(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4961214号
(P4961214)
(45)発行日　平成24年6月27日(2012.6.27)　(24)登録日　平成24年3月30日(2012.3.30)

(51)Int.Cl.　F I
G06T 7/00 (2006.01)　G06T 7/00 510B

請求項の数 28 (全 21 頁)

(21)出願番号　特願2007-671(P2007-671)
(22)出願日　平成19年1月5日(2007.1.5)
(65)公開番号　特開2007-293807(P2007-293807A)
(43)公開日　平成19年11月8日(2007.11.8)
審査請求日　平成21年8月27日(2009.8.27)
(31)優先権主張番号　特願2006-91807(P2006-91807)
(32)優先日　平成18年3月29日(2006.3.29)
(33)優先権主張国　日本国(JP)

(73)特許権者　000153443
株式会社日立情報制御ソリューションズ
茨城県日立市大みか町５丁目２番１号
(74)代理人　110000350
ポレール特許業務法人
(72)発明者　高橋　健太
神奈川県川崎市麻生区王禅寺１０９９番地
株式会社日立製作所システム開発研究所内
(72)発明者　比良田　真史
神奈川県川崎市麻生区王禅寺１０９９番地
株式会社日立製作所システム開発研究所内

最終頁に続く

(54)【発明の名称】生体認証方法およびシステム

(57)【特許請求の範囲】
【請求項１】
個人の生体情報の登録画像と照合画像との相互相関に基づいて個人を認証する生体認証方法において、
該画像を撹乱するためのフィルタ、および該フィルタの逆フィルタを作成し、該生体情報から作成された該登録画像に該フィルタを作用させて登録テンプレートを作成して記憶装置に登録しておき、
認証時に、個人から取得した生体情報から作成された照合画像に該逆フィルタを作用させ、該逆フィルタの作用後の照合画像と該登録テンプレートとの相互相関に基づいて個人を判定することを特徴とする生体認証方法。
【請求項２】
生体情報の登録時には、該登録画像をフーリエ変換して、前記撹乱するためのフィルタを周波数空間上で作用させ、認証時には、該照合画像をフーリエ変換し、該逆フィルタを周波数空間上で作用させることを特徴とする請求項１の生体認証方法。
【請求項３】
登録時には、該登録画像を数論変換し、前記撹乱するためのフィルタを数論変換後空間上で作用させ、認証時には、該照合画像を数論変換し、該逆フィルタを数論変換後空間上で作用させることを特徴とする請求項１の生体認証方法。
【請求項４】
前記撹乱するためのフィルタおよび該逆フィルタは、該フィルタを作用させて作成する登

録テンプレート、および該逆フィルタを作用させて作成する照合画像がランダムな値を有するように設定することを特徴とする請求項１の生体認証方法。
【請求項５】
該登録画像および該照合画像の輝度値は、０、１、２の３種類の値を有する３値画像であり、
登録時には、該登録画像で輝度値が２となる画素の輝度値を０に変更し、輝度値が０、１の２種類の値を有する２値画像を登録２値画像として作成し、該登録画像と前記登録２値画像それぞれに該撹乱するためのフィルタを作用させ登録テンプレートとし、
認証時には、該照合画像で輝度値が２となる画素の輝度値を０に変更し、輝度値が０、１の２種類の値を有する２値画像を照合２値画像として作成し、該照合画像と該照合２値画像それぞれに該逆フィルタを作用させ、
該登録テンプレートの登録画像と照合画像の相互相関、および登録２値画像と照合２値画像の相互相関を用いて距離値を算出して本人か否かを判定することを特徴とする請求項１の生体認証方法。
【請求項６】
生成された前記逆フィルタは、ユーザが所持する記録媒体又は該端末装置内の記憶部に記憶することを特徴とする請求項１乃至５のいずれかの生体認証方法。
【請求項７】
適用する対象に応じて該フィルタおよび該逆フィルタの係数を変更して使用することを特徴とする請求項１乃至６のいずれかの生体認証方法。
【請求項８】
ネットワークを介して接続される端末装置とサーバとを用いて、個人の生体認証を行う生体認証システムにおいて、
該端末装置は：
採取された個人の生体情報から登録又は照合のための画像を作成する画像作成部と、該画像を撹乱するためのフィルタおよび逆フィルタを作成するフィルタ生成部と、該画像作成部により作成された該画像に、該フィルタ生成部で生成されたフィルタを作用させて登録テンプレートを作成し、又は該画像に該逆フィルタを作用させて照合画像を作成する変換部と、少なくとも該登録テンプレート又は該照合画像を含む情報を該サーバに送信する第１通信部と、を有し、
該サーバは：
該端末装置から送信される情報を受信する第２通信部と、第２通信部を介して受信された該登録テンプレートを記憶装置に記憶する登録部と、認証時に該第２通信部を介して得られた該照合画像と該記憶装置に記憶された該登録テンプレートとを照合して両者の相互相関を判断する照合部と、を有し、該照合部の判断結果に応じて個人を認証することを特徴とする生体認証システム。
【請求項９】
登録テンプレートを更新する時に、該端末装置は、新たにフィルタおよび逆フィルタを作成して保存し、既存のフィルタと新たなフィルタの差分を求め、フィルタの差分を該サーバへ送信し、該サーバは、受信したフィルタの差分を既に登録済みの該登録テンプレートに作用させて、新たなテンプレートを作成して該記憶装置に登録することを特徴とする請求項８の生体認証システム。
【請求項１０】
生体情報の登録時には、登録画像をフーリエ変換して、前記撹乱するためのフィルタを周波数空間上で作用させ、認証時には、照合画像をフーリエ変換し、該逆フィルタを周波数空間上で作用させることを特徴とする請求項８又は９の生体認証システム。
【請求項１１】
前記撹乱するためのフィルタおよび該逆フィルタは、該フィルタを作用させて作成する登録テンプレート、および該逆フィルタを作用させて作成する照合画像がランダムな値を有するように設定することを特徴とする請求項８乃至１０のいずれかの生体認証システム。

【請求項１２】
適用するシステムに応じて該フィルタおよび該逆フィルタの係数を変更して使用することを特徴とする請求項８乃至１１のいずれかの生体認証システム。
【請求項１３】
個人の生体情報の登録画像と照合画像との相互相関に基づいて生体認証を行うサーバに接続して使用される端末装置において、
生体情報を採取する生体採取手段と、採取された個人の生体情報から登録又は照合のための画像を作成する画像作成部と、該画像を撹乱するためのフィルタおよび逆フィルタを作成するフィルタ生成部と、該画像作成部により作成された該画像に、該フィルタ生成部で生成されたフィルタを作用させて登録テンプレートを作成し、又は該画像に該逆フィルタを作用させて照合画像を作成する変換部と、少なくとも該登録テンプレート及び該照合画像を含む情報を該サーバに送信する通信部と、を有し、作成された該登録テンプレート又は該照合画像を含む情報を該サーバへ送信して生体認証に供することを特徴とする端末装置。
【請求項１４】
個人の生体情報の登録画像と照合画像との相互相関に基づいて生体認証を行う他の装置に接続して使用される生体デバイスであって、
個人の生体情報を採取するセンサと、採取された個人の生体情報から登録又は照合のための画像を作成する画像作成部と、該画像を撹乱するためのフィルタおよび逆フィルタを作成するフィルタ生成部と、該画像作成部により作成された該画像に、該フィルタ生成部で生成されたフィルタを作用させて登録テンプレートを作成し、又は該画像に該逆フィルタを作用させて照合画像を作成する変換部と、を有し、作成された該登録テンプレート又は該照合画像を含む情報を該他の装置へ送信して生体認証に供することを特徴とする生体デバイス。
【請求項１５】
生体情報の登録時には、登録画像をフーリエ変換して、前記撹乱するためのフィルタを周波数空間上で作用させ、認証時には、照合画像をフーリエ変換し、該逆フィルタを周波数空間上で作用させることを特徴とする請求項１４の生体デバイス。
【請求項１６】
ネットワークを介して接続される端末装置とサーバを有する生体認証システムで実行されて個人の生体認証を行うプログラムであって、
該端末装置においては、採取された個人の生体情報から登録又は照合のための画像を作成する画像作成手段と、該画像を撹乱するためのフィルタおよび逆フィルタを作成するフィルタ生成手段と、該画像作成手段により作成された該画像に、該フィルタ生成手段で生成されたフィルタを作用させて登録テンプレートを作成し、又は該画像に該逆フィルタを作用させて照合画像を作成する変換手段と、少なくとも該登録テンプレート及び該照合画像を含む情報を該サーバに送信する手段と、を実現する機能を有し、
該サーバにおいては、該端末装置から送信されて得られた該登録テンプレートを記憶装置に記憶する登録手段と、認証時に該端末装置から送信して得られた該照合画像と該記憶装置に記憶された該登録テンプレートとを照合して両者の相互相関を判断する照合手段と、を実現する機能を有し、該照合手段による判断結果に応じて認証することを特徴とする端末装置及びサーバ上で実行されるプログラム。
【請求項１７】
登録画像上で一箇所以上の座標を選択し、該座標のそれぞれを中心とする所定の大きさの局所画像を切り出し、照合画像上で該座標の周辺画像と該局所画像との相互相関または距離により該局所画像に関する一致または不一致を判定し、一致となった局所画像の数に基づいて本人を判定することを特徴とする請求項１乃至７のいずれかの生体認証方法。
【請求項１８】
前記登録画像上で選択される座標は、該登録画像において特徴的な構造を持つ点の座標であることを特徴とする請求項１７の生体認証方法。

【請求項１９】
前記登録画像上で選択される座標は、該登録画像において特徴的な構造を持つ点の座標およびランダムに選択された点の座標であることを特徴とする請求項１７の生体認証方法。
【請求項２０】
前記生体情報は指紋であり、前記特徴的な構造を持つ点は指紋の端点または分岐点であり、前記座標は指紋のコアを原点として計算されることを特徴とする請求項１８又は１９の生体認証方法。
【請求項２１】
前記生体情報は指静脈であることを特徴とする請求項１乃至７のいずれかの生体認証方法。
【請求項２２】
ネットワークを介して接続される端末装置とサーバとを用いて、個人の生体認証を行う生体認証システムにおいて、
該端末装置は：
採取された個人の生体情報から登録又は照合のための画像を作成する画像作成部と、該画像上で一箇所以上の座標を選択し、該座標のそれぞれを中心とする所定の大きさの局所画像を切り出す局所画像切り出し部と、該局所画像の各々に対してそれを撹乱するためのフィルタおよび逆フィルタを作成するフィルタ生成部と、該局所画像切り出し部により作成された該局所画像に、該フィルタ生成部で生成されたフィルタを各々作用させて登録テンプレートを作成し、又は該画像に該逆フィルタを作用させて照合用局所画像を作成する変換部と、少なくとも該登録テンプレート又は該照合用局所画像を含む情報を該サーバに送信する第１通信部と、を有し、
該サーバは：
該端末装置から送信される情報を受信する第２通信部と、第２通信部を介して受信された該登録テンプレートを記憶装置に記憶する登録部と、認証時に該第２通信部を介して得られた該照合用局所画像と該記憶装置に記憶された該登録テンプレートとを照合して両者の相互相関により一致または不一致を判断する局所画像照合部と、該局所画像のうち一致したものの数に基づいて生体情報の一致または不一致を判定する判定部と、を有し、該判定部の判断結果に応じて個人を認証することを特徴とする生体認証システム。
【請求項２３】
登録テンプレートを更新する時に、該端末装置は、前記各座標に対して新たにフィルタおよび逆フィルタを作成して保存し、各々既存のフィルタと新たなフィルタの差分を求め、フィルタの差分を該サーバへ送信し、該サーバは、受信した各フィルタの差分を既に登録済みの該登録テンプレートに各々作用させて、新たなテンプレートを作成して該記憶装置に登録することを特徴とする請求項２２の生体認証システム。
【請求項２４】
生体情報の登録時には、登録から切出した各局所画像をフーリエ変換して、前記撹乱するためのフィルタを周波数空間上で作用させ、認証時には、照合画像から切出した各局所画像をフーリエ変換し、該逆フィルタを周波数空間上で作用させることを特徴とする請求項２２又は２３の生体認証システム。
【請求項２５】
生体情報の登録時には、登録から切出した各局所画像を数論変換して、前記撹乱するためのフィルタを数論変換後の画像に作用させ、認証時には、照合画像から切出した各局所画像を数論変換し、該逆フィルタを数論変換後の画像に作用させることを特徴とする請求項２２又は２３の生体認証システム。
【請求項２６】
前記撹乱するためのフィルタおよび該逆フィルタは、該フィルタを作用させて作成する登録テンプレート、および該逆フィルタを作用させて作成する照合画像がランダムな値を有するように設定することを特徴とする請求項２２乃至２５のいずれかの生体認証システム。

【請求項２７】
登録画像上で一箇所以上の座標を選択し、該座標のそれぞれを中心とする所定の大きさの局所画像を切り出し、照合画像上で該座標の周辺画像と該局所画像との相互相関または距離により該局所画像に関する一致または不一致を判定し、一致となった局所画像の数に基づいて本人を判定することを特徴とする請求項１６のプログラム。
【請求項２８】
個人の生体認証を行う生体認証システムにおいて、
採取された個人の生体情報から登録又は照合のための画像を作成する画像作成部と、該画像を撹乱するためのフィルタおよび逆フィルタを作成するフィルタ生成部と、該画像作成部により作成された該画像に、該フィルタ生成部で生成されたフィルタを作用させて登録テンプレートを作成し、又は該画像に該逆フィルタを作用させて照合画像を作成する変換部と、該登録テンプレートを記憶装置に記憶する登録部と、認証時に得られる該照合画像と該記憶装置に記憶された該登録テンプレートとを照合して両者の相互相関を判断する照合部と、を有し、該照合部の判断結果に応じて個人を認証することを特徴とする生体認証システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、個人の生体情報を用いて本人を認証する生体認証方法およびシステムに関する。
【背景技術】
【０００２】
生体情報を用いた個人認証システムは、初期の登録時に個人の生体情報を取得し、特徴量と呼ばれる情報を抽出して登録する。この登録情報をテンプレートという。認証時には、再び個人から生体情報を取得して特徴量を抽出し、先に登録されたテンプレートと照合して本人か否かを確認する。
【０００３】
クライアントとサーバがネットワークを介して接続されたシステムにおいて、サーバがクライアント側にいるユーザを生体認証する場合、典型的にはサーバがテンプレートを保持する。クライアントは認証時にユーザの生体情報を取得し、特徴量を抽出してサーバへ送信し、サーバは特徴量をテンプレートと照合して本人か否かを確認する。
【０００４】
しかし、テンプレートは個人を特定することのできる情報であるため、個人情報として厳密な管理が必要とされ、高い管理コストが必要となる。例え厳密に管理されていても、プライバシの観点からテンプレートを登録することに心理的な抵抗を感じる人も多い。また、一人の個人が持つ一種類の生体情報の数には限りがある（例えば指紋は１０本の指のみ）ため、パスワードや暗号鍵のように容易にテンプレートを変更することができない。仮にテンプレートが漏洩して偽造の危険が生じた場合、その生体認証を使用することができなくなるという問題がある。さらに、異なるシステムに対して同じ生体情報を登録している場合には他のシステムまで脅威にさらされることになる。
【０００５】
上記問題に関する対策として、特許文献１（特開２００１－７８０２号公報）には、生体情報を暗号して認証サーバに送信する方法が開示されている。この方法によれば、認証時には一旦復号化する必要があるため、高度な攻撃による漏洩や、サーバ管理者による意図的な漏洩を防ぐことが困難であり、プライバシ問題への対策としても不十分である。
【０００６】
そこで、生体情報の登録時に特徴量を一定の関数とクライアントが持つ秘密のパラメータで変換し、元の情報を秘匿した状態でテンプレートとしてサーバに保管し、認証時にクライアントが新たに抽出した生体情報の特徴量を、同じ関数とパラメータで変換してサーバへ送信し、サーバは受信した特徴量とテンプレートを変換された状態のまま照合する方

法（キャンセラブル生体認証という）が提案されている。
【０００７】
この方法によれば、クライアントが変換パラメータを秘密に保持することで、サーバは認証時においても元の特徴量を知ることができず、個人のプライバシが保護される。またテンプレートが漏洩した場合にも、変換パラメータを変更して再度テンプレートを作成、登録することで、安全性を保つことができる。更に異なるシステムに対して同じ生体情報を用いる場合に、各々異なるパラメータで変換したテンプレートを登録することで、一つのテンプレートが漏洩しても他のシステムの安全性が低下することを防止することができる。
【０００８】
キャンセラブル生体認証の具体的な実現方法は、生体情報の種類や照合アルゴリズムに依存する。非特許文献１において、顔画像を用いたキャンセラブル生体認証の実現方法が提案されている。この方法は、顔画像を周波数空間に変換し、登録時には照明変動などを吸収するフィルタを作成してテンプレートとし、認証時には入力した顔画像に対してテンプレートを用いたフィルタ処理を行い、出力パターンに対するしきい値判定により認証を行うものである。
【０００９】
【特許文献１】特開２００１－７８０２号公報
【特許文献２】特開２００４－１７８６０６号公報
【特許文献３】特開２００１－３４４２１３号公報
【非特許文献１】M.Savvides, B.V.K.Vijayakumar and P.K.Khosla, “Authentication-Invariant Cancelable Biometric Filters for Illumination-Tolerant Face Verification”, Biometric Technology for Human Identification, Proceedings of SPIE Vol.5404, P156-163
【非特許文献２】Naoto Miura, Akio Nagasaka, Takafumi Miyatake, “Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification”, Machine Vision and Applications (2004) Vol.15, P.194-203
【発明の開示】
【発明が解決しようとする課題】
【００１０】
上記特許文献１によれば、生体情報を利用した遠隔本人認証システムにおいて、入力された生体情報をクライアント側で暗号化して送信し、認証サーバで復号化している。これにより、ネットワークを介した生体認証システムにおいても生体情報を安全に送受信することができる。しかしながら、認証サーバ内で生体情報を復号化するため、個人の生体情報をサーバ管理者に対して秘匿することができない。このため、不慮の事故やサーバ管理者の不正に起因して平文の生体情報が漏洩してしまう可能性がある。また個人にとってのプライバシに関する抵抗感を低減することができないという課題も残る。
【００１１】
非特許文献１によれば、登録テンプレートにランダムフィルタを作用させることによりキャンセラブル化を実現することができるが、画像どうしの相互相関を照合値とするような照合アルゴリズムに対してこの方法を適用してキャンセラブル化する場合、照合値が大きく異なってしまい照合精度を劣化させるという問題が生じる。
【００１２】
また、登録画像と照合画像の輝度値が生体としての特徴を示す程度に応じて３種類の値を有する３値画像である場合に、３値画像同士の距離値を照合値とするような照合アルゴリズムに対しても、非特許文献１で提案されている方法ではキャンセラブル化を実現することができない。
【００１３】
本発明の目的は、所定の特性を持つ照合アルゴリズムに対し、照合精度を劣化させるこ

となくキャンセラブル化を実現する生体認証を提供することにある。
【課題を解決するための手段】
【００１４】
本発明は、個人の生体情報の登録画像と照合画像との相互相関に基づいて個人を認証する方法において、登録時には、画像を撹乱するためのフィルタ、および逆フィルタを作成し、生体画像から作成された登録画像に該フィルタを作用させて登録テンプレートを作成して記憶装置に登録しておき、認証時には、個人から取得した生体情報から作成された照合画像に逆フィルタを作用させ、逆フィルタの作用後の照合画像と登録テンプレートとの相互相関を用いて個人を判定するものである。
【００１５】
また、本発明に係る生体認証システムは、好ましくは個人の生体認証を行う生体認証システムにおいて、採取された個人の生体情報から登録又は照合のための画像を作成する画像作成部と、該画像を撹乱するためのフィルタおよび逆フィルタを作成するフィルタ生成部と、該画像作成部により作成された該画像に、該フィルタ生成部で生成されたフィルタを作用させて登録テンプレートを作成し、又は該画像に該逆フィルタを作用させて照合画像を作成する変換部と、該登録テンプレートを記憶装置に記憶する登録部と、認証時に得られる該照合画像と該記憶装置に記憶された該登録テンプレートとを照合して両者の相互相関を判断する照合部と、を有し、該照合部の判断結果に応じて個人を認証する生体認証システムとして構成される。
【００１６】
好ましい例によれば、本発明に係る生体認証システムは、ネットワークを介して接続される端末装置とサーバとを用いて、個人の生体認証を行う生体認証システムにおいて、端末装置は、採取された個人の生体情報から登録又は照合のための画像を作成する画像作成部と、画像を撹乱するためのフィルタおよび逆フィルタを作成するフィルタ生成部と、画像作成部により作成された画像に、フィルタ生成部で生成されたフィルタを作用させて登録テンプレートを作成し、又は画像に逆フィルタを作用させて照合画像を作成する変換部と、少なくとも登録テンプレート又は照合画像を含む情報をサーバに送信する第１通信部と、を有する。
サーバは、端末装置から送信される情報を受信する第２通信部と、第２通信部を介して受信された登録テンプレートを記憶装置に記憶する登録部と、認証時に第２通信部を介して得られた照合画像と記憶装置に記憶された登録テンプレートとを照合して両者の相互相関を判断する照合部と、を有し、照合部の判断結果に応じて個人の生体認証を行なう。
【００１７】
また、本発明は、好ましくは、個人の生体情報の登録画像と照合画像との相互相関に基づいて生体認証を行う他の装置に接続して使用される生体デバイスであって、個人の生体情報を採取するセンサと、採取された個人の生体情報から登録又は照合のための画像を作成する画像作成部と、画像を撹乱するためのフィルタおよび逆フィルタを作成するフィルタ生成部と、画像作成部により作成された画像に、フィルタ生成部で生成されたフィルタを作用させて登録テンプレートを作成し、又は画像に逆フィルタを作用させて照合画像を作成する変換部と、を有し、作成された登録テンプレート又は照合画像を含む情報を他の装置へ送信して生体認証に供する生体デバイスとしても構成される。
【００１８】
また、本発明は、好ましくはネットワークを介して接続される端末装置とサーバを有する生体認証システムで実行されて個人の生体認証を行うプログラムであって、端末装置においては、採取された個人の生体情報から登録又は照合のための画像を作成する画像作成手段と、画像を撹乱するためのフィルタおよび逆フィルタを作成するフィルタ生成手段と、画像作成手段により作成された画像に、フィルタ生成手段で生成されたフィルタを作用させて登録テンプレートを作成し、又は画像に逆フィルタを作用させて照合画像を作成する変換手段と、少なくとも登録テンプレート又は照合画像を含む情報をサーバに送信する手段と、を実現する機能を有し、

サーバにおいては、端末装置から送信されて得られた登録テンプレートを記憶装置に記憶する登録手段と、認証時に端末装置から送信して得られた照合画像と記憶装置に記憶された登録テンプレートとを照合して両者の相互相関を判断する照合手段と、を実現する機能を有し、照合手段による判断結果に応じて認証する、端末装置及びサーバ上で実行されるプログラムとして構成される。

【発明の効果】

【００１９】

本発明によれば、画像どうしの相互相関に基づいた照合アルゴリズムにおいて、登録画像および照合画像をランダム化してサーバ管理者に対し画像を秘匿したまま認証を行うことが可能なキャンセラブル生体認証を実現することができる。

また、画像が３値画像である場合でかつ距離値を照合値とするような照合アルゴリズムにおいて、キャンセラブル生体認証を実現するとこができる。また、ランダム化した画像から元画像の復元を一層困難にするためのランダムなフィルタを作成することができる。

【発明を実施するための最良の形態】

【００２０】

以下、図面を参照して、本発明の実施形態について説明する。

【実施例１】

【００２１】

本実施形態では、指静脈画像をサーバに対して秘匿したまま、サーバ内で指静脈照合を行う、キャンセラブル指静脈認証システムを例に揚げて説明する。

【００２２】

図1は、キャンセラブル指静脈認証のシステム構成を示す。

このキャンセラブル指静脈認証システムは、登録・認証時の指静脈画像取得、３値画像作成、およびランダム変換を行うクライアント端末（以下単にクライアント）１００と、テンプレートの保管と照合を行うサーバ１３０が、インターネットやイントラネットのようなネットワークを介して接続して構成される。

【００２３】

クライアント１００はユーザ自身か又は信頼できる第三者によって管理され、指静脈の画像化を行う指静脈センサ１１０を有する共に、ユーザが携帯する携帯型記録媒体１２０を扱う。携帯型記憶媒体１２０はユーザが所持して管理する、ＩＣカードやＵＳＢメモリの如き記憶媒体である。勿論、携帯端末やフレキシブルディスクの媒体も利用可能である。例えば自宅からインターネットバンキングを行う場合、クライアント１００はユーザが管理する自宅のＰＣであり、サーバ１３０は銀行が管理するサーバマシンとするような構成も可能である。

【００２４】

クライアント端末１００は、指静脈画像から指静脈パターンを抽出し３値化する３値画像作成部１０１と、登録時に各ピクセルにランダムな値を持つランダムフィルタのペアを生成するランダムフィルタ生成部１０３と、このランダムフィルタを用いて３値画像を変換してランダム画像を作成するランダム変換部１０２と、携帯型記録媒体１２０との間で通信を行う記録媒体Ｉ／Ｆ部１０４と、ネットワークを介して通信を行う通信部１０５を有して構成される。上記３値画像作成部１０１、ランダムフィルタ生成部１０３及びランダム変換部１０２の処理は、クライアント１００のプロセッサがプログラムを実行することで実現される。なお、３値画像作成は、例えば、特開２００４－１７８６０６公報（特許文献２）に開示された方法により実現できる。

【００２５】

サーバ１３０は、ネットワークを介して通信を行う通信部１31と、ランダム画像をテンプレートとして登録する登録部１３２と、テンプレートを記憶する記憶装置１３３と、認証時に新たに受信したランダム画像をテンプレートと照合してミスマッチ率を計算する照合部１３４を備えて構成される。登録部１３２及び照合部１３４における処理は、サーバ１３０がプログラムを実行することで実現される。

ここで、ミスマッチ率とは、対象としたランダム画像とテンプレートがどの程度似ていないかを示す指標であり、ミスマッチ率が小さいほど似ていると言える。なお、ミスマッチ率算出は、例えば非特許文献２に開示された方法を適用して実現できる。

【００２６】

図２は、指静脈の登録処理及び認証処理動作のフローを示す。

まず、登録処理動作について説明する。

クライアント１００において、指静脈センサ１１０はユーザの指静脈画像を取得する（Ｓ２０１）。そして、クライアント１００は、指静脈画像から指静脈パターンを抽出し、３値化し、３値画像を作成する（Ｓ２０２）。

【００２７】

ここで、３値画像の作成は、例えば特開２００４－１７８６０６公報に記載の方法により実現できる。その方法によれば、登録時に作成する３値画像ｇの縦幅をHe、横幅をWeとし、認証時に作成する３値画像ｆの縦幅をHv、横幅をWvとすると、He＜Hv、We＜Wvである。しかし本実施形態では、登録時の３値画像ｇのサイズを認証時の３値画像ｆのサイズに次の方法により拡張する。

始めに、ｇの中心をｆの中心に合わせ、次にｇの外側でｆの内側の領域（つまりｇからはみ出た領域）の画素の輝度値を１とする。これにより、ｇのサイズを縦幅Hv、横幅Wvに拡張できる。

【００２８】

次に、クライアント１００は、ランダムフィルタペア（Ｋ，Ｌ）を生成する（Ｓ２０３）。ここで、Ｋをランダムフィルタ、Ｌを逆ランダムフィルタと呼ぶ。

クライアント１００は、逆ランダムフィルタＬを、携帯型記憶装置１２０に書き込み、また逆ランダムフィルタＬをクライアント内の記憶装置から消去する（Ｓ２０４）。この逆ランダムフィルタＬは携帯型記憶媒体１２０内で保管され、サーバ１３０に対して秘匿する。

【００２９】

クライアント１００は、ランダム変換部１０２に上記ランダムフィルタＫおよび前記３値画像ｇを入力し、出力されたランダム画像ＫＧをサーバ１３０へ送信する（Ｓ２０5）。ランダム変換の詳細については後述する。

サーバ１３０はそのランダム画像ＫＧを受信し、これをテンプレートとして記憶装置１３３に登録する（Ｓ２０6）。

【００３０】

次に、認証時の処理動作について説明する。

クライアント１００は、指静脈センサ１１０を介してユーザの指静脈画像を取得する（Ｓ２１１）。クライアント１００は、指静脈画像から３値画像ｆを作成する（Ｓ２１２）。ここで、３値画像の作成は、例えば特開２００４－１７８６０６公報に記載された方法による。３値画像ｆのサイズは、縦幅Hv、横幅Wvとする。

【００３１】

次に、クライアント１００は、携帯型記憶媒体１２０から前記逆ランダムフィルタＬを読み込む（Ｓ２１３）。そして、クライアント１００は、ランダム変換部１０２に前記逆ランダムフィルタＬおよびこの３値画像ｆを入力し、出力されたランダム画像ＬＦをサーバ１３０へ送信する（Ｓ２１４）。なお、ランダム変換の詳細については後述する。

【００３２】

サーバ１３０はランダム画像ＬＦを受信し、これを前記テンプレートＫＧと照合して本人の指静脈か否かを判定する（Ｓ２１５）。なお、認証処理終了後、クライアント１００は内部の記憶装置から前記逆ランダムフィルタＬを消去する。

【００３３】

以上の通り、サーバ１３０は変換されたランダム画像ＫＧをテンプレートとして保管し、また認証時にも変換されたランダム画像ＬＦを受信する。ランダムフィルタＫ、および逆ランダムフィルタＬをサーバ１３０に対して秘匿することにより、サーバ１３０は元の

指静脈３値画像ｇおよびｆを知ることができない。このためサーバ１３０に対してユーザの匿名性が高まり、プライバシが保護される。また仮に、サーバ１３０からテンプレートＫＧが漏洩したとしても、元の３値画像ｇが不明なため指静脈を偽造することができない。また、ランダムフィルタＫおよび逆ランダムフィルタＬを変更してテンプレートを更新することにより、同じ指を利用しつつ古いテンプレートを無効にすることができる。これにより高い安全性を実現し、かつサーバのテンプレート管理コストを削減することができる。

なお、本実施形態において、逆ランダムフィルタＬはユーザが所持する記録媒体に保管するが、クライアント１００内に保管してもよく、またユーザが入力するパスワードから動的に生成するなどとしても良い。

【００３４】

次に、図３を参照して、上述したランダムフィルタペア生成の動作について説明する。ここでは、ランダム変換中の基底変換をフーリエ変換した場合について、ランダムフィルタ生成部１０3でのランダムフィルタペア（Ｋ、Ｌ）生成方法について述べる。この方法では、まずランダムフィルタＫ（u，v）を設定する。（u，v）を基底変換後空間での座標とし、（u，v）ごとに乱数を発生させ、それをＫ（u，v）の値とする（Ｓ３０1）。次に、逆ランダムフィルタＬ（u，v）を設定する。Ｌ（u，v）は、（u，v）ごとに対応するＫ（u，v）の逆数（あるいは乗法に関する逆元）を値として設定する（Ｓ３０２）。また、後述する通り、ランダム変換において２値画像作成を行うが、この２値画像を撹乱するためのランダムフィルタペアＫ'（u，v）とＬ'（u，v）は、上記と同様のフローを用いて別途作成する。

【００３５】

このように生成されたランダムフィルタペアＫ（u，v）を用いれば、テンプレートとしてサーバに登録すべき画像Ｋ（u，v）・Ｇ（u，v）、Ｋ'（u，v）・Ｇ'（u，v）は撹乱されており、仮にサーバからＫ（u，v）・Ｇ（u，v）、Ｋ'（u，v）・Ｇ'（u，v）が漏洩しても、ランダムフィルタＫ（u，v）、Ｋ'（u，v）を知らければ、Ｇ（u，v）、Ｇ'（u，v）を復元することは困難である。また、認証時にサーバに送信する画像についても、逆フィルタＬ（u，v）とＬ'（u，v）を用いてＬ（u，v）・Ｆ（u，v）、Ｌ'（u，v）・Ｆ´（u，v）を作成することにより、撹乱することができる。これにより指静脈照合のキャンセラブル化が可能となる。

【００３６】

なお、他の例として、ランダムフィルタ生成部１０３におけるランダムフィルタペア（Ｋ、Ｌ）生成を次のような方法によって実現しても良い。この方法では、ランダム変換部１０２の出力であるランダム画像Ｋ（u，v）・Ｇ（u，v）、Ｌ（u，v）・Ｆ（u，v）が一様な乱数となるように、Ｋ（u，v）、Ｌ（u，v）を設定する。

【００３７】

以下、図４を用いて、この例について説明する。

クライアントは、まず、一様な乱数を（u，v）ごとに発生させる（Ｓ４０1）。次に、画像Ｇ（u，v）を受け取り、乱数Ｒ（u，v）をＧ（u，v）で割り、これをランダムフィルタＫ（u，v）とする（Ｓ402）。次に、Ｋ（u，v）の逆数を計算し、これを逆ランダムフィルタＬ（u，v）とする（Ｓ４０３）。

このように生成されたランダムフィルタＫ（u，v）を用いれば、テンプレートとしてサーバに登録すべきランダム画像Ｋ（u，v）・Ｇ（u，v）はＲ（u，v）に等しく、一様な乱数となる。仮にサーバからＫ（u，v）・Ｇ（u，v）が漏洩しても、これが一様な乱数であるために、ランダムフィルタＫ（u，v）を知らければ、指静脈画像であると判別できず、またＧ（u，v）を復元することも困難である。このような方法によるランダムフィルタペアを生成すれば、サーバに保存するランダム画像Ｋ（u，v）・Ｇ（u，v）の復元をさらに困難にすることができる。また、２値画像Ｇ´（u，v）、Ｆ´（u，v）に対して作用させるべきフィルタＫ'（u，v）、Ｌ'（u，v）に関しても、上記と同様のフローを用いて設定することができる。

【００３８】
次に、図５を参照してランダム変換の処理動作について説明する。
クライアント１００は、ランダム変換部１０２に３値画像（ｇまたはｆ）を入力する。ランダム変換部１０２は、まず、３値画像の静脈画素数を計算する（Ｓ５０１）。登録時に、３値画像ｇ（x，y）上で輝度値が２となるピクセルの総和を求める。これをＳｇとする。認証時に、３値画像ｆ（x，y）上で輝度値が２となるピクセルの総和を求める。これをＳｆとする。
次に、ランダム変換部１０２は、３値画像から２値画像を作成する（Ｓ５０２）。この２値画像作成では、３値画像（ｇ（x，y）またはｆ（x，y））の各ピクセルの輝度値が０および１の場合はそのままの値とし、２の場合はその値を０に置き換える。ここで作成した２値画像をｇ´（x，y）およびｆ´（x，y）と呼ぶ。
【００３９】
次に、ランダム変換部１02は、３値画像（ｇ（x，y）またはｆ（x，y））および２値画像（ｇ´（x，y）またはｆ´（x，y））に対して基底変換を行う（Ｓ５０３）。
ここでは、基底変換としてフーリエ変換を例にとる。フーリエ変換により、画像ｇ（x，y）はフーリエ画像Ｇ（u，v）に変換される。Ｇ（u，v）の値は、x方向の周波数をu、y方向の周波数をvとしたとき、ｇ（x，y）の空間周波数成分を示す。以降、ｇ（x，y）のフーリエ画像をＧ（u，v）、ｆ（x，y）のフーリエ画像をＦ（u，v）、ｇ´（x，y）のフーリエ画像をＧ´（u，v）、ｆ´（x，y）のフーリエ画像をＦ´（u，v）と呼ぶ。なお、基底変換としてフーリエ変換以外の数論変換を用いても良い。
【００４０】
次に、ランダム変換部１０２は、ランダムフィルタを用いて前記フーリエ画像に対してランダムフィルタ演算を行う（Ｓ５０４）。登録時にはランダムフィルタＫを用いてＧおよびＧ´に対して演算を行い、認証時には逆ランダムフィルタＬを用いてＦおよびＦ´に対して演算を行う。
ここで、ＫおよびＬは、フーリエ画像のようなものであり、x方向の周波数uおよびy方向の周波数vの組み合わせごとに値を持ち、Ｋ（u，v）、Ｌ（u，v）と表せる。Ｋ（u，v）、Ｌ（u，v）の値はランダムであるが、Ｋ（u，v）・Ｌ（u，v）＝１という関係を持つものとする。さて、ランダムフィルタ演算の内容であるが、登録時には、Ｋ（u，v）・Ｇ（u，v）およびＫ（u，v）・Ｇ´（u，v）を計算し、認証時にはＬ（u，v）・Ｆ（u，v）およびＬ（u，v）・Ｆ´（u，v）を計算する。以降、これらの計算結果をランダム画像と呼ぶ。
このように、Ｋ（u，v）、Ｌ（u，v）を知らない場合、これらランダム画像から元の画像Ｇ（u，v）やＦ（u，v）を復元できないため、指静脈３値画像をサーバ１３０に対して秘匿させることができる。
【００４１】
次に、図６を参照して、サーバ１３０の照合部１３４の処理動作について説明する。
サーバ１３０は、照合部１３４に、ランダム画像Ｌ（u，v）・Ｆ（u，v）、Ｌ（u，v）・Ｆ´（u，v）、およびテンプレートＫ（u，v）・Ｇ（u，v）、Ｋ（u，v）・Ｇ´（u，v）を入力する。
照合部１３４は、まず、Ｌ（u，v）・Ｆ（u，v）とＫ（u，v）・Ｇ（u，v）の積、Ｌ（u，v）・Ｆ´（u，v）とＫ（u，v）・Ｇ´（u，v）の積、を計算する（Ｓ６０１）。計算結果をそれぞれＷ（u，v）、Ｗ´（u，v）と呼ぶ。
【００４２】
次に、照合部１３４は、Ｗ（u，v）、Ｗ´（u，v）に対して逆基底変換を行う（Ｓ６０２）。ここでは、逆基底変換として、フーリエ変換に対応する逆フーリエ変換を例にとる。Ｗ（u，v）の逆フーリエ変換の結果であるｗ（ｐ、ｑ）は、ｆ（x，y）に対してｇ（x，y）を（ｐ、ｑ）だけ平行移動した場合の相互相関の値を示す。また、Ｗ´（u，v）の逆フーリエ変換ｗ´（ｐ、ｑ）は、同様に、ｆ´（x，y）に対してｇ´（x，y）を（ｐ、ｑ）だけ平行移動した場合の相互相関の値を示す。なお、基底変換としてフーリエ変換以

外の数論変換などを用いるならば、対応する逆変換を用いるのが好ましい。

【００４３】

次に、照合部１３４は、ｗ（ｐ、ｑ）、ｗ´（ｐ、ｑ）、Ｓｇ、Ｓｆからミスマッチ率Ｒｍ（ｐ、ｑ）を計算する（Ｓ６０３）。

ミスマッチ率Ｒｍ（ｐ、ｑ）は、Ｓｆ＋Ｓｇ－｛ｗ（ｐ、ｑ）－ｗ´（ｐ、ｑ）｝／２を　Ｓｆ＋Ｓｇ　で割ったものである。（ｐ、ｑ）を変数としたときのミスマッチ率Ｒｍ（ｐ、ｑ）の最小値を計算し、設定されたしきい値と比較し、しきい値より小さい場合には本人と判定し、しきい値より大きい場合には他人と判定する（Ｓ６０４）。

【００４４】

ここで、ランダム画像Ｋ（u，ｖ）・Ｇ（u，ｖ）、Ｋ（u，ｖ）・Ｇ´（u，ｖ）、Ｌ（u，ｖ）・Ｆ（u，ｖ）、Ｌ（u，ｖ）・Ｆ´（u，ｖ）から元の３値あるいは２値画像を復元することなく、照合を行っている点に注目すべきである。つまり、サーバ１３０に対し指静脈の３値画像あるいは２値画像を秘匿したまま、認証処理が可能となっている。これにより、テンプレート（ここでは指静脈の３値画像あるいは２値画像）保護型の指静脈認証を実現できる。なお、本実施形態では、ＳｆおよびＳｇはサーバ１３０に対して公開されるが、これらから元の３値画像を復元することは困難であり、秘匿上問題とはることはない。

【００４５】

なお、本実施形態において、次のような方法に従って、元の３値画像の復元困難性を向上させても良い。これは、ランダム変換部１０2での基底変換（Ｓ３０３）に数論変換を用いることにより、実現可能である。

はじめに２次元の場合の数論変換の概略について説明する。２次元データ列ｄ（x，ｙ）を与え、ｘ、ｙの範囲を０≦ｘ≦Ｎ－１０≦ｙ≦Ｎ－１とする。ある整数Ｍとして、次式を満たす１の原始Ｎ乗根αが存在する。

【００４６】

【数１】

$$\alpha^N = 1 \pmod{M}$$

【００４７】

ｄ（ｘ）に対する数論変換は、整数Ｍを法とする演算のもとで次式により定義される。

【００４８】

【数２】

$$D(u,v)=\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} d(x,y)\,\alpha^{ux+vy} \qquad (0 \le u,v \le N-1)$$

【００４９】

逆変換は次式で定義される。

【００５０】

【数３】

$$d(x,y)=N^{-1}\cdot N^{-1}\sum_{u=0}^{N-1}\sum_{v=0}^{N-1} D(u,v)\,\alpha^{-(ux+vy)} \qquad (0 \le x,y \le N-1)$$

【００５１】

さて、本実施形態では、上記した３値画像（ｇ（x，ｙ）またはｆ（x，ｙ））および２値画像（ｇ´（x，ｙ）またはｆ´（x，ｙ））に対して２次元の数論変換を施し、変換後画像Ｇｎ（u，ｖ）、Ｇ´ｎ（u，ｖ）、Ｆｎ（u，ｖ）、Ｆ´ｎ（u，ｖ）を作成する。

登録時には、上記のランダム変換で用いたランダムフィルタＫ（u，ｖ）をＧｎ（u，ｖ）とＧ´ｎ（u，ｖ）に作用させるが、このとき整数Ｍを法として乗算を行う。また、上記の逆ランダムフィルタＬ（u，ｖ）に対応するものは、Ｋ（u，ｖ）の整数Ｍを法とした場合の逆

元Ｌｎ（u，v）を用いる。つまり、Ｋ（u，v）・Ｌｎ（u，v）＝１（mod Ｍ）が成立する。認証時には、このＬｎ（u，v）をＦｎ（u，v）、Ｆ´ｎ（u，v）に作用させる。

【００５２】

次に、図７を参照して、復元困難性が向上する理由を説明する。ここでは、Ｋ（u，v）・Ｇｎ（u，v）を例にあげる。

攻撃者は、Ｋ（u，v）・Ｇｎ（u，v）が既知の場合に、Ｋ（u，v）およびＧｎ（u，v）を知ることを目的としている。整数Ｍを法としてＫ（u，v）・Ｇｎ（u，v）を求めるが、単なる整数としての演算により求めたＫ（u，v）・Ｇｎ（u，v）がＭよりも大きい場合には、図７の数直線上で示すように、それをＭで割った余りと同一視する。したがって、この例では、Ｋ（u，v）・Ｇｎ（u，v）は、Ｋ（u，v）、Ｇｎ（u，v）それぞれの値よりも小さい値となる。その結果、攻撃者が求めるべきＫ（u，v）、Ｇｎ（u，v）の候補として、Ｋ（u，v）・Ｇｎ（u，v）よりも小さいＫ（u，v）、Ｇｎ（u，v）が挙がる。

【００５３】

一方、上記フーリエ変換を用いる場合には、このような候補は挙がらない。したがって、攻撃者にとっては、可能な値の組み合わせが増大したため、総当り攻撃に必要な計算量が増大することとなり、事実上、復元困難性が向上する。

【００５４】

サーバ１３０からテンプレートが漏洩しリプレイアタックなどのリスクを回避するためには、定期的に、あるいはテンプレート漏洩発覚時に、サーバ１３０に登録されているキャンセラブル化されたテンプレートを更新することが好ましい。この際、指静脈自体の再登録は行わず、ユーザへの負荷を低減することも目的とする。以下、テンプレート更新方法の例について述べる。なお、この例ではランダム変換における基底変換にフーリエ変換を用いる前提で説明するが、数論変換など他の基底変換にも適用可能である。

【００５５】

図８は、テンプレートの更新方法の処理動作を示す。

クライアント１００は、新規にランダムフィルタペアを作成する（Ｓ８０１）。ここで、既存のランダムフィルタペアを（K_1、L_1）、新規のランダムフィルタペアを（K_2、L_2）とする。ランダムフィルタペアの作成方法は、先に述べた例に従うのがよい。

【００５６】

次に、クライアント１００は、新規の逆ランダムフィルタL_2を携帯型記録媒体に書込み、既存の逆ランダムフィルタL_1を上書きする（Ｓ８０２）。次に、クライアント１００は、K_2／K_1を計算し、これをランダムフィルタ差分ΔＫとする（Ｓ８０３）。次に、サーバ１３０は、クライアント１００からランダムフィルタ差分ΔＫを受信し、既存のテンプレートK_1Ｇに作用させる（Ｓ８０４）。つまり、ΔＫ（u，v）・K_1（u，v）Ｇ（u，v）を計算する。ΔＫ（u，v）＝K_2（u，v）／K_1（u，v）であるため、この値は、K_2（u，v）Ｇ（u，v）に等しくなる。次に、サーバ１３０は、K_2（u，v）Ｇ（u，v）をテンプレートとして登録し、テンプレートを更新する（Ｓ８０５）。

【００５７】

以上の処理により、新旧のランダムフィルタK_1、K_2をサーバ１３０に漏洩すること無く、また指静脈自体を再登録せずに、テンプレートの更新が可能となる。これにより、ユーザによる指静脈再登録の負荷を低減しつつ、キャンセラブル化されたテンプレートを更新し、リプレイアタックなどのリスクを回避することができる。

【００５８】

上記した本実施形態に係る、生体情報をサーバに登録して照合を行う生体認証システムは、上記した例に限定されることなく、他にも適用可能である。例えば、社内ネットワークにおける情報アクセス制御や、インターネットバンキングシステム、ＡＴＭ（銀行自動取引装置）における本人確認、会員向けＷｅｂサイトへのログイン、保護エリアへの入場時の個人認証などに適用できる。

【００５９】

この場合、同じ個人が複数のシステムを利用するために個々のシステムに生体情報を登

録する事態が想定されるが、その場合には対象とするシステムに応じて上記のフィルタ及び逆フィルタの係数を変更して適用するのが好ましい。このように係数を変更しておくことで、あるシステムからの生体情報の漏洩に対して、他のシステムでの同じ生体情報の利用を保護することができる。

【実施例２】

【００６０】

次に、図９乃至１２を参照して、第二の実施形態について説明する。

本実施形態は、指紋画像をサーバに対して秘匿したまま、サーバ内で指紋照合を行う、キャンセラブル指紋認証システムである。

【００６１】

図９は、キャンセラブル指紋認証のシステム構成を示す。

このキャンセラブル指紋認証システムは、登録・認証時の指紋画像取得、２値画像作成、コア・特徴点抽出、画像切り出し、およびランダム変換を行うクライアント端末（以下単にクライアント）９００と、テンプレートの保管と照合を行うサーバ９３０が、インターネットやイントラネットのようなネットワークを介して接続して構成される。

【００６２】

クライアント９００はユーザ自身か又は信頼できる第三者によって管理され、指紋の画像化を行う指紋センサ９１０を有する共に、ユーザが携帯する携帯型記録媒体９２０を扱う。携帯型記憶媒体９２０は上記第一の実施例と同様、ユーザが所持して管理する、ＩＣカードやＵＳＢメモリの如き記憶媒体である。例えば、自宅からインターネットバンキングを行う場合、クライアント９００はユーザが管理する自宅のＰＣであり、サーバ９３０は銀行が管理するサーバマシンとするような構成も可能である。

【００６３】

クライアント９００は、指紋画像を２値化する２値画像作成部９０１と、２値画像からコア（指紋の渦の中心）と特徴点（指紋の隆線の端点および分岐点）の位置を検出するコア・特徴点抽出部９０２と、本来の特徴点座標とは別にダミーの特徴点の座標をランダムに生成するダミー特徴点生成部９０３と、各特徴点（本来の特徴点とダミー特徴点）に対してランダムフィルタのペアを生成するランダムフィルタ生成部９０４と、各特徴点を中心にチップ画像または周辺画像を切り出す画像切出し部９０６と、各チップ画像または周辺画像に対してそれぞれランダムフィルタを用いて２値画像を変換してランダム画像を生成するランダム変換部９０７と、携帯型記録媒体９２０との間で通信を行う記録媒体Ｉ／Ｆ部９０５と、ネットワークを介して通信を行う通信部９０８を有して構成される。

上記２値画像作成部９０１、コア・特徴点抽出部９０２、ダミー特徴点生成部９０３、ランダムフィルタ生成部９０４、画像切り出し部９０６、ランダム変換部９０７の処理は、クライアント９００のプロセッサがプログラムを実行することで実現される。なお、２値画像作成、コア・特徴点抽出、画像切出しは、例えば、特許文献３に開示された方法により実現できる。

【００６４】

サーバ９３０は、ネットワークを介して通信を行う通信部９３１と、ランダム画像をテンプレートとして登録する登録部９３２と、テンプレートを記憶する記憶装置９３３と、認証時に新たに受信したランダム画像をテンプレートと照合して類似度を計算する照合部９３４を備えて構成される。登録部９３２及び照合部９３４における処理は、サーバ９３０がプログラムを実行することで実現される。

【００６５】

ここで、類似度とは、登録時に切り出した複数のチップ画像と照合時に切り出した複数の周辺画像を各々比較したときの、一致した画像数である。類似度が大きいほど、登録指紋と照合指紋が似ていることを示す。チップ画像と周辺画像の一致／不一致は、画像を重ね合わせたときに一致したピクセル数を元に判定する。ただし、登録時と照合時で、歪みや回転などの影響により特徴点の位置がずれる場合があるため、周辺画像のサイズはチップ画像のサイズより大きくとり、チップ画像を周辺画像上で平行移動させながら、一致ピ

クセル数が最大になるところを探索し、その最大値を元に一致／不一致を判定する。より詳細には特許文献３の記載より理解できるであろう。

【００６６】

次に、図１０および図１２を用いて、本実施形態における指紋の登録処理動作を説明する。

まず、クライアント９００がユーザの指紋画像を取得する（Ｓ１００１）。次に取得した指紋画像を２値化して、登録用２値画像１２００を作成する（Ｓ１００２）。ここで各ピクセルの値は、－１（白）または１（黒）とする。次に、登録用２値画像からコアおよび特徴点の位置を抽出し、コア位置を原点（０，０）として各特徴点の座標を計算する（Ｓ１００３）。更に抽出した特徴点に加え、ダミー特徴点としてランダムな座標を複数生成する（Ｓ１００４）。以下、本来の特徴点とダミー特徴点をまとめて特徴点と呼ぶことにする。次に登録用２値画像から各特徴点座標（Ｘｉ，Ｙｉ）（ｉ＝１，…，ｎ）を中心に所定のサイズ（ｗ×ｗピクセル）のチップ画像１２０１（ｇｉ）を切り出す（Ｓ１００５）。

【００６７】

次に各特徴点に対し、ランダムフィルタペア（Ｋｉ，Ｌｉ）を作成する（Ｓ１００６）。ここでＫｉをランダムフィルタ、Ｌｉを逆ランダムフィルタと呼ぶ。ランダムフィルタＫｉのサイズはＷ×Ｗピクセル（Ｗ≧ｗ）とし、前記第一の実施例と同様に各ピクセル値をランダムに生成する。またＫｉの各ピクセル値の逆数をとったものを逆ランダムフィルタＬｉとする。次に特徴点座標と逆ランダムフィルタの組１２０４（Ｘｉ，Ｙｉ，Ｌｉ）（ｉ＝１，…，ｎ）を携帯型記録媒体９２０に書き込む（Ｓ１００７）。

【００６８】

次に各チップ画像１２０１（gi）をランダムフィルタＫｉを用いて変換し、ランダム画像を作成する。具体的には、チップ画像１２０１（ｇｉ）の周りを０（灰色）でパディングしてＷ×Ｗピクセルに拡張し、これを基底変換（数論変換またはフーリエ変換）する。基底変換後の画像１２０２（Ｗ×Ｗピクセル）をＧｉとする。Ｇｉに対してランダムフィルタＫｉを各ピクセル毎に掛け合わせることで、ランダム画像１２０５（Ｇｉ・Ｋｉ）を作成する。これを各チップ画像ｇｉ（ｉ＝１，…，ｎ）に対して行う。作成したランダム画像Ｋｉ・Ｇｉ（ｉ＝１，…，ｎ）をサーバ９３０に送信する（Ｓ１００８）。

サーバ９３０はランダム画像Ｋｉ・Ｇｉを受け取り、これをテンプレートとして登録する（Ｓ１００９）。

【００６９】

次に、図１１および図１２を用いて本実施形態における指紋の認証処理動作を説明する。

まず、クライアント９００がユーザの指紋画像を取得する（Ｓ１１０１）。次に取得した指紋画像を２値化して、照合用２値画像１２１０を作成する（Ｓ１１０２）。ここで各ピクセルの値は、－１（白）または１（黒）とする。次に携帯型記録媒体９２０から特徴点座標と逆ランダムフィルタの組１２０４（Ｘｉ，Ｙｉ，Ｌｉ）（ｉ＝１，…，ｎ）を読み込む（Ｓ１１０３）。次に照合用２値画像から各特徴点座標（Ｘｉ，Ｙｉ）を中心とする周辺画像１２１１（ｆｉ）を切り出す（Ｓ１１０４）。周辺画像のサイズはＷ×Ｗピクセルとする。

次に周辺画像ｆｉを基底変換（数論変換またはフーリエ変換）した画像１２１２（Ｆｉ）と、逆ランダムフィルタＬｉとを、各ピクセル毎に掛け合わせることで、ランダム画像１２１４（Ｆｉ・Ｌｉ）を作成する。これを各周辺画像ｆｉ（ｉ＝１，…，ｎ）に対して行う。作成したランダム画像Ｆｉ・Ｌｉ（ｉ＝１，…，ｎ）をサーバ９３０に送信する（Ｓ１１０５）。

【００７０】

サーバ９３０は、ランダム画像Ｆｉ・Ｌｉを受け取り、テンプレート中の各ランダム画像Ｇｉ・Ｋｉと照合してチップ画像１２０１（ｇｉ）と周辺画像１２１１（ｆｉ）の一致／不一致を判定する。具体的にはランダム画像同士をピクセル毎に掛け合わせる。Ｌｉの

各ピクセル値はＫｉの各ピクセル値の逆数であったので、掛け合わせることで打ち消しあい、（Ｆｉ・Ｌｉ）・（Ｇｉ・Ｋｉ）＝Ｆｉ・Ｇｉとなる。これを逆基底変換（逆数論変換または逆フーリエ変換）し、ｆｉとｇｉの相関画像１２１５を得る。相関画像上の座標（ΔＸ，ΔＹ）におけるピクセル値は、チップ画像ｇｉを周辺画像ｆｉ上で（ΔＸ，ΔＹ）だけ平行移動して重ね合わせたときの相関値を表す。２値画像の各ピクセル値は－１（白）と１（黒）であったため、

相関値＝（白黒が一致したピクセル数）－（白黒が不一致のピクセル数）

＝２×（白黒が一致したピクセル数）－Ｗ×Ｗ

となる。

【００７１】

そこで相関画像上のピクセル値（相関値）の最大値を所定のしきい値と比較することで、２値画像ｆｉとｇｉの一致／不一致を判定することができる。このように各チップ画像、周辺画像の対毎に一致／不一致を判定し、一致した画像の数をカウントして類似度とする（Ｓ１１０６）。最後に類似度を所定の認証しきい値と比較し、認証しきい値以上なら指紋が一致したと判定し、認証しきい値未満なら不一致と判定する（Ｓ１１０７）。

【００７２】

以上のように、本実施形態の指紋認証によれば、指紋のチップ画像および周辺画像をランダムフィルタおよび逆ランダムフィルタにより攪乱してからサーバへ送信するため、サーバは元の画像を知ることができないにも拘わらず、相関値の計算が可能となる。これにより、ユーザはサーバに対して指紋を秘匿したまま指紋認証を受けることが可能となる。なお、第一の実施形態のように指紋画像全体を変換、照合する方法も考えられるが、指紋は指静脈と異なり歪みが生じやすいため、画像全体の相関に基づく照合では十分な認証精度が得られないことがある。これに対し、画像を局所的に見て一致／不一致を判定することで、歪みの影響を低減することができる。特に指紋の特徴点（端点または分岐点）周辺は特殊な構造を持つため、指紋の識別に好適である。

【００７３】

本実施形態においては、特徴点座標を記録しておく必要がある。特徴点座標はそれ自体が指紋を識別するのに有力な情報であり、一種の指紋情報であると言える。このため、クライアントから特徴点座標が漏洩した場合、指紋を偽造するための手がかりとなる可能性がある。そこで本実施形態では、ダミー特徴点を追加することによって、このような危険性を排除できる。ダミー特徴点のチップ画像は本人の指紋のみならず他人の指紋でも一致する確率が高いため、本来のチップ画像のみを使った場合と比較して本人／他人ともに一致チップ数（類似度）が増加するが、その分だけ認証しきい値を適切に増加させれば、精度が劣化することはない。

【００７４】

なお、本発明は、上記実施形態に限定されずに、更に種々変形して実施することができる。例えば、図１の例では、指静脈センサ１１０から個人の生体情報を採取して、クライアント１００内で登録画像及び照合画像を作成する等の処理を行う構成としている。しかし、他の変形例によれば、図１に示したクライアント１００内の諸機能１０１～１０５を指静脈センサ１１０と共に一体的に実装することにより生体デバイスを構成することも可能である。この構成の生体デバイスによれば、生体デバイスを携帯して、任意の時、場所で個人の生体情報を採取して個人認証に利用することができる。

なお、本発明は上記実施例に記載した指静脈や指紋による認証に限らず、手相や他の生体情報による認証にも適用できることは言うまでもない。

【図面の簡単な説明】

【００７５】

【図１】一実施形態におけるキャンセラブル指静脈認証システムの構成を示す図。

【図２】一実施形態における指静脈の登録処理および認証処理を示すフロー図。

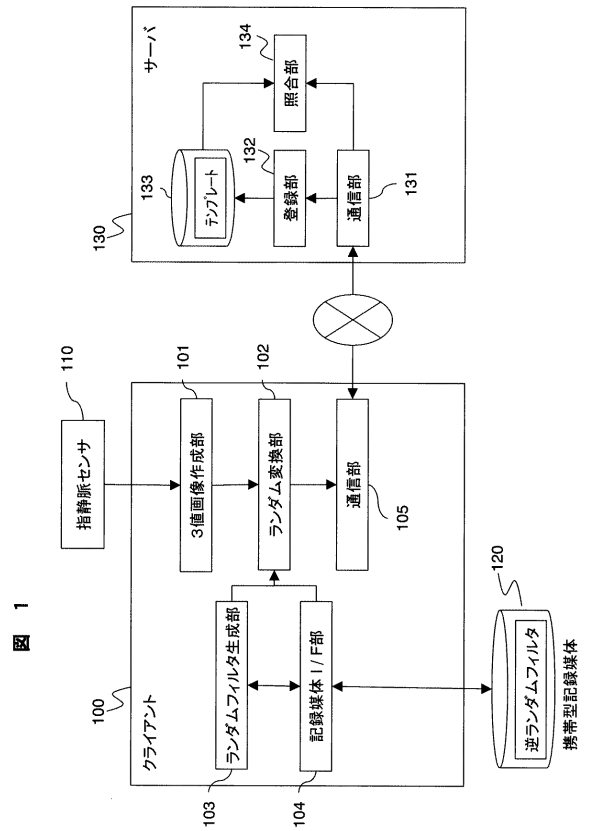
【図３】一実施形態におけるランダム変換の処理を示すフロー図。

【図４】他の例によるランダム変換の処理を示すフロー図。

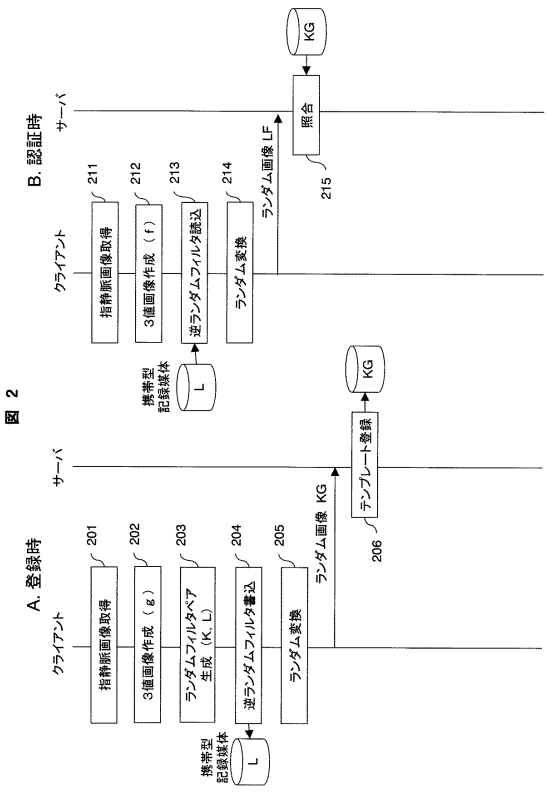
【図５】他の例によるランダム変換の処理を示すフロー図。
【図６】一実施形態における照合処理の詳細を示すフロー図。
【図７】一実施形態における復元困難性の向上理由を説明するための図。
【図８】一実施形態におけるテンプレート更新方法の処理を示すフロー図。
【図９】第二の実施形態におけるキャンセラブル指紋認証システムの構成を示す図。
【図１０】第二の実施形態における指紋の登録処理を示すフロー図。
【図１１】第二の実施形態における指紋の認証処理を示すフロー図。
【図１２】第二の実施形態における指紋の登録・認証処理の詳細を示すフロー図。
【符号の説明】
【００７６】

１００：クライアント　　１０１：３値画像作成部
１０２：ランダム変換部　　１０３：ランダムフィルタ生成部
１０４：記録媒体I/F部
１０５：通信部　　１１０：指静脈センサ
１２０：携帯型記録媒体　　１３０：サーバ
１３１：通信部　　１３２：登録部
１３３：記憶装置　　１３４：照合部

【図１】



【図２】



【図３】

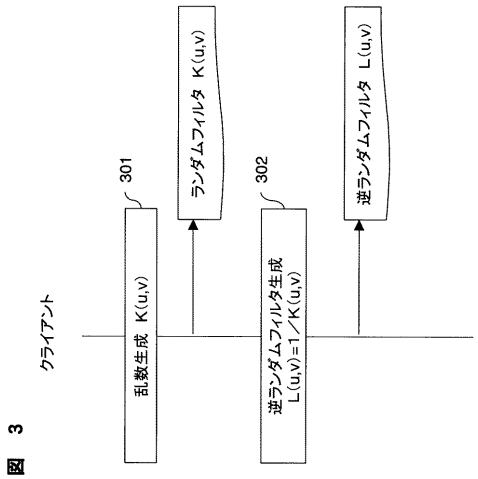


図 3
クライアント
乱数生成 K(u,v)
301
ランダムフィルタ K(u,v)
逆ランダムフィルタ生成
L(u,v)=1／K(u,v)
302
逆ランダムフィルタ L(u,v)

【図４】

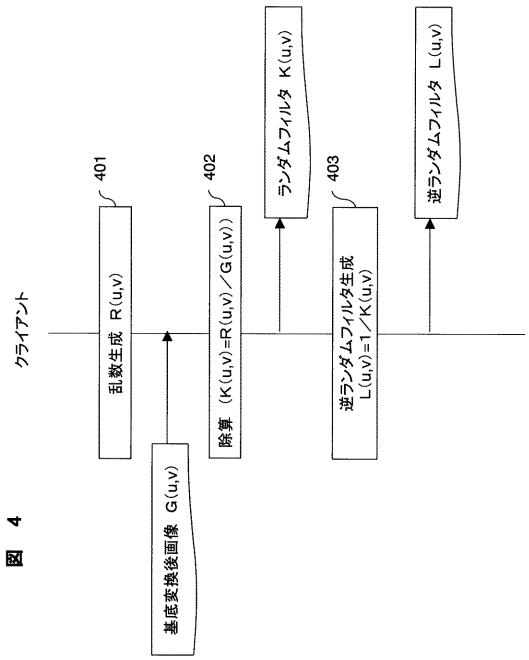


図 4
クライアント
乱数生成 R(u,v)
401
基底変換後画像 G(u,v)
除算 (K(u,v)=R(u,v)／G(u,v))
402
ランダムフィルタ K(u,v)
逆ランダムフィルタ生成
L(u,v)=1／K(u,v)
403
逆ランダムフィルタ L(u,v)

【図５】

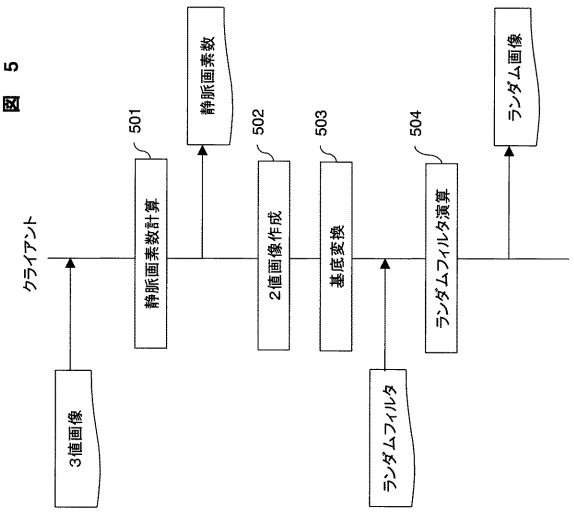


図 5
クライアント
3値画像
静脈画素数計算
501
静脈画素数
2値画像作成
502
基底変換
503
ランダムフィルタ
ランダムフィルタ演算
504
ランダム画像

【図６】

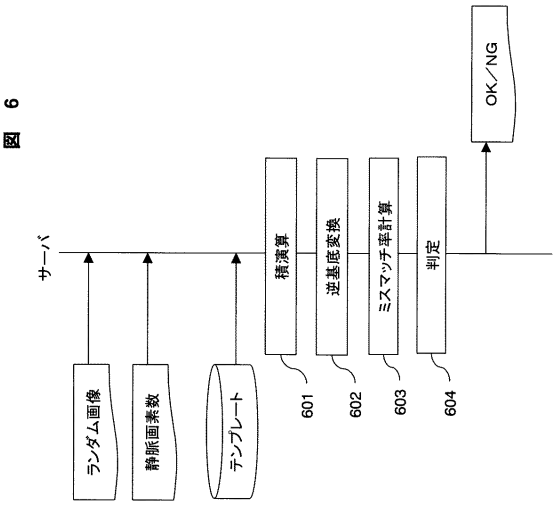


図 6
サーバ
ランダム画像
静脈画素数
テンプレート
積演算
601
逆基底変換
602
ミスマッチ率計算
603
判定
604
OK／NG

【図７】

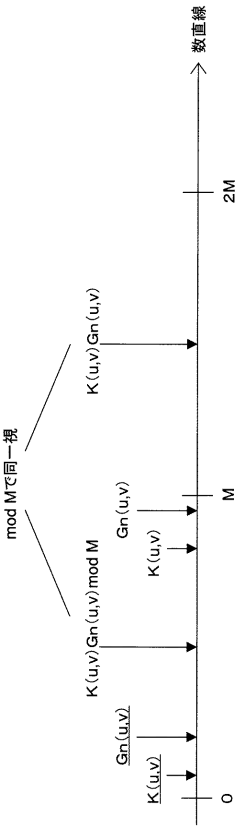


図 7

【図８】

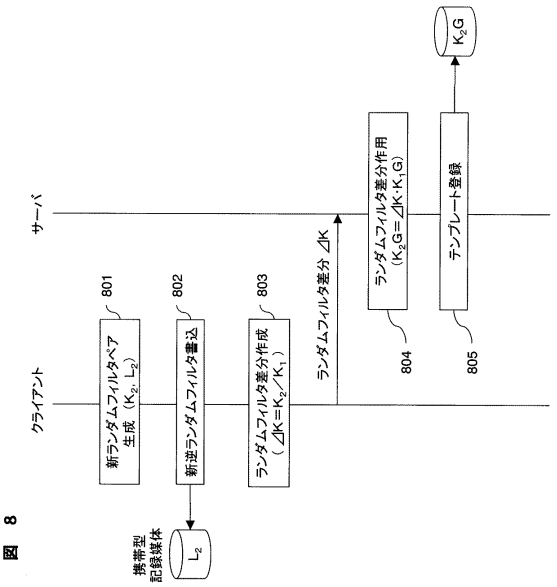


図 8

【図９】

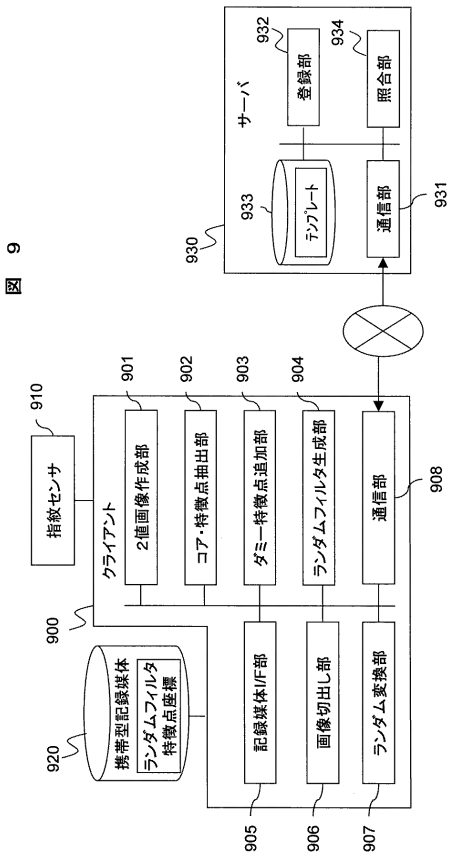


図 9

【図１０】

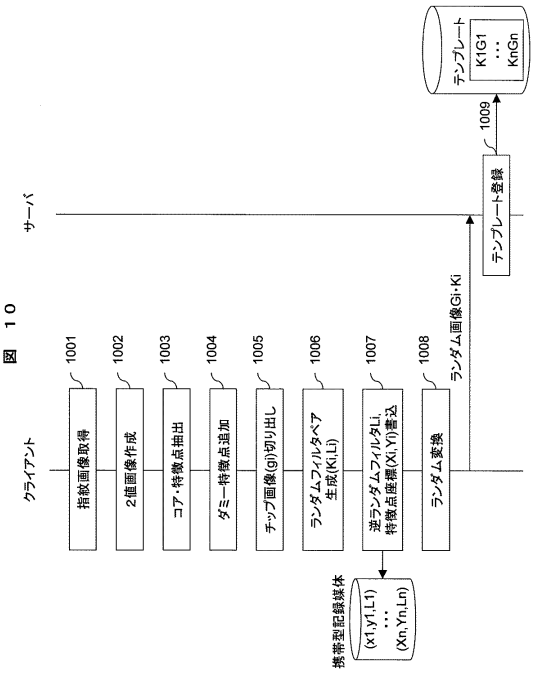


図 10

【図１１】

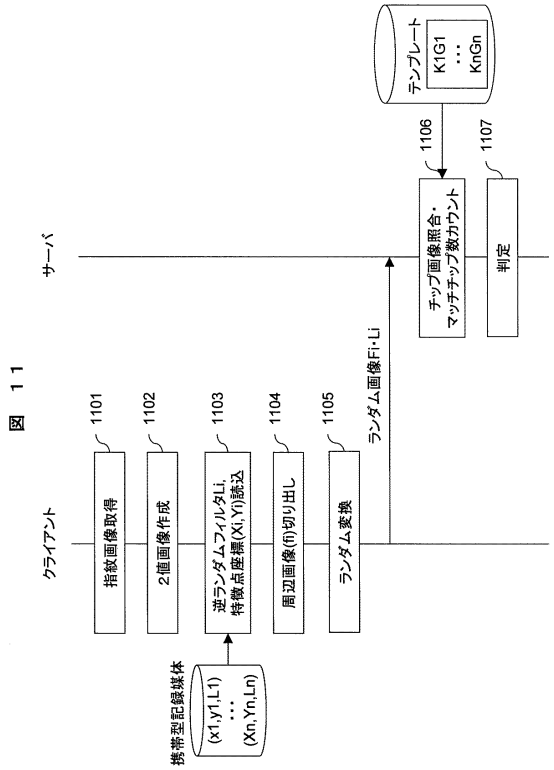


図 １１
サーバ
クライアント
テンプレート
K1G1
…
KnGn
1106
1107
チップ画像照合・
マッチチップ数カウント
判定
1101
指紋画像取得
1102
2値画像作成
1103
逆ランダムフィルタLi,
特徴点座標(Xi,Yi)読込
1104
周辺画像(fi)切り出し
1105
ランダム変換
ランダム画像Fi･Li
携帯型記録媒体
(x1,y1,L1)
…
(Xn,Yn,Ln)

【図１２】

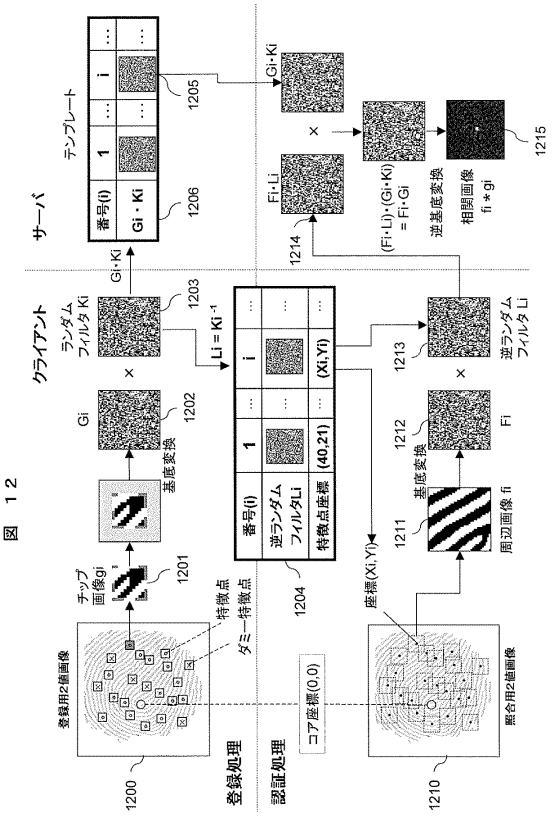


図 １２
サーバ
クライアント
テンプレート
番号(i)
Gi・Ki
1
…
i
1205
1206
Gi･Ki
ランダム
フィルタ Ki
1203
Li = Ki⁻¹
Gi
1202
基底変換
チップ
画像gi'
1201
番号(i)
逆ランダム
フィルタLi
特徴点座標
(40,21)
(Xi,Yi)
1204
特徴点
ダミー特徴点
登録用2値画像
1200
コア座標(0,0)
座標(Xi,Yi)
1211
基底変換
1212
Fi
周辺画像 fi
逆ランダム
フィルタ Li
1213
Fi･Li
1214
(Fi･Li)･(Gi･Ki)
= Fi･Gi
逆基底変換
相関画像
fi＊gi
1215
照合用2値画像
1210
登録処理
認証処理

フロントページの続き

(72)発明者　日野　英逸
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
(72)発明者　三村　昌弘
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内

審査官　新井　則和

(56)参考文献　特開２００４－２６６６４６（ＪＰ，Ａ）
特開平１１－２５０２６１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｔ　　７／００