(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6037366号
(P6037366)

(45)発行日　平成28年12月7日(2016.12.7)　(24)登録日　平成28年11月11日(2016.11.11)

(51)Int.Cl.　F I
H04L 9/32 (2006.01)　H04L 9/00 673D
G06F 21/32 (2013.01)　H04L 9/00 673C
G06F 21/32

請求項の数 14　(全 21 頁)

(21)出願番号　特願2015-550578 (P2015-550578)
(86)(22)出願日　平成26年3月4日 (2014.3.4)
(65)公表番号　特表2016-508323 (P2016-508323A)
(43)公表日　平成28年3月17日 (2016.3.17)
(86)国際出願番号　PCT/JP2014/056086
(87)国際公開番号　WO2014/142042
(87)国際公開日　平成26年9月18日 (2014.9.18)
審査請求日　平成27年6月30日 (2015.6.30)
(31)優先権主張番号　13/836,457
(32)優先日　平成25年3月15日 (2013.3.15)
(33)優先権主張国　米国 (US)

(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】暗号化したものに対応するユーザーを認証する方法及びバイオメトリックデータに対応するユーザーを認証するシステム

(57)【特許請求の範囲】

【請求項１】

バイオメトリックデータの識別的要素の整合性を用いて、前記バイオメトリックデータの登録ベクトルを暗号化したものに基づいて、前記バイオメトリックデータのプローブベクトルを暗号化したものに対応するユーザーを認証する方法であって、

特定のユーザー用の前記バイオメトリックデータの特定の識別的特徴の位置を指定するインジケーターベクトルを暗号化したものを記憶するステップと、

暗号化領域において、サーバーに記憶された登録ベクトルの識別的要素と、認証のために提示されたプローブベクトルの識別的要素との間の第１の距離を暗号化したものを求めるステップであって、前記登録ベクトルの前記識別的要素の位置及び前記プローブベクトルの前記識別的要素の位置は、前記インジケーターベクトルによって指定されたユーザーの前記識別的特徴の前記位置に対応するステップと、

前記暗号化領域において、前記サーバーに記憶された第１の整合性ベクトルの識別的要素と、前記認証のために提示された第２の整合性ベクトルの識別的要素との間の第２の距離を暗号化したものを求めるステップと、

前記第１の距離及び前記第２の距離を暗号化したものに基づいて前記バイオメトリックデータのプローブベクトルを暗号化したものに対応するユーザーを認証するステップと、

を含み、前記方法のステップは、プロセッサを用いることによって実行される、バイオメトリックデータの識別的要素の整合性を用いて、前記バイオメトリックデータの登録ベクトルを暗号化したものに基づいて、前記バイオメトリックデータのプローブベクトルを暗

号化したものに対応するユーザーを認証する方法。
【請求項２】
前記認証することは、前記第１の距離及び前記第２の距離を前記暗号化したものを認証サーバーに送信することを含む、請求項１に記載の方法。
【請求項３】
前記第１の距離及び前記第２の距離は、準同型成分の線形結合として表される距離関数に従って求められ、前記方法は、
前記登録ベクトル、前記インジケーターベクトル、及び前記第１の整合性ベクトルを暗号化したものの代数結合の第１のセットを記憶することと、
前記プローブベクトル及び前記第２の整合性ベクトルを暗号化したものの代数結合の第２のセットを受信することと、
前記第１の距離の準同型成分の第１の線形結合及び前記第２の距離の準同型成分の第２の線形結合を生成するように前記第１のセットの前記代数結合を結合し、及び前記第２のセットの前記代数結合を結合することであって、前記結合することは、準同型特性を用いて前記暗号化領域において実行されることと、
前記第１の線形結合の前記準同型成分を結合することであって、前記第１の距離を前記暗号化したものを生成することと、
前記第２の線形結合の前記準同型成分を結合することであって、前記第２の距離を前記暗号化したものを生成することと、
を更に含む、請求項１に記載の方法。
【請求項４】
前記バイオメトリックデータは、指紋用、虹彩用、又は顔用のものである、請求項１に記載の方法。
【請求項５】
バイオメトリックデータを暗号化したものを認証する方法であって、前記方法のステップを実行するためのプロセッサを含み、前記方法は、
登録ベクトルを暗号化したものを記憶するステップであって、前記登録ベクトルの要素は、前記バイオメトリックデータの特徴を含むステップと、
前記バイオメトリックデータの識別的特徴の位置を指定するインジケーターベクトルを暗号化したものを記憶するステップと、
前記登録ベクトル内の対応する要素が複数の測定にわたって不変である確率に比例した大きさを有する要素からなる第１の整合性ベクトルを暗号化したものを記憶するステップと、
前記バイオメトリックデータの認証のために提示されたプローブベクトルを暗号化したものを受信するステップと、
前記プローブベクトル内の対応する要素が複数の測定にわたって不変である確率に比例した大きさを有する要素からなる第２の整合性ベクトルを暗号化したものを受信するステップと、
暗号化領域において、前記登録ベクトルの識別的要素と前記プローブベクトルの識別的要素との間の第１の距離を暗号化したものを求めるステップであって、前記登録ベクトルの前記識別的要素の位置及び前記プローブベクトルの前記識別的要素の位置は、前記インジケーターベクトルによって指定されたユーザーの前記識別的特徴の前記位置に対応するステップと、
前記暗号化領域において、前記第１の整合性ベクトルの識別的要素と前記第２の整合性ベクトルの識別的要素との間の第２の距離を暗号化したものを求めるステップであって、前記第１の整合性ベクトルの前記識別的要素の位置及び前記第２の整合性ベクトルの前記識別的要素の位置は、前記インジケーターベクトルによって指定された前記ユーザーの前記特徴の前記位置に対応するステップと、
前記第１の距離及び前記第２の距離に基づいて前記バイオメトリックデータを認証するステップと、

を含む、請求項１に記載の方法。
【請求項６】
前記認証することは、前記第１の距離及び前記第２の距離を前記暗号化したものを認証サーバーに送信することを含む、請求項５に記載の方法。
【請求項７】
前記認証することは、
前記第１の距離を第１の閾値と比較することと、
前記第２の距離を第２の閾値と比較することと、
前記第１の距離が前記第１の閾値よりも小さく、前記第２の距離が前記第２の閾値よりも小さい場合には、肯定的な認証を決定することと、
を含む、請求項５に記載の方法。
【請求項８】
前記第１の距離及び前記第２の距離を解読することを更に含む、請求項５に記載の方法。
【請求項９】
前記認証することは、
前記第１の距離及び前記第２の距離を前記暗号化したものを認証サーバーに送信することと、
前記第１の距離及び前記第２の距離を前記認証サーバーによって解読することと、
前記第１の距離が第１の閾値よりも小さく、前記第２の距離が第２の閾値よりも小さい場合には、前記認証サーバーによって肯定的な認証を決定することと、
を含む、請求項５に記載の方法。
【請求項１０】
前記登録ベクトル、前記プローブベクトル、前記インジケーターベクトル、前記第１の整合性ベクトル、及び前記第２の整合性ベクトルは、準同型暗号化の公開鍵を用いて暗号化され、前記方法は、
準同型特性を用いて前記暗号化領域において前記第１の距離及び前記第２の距離を前記暗号化したものを求めること、
を更に含む、請求項５に記載の方法。
【請求項１１】
前記第１の距離及び前記第２の距離は、準同型成分の線形結合として表される距離関数に従って求められ、前記方法は、
前記登録ベクトル、前記インジケーターベクトル、及び前記第１の整合性ベクトルを暗号化したものの代数結合の第１のセットを記憶することと、
前記プローブベクトル及び前記第２の整合性ベクトルを暗号化したものの代数結合の第２のセットを受信することと、
前記第１の距離の準同型成分の第１の線形結合及び前記第２の距離の準同型成分の第２の線形結合を生成するように前記第１のセットの前記代数結合を結合し、及び前記第２のセットの前記代数結合を結合することであって、前記結合することは、準同型特性を用いて前記暗号化領域において実行されることと、
前記第１の距離を前記暗号化したものを生成するように、前記第１の線形結合の前記準同型成分を結合することと、
前記第２の距離を前記暗号化したものを生成するように、前記第２の線形結合の前記準同型成分を結合することと、
を更に含む、請求項５に記載の方法。
【請求項１２】
前記代数結合の第１のセットは、Ｅ（ｖｉ）、Ｅ（－２ｖｉｙｉ）、Ｅ（ｙｉ２）、Ｅ（－２ｖｉｒｉ）、及びＥ（ｒｉ２）を含み、ここで、ｉ＝１，２，．．．，Ｎであり、Ｅ（．）は、２次準同型性の暗号化関数であり、ｙ＝（ｙ１，ｙ２，．．．，ｙＮ）は、前記登録ベクトルであり、ｖ＝（ｖ１，ｖ２，．．．，ｖＮ）は、前記インジケーターベ

クトルであり、ｒ＝（ｒ１，ｒ２，．．．，ｒＮ）は、前記第１の整合性ベクトルであり、前記代数結合の第２のセットは、Ｅ（ｘｉ２）、Ｅ（ｘｉ）、Ｅ（ｓｉ２）、及びＥ（ｓｉ）を含み、ｘ＝（ｘ１，ｘ２，．．．，ｘＮ）は、前記プローブベクトルであり、ｓ＝（ｓ１，ｓ２，．．．，ｓＮ）は、前記第２の整合性ベクトルであり、前記方法は、

前記第１の距離

【数１】

$$D(\mathbf{x},\mathbf{y})=\sum_{i=1}^{N}v_i(x_i-y_i)^2$$

を前記暗号化したものを、

【数２】

$$\prod_{i=1}^{N}F(v_ix_i^2)F(-2v_ix_iy_i)F(v_iy_i^2)=\prod_{i=1}^{N}F(v_ix_i^2-2v_ix_iy_i+v_iy_i^2)$$

$$=F\left(\sum_{i=1}^{n}v_ix_i^2-2v_ix_iy_i+v_iy_i^2\right)=F(D(\mathbf{x},\mathbf{y}))$$

に従って求めることであって、ｅ（Ｅ（ｖｉ），Ｅ（ｘｉ２））＝Ｆ（ｖｉｘｉ２）であり、ｅ（Ｅ（－２ｖｉｙｉ），Ｅ（ｘｉ））＝Ｆ（－２ｖｉｘｉｙｉ）であり、ｅ（Ｅ（ｖｉ），Ｅ（ｙｉ２））＝Ｆ（ｖｉｙｉ２）であり、ｅ（．，．）は、前記関数ｅ（．，．）の２つの暗号化されたパラメーターの積の可逆関数Ｆ（．）を生成する前記２次準同型性の関数であることと、

前記第２の距離

【数３】

$$D(\mathbf{r},\mathbf{s})=\sum_{i=1}^{N}v_i(r_i-s_i)^2$$

を前記暗号化したものを、

【数４】

$$\prod_{i=1}^{N}F(v_ir_i^2)F(-2v_ir_is_i)F(v_is_i^2)=\prod_{i=1}^{N}F(v_ir_i^2-2v_ir_is_i+v_is_i^2)$$

$$=F\left(\sum_{i=1}^{N}v_ir_i^2-2v_ir_is_i+v_is_i^2\right)=F(D(\mathbf{r},\mathbf{s}))$$

に従って求めることであって、ｅ（Ｅ（ｖｉ），Ｅ（ｒｉ２））＝Ｆ（ｖｉｒｉ２）であり、ｅ（Ｅ（－２ｖｉｓｉ），Ｅ（ｒｉ））＝Ｆ（－２ｖｉｒｉｓｉ）であり、ｅ（Ｅ（ｖｉ），Ｅ（ｓｉ２））＝Ｆ（ｖｉｓｉ２）であることと、

を更に含む、請求項１１に記載の方法。

【請求項１３】

バイオメトリックデータに対応するユーザーを認証するシステムであって、

データベースサーバーであって、特定のユーザー用の前記バイオメトリックデータの特定の識別的特徴の位置を指定するインジケーターベクトルを暗号化したものを記憶し、暗号化領域において、前記サーバーに記憶された登録ベクトルの識別的要素と、認証のために提示されたプローブベクトルの識別的要素との間の第１の距離を暗号化したものを求めるとともに、ここで、前記登録ベクトルの前記識別的要素の位置及び前記プローブベクトルの前記識別的要素の位置は、前記インジケーターベクトルによって指定されたユーザーの前記識別的特徴の前記位置に対応し、前記暗号化領域において、前記サーバーに記憶された第１の整合性ベクトルの識別的要素と、前記認証のために提示された第２の整合性ベ

クトルの識別的要素との間の第２の距離を暗号化したものを求めるデータベースサーバーと、
前記プローブベクトルを暗号化したもの及び前記第２の整合性ベクトルを暗号化したものを求めるとともに、前記プローブベクトル及び前記第２の整合性ベクトルを前記暗号化したものを前記データベースサーバーに送信するアクセス制御デバイスと、
前記データベースサーバーから受信された前記第１の距離及び前記第２の距離を前記暗号化したものを解読するとともに、前記第１の距離及び前記第２の距離と少なくとも１つの閾値との比較に基づいて前記バイオメトリックデータを認証する認証サーバーと、
を備える、バイオメトリックデータに対応するユーザーを認証するシステム。
【請求項１４】
前記データベースサーバーは、前記登録ベクトルを暗号化したものを記憶し、前記登録ベクトルの要素は、前記バイオメトリックデータの特徴を含み、前記データベースサーバーは、前記登録ベクトルの各要素の整合性を指定する前記第１の整合性ベクトルを暗号化したものを記憶する、請求項１３に記載のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、包括的には、ユーザーのセキュアな認証に関し、より詳細には、ユーザーのバイオメトリックデータを暗号化したものを認証することに関する。
【背景技術】
【０００２】
バイオメトリック認証は、実用化されている指紋、静脈、顔画像、及び虹彩等の身体部分の特徴に基づいて認証を行う。バイオメトリック認証は、通常、登録段階及び認証段階を用いる。登録段階の間、ユーザーのバイオメトリックデータが取得され、データベースに記憶される。検証段階の間、認証を要求するユーザーのバイオメトリックデータが、記憶されたバイオメトリックデータと比較される。一致するものがある場合、ユーザーはアクセスを許可される。
【０００３】
バイオメトリック認証を達成するために考慮すべき事項のうちの１つは、登録段階において得られたバイオメトリックデータの同じ特徴を認証段階において得ることができるか否かである。例えば、手のひら静脈に基づくバイオメトリック認証では、登録時にユーザーの手のひらの右上部分の手のひら静脈の特徴を取得して記憶し、認証時にその手のひらの左下部分の手のひら静脈の特徴を取得することによって、高精度の認証を行うことができる。特許文献１は、バイオメトリック認証のための１つの方法を記載している。
【０００４】
加えて、セキュアな方法で認証を行うことが必要とされることもあり得る。例えば、登録されたユーザーのバイオメトリックデータは、多くの場合、第三者によって解析及び記憶される。プライベートなバイオメトリックデータがこの第三者に暴露されないことが重要である。同様に、認証のために提示されたバイオメトリックデータのプライバシーも保護されるべきである。
【０００５】
多くの場合、暗号化された信号に適用される関数の結果をセキュアに求めることが必要とされる。例えば、最小２乗誤差／重み付き２乗誤差又はハミング距離等の様々な関数を用いて、２つの暗号化された信号間の距離を測定することができる。次に、２つの信号間の距離は、様々な認証目的に広く用いられる。この問題は、多くの場合、セキュアマルチパーティ計算（ＳＭＣ：ｓｅｃｕｒｅ ｍｕｌｔｉｐａｒｔｙ ｃｏｍｐｕｔａｔｉｏｎ）として定義される。紛失通信（ＯＴ：ｏｂｌｉｖｉｏｕｓ ｔｒａｎｓｆｅｒ）、セキュア内積（ＳＩＰ：ｓｅｃｕｒｅ ｉｎｎｅｒ ｐｒｏｄｕｃｔ）等の計算的にセキュアな方法をプリミティブとして用いて、より複雑な演算を行うことができる。特許文献２は、そのような方法を記載している。

【先行技術文献】
【特許文献】
【０００６】
【特許文献１】米国特許第８，２６４，３２５号明細書
【特許文献２】米国特許出願公開第２０１１／００５２９３号明細書
【発明の概要】
【発明が解決しようとする課題】
【０００７】
したがって、ユーザーのバイオメトリックデータを暗号化したものを認証する方法が必要とされている。
【課題を解決するための手段】
【０００８】
本発明の幾つかの実施の形態は、認証を援助するのにバイオメトリックデータの識別的特徴（ｄｉｓｃｒｉｍｉｎａｔｉｖｅ　ｆｅａｔｕｒｅ）を用いることができるという認識に基づいている。プライバシーを保護するために、様々な実施の形態では、識別可能な特徴の位置が暗号化される。しかしながら、幾つかの状況では、識別可能な特徴の位置の暗号化は、完全にセキュアというわけではない。例えば、敵対者が、正当なユーザーの値と同様の要素を十分多く生成した場合、その敵対者は、誤って認証を受けることができる。
【０００９】
誤った認証の可能性を最小にするために、様々な実施の形態は、識別的特徴の整合性（ｃｏｎｓｉｓｔｅｎｃｙ）を利用する。幾つかの実施の形態では、識別的特徴の整合性は、整合性ベクトルによって表される。この整合性ベクトルは、特徴ベクトル内の対応する要素が複数の測定にわたって不変である確率に比例した大きさを有する要素からなるベクトルである。特徴ベクトルの要素及び整合的ベクトルの要素の間のそのような相関は、バイオメトリックデータの識別的要素のロケーションと異なり、セキュアなプロトコルにおいて敵対者による利用がより困難である。
【００１０】
幾つかの実施の形態は、次の知見に基づいている。定義によれば、第ｉのバイオメトリック特徴、すなわち、ユーザー（アリス）のバイオメトリックデータから抽出された第ｉの要素に対応する特徴が識別可能である場合、この第ｉのバイオメトリック特徴は、このユーザーのバイオメトリックデータの複数の測定において再現することができ、ほとんどの詐称者の測定においてその値の範囲にわたってほぼ一様な分布を有する。これは、アリスの第ｉのバイオメトリック特徴の整合性r_iが、ほとんどの詐称者の第ｉのバイオメトリック特徴の整合性よりも大きいことを意味する。したがって、この整合性における距離は、敵対者がアクセスを得ることを防止するのに利用することができる。
【００１１】
様々な実施の形態では、登録されたユーザーの第ｉのバイオメトリック特徴の整合性は、データベースサーバー上で、暗号化された形態で記憶されている。認証のために提示された第ｉのバイオメトリック特徴の整合性は、例えばアクセス制御デバイスによって認証の間に求められる。
【００１２】
そのため、登録段階の間に記憶されたバイオメトリックデータの特徴を表すベクトルと、認証のために提示されたバイオメトリックデータの特徴を表すベクトルとの間の距離を暗号化領域において比較することに加えて、様々な実施の形態は、バイオメトリックデータの識別的特徴の整合性も暗号化領域において比較する。
【００１３】
したがって、１つの実施の形態は、バイオメトリックデータを暗号化したものを認証する方法を開示し、この方法は、方法のステップを実行するためのプロセッサを含む。この方法は、登録ベクトルを暗号化したものを記憶するステップであって、この登録ベクトル

の要素は、バイオメトリックデータの特徴を含むステップと、バイオメトリックデータの識別的特徴の位置を指定するインジケーターベクトルを暗号化したものを記憶するステップと、登録ベクトル内の対応する要素が複数の測定にわたって不変である確率に比例した大きさを有する要素からなる第１の整合性ベクトルを暗号化したものを記憶するステップと、バイオメトリックデータの認証のために提示されたプローブベクトルを暗号化したものを受信するステップと、プローブベクトル内の対応する要素が複数の測定にわたって不変である確率に比例した大きさを有する要素からなる第２の整合性ベクトルを暗号化したものを受信するステップと、暗号化領域において、登録ベクトルの識別的要素とプローブベクトルの識別的要素との間の第１の距離を暗号化したものを求めるステップであって、登録ベクトルの識別的要素の位置及びプローブベクトルの識別的要素の位置は、インジケーターベクトルによって指定されたユーザーの識別的特徴の位置に対応するステップと、暗号化領域において、第１の整合性ベクトルの識別的要素と第２の整合性ベクトルの識別的要素との間の第２の距離を暗号化したものを求めるステップであって、第１の整合性ベクトルの識別的要素の位置及び第２の整合性ベクトルの識別的要素の位置は、インジケーターベクトルによって指定されたユーザーの特徴の位置に対応するステップと、第１の距離及び第２の距離に基づいてバイオメトリックデータを認証するステップと、を含む。認証することは、第１の距離及び第２の距離を暗号化したものを認証サーバーに送信すること、を含むことができる。

【００１４】

別の実施の形態は、バイオメトリックデータの識別的要素の整合性を用いて、このバイオメトリックデータの登録ベクトルを暗号化したものに基づいて、バイオメトリックデータのプローブベクトルを暗号化したものに対応するユーザーを認証する方法を開示する。この方法は、特定のユーザー用のバイオメトリックデータの特定の識別的特徴の位置を指定するインジケーターベクトルを暗号化したものを記憶するステップと、暗号化領域において、サーバーに記憶された登録ベクトルの識別的要素と、認証のために提示されたプローブベクトルの識別的要素との間の第１の距離を暗号化したものを求めるステップであって、登録ベクトルの識別的要素の位置及びプローブベクトルの識別的要素の位置は、インジケーターベクトルによって指定されたユーザーの識別的特徴の位置に対応するステップと、暗号化領域において、サーバーに記憶された第１の整合性ベクトルの識別的要素と、認証のために提示された第２の整合性ベクトルの識別的要素との間の第２の距離を暗号化したものを求めるステップと、第１の距離及び第２の距離を暗号化したものに基づいてバイオメトリックデータのプローブベクトルを暗号化したものに対応するユーザーを認証するステップと、を含む。この方法のステップは、プロセッサを用いることによって実行される。

【００１５】

また別の実施の形態は、バイオメトリックデータに対応するユーザーを認証するシステムを開示する。このシステムは、データベースサーバーであって、特定のユーザー用のバイオメトリックデータの特定の識別的特徴の位置を指定するインジケーターベクトルを暗号化したものを記憶し、暗号化領域において、このサーバーに記憶された登録ベクトルの識別的要素と、認証のために提示されたプローブベクトルの識別的要素との間の第１の距離を暗号化したものを求めるとともに、ここで、登録ベクトルの識別的要素の位置及びプローブベクトルの識別的要素の位置は、インジケーターベクトルによって指定されたユーザーの識別的特徴の位置に対応し、暗号化領域において、このサーバーに記憶された第１の整合性ベクトルの識別的要素と、認証のために提示された第２の整合性ベクトルの識別的要素との間の第２の距離を暗号化したものを求めるデータベースサーバーと、プローブベクトルを暗号化したもの及び第２の整合性ベクトルを暗号化したものを求めるとともに、プローブベクトル及び第２の整合性ベクトルを暗号化したものをデータベースサーバーに送信するアクセス制御デバイスと、データベースサーバーから受信された第１の距離及び第２の距離を暗号化したものを解読するとともに、第１の距離及び第２の距離と少なくとも１つの閾値との比較に基づいてバイオメトリックデータを認証する認証サーバーと、

を備える。
【図面の簡単な説明】
【００１６】
【図１】本発明の実施の形態によるユーザーのバイオメトリックデータを暗号化したものを認証するための方法のブロック図である。
【図２】本発明の実施の形態によるバイオメトリックデータを暗号化したものを、ユーザーの登録中にサーバーに記憶するための方法のブロック図である。
【図３】本発明の実施の形態によるバイオメトリックデータを暗号化したものを、バイオメトリックデータの認証中にサーバーで受信するための方法のブロック図である。
【図４】本発明の実施の形態による認証のために提示されたデータとサーバーに記憶されたデータとの間の距離を求めるための方法のブロック図である。
【図５】本発明の実施の形態による準同型成分の線形結合として表された距離関数の暗号化結果をセキュアに求めるための方法の図である。
【図６】本発明の実施の形態によるバイオメトリックデータを認証するための方法のブロック図である。
【発明を実施するための形態】
【００１７】
図１は、本発明の幾つかの実施の形態によるバイオメトリックデータ１０５を暗号化したものを認証するための認証方法及びシステム１００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の形態は、システム１００の１つ又は幾つかのモジュールを用いる。
【００１８】
これらのモジュールは、認証を受けようとするユーザーのバイオメトリックデータ１０５を取得して、公開鍵１４０を用いて暗号化するアクセス制御デバイス１１０を含むことができる。このアクセス制御デバイスは、暗号化されたバイオメトリックデータ１１５をデータベースサーバー１２０に送信する。データベースサーバー１２０は、公開鍵１４０を用いて暗号化されたバイオメトリックデータのユーザー固有の登録ベクトルを記憶する。この登録ベクトルの要素は、バイオメトリックデータの特徴を含む。
【００１９】
サーバー１２０は、暗号化されたバイオメトリックデータ１１５とサーバーに記憶されたバイオメトリックデータとの間の、暗号化領域における距離を求める。その結果得られた距離１２５は、認証判定１３５を下すための認証サーバー１３０に送信される。この認証サーバーは、距離を解読するための秘密鍵１４５にアクセスできる。公開鍵１４０及び秘密鍵１４５は、準同型暗号化の公開鍵／秘密鍵ペアを形成している。
【００２０】
本方法及び本システムは、ユーザーがデータベースに記憶されたバイオメトリックデータのいずれも発見することがないことを確実にすることによってプライバシーを保護する。データベース及び認証サーバーは、ユーザーのバイオメトリックデータを発見せず、ユーザーになりすました外部の敵対者は、データベースに記憶された特徴バイオメトリックデータを発見することができない。
【００２１】
認証の性能を改善するために、幾つかの実施の形態は、認証のために提示されたバイオメトリックデータの識別的特徴及び整合的特徴（ｃｏｎｓｉｓｔｅｎｔ　ｆｅａｔｕｒｅ）を考慮に入れる。プライバシーを保護するために、様々な実施の形態は、暗号化領域における識別的特徴及び整合的特徴を考慮に入れる。これらの実施の形態は、識別的特徴及び整合的特徴のロケーションを敵対者から隠蔽し、敵対者が整合的特徴を利用して、認可されていないアクセスを得ることを可能にしないことによって認証性能を改善する。
【００２２】
記号及び術語
対象となる数学記号を以下の表に示す。

【００２３】
【表１】

名称	記号及び数式
認証時に提示されるプローブベクトル。プローブベクトルの要素は、ユーザーのバイオメトリックデータの特徴を含むことができる。これらの要素は、個々に暗号化することができる整数又はビットとすることができる。	$\mathbf{x}=(x_1,x_2,...,x_N)$
データベースサーバー上にセキュアに記憶され、比較に用いられる登録ベクトル。同様に、登録ベクトルの要素も、バイオメトリックデータの特徴を含み、個々に暗号化することができる整数又はビットとすることができる。	$\mathbf{y}=(y_1,y_2,...,y_N)$
バイオメトリックデータの識別的特徴の位置を指定するインジケーターベクトル。インジケーターベクトルは、識別的特徴の位置に「１」のエントリーを有する２進数とすることができる。	$\mathrm{v}=(v_1,v_2,...,v_N)$
登録ベクトルの各要素の整合性を指定する第１の整合性ベクトル。このベクトルは、暗号化された形態でサーバーに記憶することができる。このベクトルの要素は、整数とすることができる。	$r=(r_1,r_2,...,r_N)$
プローブベクトルの各要素の整合性を指定する第２の整合性ベクトル。このベクトルは、正当なユーザー又は敵対者から暗号化された形態でサーバーにおいて受信することができる。	$s=(s_1,s_2,...,s_N)$
認証時に提示されたプローブベクトルとデータベースサーバー上にセキュアに記憶された登録ベクトルとの間の距離。ベクトル要素が整数であるとき、この距離は、これらのベクトル間のユークリッド距離の２乗を表す。ベクトル要素が０又は１であるとき、これは、これらのベクトル間のハミング距離を表す。他の距離尺度も可能である。	$d(\mathbf{x},\mathbf{y})=\sum_{i=1}^{N}(x_i-y_i)^2$
プローブベクトルの識別的要素と登録ベクトルの識別的要素との間の距離。	$D(\mathbf{x},\mathbf{y})=\sum_{i=1}^{N}v_i(x_i-y_i)^2$
第１の整合性ベクトルの識別的要素と第２の整合性ベクトルの識別的要素との間の距離。	$D(\mathbf{r},\mathbf{s})=\sum_{i=1}^{N}v_i\,(r_i-s_i)^2$
少なくとも１つの乗算及び多数の加算を可能にする２次準同型特性を有する暗号化関数。	$e\big(E(a),E(b)\big)=F(ab)$ $F(ab)F(cd)=F(ab+cd)$

【００２４】
性能尺度
幾つかの実施の形態では、認証システムの性能は、以下のメトリックを用いて測定される。
１．本人拒否の確率、すなわち、本人拒否率（ＦＲＲ：ｆａｌｓｅ　ｒｅｊｅｃｔｉｏｎ　ｒａｔｅ）。これは、アリスのバイオメトリックデータの特徴ベクトルが与えられているが、システムが認証に失敗する確率である。例えば、これは、アリスの登録ベクトルとプローブベクトルとの間の距離が所定の閾値よりも大きい場合に起こる。
２．他人受入の確率、すなわち、他人受入率（ＦＡＲ：ｆａｌｓｅ　ａｃｃｅｐｔａｎｃｅ　ｒａｔｅ）。これは、アリス以外のユーザーの特徴ベクトルが与えられているが、システムがアリスの特徴ベクトルと一致すると判断する確率である。例えば、これは、アリスの登録ベクトルとデータベース内の他の任意のユーザーのプローブベクトルとの間の距離が所定の閾値未満である場合に起こる。

【００２５】
ユーザーの所与のデータベースについて、ＦＲＲの値及びＦＡＲの値は、上記で説明した距離閾値に依存する。小さな距離閾値を用いるほど、ＦＡＲは低減するが、ＦＲＲは増加する。大きな距離閾値を用いるほど、ＦＲＲは低減するが、ＦＡＲは増加する。或る値の範囲にわたって距離閾値を掃引することによって、ＦＲＲ対ＦＡＲの曲線が得られる。ＦＲＲがＦＡＲに等しい曲線上の点は、等誤り率（ＥＥＲ：ｅｑｕａｌ　ｅｒｒｏｒ　ｒａｔｅ）と呼ばれる。認証システムの設計者の目標は、可能な最小のＥＥＲを有することである。

【００２６】
識別的特徴
ほとんどのバイオメトリックデータ抽出アルゴリズムでは、真正一致を確認する際、及び誤一致を拒否する際に、幾つかの特徴が他の特徴よりも有用である。そのような特徴は、システムが、真正なユーザーと詐称者とをより良好に識別することを可能にするので、より「識別的」であると言われる。例えば、指紋照合では、特徴点（ｍｉｎｕｔｉａｅ　ｐｏｉｎｔｓ）に基づく特徴が、隆線波長（ｒｉｄｇｅ　ｗａｖｅｌｅｎｇｔｈｓ）に基づく特徴よりも識別的であることが分かっている。

【００２７】
登録されたユーザーの特徴ベクトルを構築するときには、最も識別的な特徴を用いることが望ましい。アリスの特徴ベクトルの要素が識別的である場合、それらの要素の比較の結果、アリスについて低いＦＲＲ及び低いＦＡＲを得ることができる。しかしながら、識別的特徴は、多くの場合、ユーザーごとに変化する。そのため、例えば、アリスの場合、指の中心から抽出された特徴が最も識別的である場合があるが、ボブの場合、指の側面から抽出された特徴が最も識別的である場合がある。そのため、データベースに登録された全てのユーザー用の共通の識別的特徴のセットと比べて、特定のユーザー用の特定の識別的特徴を用いることが望ましい。

【００２８】
識別的特徴は、ＦＡＲ対ＦＲＲのトレードオフの改善に有用であるが、識別的特徴は、実際のシステム設計に２つの難題を呈する可能性がある。第１に、登録された人物からの複数のサンプルを収集することができ、これらの特徴ベクトルの統計的解析が実行される登録時にしか、識別的特徴は求めることができない。認証時には、照会人物からの１つの特徴ベクトルしか利用可能でない。第２に、識別的特徴のロケーションがプライバシーセンシティブである。詐称者ボブがアリスの識別的特徴のロケーションを見つけ出した場合、ボブは、この情報を用いて人工的な特徴ベクトルの合成を試みることができる。

【００２９】
整合的特徴
測定ごとに実質的に変化しないバイオメトリックデータの特徴は、整合的特徴とみなされる。これらの整合的特徴は、経時的に取得された測定について再現性があり、ＦＲＲを低くすることに寄与する。実施の形態によって用いられる或るバイオメトリックデータ抽出方法では、実数値又は整数値の信号が閾値（又は閾値のベクトル）と比較され、２進数又は整数値の特徴が提供される。そのような抽出方法は、結果として得られた特徴ベクトルがデータベースに記憶される前又は認証のためにデータベースに送信される前に暗号化されるシステムにとって有利である可能性がある。この場合、整合性は、閾値点（複数の場合もある）とバイオメトリックデータの値との間の絶対距離に依存し得る。具体的には、距離が大きいほど、特徴が異なる値に量子化される確率が小さくなり、そのため、特徴はより整合的となる。

【００３０】
幾つかの実施の形態では、識別的特徴の整合性は、整合性ベクトルによって表される。この整合性ベクトルは、特徴ベクトル内の対応する要素が複数の測定にわたって不変である確率に比例した大きさを有する要素からなるベクトルである。特徴ベクトルの要素及び整合性ベクトルの要素の間のそのような相関は、バイオメトリックデータの識別的要素の

ロケーションと異なり、セキュアなプロトコルにおいて敵対者による利用がより困難である。

【００３１】

定義によれば、識別的特徴は整合的であるが、整合的特徴は必ずしも識別的ではない。識別的であるには、バイオメトリックデータ内の整合的特徴が、追加の要件、すなわち、他のユーザーのバイオメトリックデータ内のこの特徴の値がその範囲にわたってほぼ一様に分布しているという要件を満たさなければならない。例えば、アリスの指紋の中心から抽出された特定のビットが、常に値０を取る場合、そのビットは、アリスによって提供される種々の測定にわたって整合的であるが、そのビットは、データベース内の他の任意のユーザーの指紋の中心から抽出された同じビットが値０又は１を取る可能性が同程度にある場合にのみ識別的である。

【００３２】

例えば、１つの実施の形態では、ベクトルｘ及びｙは、２進数であり、Ｎビットを含み、これらのビットのそれぞれの整合性は、バイオメトリック信号を量子化するプロセスの間に得られる。例えば、アリスのバイオメトリックデータの第ｉの特徴ビットは、アリスのバイオメトリックデータから抽出された第ｉの信号の値を、登録及びトレーニングに用いられる全てのバイオメトリクスから抽出された第ｉの信号値の中央値と比較することによって求められるものと仮定する。この場合、整合性は、この中央値とアリスについて得られた信号値との間の距離の関数である。この距離が大きいほど、第ｉの特徴ビットが測定ごとに非整合的である確率は小さくなる。逆に、この距離が小さいほど、第ｉの特徴ビットが測定ごとに変化する確率は大きくなる。

【００３３】

１つの実施の形態では、整合性は、アリスのバイオメトリックデータから抽出された第ｉの特徴の値と、登録及びトレーニングにおいて用いられる全てのバイオメトリクスから抽出された第ｉの特徴の値の中央値との間の距離の整数値関数として定義される。様々な実施の形態では、登録及びトレーニングの間に得られたＮ個までの特徴の整合性情報が、敵対者が不正に認証されることを防止するのに利用される。

【００３４】

整合性の概念を明確にするために、登録の間に単一のユーザーから得られたバイオメトリック信号がベクトル［４，５，－１０，１２，３］である簡単な例を考えることにする。信号ベクトルの各要素の中央値は４であると仮定する。ここで、この中央値は、登録された全てのユーザーにわたって測定される。その場合、中央値からの信号値の絶対距離は、［０，１，１４，８，１］である。次に、抽出されたバイオメトリック特徴ベクトルは２進数であり、次の簡単なルール、すなわち、特徴要素は、信号ベクトル要素が中央値以下である場合に値０を取り、信号ベクトル要素が中央値よりも大きいときに値１を取る、というルールに従って得られるものと考える。このルールによれば、各測定について４の中央値を有する信号［４，５，－１０，１２，３］に対応する特徴ベクトルは［０，１，０，１，０］である。

【００３５】

しかしながら、上記例では、上記５ビットは等しく整合的でない。これは、幾つかの信号ベクトル要素が中央値に近かった（例えば、値４、５、及び３の測定）一方、他の信号ベクトル要素が中央値から遠かった（例えば、値－１０及び１２の測定）からである。これは重要である。なぜならば、バイオメトリック信号は、測定ごとに僅かに変化するからである。第１の信号ベクトル要素、第２の信号ベクトル要素、及び第５の信号ベクトル要素は中央値に近かったので、特徴ベクトル内の対応するビットは整合的ではなく、それらのビットは、測定ごとに変化する場合がある。これとは対照的に、第３の信号ベクトル要素及び第４の信号ベクトル要素は中央値から遠く、特徴ベクトル内の対応するビットは、測定ごとに変化する可能性が少ないので、非常に整合的である。

【００３６】

整合的な信号ベクトル要素のロケーションは、ユーザーが異なれば異なる。さらに、整

合的な信号ベクトル要素のロケーションは、識別的要素のロケーションと必ずしも同一ではない。このことが、本発明において利用される。特に、特徴抽出アルゴリズムが与えられると、敵対者は、識別的要素のロケーションを知らなくても、識別的要素を利用することができる。しかしながら、特徴抽出アルゴリズムは、特徴ビットの整合性についての情報を敵対者に与えない。本発明者らの提案は、登録されたユーザーであると主張する人物の特徴ビットの整合性が、正当に登録されたユーザーの特徴ビットの整合性と、閾値よりも大きな量だけ異なる場合には、認証を許可しないことである。

【００３７】

準同型暗号化

プライバシーの関心が高まったことに起因して、バイオメトリックデータのペアワイズ比較がセキュアな方法で行われる。幾つかの実施の形態では、データベースに登録されたユーザーのプライバシー及びセキュリティを保護するために、認証時に提示されたバイオメトリックデータとサーバーに記憶されたバイオメトリックデータとの間の距離の計算は、暗号化領域において行われる。

【００３８】

従来の公開鍵暗号化アルゴリズムは、暗号化領域の計算が可能ではない。準同型暗号システムは、暗号化領域における加算及び／又は乗算等の単純な演算を可能にする特殊な公開鍵暗号システムである。これらの暗号システムの例には、パエリア（Ｐａｉｌｌｉｅｒ）及びダムガード・ジュリック（Ｄａｍｇａｒｄ－Ｊｕｒｉｋ）によって記載された加法準同型システム、エル・ガマル（Ｅｌ　Ｇａｍａｌ）によって記載された乗法準同型システム、ボネ（Ｂｏｎｅｈ）他によって記載された２次準同型システム、及びジェントリー（Ｇｅｎｔｒｙ）によって記載された完全準同型システムが含まれる。

【００３９】

暗号化関数をＥ（．）によって表し、ａ、ｂ、ｃ、及びｄを４つの整数とする。その場合、パエリアシステム等の加法準同型システムでは、Ｅ（ａ）Ｅ（ｂ）＝Ｅ（ａ＋ｂ）であり、$E(a)^{b}=E(ab)$である。

【００４０】

２次多項式上で準同型性を用いる２次準同型システムは、暗号化領域における１つの乗算及び無制限の数の加算が可能である。そのため、２次準同型システムでは、$C_1=E(a)$及び$C_2=E(b)$である場合、$C_1C_2=E(a)E(b)=E(a+b)$である。これは、暗号化領域において加算を実行することができることを意味する。さらに、２次準同型システムでは、$e(C_1, C_2)=e(E(a), E(b))=F(ab)$となるような関数ｅ（．，．）が存在する。ここで、関数Ｆ（．）は、可逆である。すなわち、この関数は、解読して積ａｂを明らかにすることができる。これは、暗号化領域において乗算を実行することができることを意味する。関数ｅ（．，．）の一例は、乗法巡回群上の双線形写像である。

【００４１】

関数Ｆ（．）も、加法準同型であり、無制限の数の加算をサポートしている。例えば、Ｆ（ａｂ）Ｆ（ｃｄ）＝Ｆ（ａｂ＋ｃｄ）である。しかしながら、関数Ｆ（．）は、乗法準同型ではない。そのため、Ｆ（ａｂ）及びＦ（ｃｄ）が与えられても、写像ｅ（Ｆ（ａｂ），Ｆ（ｃｄ））を用いてＦ（ａｂｃｄ）を得ることは可能でない。ジェントリーのシステム等の完全準同型システムは、暗号化領域における無制限の数の乗算及び無制限の数の加算が可能である。

【００４２】

様々な実施の形態は、任意の加法準同型システム、２次準同型システム、又は２重準同型システムを用いることができる。以下で説明する実施の形態では、２次準同型システムを有する一実施態様が、その低い計算オーバーヘッド及び送信オーバーヘッドに起因して用いられている。しかしながら、加法準同型システム及び２重準同型システムへのこの方法の拡張は単純明快である。

【００４３】

以下で説明する実施の形態では、距離尺度は、バイオメトリックデータの特徴間のユークリッド距離を２乗したものが用いられる。一方、他の実施の形態は、２進ハミング距離、重み付きハミング距離、及び重み付きユークリッド距離等の異なる距離尺度を用いる。

【００４４】

セットアップフェーズ

１つの実施の形態では、バイオメトリックアクセス制御デバイス、データベースサーバー、及び認証サーバーが、準同型システムの公開鍵、例えば鍵１４０を所有することができる。認証サーバーのみが、暗号文を解読するのに必要な秘密鍵、例えば鍵１４５を所有する。

【００４５】

図２は、本発明の実施の形態によるバイオメトリックデータを暗号化したものを、登録状態の間にサーバー１２０で記憶するための方法のブロック図を示している。バイオメトリック認証システムに登録される各バイオメトリックデータ２１０について、データベースサーバー１２０又は第三者サービスは、登録ベクトルの要素がバイオメトリックデータ２１０の特徴を含むように、登録ベクトル２１４を求める。また、バイオメトリックデータの識別的特徴の位置を指定するインジケーターベクトル２１２及び登録ベクトルの各要素の整合性を指定する第１の整合性ベクトル２１６が求められる。登録ベクトル２１４、インジケーターベクトル２１２、及び第１の整合性ベクトル２１６は、準同型暗号化、例えば２次暗号化を用いて暗号化される（２３０）。

【００４６】

様々な実施の形態では、登録ベクトル、インジケーターベクトル、及び第１の整合性ベクトルを暗号化したものは、その後の認証に備えてデータベースサーバー１２０に記憶される（２２０）。幾つかの実施の形態では、登録ベクトル、インジケーターベクトル、及び第１の整合性ベクトルは、その後の認証を容易にするために、暗号化された代数成分の形態で記憶される（２４０）。

【００４７】

例えば、１つの実施の形態では、バイオメトリック認証システムに登録された各ユーザーについて、データベースサーバーは、$E(v_i)$と$E(-2v_i y_i)$と$E(y_i^2)$とを含む代数成分の第１のセットを記憶する。ここで、$i=1, 2, \ldots, N$である。同様に、バイオメトリック認証システムに登録された各ユーザーについて、データベースサーバーは、$E(v_i)$と$E(-2v_i r_i)$と$E(r_i^2)$とを上記第１のセットに記憶する。ここで、$i=1, 2, \ldots, N$である。登録ベクトル、インジケーターベクトル、及び第１の整合性ベクトルを暗号化された代数成分の形態で記憶することによって、暗号化領域において、準同型特性を用いて、すなわち、ベクトルを解読することなく、暗号化されたベクトル間の距離を求めることが可能になる。

【００４８】

この実施の形態は、ベクトルの幾つかの距離関数が、暗号化領域においてそれらの関数の解を見つけることを容易にする特定の特性を有するという認識に基づいている。それらの距離関数は、準同型成分の線形結合に変換することができる。準同型成分は、この準同型成分の暗号化された値が、準同型特性を用いて、すなわち、解読することなく、ベクトルの暗号化された値から直接計算することができるような入力の代数結合、すなわち、ベクトルである。そのため、準同型成分の暗号化結果の計算は、データの秘密性を維持する暗号化領域において実行される。

【００４９】

暗号化された準同型成分は、準同型特性を用いて処理することができる。そのため、登録ベクトル、インジケーターベクトル、及び第１の整合性ベクトルを、特定の距離関数に基づいて求められた暗号化された代数成分の形態で記憶することによって、暗号化領域においてその関数の結果を求めることが可能になる。暗号化された代数成分の使用法の一例を以下に提供する。

【００５０】

図３は、本発明の実施の形態によるバイオメトリックデータを暗号化したものを確証段階において求めるための方法のブロック図を示している。バイオメトリックアクセス制御デバイス１１０は、主張識別情報の名前、例えば「アリス」を受信する。アクセス制御デバイスは、次に、そのユーザー又は詐称者から指紋３１０等のバイオメトリックデータを受け取り、そのバイオメトリック信号に対してバイオメトリック特徴抽出アルゴリズムを実行する。この特徴抽出アルゴリズムの出力は、プローブベクトルｘ３１２及び第２の整合性ベクトルｓ３１４である。これらのベクトルのそれぞれは、長さＮを有し、プローブベクトルの要素は、バイオメトリックデータ３１０の特徴を含み、s_iは、プローブベクトルの特徴x_iの整合性を表す。

【００５１】

幾つかの実施の形態では、アクセス制御デバイスは、準同型暗号化を用いてプローブベクトル及び第２の整合性ベクトルを暗号化し（３２０）、暗号化されたベクトルをデータベースサーバー１２０に送信する（３４５）。したがって、データベースサーバーは、バイオメトリックデータの認証のために提示されたプローブベクトルを暗号化したもの及びプローブベクトルの各要素の整合性を指定する第２の整合性ベクトルを暗号化したものを受信する（３４０）。

【００５２】

データベースサーバーにおける動作と同様に、幾つかの実施の形態のアクセス制御デバイスは、暗号化された代数成分の第２のセットを求めて（３３０）送信する。例えば、１つの実施の形態では、この第２のセットは、ｉ＝１，２，．．．，Ｎについての$E(x_i^2)$、$E(x_i)$、$E(s_i^2)$、及び$E(s_i)$を含む。

【００５３】

図４は、認証のために提示されたデータ４２０とサーバーに記憶されたデータ４１０との間の距離を求めるための方法のブロック図を示している。幾つかの実施の形態では、登録プロセスの間にサーバーに記憶されたデータ４１０は、登録ベクトルを暗号化したものを含み、この登録ベクトルの要素は、上記で説明したように、バイオメトリックデータの特徴と、バイオメトリックデータの識別的特徴の位置を指定するインジケーターベクトルを暗号化したものとを含む。また、認証の間にサーバーによって受信されたデータ４２０は、バイオメトリックデータの認証のために提示されたプローブベクトルを暗号化したものと、プローブベクトルの各要素の整合性を指定する第２の整合性ベクトルを暗号化したものとを含む。

【００５４】

サーバーは、暗号化領域において、登録ベクトルの識別的要素とプローブベクトルの識別的要素との間の第１の距離を暗号化したもの４４０を求める（４３０）。これらの登録ベクトルの識別的要素の位置及びプローブベクトルの識別的要素の位置は、インジケーターベクトルによって指定されたユーザーの識別的特徴の位置に対応する。同様に、サーバーは、暗号化領域において、第１の整合性ベクトルの識別的要素と第２の整合性ベクトルの識別的要素との間の第２の距離を暗号化したもの４５０を求める（４３０）。これらの第１の整合性ベクトルの識別的要素の位置及び第２の整合性ベクトルの識別的要素の位置は、インジケーターベクトルによって指定されたユーザーの特徴の位置に対応する。

【００５５】

様々な実施の形態では、バイオメトリックデータは、第１の距離及び第２の距離に基づいて認証される。例えば、この認証は、第１の距離及び第２の距離を暗号化したものを認証サーバー１３０に送信する（４６０）ことを含むことができる。

【００５６】

幾つかの実施の形態では、登録ベクトル、プローブベクトル、インジケーターベクトル、第１の整合性ベクトル、及び第２の整合性ベクトルは、準同型暗号化の公開鍵を用いて暗号化される。これらの実施の形態では、第１の距離及び第２の距離を暗号化したものは、暗号化領域において、準同型特性を用いて求められる。

【００５７】

図５は、準同型成分の線形結合５４０として表された（５３０）距離関数５１０の暗号化結果５２０をセキュアに求めるための方法の図を示している。暗号化結果５２０は、暗号化領域において求められた第１の距離４４０又は第２の距離４５０とすることができる。暗号化結果は、セキュアに通信することができ、公開鍵１４０に関連付けられた秘密鍵１４５を用いて解読することができる。

【００５８】

本発明の実施の形態は、距離関数５１０を、準同型成分、例えば、５４１、５４２、及び５４３の線形結合５４０に変換する（５３０）。線形結合の例は、準同型成分の加算及び減算である。これらの準同型成分は、公開鍵１４０を用いて暗号化される。準同型成分の暗号化結果の値は、例えば、準同型暗号化の特性を用いて個々に求める（５６０）ことができる。準同型暗号化の特性及び線形結合によって、個々の暗号化結果５６５を結合して（５７０）、関数の最終的な暗号化結果５２０が生成される。

【００５９】

例えば、データベースサーバー１２０は、登録ベクトル、インジケーターベクトル、及び第１の整合性ベクトルを暗号化したものの代数結合の第１のセットを記憶することができる。この第１のセットは、暗号化領域におけるその後の計算を容易にするために距離関数に従って求めることができる。

【００６０】

例えば、１つの実施の形態では、距離関数はユークリッド距離であり、代数結合の第１のセットは、Ｅ（v_i）、Ｅ（$-2v_iy_i$）、Ｅ（y_i^2）、Ｅ（$-2v_ir_i$）、及びＥ（r_i^2）を含み、ここで、ｉ＝１，２，．．．，Ｎであり、Ｅ（．）は、２次準同型性の暗号化関数であり、ｙ＝（y_1，y_2，．．．，y_N）は、登録ベクトルであり、ｖ＝（v_1，v_2，．．．，v_N）は、インジケーターベクトルであり、ｒ＝（r_1，r_2，．．．，r_N）は、第１の整合性ベクトルである。

【００６１】

認証の間、データベースサーバーは、プローブベクトル及び第２の整合性ベクトルを暗号化したものの代数結合の第２のセットを受信する。例えば、ユークリッド距離関数を用いる実施の形態では、サーバーは、Ｅ（x_i^2）、Ｅ（x_i）、Ｅ（s_i^2）、及びＥ（s_i）を含む代数結合の第２のセットを受信することができる。ここで、ｘ＝（x_1，x_2，．．．，x_N）は、プローブベクトルであり、ｓ＝（s_1，s_2，．．．，s_N）は、第２の整合性ベクトルである。

【００６２】

サーバーは、暗号化結果の値を求め、暗号化結果を結合して第１の距離を暗号化したものＦ（Ｄ（ｘ，ｙ））４４０を以下の式に従って求める。

【数１】

$$\prod_{i=1}^{N} F\left(v_i x_i^2\right) F(-2v_i x_i y_i) F\left(v_i y_i^2\right) = \prod_{i=1}^{N} F(v_i x_i^2 - 2v_i x_i y_i + v_i y_i^2)$$

$$= F\left(\sum_{i=1}^{n} v_i x_i^2 - 2v_i x_i y_i + v_i y_i^2\right) = F(D(\mathbf{x}, \mathbf{y}))$$

ここで、ｅ（Ｅ（v_i），Ｅ（x_i^2））＝Ｆ（$v_i x_i^2$）であり、ｅ（Ｅ（$-2v_iy_i$），Ｅ（x_i））＝Ｆ（$-2v_ix_iy_i$）であり、ｅ（Ｅ（v_i），Ｅ（y_i^2））＝Ｆ（$v_iy_i^2$）であり、ｅ（．，．）は、当該関数ｅ（．，．）の２つの暗号化されたパラメーターの積の可逆関数Ｆ（．）を生成する２次準同型性の関数である。Ｆ（．）は、適切な解読鍵が存在する場合にのみ逆関数を求めることができることに留意されたい。

【００６３】

同様に、サーバーは、第２の距離

【数２】

$$D(\mathbf{r},\mathbf{s}) = \sum_{i=1}^{N} v_i (r_i - s_i)^2$$

を暗号化したものＦ（Ｄ（ｒ，ｓ））４５０を以下の数式に従って求める。

【数３】

$$\prod_{i=1}^{N} F(v_i r_i^2) F(-2 v_i r_i s_i) F(v_i s_i^2) = \prod_{i=1}^{N} F(v_i r_i^2 - 2 v_i r_i s_i + v_i s_i^2)$$

$$= F\left(\sum_{i=1}^{N} v_i r_i^2 - 2 v_i r_i s_i + v_i s_i^2 \right) = F(D(\mathbf{r},\mathbf{s}))$$

ここで、ｅ（Ｅ（ｖ$_i$），Ｅ（ｒ$_i^2$））＝Ｆ（ｖ$_i$ｒ$_i^2$）であり、ｅ（Ｅ（－２ｖ$_i$ｓ$_i$），Ｅ（ｒ$_i$））＝Ｆ（－２ｖ$_i$ｒ$_i$ｓ$_i$）であり、ｅ（Ｅ（ｖ$_i$），Ｅ（ｓ$_i^2$））＝Ｆ（ｖ$_i$ｓ$_i^2$）であり、ｅ（．，．）は、当該関数ｅ（．，．）の２つの暗号化されたパラメーターの積の可逆関数Ｆ（．）を生成する２次準同型性の関数である。上記と同様に、Ｆ（．）は、適切な解読鍵が存在する場合にのみ逆関数を求めることができることに留意されたい。

【００６４】

１つの実施の形態では、整合性ベクトル間の距離関数は、バイオメトリック特徴ｘ及びｙに用いられるものと同じである。他の実施の形態では、この距離関数は、ハミング距離、絶対距離、重み付き２乗距離のように異なるものである。第１の距離及び第２の距離を暗号化したものは、解読することもできるし、解読のために認証サーバーに送信することもできる。

【００６５】

図６は、本発明の実施の形態による認証サーバー１３０によって実行されるバイオメトリックデータを認証するための方法のブロック図である。認証サーバー１３０は、暗号化された距離Ｆ（Ｄ（ｘ，ｙ））４４０及びＦ（Ｄ（ｒ，ｓ））４５０を受信し、これらの第１の距離及び第２の距離を解読し、これらの第１の距離及び第２の距離を閾値と比較する。幾つかの実施の形態では、認証サーバーは、第１の距離が第１の閾値よりも小さく、第２の距離が第２の閾値よりも小さい場合に、肯定的な認証を決定する。

【００６６】

例えば、認証サーバーは、第１の距離Ｆ（Ｄ（ｘ，ｙ））を解読し（６１０）、解読された第１の距離Ｄ（ｘ，ｙ）６２０を第１の閾値と比較する（６３０）。距離Ｄ（ｘ，ｙ）６２０が第１の閾値を越えている場合、認証サーバーは、認証失敗６４０を報告する。Ｄ（ｘ，ｙ）が第１の閾値未満である場合、認証サーバーは、第２の距離Ｆ（Ｄ（ｒ，ｓ））を解読し（６１５）、解読された第２の距離Ｄ（ｒ，ｓ）６２５を第２の閾値と比較する。Ｄ（ｒ，ｓ）が第２の閾値を越えている場合、認証サーバーは、認証失敗６４０を報告する。暗号化されていない第２の距離Ｄ（ｒ，ｓ）が第２の閾値未満である場合、認証サーバーは、主張識別情報が認証されたことを報告する（６５０）。

【００６７】

識別的特徴の利用の利点

一般に、識別可能な特徴のロケーションを公然と公開して記憶することは得策ではない。アリスのバイオメトリックデータの識別的特徴のロケーション、例えば位置を発見した敵対者は、この情報を用いて、アリスとして認証を受けることができる。したがって、様々な実施の形態では、インジケーターベクトルｖにおいて提供される識別可能な特徴の位置は暗号化される。

【００６８】

幾つかの状況では、インジケーターベクトルの暗号化は、完全にセキュアというわけではない。敵対者が、識別可能な特徴の位置を知ることができない場合であっても、これら

の位置は、距離関数を求めるために幾つかの実施の形態によって用いられる。例えば、敵対者によって提供される任意のベクトルｘについて、インジケーターベクトルによって指定された位置を有するそれらの要素のみが距離計算において用いられることは確かである。そのため、敵対者が、十分多くの要素について、アリスの特徴値に十分近い特徴値を生成した場合、敵対者は、やはり、アリスに不正になりすますことができる。

【００６９】

上記状況を防止するために、実施の形態は、識別的特徴の整合性を利用する。幾つかの実施の形態は、次の知見に基づいている。定義によれば、第ｉのバイオメトリック特徴、すなわち、アリスのバイオメトリックデータから抽出された第ｉの要素に対応する特徴が識別可能である場合、この第ｉのバイオメトリック特徴は、アリスのバイオメトリックデータの複数の測定において再現することができ、ほとんどの詐称者の測定においてはその値の範囲にわたってほぼ一様な分布を有する。これは、アリスの第ｉのバイオメトリック特徴の整合性r_iが、ほとんどの詐称者の第ｉのバイオメトリック特徴の整合性よりも大きいことを意味する。したがって、この整合性における距離は、敵対者がアクセスを得ることを防止するのに利用することができる。

【００７０】

様々な実施の形態では、アリス（及びあらゆる登録されたユーザー）の第ｉのバイオメトリック特徴の整合性は、データベースサーバー上で、暗号化された形態で記憶されている。アクセス制御デバイスにおいて自身のバイオメトリックを提示した任意の個人の、s_iによって表される第ｉのバイオメトリック特徴の整合性は、アクセス制御デバイスによって利用可能である。これは、アクセス制御デバイスがそのトレーニングデータからの第ｉのバイオメトリック特徴の値の分布にアクセスできるからである。一例として、第ｉのバイオメトリック特徴の値を$x_i = 0$と閾値処理するのに中央値が用いられる場合、アクセス制御デバイスは、例えば、登録の間に得られた第ｉのバイオメトリック特徴の中央値を記憶する。

【００７１】

そのため、様々な実施の形態では、アクセス制御デバイスは、プローブベクトルｘに加えて、整合性ベクトルｓもサーバーに送信する。サーバーは、ｘとｙとの間の距離を暗号化領域において求めることに加えて、ｒとｓとの間の距離尺度も暗号化領域において求める。

【００７２】

当該技術分野における単一要素認証システムの場合、認証は、ｘとｙとの間の距離が閾値未満である場合に成功する。これとは対照的に、或る実施の形態では、このテストは十分ではない。ｘとｙとの間の距離が十分小さい場合、認証サーバーは、主張識別情報の整合性ベクトルｒと、提供されたバイオメトリックの整合性ベクトルｓとの間の距離を解読する。この第２の距離も第２の閾値未満である場合にのみ、アクセスが許可される。有利には、これらの実施の形態は、様々な種類の情報を用いて、敵対者が、登録されたユーザーの識別可能なビットを利用する能力を制限する。

【００７３】

幾つかの実施の形態は、１つの提出された特徴ベクトルが１つの記憶された特徴ベクトルに対して認証される認証を用いる。一方、代替的な実施の形態は、１つの提出された特徴ベクトルが、異なる位置に識別的要素を有する複数の記憶された特徴ベクトルと比較される「識別」シナリオに拡張される。

【００７４】

本発明の上述した実施の形態は、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、実施の形態は、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。

【００７５】

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。

【００７６】

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。

【００７７】

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。

【００７８】

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：ｃｏｍｐａｃｔ ｄｉｓｃ），光ディスク、デジタルビデオディスク（ＤＶＤ：ｄｉｇｉｔａｌ ｖｉｄｅｏ ｄｉｓｋ）、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、コンピューター可読記憶媒体ではなくコンピューター可読媒体として、例えば伝播信号として具現化することもできる。

【００７９】

「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。

【００８０】

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型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、様々な実施の形態において所望に応じて結合することもできるし、分散させることもできる。

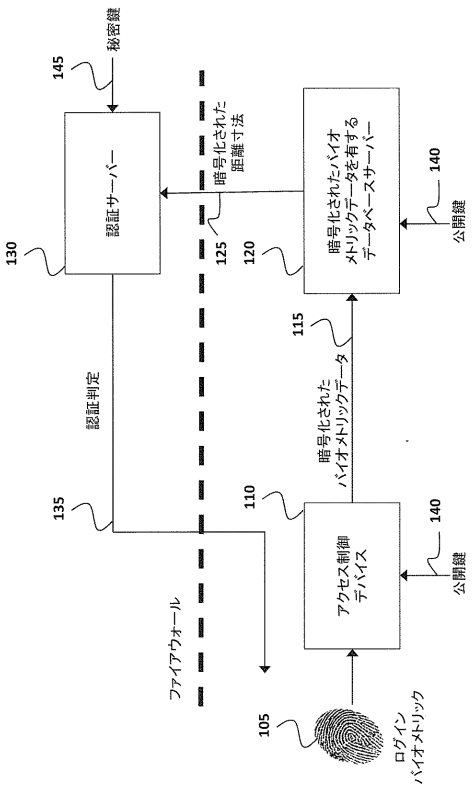
【００８１】

また、本発明の実施の形態は、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の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、例示の実施の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。

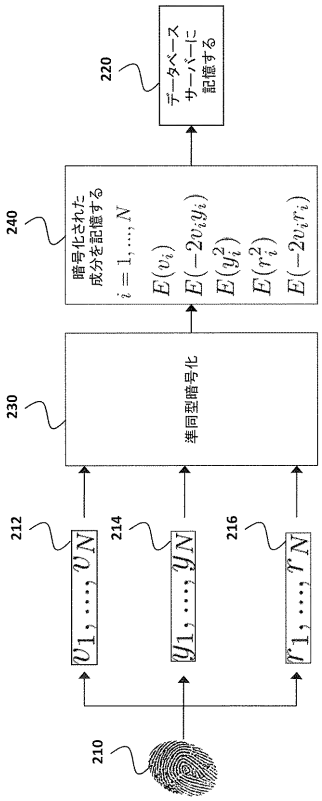
【００８２】

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、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。

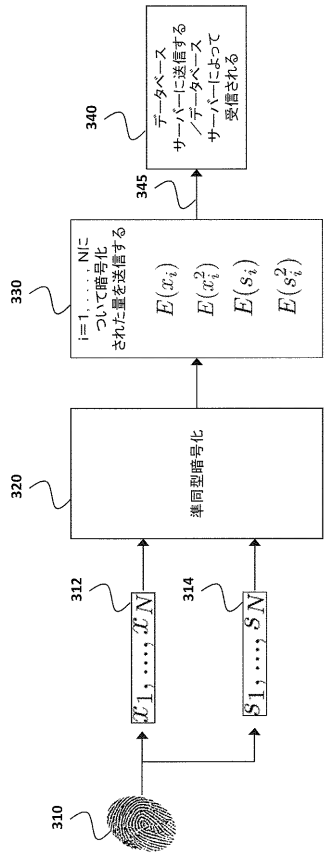
【図１】



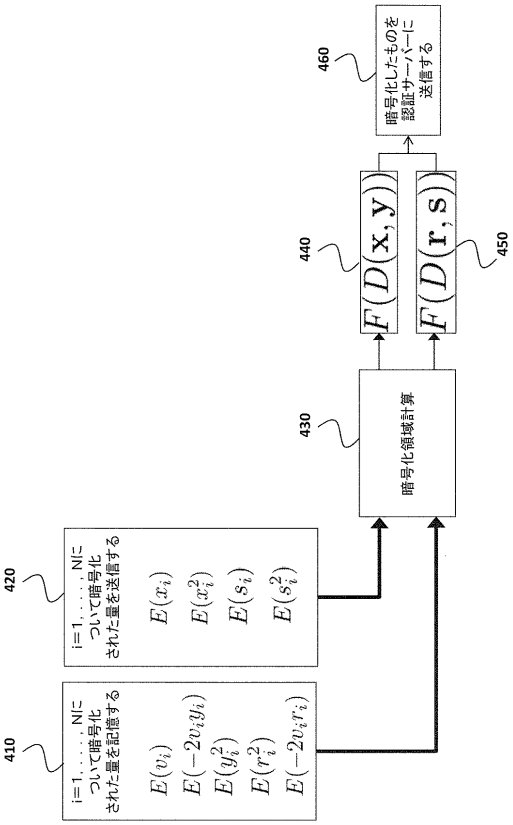
【図２】



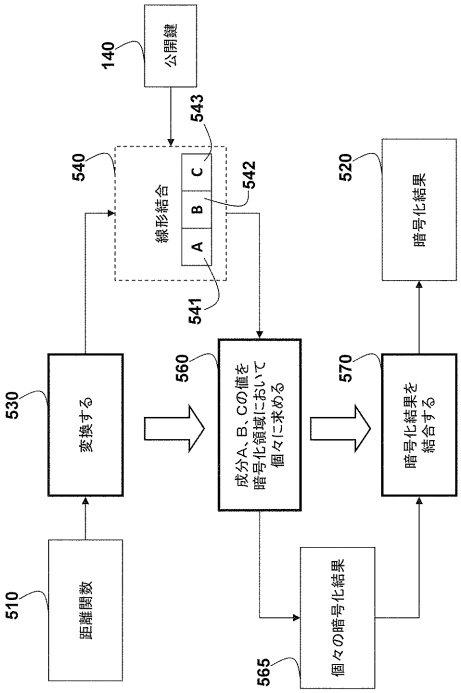
【図３】


310
312
314
320
330
340
345
準同型暗号化
データベース
サーバーに送信する
／データベース
サーバーによって
受信される

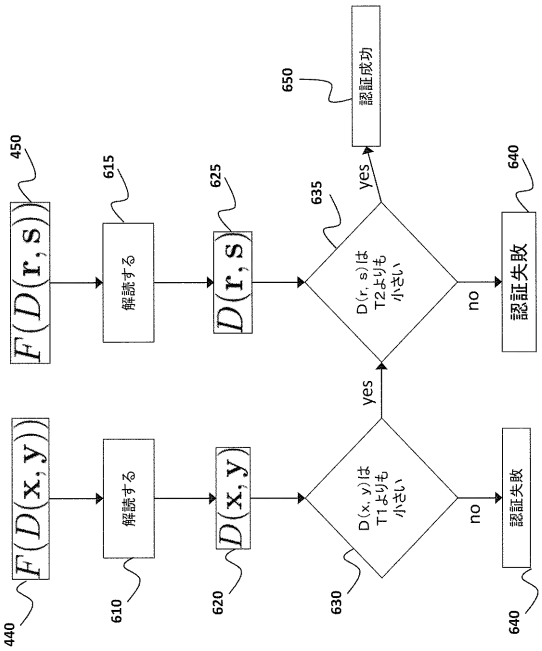
【図４】


410
420
430
440
450
460
暗号化領域計算
暗号化したものを
認証サーバーに
送信する

【図５】


510
530
540
541
542
543
560
565
570
520
140
距離関数
変換する
線形結合
A
B
C
成分A、B、Cの値を
暗号化領域において
個々に求める
個々の暗号化結果
暗号化結果を
結合する
暗号化結果
公開鍵

【図６】


440
450
610
615
620
625
630
635
640
650
解読する
解読する
D(x, y)は
T1よりも
小さい
D(r, s)は
T2よりも
小さい
yes
no
yes
no
認証成功
認証失敗
認証失敗

フロントページの続き

(74)代理人 100188329
弁理士 田村 義行
(72)発明者 ラーネ、シャンタヌ
アメリカ合衆国、マサチューセッツ州、ケンブリッジ、ウォルデン・ストリート ２２５、アパートメント ３ユー
(72)発明者 伊藤 隆
東京都千代田区丸の内二丁目７番３号 三菱電機株式会社内

審査官 青木 重徳

(56)参考文献 特開２０１１－０１３６７２（ＪＰ，Ａ）
特開２０１０－２３７６５３（ＪＰ，Ａ）
特開２００９－２３０６９２（ＪＰ，Ａ）
特表２００８－５２１０２５（ＪＰ，Ａ）
国際公開第２００９／０９６４７５（WO，Ａ１）
Shantanu Rane, et al., Privacy-Preserving Nearest Neighbor Methods, IEEE Signal Processing Magazine, 米国, IEEE, ２０１３年 2月１３日, March 2013, pp.18-28

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ ９／３２
Ｇ０６Ｆ ２１／３２