 19)
登録合成ﾃﾞｰﾀ不一致数＝2 (12, 19)

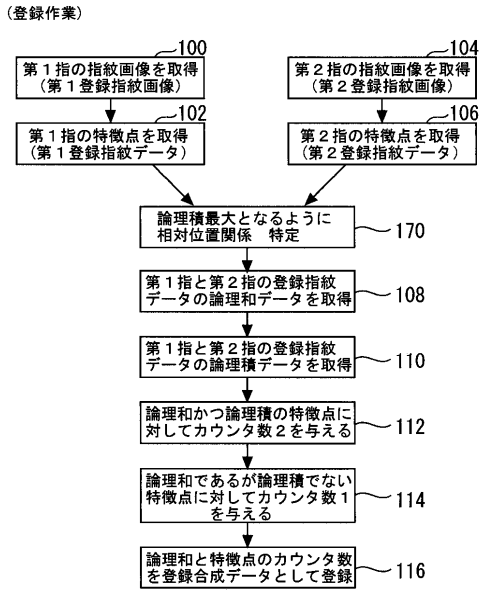
【図９】


(認証作業)
120
第１指の指紋画像を取得
（第１認証指紋画像）
122
第１指の特徴点を取得
（第１認証指紋データ）
150
登録合成データと第１認証指紋データと照合し第１一致数、第１不一致数を求め、第１認証後データを生成
126
第２指の指紋画像を取得
（第２認証指紋画像）
128
第２指の特徴点を取得
（第２認証指紋データ）
160
登録合成データと第２認証指紋データと照合し第２一致数、第２不一致数を求め、第２認証後データを生成
162
第１認証後データ及び第２認証後データより登録合成データ不一致数を求める
164
本人か否かの判断
NG
138
OK
136
本人と認める
他人と判断する

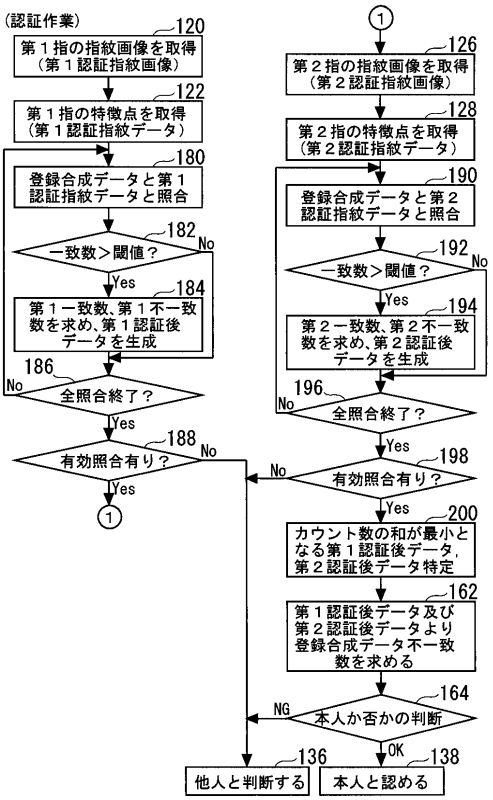
【図１０】


（登録作業）
第１登録指紋ﾃﾞｰﾀ (1, 8, 11, 12, 15, 23, 28, 30, 39, 44)
第２登録指紋ﾃﾞｰﾀ (3, 8, 10, 15, 19, 28, 30, 33, 40, 47)
論理和 (1, 3, 8, 10, 11, 12, 15, 19, 23, 28, 30, 33, 39, 40, 44, 47)
登録合成ﾃﾞｰﾀ (1, 3, 8, 10, 11, 12, 15, 19, 23, 28, 30, 33, 39, 40, 44, 47)
（認証作業）
第１認証指紋ﾃﾞｰﾀ (1, 8, 11, 15, 23, 28, 30, 39, 44)
第２認証指紋ﾃﾞｰﾀ (3, 8, 10, 15, 20, 23, 28, 30, 33, 40, 47)
第１一致数＝9 (1, 8, 11, 15, 23, 28, 30, 39, 44)
第１不一致数＝0
第１認証後ﾃﾞｰﾀ (3, 10, 12, 19, 33, 40, 47)
第２一致数＝10 (3, 8, 10, 15, 23, 28, 30, 33, 40, 47)
第２不一致数＝1 (20)
第２認証後ﾃﾞｰﾀ (1, 11, 12, 19, 39, 44)
登録合成ﾃﾞｰﾀ不一致数＝2 (12, 19)

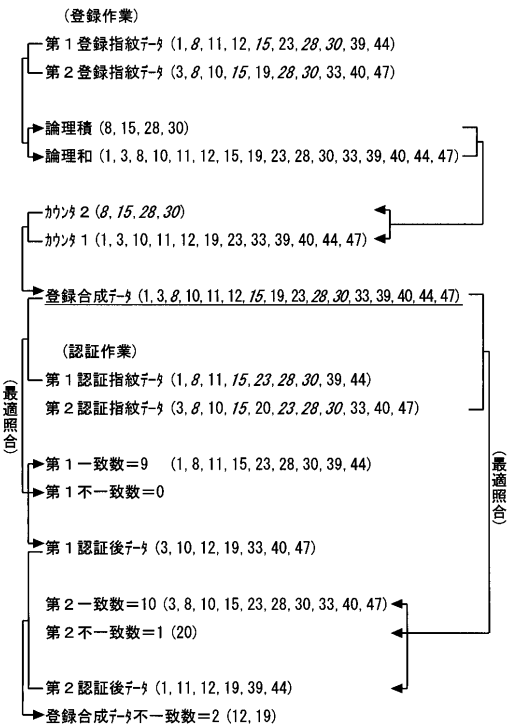
【図１１】


（登録作業）
100
第１指の指紋画像を取得（第１登録指紋画像）
102
第１指の特徴点を取得（第１登録指紋データ）
104
第２指の指紋画像を取得（第２登録指紋画像）
106
第２指の特徴点を取得（第２登録指紋データ）
論理積最大となるように相対位置関係　特定
170
第１指と第２指の登録指紋データの論理和データを取得
108
第１指と第２指の登録指紋データの論理積データを取得
110
論理和かつ論理積の特徴点に対してカウンタ数２を与える
112
論理和であるが論理積でない特徴点に対してカウンタ数１を与える
114
論理和と特徴点のカウンタ数を登録合成データとして登録
116

【図１２】


（認証作業）
120
第１指の指紋画像を取得（第１認証指紋画像）
122
第１指の特徴点を取得（第１認証指紋データ）
180
登録合成データと第１認証指紋データと照合
182
一致数＞閾値？
No
Yes
184
第１一致数、第１不一致数を求め、第１認証後データを生成
186
No
全照合終了？
Yes
188
有効照合有り？
No
Yes
①
①
126
第２指の指紋画像を取得（第２認証指紋画像）
128
第２指の特徴点を取得（第２認証指紋データ）
190
登録合成データと第２認証指紋データと照合
192
一致数＞閾値？
No
Yes
194
第２一致数、第２不一致数を求め、第２認証後データを生成
196
No
全照合終了？
Yes
198
No
有効照合有り？
Yes
200
カウント数の和が最小となる第１認証後データ，第２認証後データ特定
162
第１認証後データ及び第２認証後データより登録合成データ不一致数を求める
164
NG
本人か否かの判断
OK
136
他人と判断する
138
本人と認める

【図１３】


（登録作業）
第１登録指紋ﾃﾞｰﾀ (1, 8, 11, 12, 15, 23, 28, 30, 39, 44)
第２登録指紋ﾃﾞｰﾀ (3, 8, 10, 15, 19, 28, 30, 33, 40, 47)
論理積 (8, 15, 28, 30)
論理和 (1, 3, 8, 10, 11, 12, 15, 19, 23, 28, 30, 33, 39, 40, 44, 47)
ｶｳﾝﾀ２ (8, 15, 28, 30)
ｶｳﾝﾀ１ (1, 3, 10, 11, 12, 19, 23, 33, 39, 40, 44, 47)
登録合成ﾃﾞｰﾀ (1, 3, 8, 10, 11, 12, 15, 19, 23, 28, 30, 33, 39, 40, 44, 47)
（認証作業）
第１認証指紋ﾃﾞｰﾀ (1, 8, 11, 15, 23, 28, 30, 39, 44)
第２認証指紋ﾃﾞｰﾀ (3, 8, 10, 15, 20, 23, 28, 30, 33, 40, 47)
（最適照合）
第１一致数＝9　(1, 8, 11, 15, 23, 28, 30, 39, 44)
第１不一致数＝0
第１認証後ﾃﾞｰﾀ (3, 10, 12, 19, 33, 40, 47)
第２一致数＝10 (3, 8, 10, 15, 23, 28, 30, 33, 40, 47)
第２不一致数＝1 (20)
（最適照合）
第２認証後ﾃﾞｰﾀ (1, 11, 12, 19, 39, 44)
登録合成ﾃﾞｰﾀ不一致数＝2 (12, 19)