

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第6226802号
(P6226802)

(45) 発行日 平成29年11月8日 (2017. 11. 8)

(24) 登録日 平成29年10月20日 (2017. 10. 20)

(51) Int. Cl.

F I

G 0 6 T 7/00 (2017. 01)

G 0 6 T 7/00 5 3 0

G 0 6 F 21/32 (2013. 01)

G 0 6 F 21/32

請求項の数 11 外国語出願 (全 19 頁)

(21) 出願番号 特願2014-78429 (P2014-78429)
 (22) 出願日 平成26年4月7日 (2014. 4. 7)
 (65) 公開番号 特開2014-219967 (P2014-219967A)
 (43) 公開日 平成26年11月20日 (2014. 11. 20)
 審査請求日 平成28年12月16日 (2016. 12. 16)
 (31) 優先権主張番号 13/874, 766
 (32) 優先日 平成25年5月1日 (2013. 5. 1)
 (33) 優先権主張国 米国 (US)

早期審査対象出願

(73) 特許権者 000006013
 三菱電機株式会社
 東京都千代田区丸の内二丁目7番3号
 (74) 代理人 100110423
 弁理士 曾我 道治
 (74) 代理人 100111648
 弁理士 梶並 順
 (74) 代理人 100122437
 弁理士 大宅 一宏
 (74) 代理人 100147566
 弁理士 上田 俊一
 (74) 代理人 100161171
 弁理士 吉田 潤一郎
 (74) 代理人 100161115
 弁理士 飯野 智史

最終頁に続く

(54) 【発明の名称】 ユーザーの指紋から得られるバイオメトリックデータを認証する方法及びシステム、および、バイオメトリック認証システム

(57) 【特許請求の範囲】

【請求項 1】

ユーザーの指紋から得られるバイオメトリックデータを認証する方法であって、
 各領域が前記指紋の複数の細部を含むように前記指紋の一組の領域を決定するステップと、

前記各領域について、第1の一組の記述子を生成するために、該領域における前記指紋の構造を表す記述子を求めるステップと、

一致する記述子の数を求めるために、前記第1の一組の記述子内の該各記述子を、前記ユーザーの前記バイオメトリックデータの登録中に求められた第2の一組の記述子内の該各記述子と比較するステップと、

前記一致する記述子の数を、前記バイオメトリックデータを認証するための閾値と比較するステップと

を含み、

該方法の前記ステップは、プロセッサが実行し、

前記一組の領域を決定するステップは、

前記領域の形状及び寸法を決定するステップと、

前記指紋における前記各細部の周囲に前記領域を配置するステップと、

前記一組の領域内の前記領域の前記細部が、該領域内における少なくともn個の細部の近傍にある場合、該領域を選択するステップであって、ここで、nは1よりも大きな予め設定された数である、ステップと

を含む、
方法。

【請求項 2】

前記組内の領域の数をカウントするステップと、
前記領域の前記形状、前記領域の前記寸法、又は、前記予め設定された数のうちの少なくとも 1 つを変更するステップと、
前記一組の領域を決定するステップを繰り返すステップと
を更に含む、
請求項 1 に記載の方法。

【請求項 3】

前記第 2 の一組の記述子は、準同形暗号システムの公開鍵を用いて暗号化され、
前記各記述子の前記比較が、準同形性を用いて暗号化領域において実行されるように、
前記第 1 の一組の記述子を前記公開鍵を用いて暗号化するステップ
を更に含む、
請求項 1 に記載の方法。

【請求項 4】

前記一致する記述子の数に対応する暗号化結果を生成するステップと、
認証サーバーにおいて前記暗号化結果を解読して、認証判定を決定するステップと
を更に含む、
請求項 3 に記載の方法。

【請求項 5】

前記領域の前記記述子は、前記領域内の細部の相対的な距離、前記領域内の前記細部の相対的な方向、及び、前記領域内の前記細部の相対的な径方向の配置のうちの少なくとも 1 つ又は組み合わせを表す、細部に基づく特徴を含む、
請求項 1 に記載の方法。

【請求項 6】

前記領域の前記記述子は、細部に基づく特徴、テクスチャに基づく特徴、及び、方向に基づく特徴の組み合わせを含む、
請求項 1 に記載の方法。

【請求項 7】

前記各記述子を比較するステップは、
前記第 1 の一組内の記述子について、前記第 2 の一組から最も近い記述子を決定するステップと、
前記記述子と前記最も近い記述子との間の距離を求めるステップと、
前記一致する記述子を求めるために、前記距離を距離閾値と比較するステップと
を含む、
請求項 1 に記載の方法。

【請求項 8】

ユーザーの指紋から得られるバイオメトリックデータを認証するシステムであって、
前記指紋の一組の領域を、該各領域が前記指紋の複数の細部を含むように決定し、
前記各領域について、該領域における前記指紋の構造を表す記述子を求めて、第 1 の一組の記述子を生成し、
前記第 1 の一組の記述子内の該各記述子を、前記ユーザーの前記バイオメトリックデータの登録中に求められる第 2 の一組の記述子内の該各記述子と比較して、一致する記述子の数を求め、
前記一致する記述子の数を、前記バイオメトリックデータを認証するための閾値と比較する、

プロセッサを備え、
前記プロセッサは、
前記領域の形状及び寸法を決定し、

10

20

30

40

50

前記指紋における前記各細部の周囲に前記領域を配置し、
前記一組の領域内の前記領域の前記細部が、該領域内における少なくとも n 個の細部の
近傍にある場合、該領域を選択することで、
前記一組の領域を決定し、ここで、n は 1 よりも大きな予め設定された数である、
システム。

【請求項 9】

バイオメトリック認証システムであって、
ユーザの認証用に提示されたプローブ指紋の第 1 の一組の記述子を求めるアクセス制御デバイスであって、前記第 1 の一組内の前記各記述子は、複数の細部を含む前記プローブ指紋の領域を表す、アクセス制御デバイスと、
前記ユーザの登録用に提示された登録指紋の第 2 の一組の記述子を求めるサーバーであって、前記第 2 の一組内の前記各記述子は、複数の細部を含む前記登録指紋の領域を表す、サーバーと、
前記第 1 の一組の記述子内の該各記述子を前記第 2 の一組の記述子内の該各記述子と比較して、一致する記述子の数を求めるプロセッサと、
前記一致する記述子の数を閾値と比較して認証判定を行う認証サーバーと
を備え、

前記アクセス制御デバイスは、前記プローブ指紋の一組の領域を、該各領域が前記指紋の複数の細部を含むように決定するものであって、

前記アクセス制御デバイスは、
前記領域の形状及び寸法を決定し、
前記指紋における前記各細部の周囲に前記領域を配置し、
前記一組の領域内の前記領域の前記細部が、該領域内における少なくとも n 個の細部の
近傍にある場合、該領域を選択することで、

前記一組の領域を決定し、ここで、n は 1 よりも大きな予め設定された数である、
バイオメトリック認証システム。

【請求項 10】

前記プロセッサは、前記アクセス制御デバイス上又は前記サーバー上で実行されている、請求項 9 に記載の認証システム。

【請求項 11】

前記アクセス制御デバイスは、前記第 1 の一組の記述子を公開鍵を用いて暗号化し、前記サーバーは、前記第 2 の一組の記述子を前記公開鍵を用いて暗号化し、前記プロセッサは、前記記述子を暗号化領域において比較する、請求項 9 に記載の認証システム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、包括的には、バイオメトリックスの分野に関し、より詳細には、バイオメトリックデータを認証することに関する。

【背景技術】

【0002】

バイオメトリックデータ、例えば、発話、指紋、虹彩の見え方を用いた認証は、従来のパスワードに代わるものである。このバイオメトリックデータは、思い出す必要も記憶する必要もなく、複製するのが困難である。

【0003】

指紋は、認証用のバイオメトリックデータの最も一般的な情報源のうちの 1 つである。認証中、登録指紋からの識別的特徴が、プローブ指紋 (probe fingerprint: 認証対象の指紋) からの特徴と比較される。しかしながら、多くの従来の指紋に基づく認証システムは、登録バイオメトリックスから決定された特徴が、アクセス制御デバイスに接続されたバイオメトリックデータベースに暗号化されていない形で記憶されていることを前提としている。

【 0 0 0 4 】

この前提は、登録指紋及びプローブ指紋からの特徴が暗号化されていない場合にセキュリティリスクを呈する可能性がある。暗号化は、データベースを危険にさらす敵対者が登録されたユーザーの指紋特徴を発見することを確実にできなくする。しかしながら、そのようなシステムの場合、アクセス制御デバイスは、暗号化領域でプローブ特徴と登録特徴との比較を行わなければならない。

【 0 0 0 5 】

暗号化されたバイオメトリック特徴を比較する方法のほとんどは、幾つかの共通の特性を有する。特徴抽出プロセスが、所定の長さを有する特徴ベクトルを生成する。これによって、ベクトル間の距離に基づくバイオメトリック特徴の比較が容易になる。ユークリッド距離、ハミング距離、及び絶対距離等の距離メトリックを求めるためのセキュア（安全）でほぼリアルタイムのプロトコルが知られている。

10

【 0 0 0 6 】

正確なバイオメトリック照合を保証するには、特徴抽出の前に、登録指紋とプローブ指紋との間の位置合わせを行わなければならない。通常、登録指紋上の曲率の大きな点のロケーション等の暗号化されていない位置合わせパラメーターが位置合わせに用いられる。これについては、例えば、特許文献 1 を参照されたい。これらの位置合わせパラメーターによって、アクセス制御デバイスは、プローブ特徴の抽出及び暗号化領域におけるプローブ特徴と登録特徴との比較を行う前に、プローブ指紋を登録指紋に位置合わせすることが可能になる。しかしながら、暗号化されていない位置合わせパラメーターを記憶することは、セキュリティリスクを呈する。

20

【 0 0 0 7 】

上記特性は、アクセス制御システムの設計に制約を課す。固定長の特徴表現は、特徴比較の柔軟性を低減する。なぜならば、そのような表現は、例えば、クロッピングされた指紋画像又は少数の細部（minutia, minutiae：特徴点の細部）を生成する指紋からの特徴の照合に対応することができないからである。暗号化されていない位置合わせ情報によって、敵対者は、指紋がコア構造、又はテント構造若しくはデルタ構造を含むか否かを推測し、それによって、システムを攻撃するのに用いることができるベクトルを単純化することが可能になる場合がある。

【 先行技術文献 】

30

【 特許文献 】

【 0 0 0 8 】

【 特許文献 1 】 米国特許出願公開第 2 0 1 1 / 0 1 3 3 5 6 7 号明細書

【 発明の概要 】

【 発明が解決しようとする課題 】

【 0 0 0 9 】

したがって、登録特徴及びプローブ特徴が異なる長さを有することを可能にするとともに、明示的な位置合わせを必要とせず、したがって、暗号化されていない位置合わせパラメーターを記憶する必要がなくなる、暗号化領域におけるバイオメトリック認証に適した指紋特徴抽出及びバイオメトリック認証方法が必要とされている。

40

【 課題を解決するための手段 】

【 0 0 1 0 】

本発明の幾つかの実施の形態は、登録段階中及び認証段階中に抽出された指紋の特徴の位置合わせが、対応する特徴の対比較に必要とされるという認識に基づいている。具体的には、指紋の特定のロケーションから抽出された登録特徴は、指紋の同じロケーションから抽出されたプローブ特徴と比較される。通常、全ての特徴が同時に比較され、位置合わせによって、対応する特徴の正しい識別が保証される。

【 0 0 1 1 】

一方、特徴が個々に比較される場合、すなわち、各登録特徴が各プローブ特徴と比較される場合、位置合わせは暗黙的である、すなわち、位置合わせは、対応する特徴が照合さ

50

れるときに間接的に行われる。一致するものの数を、適した距離閾値に基づいて認証判定を行うのに利用することができる。

【 0 0 1 2 】

通常、指紋から抽出された特徴は細部を表す。幾つかの実施の形態は、これらの細部を表す特徴の比較が準最適である可能性があるという認識に基づいている。この理由は、細部が十分に区別的でない場合があり、そのため、指紋の特定のロケーションにおける細部を表す登録特徴が、異なるロケーションにおける細部を表すプローブ特徴と一致する可能性があるからである。したがって、細部の対比較は、誤った認証の確率を高める可能性がある。

【 0 0 1 3 】

しかしながら、そのような問題は、比較が、細部の局所的な近傍の幾何学的配列を表す特徴間で実行されるときに回避することができる。近傍における各細部の個々の特性、並びにそれらの細部間の相対的な位置及び方向は、抽出された特徴の区別性を高め、したがって、そのような区別的な特徴の個々の比較が指紋における同じロケーションから抽出された対応する特徴のみと一致する確率を高める。

【 0 0 1 4 】

この認識に基づいて、幾つかの実施の形態は、或る特定の検出された細部の周囲の局所的な近傍を決定し、それらの近傍に基づいて特徴を抽出する。特徴の局所性は、特徴が回転及び並進を受けたときに正確さを提供する。特徴ベクトルは、セキュアなプリミティブを用いて比較することができる。スコアを求めて真正なユーザー又は氏名詐称者を識別するプロセスは、暗号化されていない位置合わせパラメーターを記憶する必要なく、最良の位置合わせを暗黙的にもたらす。

【 0 0 1 5 】

したがって、1つの実施形態は、ユーザーの指紋から得られるバイオメトリックデータを認証する方法を開示する。該方法は、前記指紋の一組の領域を、該各領域が前記指紋の複数の細部を含むように決定するステップと、

前記各領域について、該領域における前記指紋の構造を表す記述子を求めて、第1の一組の記述子を生成する、求めるステップと、

前記第1の一組の記述子内の該各記述子を第2の一組の記述子内の該各記述子と比較するステップであって、一致する記述子の数を求め、前記第2の一組の記述子は、前記ユーザーの前記バイオメトリックデータの登録中に求められる、比較するステップと、

前記一致する記述子の数を、前記バイオメトリックデータを認証するための閾値と比較するステップと、

を含み、該方法の前記ステップは、プロセッサによって実行され、

前記一組の領域を決定するステップは、

前記領域の形状及び寸法を決定するステップと、

前記指紋における前記各細部の周囲に前記領域を配置するステップと、

前記一組の領域内の前記領域の前記細部が、該領域内における少なくともn個の細部の近傍にある場合、該領域を選択するステップであって、ここで、nは1よりも大きな予め設定された数である、ステップと

を含む。

【 0 0 1 6 】

別の実施形態は、ユーザーの指紋から得られるバイオメトリックデータを認証するシステムを開示する。該システムは、

前記指紋の一組の領域を、該各領域が前記指紋の複数の細部を含むように決定し、

前記各領域について、該領域における前記指紋の構造を表す記述子を求めて、第1の一組の記述子を生成し、

前記第1の一組の記述子内の該各記述子を第2の一組の記述子内の該各記述子と比較して、一致する記述子の数を求め、なお、前記第2の一組の記述子は、前記ユーザーの前記バイオメトリックデータの登録中に求められ、

10

20

30

40

50

前記一致する記述子の数を、前記バイOMETリックデータを認証するための閾値と比較する、

プロセッサを備え、

前記プロセッサは、

前記領域の形状及び寸法を決定し、

前記指紋における前記各細部の周囲に前記領域を配置し、

前記一組の領域内の前記領域の前記細部が、該領域内における少なくとも n 個の細部の近傍にある場合、該領域を選択することで、

前記一組の領域を決定し、ここで、n は 1 よりも大きな予め設定された数である。

【 0 0 1 7 】

更に別の実施形態は、バイOMETリック認証システムであって、

ユーザーの認証用に提示されたプローブ指紋の第 1 の一組の記述子を求めるアクセス制御デバイスであって、前記第 1 の一組内の前記各記述子は、複数の細部を含む前記プローブ指紋の領域を表す、アクセス制御デバイスと、

前記ユーザーの登録用に提示された登録指紋の第 2 の一組の記述子を求めるサーバーであって、前記第 2 の一組内の前記各記述子は、複数の細部を含む前記登録指紋の領域を表す、サーバーと、

前記第 1 の一組の記述子内の該各記述子を前記第 2 の一組の記述子内の該各記述子と比較して一致する記述子の数を求めるプロセッサと、

前記一致する記述子の数を閾値と比較して認証判定を行う認証サーバーと、
を備え、

前記アクセス制御デバイスは、前記プローブ指紋の一組の領域を、該各領域が前記指紋の複数の細部を含むように決定するものであって、

前記アクセス制御デバイスは、

前記領域の形状及び寸法を決定し、

前記指紋における前記各細部の周囲に前記領域を配置し、

前記一組の領域内の前記領域の前記細部が、該領域内における少なくとも n 個の細部の近傍にある場合、該領域を選択することで、

前記一組の領域を決定し、ここで、n は 1 よりも大きな予め設定された数である、
バイOMETリック認証システムを開示する。

【図面の簡単な説明】

【 0 0 1 8 】

【図 1】本発明の幾つかの実施形態によるユーザーの指紋のバイOMETリックデータを用いたバイOMETリック認証の方法のブロック図である。

【図 2 A】本発明の様々な実施形態による指紋の一組の領域の概略図である。

【図 2 B】本発明の様々な実施形態による指紋の一組の領域の概略図である。

【図 2 C】本発明の幾つかの実施形態による一組の領域を決定する方法のフローチャートである。

【図 3】本発明の種々の実施形態によるバイOMETリクス表現の概略図である。

【図 4 A】バイOMETリックデータの概略図である。

【図 4 B】バイOMETリックデータの概略図である。

【図 5】ガボールフィルタリングを用いて指紋の画像におけるテクスチャに基づく特徴を抽出する概略図である。

【図 6】本発明の 1 つの実施形態による規則的なラディアルサンプリンググリッドにおいて稜線方向をサンプリングすることによって方向に基づく特徴を抽出する概略図である。

【図 7】本発明の幾つかの実施形態によるバイOMETリックデータを暗号化したものを認証する認証方法及びシステムの様々なモジュールのブロック図である。

【発明を実施するための形態】

【 0 0 1 9 】

図 1 は、ユーザーの指紋の画像から得られるバイOMETリックデータ 1 1 0 を用いたバ

10

20

30

40

50

イオメトリック認証のシステム及び方法を示している。バイオメトリックデータ 110 は、例えば、ユーザーが自身の指紋に基づく認証を要求したときの、例えば認証段階中に取得することができる。第 1 の一組の記述子 135 が、バイオメトリックデータ 110 から求められ、認証中に提示された第 2 の一組の記述子 136 と比較される (145)。例えば、第 2 の一組の記述子は、ユーザーがバイオメトリックデータベースに登録される登録段階中に求められる。第 1 の一組の記述子及び第 2 の一組の記述子は、以下で説明する同じ原理を用いて求められる。この方法の幾つかのステップは、プロセッサ 101、例えば、アクセス制御デバイスのプロセッサが実行することができる。加えて又は代替的に、この方法のステップは、バイオメトリックデータベースに関連付けられたプロセッサによって実行することができる。

10

【0020】

指紋のバイオメトリック 110 から、一組の領域 125 が求められる。本発明の幾つかの実施形態は、登録段階及び認証段階中に取得された特徴の個々の比較が間接的な位置合わせを実行するという認識に基づいている。複数の一致する特徴を、認証判定を行うのに用いることができる。

【0021】

比較プロセスを効率的にするために、抽出された特徴を区別する必要がある。したがって、幾つかの実施形態は、各領域が指紋の複数の細部を取り囲むように指紋の一組の領域を決定する (120)。この実施形態は、領域内の各細部の個々の特性、並びに細部間の相対的な位置及び方向が、領域の区別性を高め、したがって、領域から抽出された特徴の区別性を高めるという認識に基づいている。

20

【0022】

加えて、特徴の局所性は、登録指紋に対する相対的なプローブ指紋の回転及び平行移動に正確さ及び不変性を提供する。このとき、暗号化領域において距離又は相関を計算する暗号プリミティブを用いて実行することができる操作を用いて、特徴ベクトルを比較することができる。真正なユーザー又は氏名詐称者のスコアを求めるプロセスは、暗号化されていない位置合わせパラメーターを記憶する必要なく、最良の位置合わせを暗黙的に与える。

【0023】

したがって、幾つかの実施形態は、領域ごとに、その領域内の指紋の構造を表す記述子を求めて (130)、第 1 の一組の記述子 135 を生成し、この第 1 の一組の記述子内の各記述子を、バイオメトリック認証用に提示された第 2 の一組の記述子 136 内の各記述子と比較する (145)。記述子の双方の組は、同じルールに基づいて決定された一組の領域から同じ原理を用いて求められる。唯一の相違は、1 つの組の記述子、例えば組 135 は、アクセス制御デバイスによって認証段階中に取得された指紋から求められ、別の組、例えば組 136 は、登録段階中に取得された指紋から求められるということである。

30

【0024】

比較 145 は、記述子の個々の比較を含む。すなわち、第 1 の一組の記述子内の各記述子が、バイオメトリック認証用に提示された第 2 の一組の記述子内の各記述子と比較されて、一致する記述子の数 150 が求められる。一致するものが見つかった場合、例えば、第 1 の一組のうちの第 1 の要素が第 2 の一組のうちの第 2 の要素と一致する (151) 場合、数 150 が 1 つだけ増加される。次に、一致する記述子の数 150 は、ユーザーを認証する閾値 165 と比較される (160)。

40

【0025】

1 つの実施形態では、記述子の一致するものは、2 つの段階で求められる。認証時に提示されたプローブ指紋における各記述子について、第 1 のステップは、登録指紋における最近傍記述子を見つけることを含む。第 2 のステップは、この最近傍記述子の距離を距離閾値と比較して、この最近傍記述子が確かに十分近いことを保証することを含む。

【0026】

上述したように、記述子の個々の比較の結果、指紋が間接的に位置合わせされ、したが

50

って、通例、暗号化されていない情報を用いて実行される明示的な位置合わせステップの必要がなくなる。したがって、本発明の様々な実施形態によって用いられる原理は、セキュアなバイオメトリック認証に特に有利である。

【 0 0 2 7 】

そのために、本発明の幾つかの実施形態は、第 1 の一組の記述子及び / 又は第 2 の一組の記述子の暗号化のみを求める。例えば、第 1 の一組の記述子は、アクセス制御デバイスによって公開鍵を用いて暗号化され、第 2 の一組の記述子は、登録サーバーによって同じ公開鍵を用いて暗号化され、暗号化されたフォーマットでバイオメトリックデータベースに記憶される。認証中、第 1 の記述子及び第 2 の記述子は、暗号化領域において照合される (1 4 5)。

10

【 0 0 2 8 】

例えば、幾つかの実施形態は、第 1 の一組の記述子及び第 2 の一組の記述子のユークリッド距離、ハミング距離、及び絶対距離等の距離メトリックを求めるのに準同形暗号システムの性質を用いる。それらの実施形態では、各記述子の比較が暗号化領域において準同形の性質を用いて実行されるように、第 1 の一組の記述子及び第 2 の一組の記述子は、準同形暗号システムの公開鍵を用いて暗号化される。

【 0 0 2 9 】

領域の決定

図 2 A は、指紋 2 1 0 を一組の領域 1 2 5 に分割する一例を示している。例えば、1つの実施形態では、領域は長方形の形状を有する。各長方形は、例えば、長方形の左上角を示す原点 2 2 0 において生成され、幅及び高さを用いて指定される。通常、領域の形状及び寸法は、事前に決定されるが、異なるユーザーの指紋について変化し得る。

20

【 0 0 3 0 】

図 2 B は、キーポイントの細部を用いて決定された別の領域 2 4 5 の概略図を示している。このキーポイントは、所定の形状及び寸法の領域内、例えば半径 R 2 3 5 の球 2 3 0 内にその近傍細部として少なくとも n 個の細部を有する細部 2 4 0 として規定される。ここで、n は、1 よりも大きな所定の数である。図 2 B の例では、この所定の数 n は 3 に等しく、領域 2 4 5 は、細部 2 4 1、2 4 2、及び 2 4 3 を含む。

【 0 0 3 1 】

U_k を、指紋の第 k 画像における細部の数とする。通常、 U_k は、指が異なるごとに变化する。さらに、 U_k は、同じ指についてもノイズに起因して变化する。第 k 指紋画像における第 i 細部は、当該細部の点の X 座標、Y 座標、及び座標を用いた $m^k_i = \{x^k_i, y^k_i\}$ として表される。

30

【 0 0 3 2 】

m^k_i の一組の近傍細部は、以下のとおりである。

【 0 0 3 3 】

【数 1】

$$\mathcal{D}(m^k_i) = \{m^k_j : d(m^k_i, m^k_j) < R, j = 1, \dots, U_k, j \neq i\}$$

$$\text{where } d(m^k_i, m^k_j) = \sqrt{(x^k_i - x^k_j)^2 + (y^k_i - y^k_j)^2}$$

40

【 0 0 3 4 】

ここで、R は所定の半径である。この場合、 m^k_i の n 個の最近傍細部の組は、 m^k_i までのユークリッド距離において最も接近した n 個の要素を含む $\mathcal{D}(m^k_i)$ のサブセットである。 m^k_i の n 個の最近傍細部の組は、

【数 2】

$$\mathcal{N}(m^k_i) = \{\bar{m}^k_1, \dots, \bar{m}^k_n\}$$

によって示される。ここで、

50

【数 3】

$$\bar{m}_i^k = \{\bar{x}_i^k, \bar{y}_i^k, \bar{\theta}_i^k\}, i = 1, 2, \dots, n$$

は、 m_i^k の 1 番目の最近傍細部である。n 個の最近傍細部の組を有するいずれの細部も、キーポイントと呼ばれる。

【0035】

図 2 C は、本発明の幾つかの実施形態による一組の領域を決定する方法のフローチャートを示している。領域の形状及び寸法が決定され (250)、その形状及び寸法の領域が、指紋における各細部の周囲に配置される (255)。或る領域の細部が、その領域内における少なくとも n 個の細部の近傍にある場合、その領域が一組の領域において選択される (260)。ここで、n は、1 よりも大きな所定の数である。

10

【0036】

加えて、1 つの実施形態は、一組の領域が、効率的な比較に十分な領域を含まない場合、その組を更新する。例えば、幾つかのユーザーの指紋は、細部のまばらな配置を含む場合があり、それらのユーザーについては、半径 R 235 は増加される。したがって、この実施形態は、組内の領域の数をカウントし (265)、領域の数を閾値と比較する (270)。領域の数が閾値よりも大きい場合 (271)、その組が決定される (275)。そうでない場合 (272)、この実施形態は、領域の形状 (例えば、円の半径を拡大する)、領域の寸法、又は n 個の細部の所定の数のうちの少なくとも 1 つを変更し、一組の領域を決定するためのステップを繰り返す。

20

【0037】

バイオメトリックデータ

図 3 は、種々の実施形態によって用いられるユーザーの指紋のバイオメトリックデータの例を示している。例えば、指紋 210 の画像は、細部マップ 320 及び / 又は稜線マップ 330、330' 又は稜線波長 (ridge wavelength) マップ 340 によって表すことができる (310)。稜線マップは、細い稜線マップ 330 又は太い稜線マップ 330' とすることができる。細部マップ 320 並びに稜線マップ画像 330 及び 330' は、当該技術分野において知られている方法によって求めることができる。

【0038】

指紋細部マップは、指紋の画像を表すのに用いられるデータ構造である。この細部マップは、例えば、2 次元空間又は 3 次元空間に細部を含む。これらの細部は、指紋の画像 305 から抽出される。ロケーション及び方向は、細部に関連付けられ、指紋における稜線に関係付けられる。具体的には、各細部は、指紋稜線が終了するか又は二又に分岐する箇所生成される。

30

【0039】

図 4 A は、各細部 430 が 2 つの座標 X 及び Y に関連付けられている 1 つの実施形態の一例を示している。ここで、X 及び Y は、画像における細部の空間座標である。この実施形態では、領域 125 は、2 次元であり、例えば、正方形、長方形、円、又は楕円である。

【0040】

図 4 B は、細部の方向等の指紋についての追加のデータを含む別の実施形態の一例を示している。各細部 430 は、3 つの座標 X、Y、及び θ に関連付けられている。ここで、X 及び Y は、画像 305 における細部の空間座標であり、 θ は、細部が得られる指紋稜線に対する正接の角度 350 である。角度 θ は、0 度 ~ 360 度の範囲にある。この実施形態では、領域 125 は 3 次元であり、例えば、立方体、楕円体、又は球体である。

40

【0041】

指紋稜線マップは、指紋の稜線の画像 330 である。この稜線マップは、細部に含まれる情報から十分に独立した指紋情報を識別する。時に、指紋画像に非常に多くのノイズがある場合、細部抽出が困難であるか又は信頼できないものとなるが、この場合、指紋稜線は、より信頼できる特徴を生成することができる。幾つかの実施形態では、稜線波長画像

50

340が指紋稜線マップから抽出される。

【0042】

記述子

本発明の様々な実施形態は、領域内の指紋の局所的な構造を表す領域の特徴に基づいて記述子を求める。幾つかの実施形態では、これらの特徴は、接近した細部の点の相対的なロケーション、局所的なテクスチャ、及び局所的な稜線方向のうちの1つ又は組み合わせに基づいて領域から抽出される。

【0043】

細部に基づく特徴

本発明の幾つかの実施形態では、領域の記述子は、領域内の細部の相対的な距離、領域内の細部の相対的な方向、及び領域内の細部の相対的な径方向の配置（放射状配置）のうちの少なくとも1つ又は組み合わせを表す細部に基づく特徴を含む。

10

【0044】

例えば、一組の領域を決定するのにキーポイントを用いる1つの実施形態は、各キーポイント m^k_i について、 m^k_i に関する $N(m^k_i)$ の局所幾何構造を一意に表すことができる特徴を抽出する。このために、幾つかの実施形態は、 m^k_i の周囲の細部に基づく特徴ベクトルを以下のように示す。

【0045】

【数4】

$$m^k_i = [d_{i1}^k, \dots, d_{in}^k, \theta_{i1}^k, \dots, \theta_{in}^k, \phi_{i1}^k, \dots, \phi_{in}^k]$$

20

【0046】

ここで、各特徴要素は、以下の式によって与えられる。

【0047】

【数5】

$$d_{ij}^k = (1/R) d(m_i^k, \bar{m}_j^k),$$

$$\theta_{ij}^k = \begin{cases} \frac{\bar{\theta}_j^k - \theta_i^k}{2\pi} & \text{if } \bar{\theta}_j^k \geq \theta_i^k \\ \frac{2\pi - (\theta_i^k - \bar{\theta}_j^k)}{2\pi} & \text{if } \bar{\theta}_j^k < \theta_i^k \end{cases},$$

30

$$\psi_{ij}^k = \begin{cases} \frac{\bar{\psi}_j^k - \theta_i^k}{2\pi} & \text{if } \bar{\psi}_j^k \geq \theta_i^k \\ \frac{2\pi - (\theta_i^k - \bar{\psi}_j^k)}{2\pi} & \text{if } \bar{\psi}_j^k < \theta_i^k \end{cases}$$

【0048】

式中、

【数6】

$$\bar{\psi}_j^k$$

40

は、

【数 7】

$$\beta = \tan^{-1} \left(\frac{\|\bar{y}_j^k - y_i^k\|}{\|\bar{x}_j^k - x_i^k\|} \right), \text{ and}$$

$$\bar{\psi}_j^k = \begin{cases} \beta & \text{if } \bar{y}_j^k > y_i^k, \bar{x}_j^k > x_i^k \\ \pi - \beta & \text{if } \bar{y}_j^k > y_i^k, \bar{x}_j^k < x_i^k \\ \pi + \beta & \text{if } \bar{y}_j^k < y_i^k, \bar{x}_j^k < x_i^k \\ 2\pi - \beta & \text{if } \bar{y}_j^k < y_i^k, \bar{x}_j^k > x_i^k \end{cases}$$

10

による m^k_i の周囲の最近傍細部の放射状配置の程度を示す。

【0049】

特徴ベクトルを上記のように定式化することによって、各特徴値が範囲 $[0, 1]$ であること、及びキーポイント特徴が当該キーポイントに関する回転及び平行移動に対して不変であることが確保される。キーポイント m^k_i の周囲の細部に基づく特徴の図的表現が、 $n = 3$ の場合についての図 2 B に与えられている。細部に基づく特徴は、キーポイントの周囲の相対的な細部距離、相対的な細部方向、及び相対的な放射状細部配置を表し、したがって、キーポイント m^k_i の近傍における局所構造を表す。幾つかの指紋画像では、キーポイントの数、すなわち、少なくとも n 個の最近傍細部を有する細部の数は、少ない場合があり、これによって、照合性能が低下する。

20

【0050】

そのような指紋の影響を緩和するために、幾つかの実施形態は、領域の形状又は寸法を変化させる。加えて又は代替的に、幾つかの実施形態は、後述するように、他の特徴、例えば、テクスチャ及び方向に基づく特徴を記述子に含める。

【0051】

テクスチャに基づく特徴

キーポイント m^k_i のロケーションの周囲のテクスチャ情報を抽出するために、 m^k_i の周囲の領域 R_1 は、 m^k_i に関する主要な角度

【数 8】

$$\frac{\pi \cdot p}{P}, p = \{0, 1, \dots, P-1\}$$

30

を有する方向性 (directional) ガボールフィルタによって処理される。各フィルタの出力から、実施形態は、出力画像パッチの標準偏差を特徴として求める。求められたテクスチャに基づく特徴は、以下のように表すことができる。

【0052】

【数 9】

$$t_i^k = \frac{1}{t_{\max}} [t_0, t_1, \dots, t_{P-1}]$$

【0053】

式中、 t_p , $p = \{0, 1, \dots, P-1\}$ は、

40

【数 10】

$$\frac{\pi \cdot p}{P}$$

の角度において方向性ガボールフィルタの出力として得られる画像パッチの標準偏差を示す。

【0054】

正規化定数 t_{\max} は、トレーニングセットにおける全てのキーポイントの周囲の全ての画像パッチについて求められた標準偏差の最大値であり、各特徴ベクトルを範囲 $[0, 1]$ に制限するのに用いられる。

50

【 0 0 5 5 】

図 5 は、ガボールフィルタリング 5 2 0 を用いた $P = 4$ の場合の指紋 5 1 0 の画像のテクスチャに基づく特徴 5 3 0 の抽出の一例を示している。フィルタリングされた画像は、方向性ガボールフィルターの対応する角度の範囲における主要な稜線方向を示している。領域 5 4 2、5 4 4、5 4 6、及び 5 4 8 は、標準偏差が求められる領域 R_1 の正方形パッチを表している。

【 0 0 5 6 】

方向に基づく特徴

図 6 は、キーポイントの周囲の規則的なラディアルサンプリンググリッドにおける稜線方向の抽出を示している。細部 m^{k_i} 6 1 0 の周囲のサンプリンググリッドは、半径 r_1 10
 $, 1 \dots L$ の L 個の同心円を備え、各円は、円周に沿って均等に分布した K_1 個のサンプリング点 $p_{1, m}$ を有する。

【 0 0 5 7 】

これらの特徴を、キーポイントの回りの回転に対して不変にするために、1つの実施形態では、サンプリング点における方向

【 数 1 1 】

$$\frac{2\pi r_l m}{K_l}, (0 \leq m \leq K_l - 1)$$

が、細部 m^{k_i} の方向 k_i に対して相対的に取られる。換言すれば、 $p_{1, m}$ において推定された局所的な稜線方向が $k_{1, m}$ によって示される。方向に基づく記述子は、以下 20
 のとおりである。

【 0 0 5 8 】

【 数 1 2 】

$$o_i^k = \left\{ \left\{ \frac{\min(|2\pi - (\theta_{l,m}^k - \theta_i^k)|, |\theta_{l,m}^k - \theta_i^k|)}{\pi} \right\}_{m=1}^{K_l} \right\}_{l=1}^L$$

【 0 0 5 9 】

で割ることによって、各特徴要素は範囲 $[0, 1]$ に入ることが確保される。

【 0 0 6 0 】

加えて、幾つかの実施形態は、各キーポイントの周囲の細部に基づく記述子、テクスチャに基づく記述子、及び方向に基づく記述子を導出した後、領域ごとにそれらの記述子を 30
 組み合わせて、その領域の記述子を求める。

【 0 0 6 1 】

各キーポイントの周囲の細部に基づく記述子、テクスチャに基づく記述子、及び方向に基づく記述子を導出した後、第 k の指紋画像の記述子が、以下のように、各キーポイントの記述子を連結することによって得られる。

【 0 0 6 2 】

【 数 1 3 】

$$M^k = \begin{bmatrix} m_1^k \\ \vdots \\ m_v^k \end{bmatrix} \quad T^k = \begin{bmatrix} t^k \\ \vdots \\ t_v^k \end{bmatrix} \quad O^k = \begin{bmatrix} o_1^k \\ \vdots \\ o_v^k \end{bmatrix}$$

【 0 0 6 3 】

ここで、 M^k は、指紋 k の細部に基づく特徴を含む記述子であり、 T^k は、指紋 k のテクスチャに基づく特徴を含む記述子であり、 O^k は、指紋 k の方向に基づく特徴を含む記述子である。

【 0 0 6 4 】

指紋比較

本発明の様々な実施形態は、記述子を比較するための種々の技法を用いる。例えば、本発明の 1 つの実施形態は、以下で説明するように、類似度行列を求めることによって記述 50

10

20

30

40

50

子を比較する。

【 0 0 6 5 】

M^k 及び M' は、それぞれ第 k 登録指紋の第 1 の一組の記述子及びプローブ指紋の第 2 の一組の記述子である。 M^k には U_k 個の細部キーポイントがあり、 M' には U' 個の細部キーポイントがある。比較方法は、第 1 の一組の記述子と第 2 の一組の記述子との間の 1 対 1 対応を推定する。

【 0 0 6 6 】

この実施形態は、要素が

【数 1 4】

$$S(i, j) = \| \mathbf{m}_i^k - \mathbf{m}_j' \|_1$$

10

である類似度行列 $U_k \times U'$ を用いて、記述子

【数 1 5】

$$M^k = \{\mathbf{m}_i^k\}_{i=1}^{U_k}$$

と、

【数 1 6】

$$M' = \{\mathbf{m}_j'\}_{j=1}^{U'}$$

との間の類似度の尺度を定義する。

20

【 0 0 6 7 】

行列 S における小さな値を有する要素のインデックス (i, j) は、記述子間で一致する可能性のあるものを示す。第 1 の組 M^k 内の記述子 i 及び第 2 の組 M' 内の記述子 j は、これらの対応する記述子が、 M^k 及び M' 内の他の任意の対からの記述子よりも互いに類似している場合に一致する。この関係は、第 1 の組 M^k 内の記述子 i 及び第 2 の組 M' 内の記述子 j が、これらの記述子 i と j との間の距離が i とプローブ指紋における他の任意の記述子 j' との間の距離よりも小さい場合に一致することを示している。

【 0 0 6 8 】

類似度は、以下のように定式化することができる。

【 0 0 6 9 】

30

【数 1 7】

$$P_m(i, j) = \frac{S(i, j)}{\sum_{j'=1}^{U'} S(i, j') + \sum_{i'=1}^{U_k} S(i', j) - 2S(i, j)}$$

【 0 0 7 0 】

行列 P_m が求められた後、最小の P_m の座標は、記述子間の一致を示す。対応する列及び行は除去され、プロセスは、全ての一致する記述子が識別されるまで繰り返される。最後に、その対応値が或る特定の閾値 θ_m よりも小さい一致する記述子の数は、以下のようなスコアを求めるのに用いられる。

【 0 0 7 1 】

40

【数 1 8】

$$S_m = \frac{M_{\text{matched}}}{\min(U_k, U')}$$

【 0 0 7 2 】

式中、 M_{matched} は、 $P_m(i, j) \leq \theta_m$ である一致する記述子 (i, j) の数である。

【 0 0 7 3 】

同様のスコア計算は、テクスチャに基づく記述子及び方向に基づく記述子等の異なるタイプの記述子についても実行され、スコア S_t 及び S_o がそれぞれ得られる。閾値 θ_m 並びに対応するテクスチャに基づく記述子の閾値 θ_t 及び方向に基づく記述子の閾値 θ_o の

50

値は、経験的に導出することができる。スコアは、受信機動作特性（ROC）曲線を、個々に又は2つ若しくは3つの特徴タイプの組み合わせで求めるのに用いることができる。

【0074】

特に、3つの全てのスコアが用いられるとき、融合したスコアは、以下の線形結合である。

【0075】

【数19】

$$S = w_m S_m + w_t S_t + w_o S_o$$

【0076】

式中、重み w_m 、 w_t 、 w_o は、 $w_m + w_t + w_o = 1$ を満たす。 w_m 、 w_t 、 w_o の値は、全数探索を実行して、データセットのトレーニングサブセットに関する等誤り率（EER（equal error rate））を最小にする値を求めることによって得ることができる。

【0077】

セキュアな認証システム

図7は、本発明の幾つかの実施形態によるバイOMETリックデータ705を暗号化したものを認証する認証方法及びシステムの様々なモジュールのブロック図を示している。本発明の様々な実施形態は、図7のシステムの1つ又は幾つかのモジュールを用いる。

【0078】

これらのモジュールは、認証しようとするユーザーのバイOMETリックデータ705を取得するとともに公開鍵740を用いて暗号化するアクセス制御デバイス710を含むことができる。このアクセス制御デバイスは、暗号化されたバイOMETリックデータ715をデータベースサーバー720に送信する。バイOMETリックデータ715は、第1の組の記述子135を暗号化されたフォーマットで含む。データベースサーバー720は、公開鍵740を用いて暗号化されたユーザー固有の登録バイOMETリックデータを記憶する。この登録バイOMETリックデータは、第2の組の記述子136を暗号化されたフォーマットで含むことができる。

【0079】

サーバー720は、暗号化領域において第1の組の記述子と第2の組の記述子との間の距離を求めて、一致する記述子の数725を求める。この数725は、認証判定735を行うために認証サーバー730に送信される。幾つかの実施形態では、一致する記述子の数は、認証サーバー730とデータベースサーバー720との間のインタラクティブプロトコルを介して求められる。幾つかの実施形態では、認証サーバーは、スタンドアロンサーバー（standalone server）とすることができる。他の実施形態では、認証サーバーは、アクセス制御デバイス710又はデータベースサーバー720の一部として実施することができる。認証サーバーは、数725を解読する必要がある場合、秘密鍵745を用いることができる。

【0080】

本発明の上述した実施形態は、多数の方法のうちの任意のもので実施することができる。例えば、実施形態は、ハードウェア、ソフトウェア、又はそれらの組み合わせを用いて実施することができる。ソフトウェアで実施されるとき、ソフトウェアコードは、単一のコンピューターに設けられるか又は複数のコンピューター間に分散されるかを問わず、任意の適したプロセッサ又はプロセッサの集合体上で実行することができる。そのようなプロセッサは、1つ又は複数のプロセッサを集積回路構成要素に有する集積回路として実施することができる。ただし、プロセッサは、任意の適したフォーマットの回路部を用いて実施することができる。

【0081】

さらに、コンピューターは、ラックマウント型コンピューター、デスクトップコンピューター、ラップトップコンピューター、ミニコンピューター、又はタブレットコンピューター等の複数の形態のうちの任意のもので具現化することができることが認識されるべきである。また、コンピューターは、1つ又は複数の入力デバイス及び出力デバイスを有す

10

20

30

40

50

ることができる。これらのデバイスは、特に、ユーザーインターフェースを提示するのに用いることができる。ユーザーインターフェースを提供するのに用いることができる出力デバイスの例には、出力の視覚的提示のためのプリンター又はディスプレイスクリーンと、出力の可聴提示のためのスピーカー又は他の音発生デバイスとが含まれる。ユーザーインターフェースに用いることができる入力デバイスの例には、キーボードと、マウス、タッチパッド、及び離散化タブレット等のポインティングデバイスとが含まれる。別の例として、コンピューターは、音声認識を通じて又は他の可聴フォーマットで入力情報を受信することができる。

【0082】

そのようなコンピューターは、エンタープライズネットワーク又はインターネット等のローカルエリアネットワーク又はワイドエリアネットワークを含む任意の適した形態の1つ又は複数のネットワークによって相互接続することができる。そのようなネットワークは、任意の適した技術に基づくことができ、任意の適したプロトコルに従って動作することができ、無線ネットワーク、有線ネットワーク、又は光ファイバーネットワークを含むことができる。

【0083】

また、本明細書において略述した様々な方法又はプロセスは、様々なオペレーティングシステム又はプラットフォームのうちの任意の1つを用いる1つ又は複数のプロセッサ上で実行可能なソフトウェアとしてコード化することができる。加えて、そのようなソフトウェアは、複数の適したプログラム言語及び/又はプログラムツール若しくはスクリプトツールのうちの任意のものをを用いて記述することができ、フレームワーク又は仮想機械上で実行される実行可能機械言語コード又は中間コードとしてコンパイルすることもできる。

【0084】

この点で、本発明は、コンピューター可読記憶媒体又は複数のコンピューター可読媒体、例えば、コンピューターメモリ、コンパクトディスク(CD)、光ディスク、デジタルビデオディスク(DVD)、磁気テープ、及びフラッシュメモリとして具現化することができる。代替的に又は加えて、本発明は、伝播信号等の、コンピューター可読記憶媒体以外のコンピューター可読媒体として具現化することもできる。

【0085】

「プログラム」又は「ソフトウェア」という用語は、本明細書では、コンピューター又は他のプロセッサを、上記で論述したような本発明の様々な態様を実施するようにプログラムするのに用いることができる任意のタイプのコンピューターコード又は一組のコンピューター実行可能命令を指す一般的な意味で用いられる。

【0086】

コンピューター実行可能命令は、1つ又は複数のコンピューター又は他のデバイスによって実行されるプログラムモジュール等の多くの形態とすることができる。一般に、プログラムモジュールは、特定のタスクを実行するか又は特定の抽象データタイプを実施するルーチン、プログラム、オブジェクト、コンポーネント、データ構造を含む。通常、プログラムモジュールの機能は、様々な実施形態において所望に応じて結合することもできし、分散させることもできる。

【0087】

また、本発明の実施形態は、一例を提供した方法として具現化することもできる。この方法の一部として実行される動作は、任意の適した方法で順序付けることができる。したがって、動作が例示したものとは異なる順序で実行される実施形態を構築することができる。この異なる順序で実行することは、例示の実施形態では逐次動作として示されていても、幾つかの動作を同時に実行することを含むことができる。

【0088】

請求項の要素を修飾する、特許請求の範囲における「第1」、「第2」等の序数の使用は、それ自体で、1つの請求項の要素の別の請求項の要素に対する優先順位も、優位性も

10

20

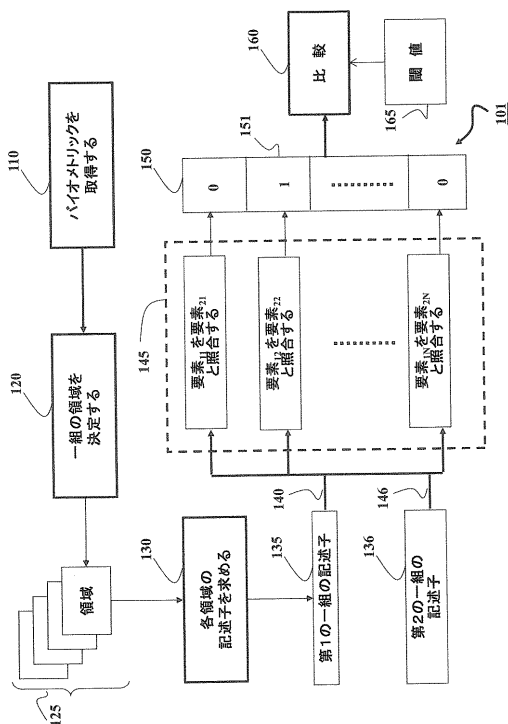
30

40

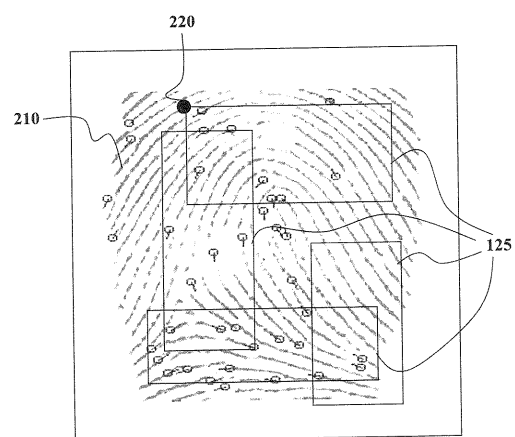
50

、順序も暗示するものでもなければ、方法の動作が実行される時間的な順序も暗示するものでもなく、請求項の要素を区別するために、単に、或る特定の名称を有する1つの請求項の要素を、同じ（序数の用語の使用を除く）名称を有する別の要素と区別するラベルとして用いられているにすぎない。

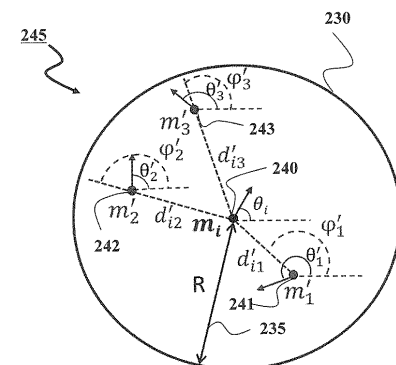
【図1】



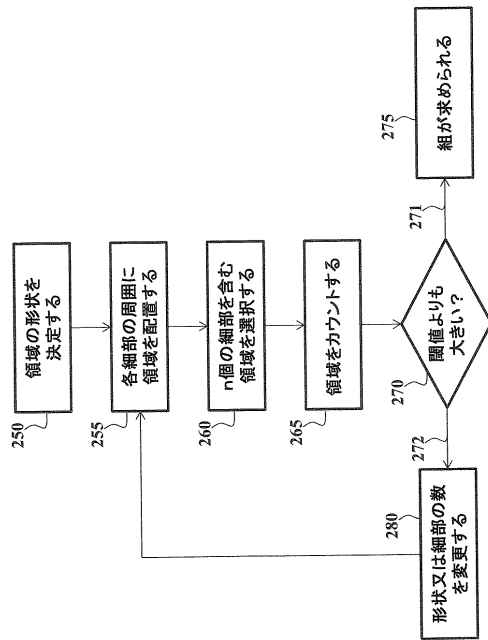
【図2A】



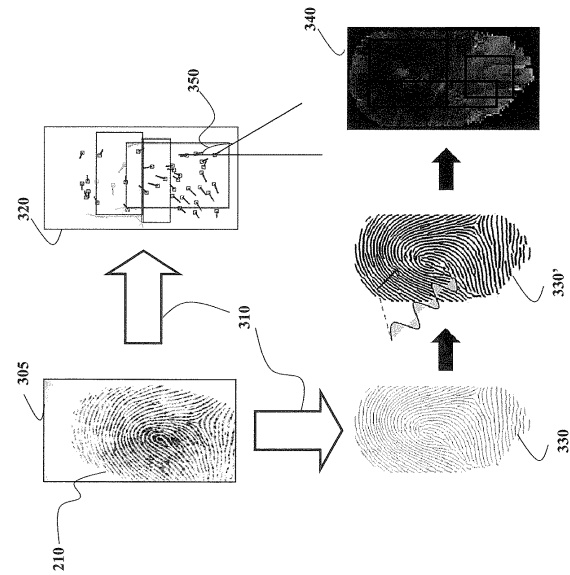
【図2B】



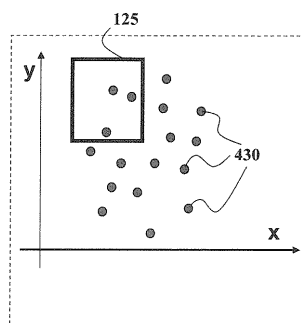
【図 2 C】



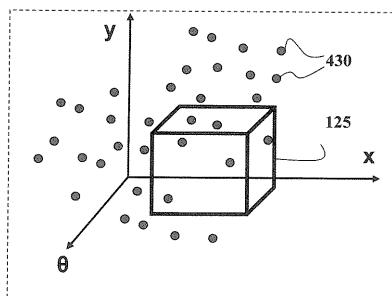
【図 3】



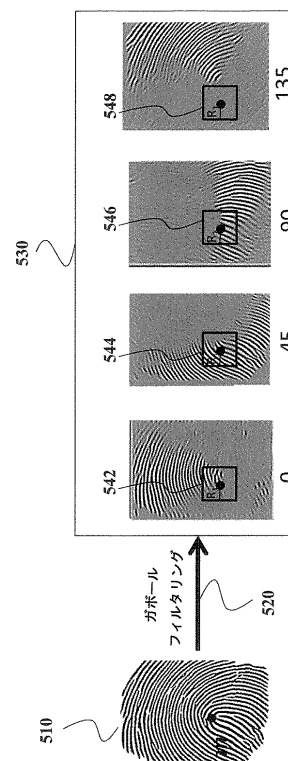
【図 4 A】



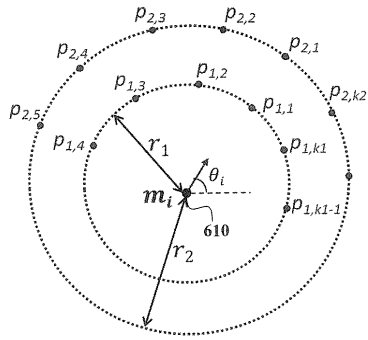
【図 4 B】



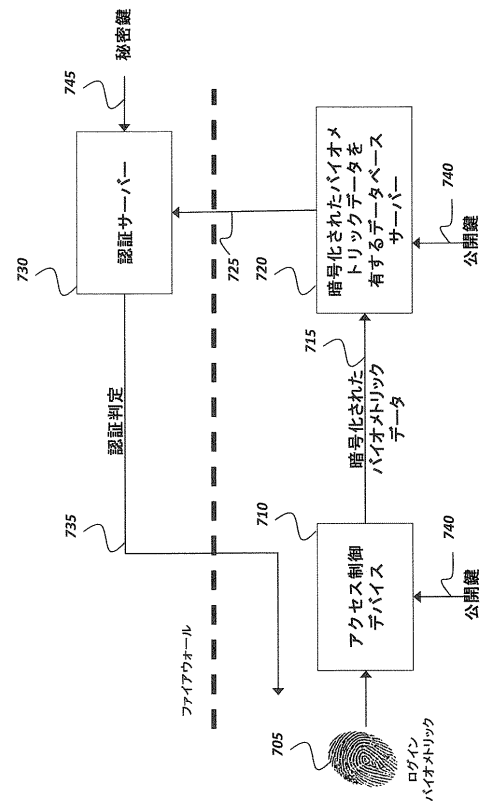
【図 5】



【図 6】



【図 7】



フロントページの続き

(72)発明者 シャンタヌ・ラーネ

アメリカ合衆国、マサチューセッツ州、ケンブリッジ、ブロードウェイ 201、ミツビシ・エレクトリック・リサーチ・ラボラトリーズ・インコーポレイテッド

(72)発明者 ラヴィ・ガーク

アメリカ合衆国、マサチューセッツ州、ケンブリッジ、ブロードウェイ 201、ミツビシ・エレクトリック・リサーチ・ラボラトリーズ・インコーポレイテッド

審査官 新井 則和

(56)参考文献 特表2011-521355(JP,A)

特開昭55-138174(JP,A)

特開2011-253378(JP,A)

特表2008-521025(JP,A)

国際公開第2009/096475(WO,A1)

特開昭61-090641(JP,A)

特開平02-196380(JP,A)

特開平02-048776(JP,A)

米国特許出願公開第2004/0252868(US,A1)

(58)調査した分野(Int.Cl., DB名)

G06T 7/00

G06F 21/32