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

特許第5028194号
(P5028194)

(45)発行日　平成24年9月19日(2012.9.19)　(24)登録日　平成24年6月29日(2012.6.29)

(51)Int.Cl.		F I		
G06F 21/20	(2006.01)	G06F	21/20	132
G06K 17/00	(2006.01)	G06F	21/20	131E
H04L 9/32	(2006.01)	G06K	17/00	V
G06T 7/00	(2006.01)	H04L	9/00	675D
		G06T	7/00	510B

請求項の数 18　(全 27 頁)

(21)出願番号　特願2007-230899 (P2007-230899)
(22)出願日　平成19年9月6日 (2007.9.6)
(65)公開番号　特開2009-64202 (P2009-64202A)
(43)公開日　平成21年3月26日 (2009.3.26)
審査請求日　平成21年11月19日 (2009.11.19)

(73)特許権者　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　100064414
弁理士　磯野　道造
(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
(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

審査官　宮司　卓佳

最終頁に続く

(54)【発明の名称】認証サーバ、クライアント端末、生体認証システム、方法及びプログラム

(57)【特許請求の範囲】

【請求項１】

クライアント端末とネットワークを介して接続可能にされ、前記クライアント端末からの生体認証による認証要求に応じてユーザの認証処理を実行する認証サーバであって、

ユーザの生体情報から前記ユーザの特徴量を抽出し、前記認証サーバから受信した情報に基づいて生成した前記特徴量を変換するためのパラメータを、前記抽出した特徴量に作用させて変換特徴量を作成するクライアント端末が前記認証要求として送信した前記変換特徴量を受信すると、

当該受信した変換特徴量と、予め登録された、当該ユーザを特定する照合用の変換特徴量とを照合することにより、当該ユーザの認証処理を実行する認証実行部と、

ユーザを識別する情報を登録するユーザ識別フィールドと、少なくとも前記照合用の変換特徴量を構成要素とするテンプレートを登録するテンプレートフィールドとを有するテンプレートデータベースを備える記憶手段と、

前記テンプレートデータベースのテンプレートを変換する第一の機能および第二の機能を有するテンプレート変換手段とを備え、

前記テンプレート変換手段の第一の機能は、

前記クライアント端末から受信した、前記認証サーバからの前記第一の機能に関する第一の情報に基づいて生成したパラメータと前記第一の情報とは異なる値を有する前記認証サーバからの第一の機能に関する情報に基づいて生成したパラメータとの差分である第一の差分パラメータを用い、受信した第一の差分パラメータを前記テンプレートデータベー

スにおける当該ユーザのテンプレートの変換特徴量に作用させることにより、前記テンプレートを変換して当該ユーザを特定する一時的な変換特徴量を構成要素とする一時的なテンプレートを作成し、前記テンプレートデータベースを備える他の認証サーバに送信し、
前記テンプレート変換手段の第二の機能は、
前記クライアント端末から受信した、前記認証サーバからの前記他の認証サーバから受信した前記一時的なテンプレートに基づいた第二の情報に基づいて生成したパラメータと前記第二の情報とは異なる値を有する前記認証サーバからの第二の機能に関する情報に基づいて生成したパラメータとの差分である第二の差分パラメータと、他の認証サーバから受信した、前記第一の差分パラメータに基づく一時的なテンプレートとを用い、受信した一時的なテンプレートの一時的な変換特徴量に、受信した第二の差分パラメータを作用させることにより、当該ユーザを特定する新たな変換特徴量を構成要素とする新たなテンプレートを作成し、自身の前記テンプレートデータベースに登録すること、
を特徴とする認証サーバ。

【請求項２】
ユーザの生体情報から前記ユーザの特徴量を抽出し、前記特徴量を変換するためのパラメータを前記抽出した特徴量に作用させて変換特徴量を作成するクライアント端末と、
前記クライアント端末から受信した変換特徴量と、予め登録された、当該ユーザを特定する変換特徴量とを照合することにより、当該ユーザの認証処理を実行する複数の認証サーバとがネットワークを介して接続される生体認証システムにおける認証サーバであって、
前記認証サーバの各々において、
ユーザを識別する情報を登録するユーザ識別フィールドと、少なくとも当該ユーザを特定する変換特徴量を構成要素とするテンプレートを登録するテンプレートフィールドとを有するテンプレートデータベースを備える記憶手段と、
前記クライアント端末から受信した、前記パラメータと前記パラメータとは異なる値を有する別のパラメータとの差分である差分パラメータを、前記テンプレートの前記変換特徴量に作用させることにより、前記テンプレートを変換するテンプレート変換手段とを備え、
一の認証サーバにおいて、
前記テンプレート変換手段が前記テンプレートを変換することにより、少なくとも当該ユーザを特定する一時的な変換特徴量を構成要素とする一時的なテンプレートを作成し、
前記一時的なテンプレートを他の認証サーバに送信する
ことを特徴とする認証サーバ。

【請求項３】
ユーザの生体情報から前記ユーザの特徴量を抽出し、前記特徴量を変換するためのパラメータを前記抽出した特徴量に作用させて変換特徴量を作成するクライアント端末と、
前記クライアント端末から受信した変換特徴量と、予め登録された、当該ユーザを特定する変換特徴量とを照合することにより、当該ユーザの認証処理を実行する複数の認証サーバとがネットワークを介して接続される生体認証システムにおける認証サーバであって、
前記認証サーバの各々において、
ユーザを識別する情報を登録するユーザ識別フィールドと、少なくとも当該ユーザを特定する変換特徴量を構成要素とするテンプレートを登録するテンプレートフィールドとを有するテンプレートデータベースを備える記憶手段と、
前記クライアント端末から受信した、前記パラメータと前記パラメータとは異なる値を有する別のパラメータとの差分である差分パラメータを、前記テンプレートの前記変換特徴量に作用させることにより、前記テンプレートを変換するテンプレート変換手段とを備え、
一の認証サーバにおいて、
他の認証サーバから、前記他の認証サーバが備える前記テンプレート変換手段によって

作成された、少なくとも当該ユーザを特定する一時的な変換特徴量を構成要素とする一時的なテンプレートを受信し、
前記クライアント端末から、前記クライアント端末が前記他の認証サーバに送信した前記差分パラメータとは異なる値を有する別の差分パラメータを受信し、
前記テンプレート変換手段が、前記クライアントから受信した前記別の差分パラメータを、前記一時的なテンプレートの前記一時的な変換特徴量に作用させることにより、少なくとも当該ユーザを特定する新たな変換特徴量を構成要素とする新たなテンプレートを作成し、
前記記憶手段が備える前記テンプレートデータベースにおいて、前記テンプレートフィールドには、前記作成した新たなテンプレートを登録し、前記ユーザ識別フィールドには、前記作成した新たなテンプレートの構成要素である新たな変換特徴量により特定されるユーザを識別する情報を登録する
ことを特徴とする認証サーバ。
【請求項４】
ユーザの生体情報から前記ユーザの特徴量を抽出し、前記特徴量を変換するためのパラメータを前記抽出した特徴量に作用させて変換特徴量を作成するクライアント端末と、
前記クライアント端末から受信した変換特徴量と、予め登録された、当該ユーザを特定する変換特徴量とを照合することにより、当該ユーザの認証処理を実行する複数の認証サーバとがネットワークを介して接続される生体認証システムにおける認証サーバであって、
前記認証サーバの各々において、
ユーザを識別する情報を登録するユーザ識別フィールドと、少なくとも当該ユーザを特定する変換特徴量を構成要素とするテンプレートを登録するテンプレートフィールドとを有するテンプレートデータベースを備える記憶手段と、
前記クライアント端末から受信した、前記パラメータと前記パラメータとは異なる値を有する別のパラメータとの差分である差分パラメータを、前記テンプレートの前記変換特徴量に作用させることにより、前記テンプレートを変換するテンプレート変換手段とを備え、
一の認証サーバにおいて、
前記テンプレート変換手段が前記テンプレートを変換することにより、少なくとも当該ユーザを特定する新たな変換特徴量を構成要素とする新たなテンプレートを作成し、
前記記憶手段が備える前記テンプレートデータベースにおいて、前記ユーザ識別フィールドを検索して、前記新たな変換特徴量により特定されるユーザを判別し、前記テンプレートフィールドには、前記判別したユーザに対応するテンプレートに替えて、前記作成した新たなテンプレートを登録する
ことを特徴とする認証サーバ。
【請求項５】
ユーザの生体情報から前記ユーザの特徴量を抽出し、前記特徴量を変換するためのパラメータを前記抽出した特徴量に作用させて変換特徴量を作成するクライアント端末と、
少なくとも当該ユーザを特定する変換特徴量と、前記クライアント端末がパラメータを作成するために用いた乱数とを構成要素とするテンプレートを有し、前記クライアント端末から受信した変換特徴量と、予め登録された、当該ユーザを特定する変換特徴量とを照合することにより、当該ユーザの認証処理を実行する複数の認証サーバとがネットワークを介して接続される生体認証システムにおけるクライアント端末であって、
前記認証サーバから乱数を取得した場合には、
前記クライアント端末に接続可能な記憶媒体から取得したマスタ鍵及び前記認証サーバから取得した乱数に対して所定の関数を用いた演算を行うことにより、前記パラメータを作成し、
前記認証サーバから、前記テンプレートの構成要素である乱数と前記テンプレートの構成要素である乱数とは異なる値を有する別の乱数とを取得した場合には、

前記マスタ鍵及び前記認証サーバから取得した前記テンプレートの構成要素である乱数に対して前記所定の関数を用いた演算を行うことにより作成されたパラメータと、前記マスタ鍵及び前記認証サーバから取得した前記テンプレートの構成要素である乱数とは別の乱数に対して前記所定の関数を用いた演算を行うことにより作成された別のパラメータとの差分である差分パラメータを作成するパラメータ作成手段とを備え、
前記認証サーバから乱数を取得した場合には、
前記作成したパラメータを前記特徴量に作用させて作成した、当該ユーザを特定する変換特徴量を、当該パラメータを作成するために用いた乱数を送信した認証サーバに送信し、
前記認証サーバから、前記テンプレートの構成要素である乱数と前記テンプレートの構成要素である乱数とは異なる値を有する別の乱数とを取得した場合には、
前記作成した差分パラメータを、当該差分パラメータを作成するために用いた前記テンプレートの構成要素である乱数と前記テンプレートの構成要素である乱数とは異なる値を有する別の乱数とを送信した認証サーバに送信することを特徴とするクライアント端末。

【請求項６】
前記所定の関数は、ハッシュ関数であり、
前記パラメータ作成手段は、
前記記憶媒体から取得したマスタ鍵と前記認証サーバから取得した乱数とをビット連結した値に対して前記ハッシュ関数を用いた演算を行うことにより作成されたハッシュ値を前記パラメータとする
ことを特徴とする請求項５に記載のクライアント端末。

【請求項７】
ユーザの生体情報から前記ユーザの特徴量を抽出し、前記特徴量を変換するためのパラメータを前記抽出した特徴量に作用させて変換特徴量を作成するクライアント端末と、
前記クライアント端末から受信した変換特徴量と、予め登録された、当該ユーザを特定する変換特徴量とを照合することにより、当該ユーザの認証処理を実行する複数の認証サーバとがネットワークを介して接続される生体認証システムであって、 前記認証サーバの各々において、
ユーザを識別する情報を登録するユーザ識別フィールドと、少なくとも当該ユーザを特定する変換特徴量を構成要素とするテンプレートを登録するテンプレートフィールドとを有するテンプレートデータベースを備える記憶手段と、
前記クライアント端末から受信した、前記パラメータと前記パラメータとは異なる値を有する別のパラメータとの差分である差分パラメータを、前記テンプレートの前記変換特徴量に作用させることにより、前記テンプレートを変換するテンプレート変換手段とを備え、
一の認証サーバにおいて、
前記クライアント端末から、前記差分パラメータを第一の差分パラメータとして受信し、
前記テンプレート変換手段が前記第一の差分パラメータを前記テンプレートの前記変換特徴量に作用させて前記テンプレートを変換することにより、少なくとも当該ユーザを特定する一時的な変換特徴量を構成要素とする一時的なテンプレートを作成し、
前記一時的なテンプレートを他の認証サーバに送信し、
前記他の認証サーバにおいて、
前記一の認証サーバから、前記一時的なテンプレートを受信し、
前記クライアント端末から、前記クライアント端末が前記一の認証サーバに送信した前記第一の差分パラメータとは異なる値を有する第二の差分パラメータを受信し、
前記テンプレート変換手段が、前記クライアントから受信した前記第二の差分パラメータを、前記一時的なテンプレートの前記一時的な変換特徴量に作用させることにより、少なくとも当該ユーザを特定する新たな変換特徴量を構成要素とする新たなテンプレートを作成し、

前記記憶手段が備える前記テンプレートデータベースにおいて、前記テンプレートフィールドには、前記作成した新たなテンプレートを登録し、前記ユーザ識別フィールドには、前記作成した新たなテンプレートの構成要素である新たな変換特徴量により特定されるユーザを識別する情報を登録する

ことを特徴とする生体認証システム。

【請求項８】

前記クライアント端末は、

前記クライアント端末に接続可能な記憶媒体から取得したマスタ鍵及び前記認証サーバから取得した乱数に対して所定の関数を用いた演算を行うことにより、前記パラメータを作成するパラメータ作成手段とを備え、

前記認証サーバの各々において、

前記記憶手段が備える前記テンプレートデータベースに登録されるテンプレートは、前記クライアント端末の前記パラメータ作成手段がパラメータを作成するために用いた前記乱数も構成要素とするテンプレートであり、

前記クライアント端末において、

前記一の認証サーバから、前記テンプレートの構成要素である第一の乱数と、前記第一の乱数とは異なる値を有する、前記一時的なテンプレートの構成要素となる第一の別の乱数とを取得し、

前記パラメータ作成手段は、前記マスタ鍵及び前記テンプレートの構成要素である第一の乱数に対して前記所定の関数を用いた演算を行うことにより作成された第一のパラメータと、前記マスタ鍵及び前記第一の別の乱数に対して前記所定の関数を用いた演算を行うことにより作成された第一の別のパラメータとの差分である前記第一の差分パラメータを作成し、

前記第一の差分パラメータを前記一の認証サーバに送信し、

前記他の認証サーバから、前記一時的なテンプレートの構成要素である第一の別の乱数と、前記第一の別の乱数とは異なる値を有する第二の乱数を取得し、

前記パラメータ作成手段は、前記マスタ鍵及び前記テンプレートの構成要素である第一の別の乱数に対して前記所定の関数を用いた演算を行うことにより作成された第二のパラメータと、前記マスタ鍵及び前記第二の乱数に対して前記所定の関数を用いた演算を行うことにより作成された第二の別のパラメータとの差分である前記第二の差分パラメータを作成し、

前記第二の差分パラメータを前記他の認証サーバに送信する

ことを特徴とする請求項７に記載の生体認証システム。

【請求項９】

ユーザの生体情報から前記ユーザの特徴量を抽出し、前記特徴量を変換するためのパラメータを前記抽出した特徴量に作用させて変換特徴量を作成するクライアント端末と、

前記クライアント端末から受信した変換特徴量と、予め登録された、当該ユーザを特定する変換特徴量とを照合することにより、当該ユーザの認証処理を実行する複数の認証サーバとがネットワークを介して接続される生体認証システムであって、

前記認証サーバの各々において、

ユーザを識別する情報を登録するユーザ識別フィールドと、少なくとも当該ユーザを特定する変換特徴量を構成要素とするテンプレートを登録するテンプレートフィールドとを有するテンプレートデータベースを備える記憶手段と、

前記クライアント端末から受信した、前記パラメータと前記パラメータとは異なる値を有する別のパラメータとの差分である差分パラメータを、前記テンプレートの前記変換特徴量に作用させることにより、前記テンプレートを変換するテンプレート変換手段とを備え、

一の認証サーバにおいて、

前記クライアント端末から、前記差分パラメータを受信し、

前記テンプレート変換手段が前記差分パラメータを前記テンプレートの前記変換特徴量

に作用させて前記テンプレートを変換することにより、少なくとも当該ユーザを特定する新たな変換特徴量を構成要素とする新たなテンプレートを作成し、
前記記憶手段が備える前記テンプレートデータベースにおいて、前記ユーザ識別フィールドを検索して、前記新たな変換特徴量により特定されるユーザを判別し、前記テンプレートフィールドには、前記判別したユーザに対応するテンプレートに替えて、前記作成した新たなテンプレートを登録する
ことを特徴とする生体認証システム。
【請求項１０】
前記クライアント端末は、
前記クライアント端末に接続可能な記憶媒体から取得したマスタ鍵及び前記認証サーバから取得した乱数に対して所定の関数を用いた演算を行うことにより、前記パラメータを作成するパラメータ作成手段とを備え、
前記認証サーバの各々において、
前記記憶手段が備える前記テンプレートデータベースに登録されるテンプレートは、前記クライアント端末の前記パラメータ作成手段がパラメータを作成するために用いた前記乱数も構成要素とするテンプレートであり、
前記クライアント端末において、
前記一の認証サーバから、前記テンプレートの構成要素である乱数と、前記乱数とは異なる値を有する別の乱数とを取得し、
前記パラメータ作成手段は、前記マスタ鍵及び前記テンプレートの構成要素である乱数に対して前記所定の関数を用いた演算を行うことにより作成されたパラメータと、前記マスタ鍵及び前記別の乱数に対して前記所定の関数を用いた演算を行うことにより作成された別のパラメータとの差分である前記差分パラメータを作成し、
前記差分パラメータを前記一の認証サーバに送信する
ことを特徴とする請求項９に記載の生体認証システム。
【請求項１１】
ユーザの生体情報から前記ユーザの特徴量を抽出し、前記特徴量を変換するためのパラメータを前記抽出した特徴量に作用させて変換特徴量を作成するクライアント端末と、
前記クライアント端末から受信した変換特徴量と、予め登録された、当該ユーザを特定する変換特徴量とを照合することにより、当該ユーザの認証処理を実行する複数の認証サーバとがネットワークを介して接続される生体認証システムにおける認証サーバにて実行される生体認証方法であって、
前記認証サーバの各々において、
ユーザを識別する情報を登録するユーザ識別フィールドと、少なくとも当該ユーザを特定する変換特徴量を構成要素とするテンプレートを登録するテンプレートフィールドとを有するテンプレートデータベースを備える記憶手段と、
前記クライアント端末から受信した、前記パラメータと前記パラメータとは異なる値を有する別のパラメータとの差分である差分パラメータを、前記テンプレートの前記変換特徴量に作用させることにより、前記テンプレートを変換するテンプレート変換手段とを備え、
一の認証サーバにおいて、
前記テンプレート変換手段が前記テンプレートを変換することにより、少なくとも当該ユーザを特定する一時的な変換特徴量を構成要素とする一時的なテンプレートを作成するステップと、
前記一時的なテンプレートを他の認証サーバに送信するステップと、
を実行することを特徴とする生体認証方法。
【請求項１２】
ユーザの生体情報から前記ユーザの特徴量を抽出し、前記特徴量を変換するためのパラメータを前記抽出した特徴量に作用させて変換特徴量を作成するクライアント端末と、
前記クライアント端末から受信した変換特徴量と、予め登録された、当該ユーザを特定

する変換特徴量とを照合することにより、当該ユーザの認証処理を実行する複数の認証サーバとがネットワークを介して接続される生体認証システムにおける認証サーバにて実行される生体認証方法であって、
前記認証サーバの各々において、
ユーザを識別する情報を登録するユーザ識別フィールドと、少なくとも当該ユーザを特定する変換特徴量を構成要素とするテンプレートを登録するテンプレートフィールドとを有するテンプレートデータベースを備える記憶手段と、
前記クライアント端末から受信した、前記パラメータと前記パラメータとは異なる値を有する別のパラメータとの差分である差分パラメータを、前記テンプレートの前記変換特徴量に作用させることにより、前記テンプレートを変換するテンプレート変換手段とを備え、
一の認証サーバにおいて、
他の認証サーバから、前記他の認証サーバが備える前記テンプレート変換手段によって作成された、少なくとも当該ユーザを特定する一時的な変換特徴量を構成要素とする一時的なテンプレートを受信するステップと、
前記クライアント端末から、前記クライアント端末が前記他の認証サーバに送信した前記差分パラメータとは異なる値を有する別の差分パラメータを受信するステップと、
前記テンプレート変換手段が、前記クライアントから受信した前記別の差分パラメータを、前記一時的なテンプレートの前記一時的な変換特徴量に作用させることにより、少なくとも当該ユーザを特定する新たな変換特徴量を構成要素とする新たなテンプレートを作成するステップと、
前記記憶手段が備える前記テンプレートデータベースにおいて、前記テンプレートフィールドには、前記作成した新たなテンプレートを登録し、前記ユーザ識別フィールドには、前記作成した新たなテンプレートの構成要素である新たな変換特徴量により特定されるユーザを識別する情報を登録するステップと、
を実行することを特徴とする生体認証方法。
【請求項１３】
ユーザの生体情報から前記ユーザの特徴量を抽出し、前記特徴量を変換するためのパラメータを前記抽出した特徴量に作用させて変換特徴量を作成するクライアント端末と、
前記クライアント端末から受信した変換特徴量と、予め登録された、当該ユーザを特定する変換特徴量とを照合することにより、当該ユーザの認証処理を実行する複数の認証サーバとがネットワークを介して接続される生体認証システムにおける認証サーバにて実行される生体認証方法であって、
前記認証サーバの各々において、
ユーザを識別する情報を登録するユーザ識別フィールドと、少なくとも当該ユーザを特定する変換特徴量を構成要素とするテンプレートを登録するテンプレートフィールドとを有するテンプレートデータベースを備える記憶手段と、
前記クライアント端末から受信した、前記パラメータと前記パラメータとは異なる値を有する別のパラメータとの差分である差分パラメータを、前記テンプレートの前記変換特徴量に作用させることにより、前記テンプレートを変換するテンプレート変換手段とを備え、
一の認証サーバにおいて、
前記テンプレート変換手段が前記テンプレートを変換することにより、少なくとも当該ユーザを特定する新たな変換特徴量を構成要素とする新たなテンプレートを作成するステップと、
前記記憶手段が備える前記テンプレートデータベースにおいて、前記ユーザ識別フィールドを検索して、前記新たな変換特徴量により特定されるユーザを判別し、前記テンプレートフィールドには、前記判別したユーザに対応するテンプレートに替えて、前記作成した新たなテンプレートを登録するステップと、
を実行することを特徴とする生体認証方法。

【請求項１４】
ユーザの生体情報から前記ユーザの特徴量を抽出し、前記特徴量を変換するためのパラメータを前記抽出した特徴量に作用させて変換特徴量を作成するクライアント端末と、
少なくとも当該ユーザを特定する変換特徴量と、前記クライアント端末がパラメータを作成するために用いた乱数とを構成要素とするテンプレートを有し、前記クライアント端末から受信した変換特徴量と、予め登録された、当該ユーザを特定する変換特徴量とを照合することにより、当該ユーザの認証処理を実行する複数の認証サーバとがネットワークを介して接続される生体認証システムにおけるクライアント端末にて実行される生体認証方法であって、
前記クライアント端末において、
前記認証サーバから乱数を取得する第１のステップと、
前記クライアント端末に接続可能な記憶媒体から取得したマスタ鍵及び前記認証サーバから取得した乱数に対して所定の関数を用いた演算を行うことにより、前記パラメータを作成する第２のステップと、
前記作成したパラメータを前記特徴量に作用させて作成した、当該ユーザを特定する変換特徴量を、当該パラメータを作成するために用いた乱数を送信した認証サーバに送信する第３のステップと、
前記認証サーバから、前記テンプレートの構成要素である乱数と前記テンプレートの構成要素である乱数とは異なる値を有する別の乱数とを取得する第４のステップと、
前記マスタ鍵及び前記認証サーバから取得した前記テンプレートの構成要素である乱数に対して前記所定の関数を用いた演算を行うことにより作成されたパラメータと、前記マスタ鍵及び前記認証サーバから取得した前記テンプレートの構成要素である乱数とは別の乱数に対して前記所定の関数を用いた演算を行うことにより作成された別のパラメータとの差分である差分パラメータを作成する第５のステップと、
前記作成した差分パラメータを、当該差分パラメータを作成するために用いた前記テンプレートの構成要素である乱数と前記テンプレートの構成要素である乱数とは異なる値を有する別の乱数とを送信した認証サーバに送信する第６のステップと、
を実行することを特徴とする生体認証方法。
【請求項１５】
ユーザの生体情報から前記ユーザの特徴量を抽出し、前記特徴量を変換するためのパラメータを前記抽出した特徴量に作用させて変換特徴量を作成するクライアント端末と、
前記クライアント端末から受信した変換特徴量と、予め登録された、当該ユーザを特定する変換特徴量とを照合することにより、当該ユーザの認証処理を実行する複数の認証サーバとがネットワークを介して接続される生体認証システムにおける認証サーバのコンピュータに生体認証方法を実行させるプログラムであって、
前記認証サーバの各々において、
ユーザを識別する情報を登録するユーザ識別フィールドと、少なくとも当該ユーザを特定する変換特徴量を構成要素とするテンプレートを登録するテンプレートフィールドとを有するテンプレートデータベースを備える記憶手段と、
前記クライアント端末から受信した、前記パラメータと前記パラメータとは異なる値を有する別のパラメータとの差分である差分パラメータを、前記テンプレートの前記変換特徴量に作用させることにより、前記テンプレートを変換するテンプレート変換手段とを備え、
一の認証サーバのコンピュータに、
前記テンプレート変換手段が前記テンプレートを変換することにより、少なくとも当該ユーザを特定する一時的な変換特徴量を構成要素とする一時的なテンプレートを作成する処理と、
前記一時的なテンプレートを他の認証サーバに送信する処理と、
を実行させることを特徴とするプログラム。
【請求項１６】

ユーザの生体情報から前記ユーザの特徴量を抽出し、前記特徴量を変換するためのパラメータを前記抽出した特徴量に作用させて変換特徴量を作成するクライアント端末と、
前記クライアント端末から受信した変換特徴量と、予め登録された、当該ユーザを特定する変換特徴量とを照合することにより、当該ユーザの認証処理を実行する複数の認証サーバとがネットワークを介して接続される生体認証システムにおける認証サーバのコンピュータに生体認証方法を実行させるプログラムであって、
前記認証サーバの各々において、
ユーザを識別する情報を登録するユーザ識別フィールドと、少なくとも当該ユーザを特定する変換特徴量を構成要素とするテンプレートを登録するテンプレートフィールドとを有するテンプレートデータベースを備える記憶手段と、
前記クライアント端末から受信した、前記パラメータと前記パラメータとは異なる値を有する別のパラメータとの差分である差分パラメータを、前記テンプレートの前記変換特徴量に作用させることにより、前記テンプレートを変換するテンプレート変換手段とを備え、
一の認証サーバのコンピュータに、
他の認証サーバから、前記他の認証サーバが備える前記テンプレート変換手段によって作成された、少なくとも当該ユーザを特定する一時的な変換特徴量を構成要素とする一時的なテンプレートを受信する処理と、
前記クライアント端末から、前記クライアント端末が前記他の認証サーバに送信した前記差分パラメータとは異なる値を有する別の差分パラメータを受信する処理と、
前記テンプレート変換手段が、前記クライアントから受信した前記別の差分パラメータを、前記一時的なテンプレートの前記一時的な変換特徴量に作用させることにより、少なくとも当該ユーザを特定する新たな変換特徴量を構成要素とする新たなテンプレートを作成する処理と、
前記記憶手段が備える前記テンプレートデータベースにおいて、前記テンプレートフィールドには、前記作成した新たなテンプレートを登録し、前記ユーザ識別フィールドには、前記作成した新たなテンプレートの構成要素である新たな変換特徴量により特定されるユーザを識別する情報を登録する処理と、
を実行させることを特徴とするプログラム。
【請求項１７】
ユーザの生体情報から前記ユーザの特徴量を抽出し、前記特徴量を変換するためのパラメータを前記抽出した特徴量に作用させて変換特徴量を作成するクライアント端末と、
前記クライアント端末から受信した変換特徴量と、予め登録された、当該ユーザを特定する変換特徴量とを照合することにより、当該ユーザの認証処理を実行する複数の認証サーバとがネットワークを介して接続される生体認証システムにおける認証サーバのコンピュータに生体認証方法を実行させるプログラムであって、
前記認証サーバの各々において、
ユーザを識別する情報を登録するユーザ識別フィールドと、少なくとも当該ユーザを特定する変換特徴量を構成要素とするテンプレートを登録するテンプレートフィールドとを有するテンプレートデータベースを備える記憶手段と、
前記クライアント端末から受信した、前記パラメータと前記パラメータとは異なる値を有する別のパラメータとの差分である差分パラメータを、前記テンプレートの前記変換特徴量に作用させることにより、前記テンプレートを変換するテンプレート変換手段とを備え、
一の認証サーバのコンピュータに、
前記テンプレート変換手段が前記テンプレートを変換することにより、少なくとも当該ユーザを特定する新たな変換特徴量を構成要素とする新たなテンプレートを作成する処理と、
前記記憶手段が備える前記テンプレートデータベースにおいて、前記ユーザ識別フィールドを検索して、前記新たな変換特徴量により特定されるユーザを判別し、前記テンプレ

ートフィールドには、前記判別したユーザに対応するテンプレートに替えて、前記作成した新たなテンプレートを登録する処理と、
を実行させることを特徴とするプログラム。
【請求項１８】
ユーザの生体情報から前記ユーザの特徴量を抽出し、前記特徴量を変換するためのパラメータを前記抽出した特徴量に作用させて変換特徴量を作成するクライアント端末と、
前記クライアント端末から受信した変換特徴量と、予め登録された、当該ユーザを特定する変換特徴量とを照合することにより、当該ユーザの認証処理を実行する複数の認証サーバとがネットワークを介して接続される生体認証システムにおけるクライアント端末のコンピュータに生体認証方法を実行させるプログラムであって、
前記クライアント端末において、
前記認証サーバから乱数を取得する第１の処理と、
前記クライアント端末に接続可能な記憶媒体から取得したマスタ鍵及び前記認証サーバから取得した乱数に対して所定の関数を用いた演算を行うことにより、前記パラメータを作成する第２の処理と、
前記作成したパラメータを前記特徴量に作用させて作成した、当該ユーザを特定する変換特徴量を、当該パラメータを作成するために用いた乱数を送信した認証サーバに送信する第３の処理と、
前記認証サーバから、前記テンプレートの構成要素である乱数と、前記テンプレートの構成要素である乱数とは異なる値を有する別の乱数とを取得する第４の処理と、
前記マスタ鍵及び前記認証サーバから取得した前記テンプレートの構成要素である乱数に対して前記所定の関数を用いた演算を行うことにより作成されたパラメータと、前記マスタ鍵及び前記認証サーバから取得した前記テンプレートの構成要素である乱数とは別の乱数に対して前記所定の関数を用いた演算を行うことにより作成された別のパラメータとの差分である差分パラメータを作成する第５の処理と、
前記作成した差分パラメータを、当該差分パラメータを作成するために用いた前記テンプレートの構成要素である乱数と、前記テンプレートの構成要素である乱数とは異なる値を有する別の乱数とを送信した認証サーバに送信する第６の処理と、
を前記クライアント端末のコンピュータに実行させることを特徴とするプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、人が持つ生体的特徴を用いて個人を認証する技術に関する。
【背景技術】
【０００２】
生体情報を用いたユーザ認証システムは、登録時にユーザから生体情報を取得し、取得した生体情報から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。認証時は、再びユーザから生体情報を取得して特徴量を抽出し、抽出した特徴量とテンプレートとを照合して本人か否かを確認する。ネットワークを介してサーバがクライアント側にいるユーザを生体情報に基づいて認証する場合、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。
【０００３】
しかし、テンプレートはユーザ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。また、厳密な管理が行われていても、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ユーザが多い。また、一人のユーザ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ず、仮にテンプレートが漏洩して偽造の危険が生じた場合、その生体認証が使用できなくなる問題がある。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晒されることになる。

【０００４】

上記の問題に対し、生体情報を暗号化して認証サーバに送信する方法が考えられる。しかし、認証時に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など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。

【０００５】

そこで、非特許文献１では、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とで変換し、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と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とを変換された状態のまま照合する方法（いわゆるキャンセラブル生体認証）が提案されている。クライアントが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、ユーザ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、パラメータを変更して再度テンプレートを作成し、登録することで、安全性を保つことができる。

【０００６】

ところで、複数のサービスプロバイダが独立にサーバを設置してキャンセラブル生体認証システムを構成する場合、以下のような構成の方法が考えられる。まず、クライアントに接続するセンサの導入コストを削減するため、使用する生体情報の種類は同一とし、生体情報を取得するためのセンサは一台とする。次に、生体情報の登録は、他のサービスプロバイダに知られることの無いように、それぞれのサービスプロバイダごとに実施し、それぞれのサーバにテンプレートとして保管する。また、登録時にクライアントが作成するパラメータはサービスプロバイダごとに異なるものとし、ユーザの所持する耐タンパデバイス（記憶媒体）に格納する。さらに、認証は、利用したいサービスに応じて対応するパラメータを耐タンパデバイスからクライアントに読み出し、読み出したパラメータを用いて変換した特徴量を対応するサーバに送信し、サーバ側で照合を行うというものである。このような構成により、センサの導入コストを削減しつつ、複数のサーバに対応したキャンセラブル生体認証システムを実現できる。また、別の方法として非特許文献２に記載の方法がある。これは、テンプレートの変換専用サーバを設置し、始めに登録したテンプレートをこの専用サーバにおいて変換し認証サーバごとのテンプレートを作成するものである。

【非特許文献１】N.K.Ratha, J.H.Connell, R.M.Bolle, “Enhancing security and privacy in biometrics-based authentication systems”, IBM Systems Journal, Vol.40, No.3, 2001

【非特許文献２】James L. Cambier, Ulf M. Cahn von Seelen, Randal Glass, Russell Moore, Ian Scott, Michael Braithwaite, John Daugman, “Application-Specific Biometric Templates”, IEEE Workshop on Automated Identification Advanced Technologies, Tarrytown, NY, March, 2002, P167-171

【発明の開示】

【発明が解決しようとする課題】

【０００７】

しかし、非特許文献１や非特許文献２に基づき、複数のサーバに対応したキャンセラブル生体認証システムを上記のような方法で構成する場合には、以下のような問題がある。

【０００８】

まず、生体情報の登録をサービスプロバイダごとに実施するため、利用したいサービスが増えるごとにユーザはサービスプロバイダの登録窓口に出向く必要がある。またサービスプロバイダは登録窓口を設置し、それを運用する必要がある。例えば、ユーザは本人であることを証明するために身分証明書を提示する等の手続的負担を必要とし、サービスプロバイダはなりすまし等の不正行為を防止するための設備を設置して、その身分証明書か

ら本人確認を厳密に行う等の手続的負担を必要とする。このように、生体情報の登録に関して、ユーザ、サービスプロバイダ双方に負担が掛かってしまう、という一点目の問題がある。

【０００９】

次に、パラメータはサービスプロバイダごとに異なるため、利用するサービスプロバイダが増えるごとにユーザの所持する耐タンパデバイスに格納すべきパラメータが増えることになる。このため、耐タンパデバイスのメモリ容量を圧迫してしまい、既存の耐タンパデバイスでは対応できなくなる、という二点目の問題がある。

【００１０】

本発明の主たる目的は、ユーザのクライアント端末と複数設置した認証サーバとが接続されるキャンセラブル生体認証システムを実現するにあたり、上記一点目の問題を解決し、生体情報の登録に関する負担を削減可能にすることにある。また、上記二点目の問題を解決し、既存の記憶媒体のメモリ容量でも対応可能にすることも目的とする。

【課題を解決するための手段】

【００１１】

本発明は、上記問題を解決するため、以下のような手段を講じる。

すなわち、未だ登録を実施していない認証サーバが既に登録を済ませた認証サーバからテンプレートを受け取り、テンプレートを共有する、というテンプレート共有処理を実行する。テンプレートを受け取った認証サーバはもはや登録を実施する必要がなく、登録に掛かる負担は軽減される。このとき、テンプレートを渡す認証サーバは、自身が管理するテンプレートとは別の一時的なテンプレートを渡すようにして、テンプレートを受け取る認証サーバには、自分のテンプレートを知られることのないように安全に処理を行う。詳細は後記する。

【００１２】

また、クライアント端末において、ユーザの所持する記憶媒体に格納された単一のマスタ鍵と、認証サーバが管理する乱数とから、パラメータを作成することで、耐タンパデバイスに格納すべきデータは単一のマスタ鍵のみとなるようにする。詳細は後記する。

【発明の効果】

【００１３】

本発明によれば、ユーザのクライアント端末と複数設置した認証サーバとが接続されるキャンセラブル生体認証システムにおいて、認証サーバ間で安全にテンプレートを共有することにより、ユーザやサービスプロバイダにとっての登録に関する負担を軽減することができる。また、クライアント端末において、既存の記憶媒体のメモリ容量で多数の認証サーバに対応可能とすることができる。

【発明を実施するための最良の形態】

【００１４】

以下、本発明の生体認証システムを実施するための最良の形態（以下、「実施形態」という。）について説明する。説明する際には、本明細書と同時に提出する図面を適宜参照する。

【００１５】

１．概要

本実施形態の生体認証システムは、認証サーバはサービスプロバイダごとに設置され、ユーザはクライアント端末で指静脈画像を入力するとともに、ユーザの所持する耐タンパデバイス（記憶媒体）を提示し、認証サーバは指静脈特徴量を秘匿したまま指静脈照合を行う、キャンセラブル指静脈認証システムを例にして説明する。本実施形態では、キャンセラブル指静脈認証システムにおいて実行される、登録処理（ユーザ登録処理）、テンプレート共有処理、認証処理及びテンプレート更新処理の４つの処理について中心的に説明する。まず、その４つの処理がどのような情報処理であるか簡単に説明する。なお、説明を分かり易くするため、認証サーバは、第一の認証サーバと第二の認証サーバの２つが設置されているものとして説明する。

【００１６】
登録処理では、以下の流れを実行する。ここでは第一の認証サーバへの登録（ユーザ登録）を行うこととする。ユーザは、クライアント端末に接続されたセンサに対して生体情報を入力する。クライアント端末は、入力された生体情報から特徴量を抽出する。また、クライアント端末は、マスタ鍵（認証サーバの各々に対応したパラメータを作成可能な鍵データ）を生成して耐タンパデバイスに格納する。第一の認証サーバは、乱数を生成してクライアント端末に送信する。クライアント端末は、第一の認証サーバから受信した乱数と耐タンパデバイス内のマスタ鍵とからパラメータを作成する。クライアント端末は、パラメータを用いて特徴量を変換し、変換特徴量を第一の認証サーバに送信する。第一の認証サーバは、受信した変換特徴量（照合用の変換特徴量）と前記乱数とをまとめてテンプレートとして登録する。
【００１７】
テンプレート共有処理では、以下の流れを実行する。ここでは第一の認証サーバから第二の認証サーバ（他の認証サーバ）へテンプレートを渡すこととする。クライアント端末は、パラメータ差分を２つ作成し、第一のパラメータ差分（第一の差分パラメータ）を第一の認証サーバに送信し、第二のパラメータ差分（第二の差分パラメータ）を第二の認証サーバに送信する。第一の認証サーバは、受信した第一のパラメータ差分を登録済みのテンプレートに作用させ、一時テンプレート（一時的なテンプレート）を作成する。第一の認証サーバは、一時テンプレートを第二の認証サーバに送信する。第二の認証サーバは、受信した一時テンプレートに対して第二のパラメータ差分を作用させてテンプレートを作成し、登録する。これにより、第一の認証サーバは、自身が管理するテンプレートを秘匿したまま（つまり、登録済みのテンプレート自体は外部に出力することなく）、第二の認証サーバへテンプレートを渡すことができ、テンプレート共有を安全に実現できる。したがって、テンプレートの共有とは、テンプレートを受け取る認証サーバ自身が、テンプレートを渡す認証サーバの管理するテンプレートを利用して、テンプレートを受け取る認証サーバにとって専用のテンプレートを作成することを意味する。
【００１８】
認証処理では、以下の流れを実行する。例として、ここでは、第一の認証サーバでの認証を行うこととする。ユーザは、クライアント端末に接続されたセンサに対して生体情報を入力する。クライアント端末は、生体情報から特徴量を抽出する。第一の認証サーバは、既に登録済みのテンプレートに含まれている乱数をクライアント端末に送信する。クライアント端末は、第一の認証サーバから受信した乱数と耐タンパデバイス内のマスタ鍵からパラメータを作成する。クライアント端末は、パラメータを用いて特徴量を変換し、変換特徴量を第一の認証サーバに送信する。第一の認証サーバは、受信した変換特徴量とテンプレートに含まれた変換特徴量とを照合し、本人か否か判定する。
【００１９】
テンプレート更新処理では、以下の流れを実行する。例として、ここでは、第一の認証サーバでの更新を行うこととする。第一の認証サーバは、第一の乱数を生成し、第一の乱数と登録済みのテンプレートに含まれている第二の乱数とをクライアント端末に送信する。クライアント端末は、第一の乱数と第二の乱数に応じてパラメータ差分を作成し、第一の認証サーバに送信する。第一の認証サーバは、パラメータ差分をテンプレートに作用させ、新たなテンプレートを作成する。これにより、テンプレートを更新する。
【００２０】
２．構成
次に、本実施形態のキャンセラブル指静脈生体認証システムの構成について詳細に説明する。
【００２１】
２．１．キャンセラブル指静脈生体認証システムの構成
図１は、本実施形態のキャンセラブル指静脈生体認証システムの構成をブロック図として図示したものである。本実施形態のキャンセラブル指静脈認証システムは第一の認証サ

ーバ１００、第二の認証サーバ１１０、クライアント端末１２０、指静脈センサ１３０、耐タンパデバイス１４０、ネットワーク網１５０から構成される。第一の認証サーバ１００、第二の認証サーバ１１０及びクライアント端末１２０はネットワーク網１５０に接続されている。また、クライアント端末１２０には、指静脈センサ１３０と耐タンパデバイス１４０が接続されている。なお、説明の便宜上、第一の認証サーバ１００や第二の認証サーバ１１０を単に「認証サーバ」と呼ぶ場合がある。

【００２２】

第一の認証サーバ１００は、登録処理により全ユーザのテンプレートを保管している。認証処理時には、クライアント端末１２０から送信されてきた変換特徴量とテンプレートに含まれた変換特徴量との照合を行う。テンプレート共有処理時には、パラメータ差分をクライアント端末１２０から受信し、一時テンプレートを作成し、一時テンプレートを第二の認証サーバ１１０に送信する。一時テンプレートを受信した第二の認証サーバ１１０は、パラメータ差分をクライアント端末１２０から受信し、テンプレートを作成し、登録する。テンプレート更新処理時には、クライアント端末１２０からパラメータ差分を受け取り、テンプレートを更新する。

【００２３】

なお、第一の認証サーバ１００は、例えば、キーボードやマウス等で実装された入力部１００ａ、ＣＰＵ（Central Processing Unit：中央制御装置）等で実装された制御部１００ｂ、読み書きされるデータを展開するための記憶領域を確保するＲＡＭ(Random Access Memory)や外部記憶装置としてのＨＤＤ（Hard Disk Drive）等で実装された記憶部１００ｃ及びディスプレイやプリンタ等で実装された出力部１００ｄといったハードウェア資源を備えた、一般的なコンピュータである。そして、制御部１００ｂは、後記する認証処理等の処理を実行するためのプログラムを格納したＲＯＭ（Read Only Memory）等の認証サーバ用の記録媒体から、そのプログラムを読み出す。

【００２４】

また、第一の認証サーバ１００は、サービスプロバイダがユーザに所定のサービスを提供するために設置したサーバであるので、一般的には、そのサービスを提供するために実行するアプリケーションを備えているが、アプリケーションを備えているか否かは任意的事項であり、本実施形態においてはアプリケーションに関する説明は省略する。

【００２５】

第二の認証サーバ１１０は、第一の認証サーバ１００と同様の機能を有する。従って、第二の認証サーバ１１０が備える入力部１１０ａ、制御部１１０ｂ、記憶部１１０ｃ及び出力部１１０ｄといったハードウェア資源は、それぞれ、入力部１００ａ、制御部１００ｂ、記憶部１００ｃ及び出力部１００ｄと同等の機能を有する。

【００２６】

クライアント端末１２０は、登録処理時には、マスタ鍵を生成し、そのマスタ鍵と認証サーバから取得した乱数とを用いてパラメータを作成する。また指静脈センサ１３０からユーザの指静脈画像を取得して特徴量を抽出し、パラメータを用いて変換する。さらに変換特徴量を認証サーバに送信し、認証サーバに登録する。最後にマスタ鍵を耐タンパデバイス１４０に書き込む。認証処理時には、耐タンパデバイス１４０からマスタ鍵を読み出し、パラメータを作成する。またユーザの指静脈画像を取得して特徴量を抽出し、パラメータを用いて変換する。さらに変換特徴量を認証サーバに送信し、認証サーバにて照合する。テンプレート更新処理時には、パラメータ差分を生成し、認証サーバに送信する。

【００２７】

なお、クライアント端末１２０は、例えば、キーボードやマウス等で実装された入力部１２０ａ、ＣＰＵ等で実装された制御部１２０ｂ、読み書きされるデータを展開するための記憶領域を確保するＲＡＭや外部記憶装置としてのＨＤＤ等で実装された記憶部１２０ｃ及びディスプレイやプリンタ等で実装された出力部１２０ｄといったハードウェア資源を備えた、一般的なコンピュータである。そして、制御部１２０ｂは、後記する、ユーザの生体情報から特徴量を抽出する処理等を実行するためのプログラムを格納したＲＯＭ等

のクライアント端末用の記録媒体から、そのプログラムを読み出す。

【００２８】

指静脈センサ１３０は、ユーザの指に近赤外光を照射し、その透過光から得られる指の指静脈画像を撮影することによりユーザの生体情報を検出する。撮影した指静脈画像は、クライアント端末１２０に送信される。

【００２９】

耐タンパデバイス１４０は、マスタ鍵を保管する記憶媒体であり、例えば、クライアント端末１２０と接続可能な耐タンパ性を備えるＩＣ（Integrated Circuit）カード等によって実装される。登録処理時には、クライアント端末１２０からマスタ鍵を受信して格納する。認証処理時には、テンプレート共有処理時及びテンプレート更新処理時においては、クライアント端末１２０からの要求に応じてマスタ鍵を出力する。

【００３０】

２．２．認証サーバの機能構成

図２は、第一の認証サーバ１００の機能構成をブロック図として図示したものである。

【００３１】

第一の認証サーバ１００は、照合部１０１、通信部１０２、変換部１０３、乱数生成部１０４及びテンプレート保管部１０５、から構成される。

【００３２】

登録処理時には、乱数生成部１０４で乱数r_1を生成し、通信部１０２によりクライアント端末１２０に送信する。通信部１０２によりクライアント端末１２０から送信されてきた変換特徴量K_1F（パラメータK_1を特徴量Ｆに作用させた値）を受け取り、乱数r_1と変換特徴量K_1Fとをまとめてテンプレート（r_1、K_1F）として保存する。本実施形態では、テンプレートとは、乱数とその乱数を用いて作成された変換特徴量とを構成要素として含んだ登録情報を意味する。テンプレート保管部１０５では、全ユーザのテンプレートを保管する。本実施形態では、テンプレートを保管する場合には、テンプレートデータベースを用いる。

【００３３】

図３は、テンプレート保管部１０５がテンプレートを保管する場合に用いるテンプレートデータベースのデータ構造を図示したものである。このテンプレートデータベースは、登録に関する手続を済ませたユーザを識別する情報としてユーザ識別番号を登録したユーザ識別番号フィールド１０５ａと、そのユーザに対応するテンプレートを登録したテンプレートフィールド１０５ｂとを備えている。例えば、ユーザ識別番号が００００１として登録されたユーザに対して、（r_1、K_1F_1）というテンプレートを割り当てることによって、そのユーザを管理している。ここで（r_1、K_1F_1）というテンプレートは、第一の認証サーバ１００が生成した乱数r_1と、ユーザ識別番号が００００１であるユーザの特徴量F_1にクライアント端末１２０が作成したパラメータK_1を作用させて作成した変換特徴量K_1F_1とを構成要素として含んだ登録情報である。

【００３４】

認証処理時には、認証の実行を要求したクライアント端末１２０のユーザのユーザ識別番号を用いてテンプレート保管部１０５からテンプレート（r_1、K_1F）を読み出し、通信部１０２により乱数r_1をクライアント端末１２０に送信する。通信部１０２により変換特徴量K_1Gをクライアント端末１２０から受信し、照合部１０１がK_1GとK_1Fとを照合し、本人か否か判定する。

【００３５】

第一の認証サーバ１００がテンプレートを渡すテンプレート共有処理時には、テンプレート保管部１０５からテンプレート（r_1、K_1F）を読み出して乱数r_1を取得し、また乱数生成部１０４で乱数ｒ’を生成し、通信部１０２によりr_1とｒ’とをクライアント端末１２０に送信する。通信部１０２によりクライアント端末１２０からパラメータ差分ΔK_1（第一の差分パラメータ）を受信し、変換部１０３はパラメータ差分ΔK_1を用いて、K_1Fを変換し、一時テンプレート（ｒ’、Ｋ’Ｆ）を作成する。通信部１０２に

より、作成した一時テンプレート（ｒ’、Ｋ’Ｆ）を第二の認証サーバ１１０に送信する。

【００３６】

テンプレート更新処理時には、乱数生成部１０４で乱数r_1’を生成し、テンプレート保管部１０５からテンプレート（r_1、K_1F）を読み出し、通信部１０２によりr_1とr_1’とをクライアント端末１２０に送信する。通信部１０２によりクライアント端末１２０からパラメータ差分ΔK_1’を受信し、変換部１０３はパラメータ差分ΔK_1’を用いて、K_1Fを変換し、K_1’Ｆを作成する。テンプレート保管部１０５には、新たなテンプレートとして（r_1’、K_1’Ｆ）を登録する。

【００３７】

なお、第二の認証サーバ１１０の機能構成は、第一の認証サーバ１００のそれと同様である。第二の認証サーバ１１０がテンプレートを受け取るテンプレート共有処理時には、通信部１０２により、第一の認証サーバ１００から一時テンプレート（ｒ’、Ｋ’Ｆ）を受信し、乱数生成部１０４で乱数r_2を生成し、通信部１０２によりr_2とｒ’とをクライアント端末１２０に送信する。クライアント端末１２０からパラメータ差分ΔK_2（第二の差分パラメータ）を受信すると、変換部１０３は、パラメータ差分ΔK_2を用いてＫ’Ｆを変換し、K_2Fを作成する。テンプレート保管部１０５には、新たなテンプレートとして（r_2、K_2F）を登録する。

【００３８】

２．３．クライアント端末の構成

図４は、クライアント端末１２０の機能構成をブロック図として図示したものである。

クライアント端末１２０は、特徴抽出部１２１、変換部１２２、通信部１２３、パラメータ作成部１２４、マスタ鍵作成部１２５および耐タンパデバイスＩ／Ｆ（Interface）部１２６、から構成される。また、指静脈センサ１３０が接続されている。

【００３９】

第一の認証サーバ１００への登録処理時には、マスタ鍵作成部１２５においてマスタ鍵Ｓを作成する。通信部１２３により第一の認証サーバ１００から乱数r_1を受信する。パラメータ作成部１２４は、乱数r_1とマスタ鍵Ｓとから所定の関数を用いた演算を行い、パラメータK_1を作成する。特徴抽出部１２１は、ユーザが指静脈センサ１３０から入力した指静脈画像から特徴量Ｆを抽出する。変換部１２２は、パラメータK_1を用いて特徴量Ｆを変換して、変換特徴量K_1Fを作成する。作成後、通信部１２３により第一の認証サーバ１００に、変換特徴量K_1Fを送信する。なお、マスタ鍵Ｓは、耐タンパデバイスＩ／Ｆ部１２６を介して耐タンパデバイス１４０に格納する。

【００４０】

第一の認証サーバ１００での認証処理時には、耐タンパデバイスＩ／Ｆ部１２６を介して耐タンパデバイス１４０からマスタ鍵Ｓを読み出し、通信部１２３により第一の認証サーバ１００から乱数r_1を受信し、パラメータ作成部１２４が乱数r_1とマスタ鍵ＳとからパラメータK_1を作成する。特徴抽出部１２１は、ユーザが指静脈センサ１３０から入力した指静脈画像から特徴量Ｇを抽出する。変換部１２２は、パラメータK_1を用いて特徴量Ｇを変換して、変換特徴量K_1Gを作成する。作成後、通信部１２３により第一の認証サーバ１００に、変換特徴量K_1Gを送信する。

【００４１】

第一の認証サーバ１００から第二の認証サーバ１１０へのテンプレート共有処理時には、まず、通信部１２３により第一の認証サーバ１００から乱数r_1とｒ’とを受信する。耐タンパデバイスＩ／Ｆ部１２６を介して耐タンパデバイス１４０からマスタ鍵Ｓを読み出す。パラメータ作成部１２４は、マスタ鍵Ｓ、r_1、およびｒ’から、パラメータ差分ΔK_1を作成し、通信部１２３によりパラメータ差分ΔK_1を第一の認証サーバ１００に送信する。その後、通信部１２３により第二の認証サーバ１１０から乱数r_2とｒ’とを受信する。耐タンパデバイスＩ／Ｆ部１２６を介して耐タンパデバイス１４０からマスタ鍵Ｓを読み出す。パラメータ作成部１２４は、マスタ鍵Ｓ、r_2、およびｒ’から、パラ

メータ差分ΔＫ$_2$を作成し、通信部１２３によりパラメータ差分ΔＫ$_2$を第二の認証サーバ１１０に送信する。

【００４２】

第一の認証サーバ１００でのテンプレート更新処理時には、通信部１２３により第一の認証サーバ１００から乱数ｒ$_1$とｒ$_1$’とを受信する。耐タンパデバイスＩ／Ｆ部１２６を介して耐タンパデバイス１４０からマスタ鍵Ｓを読み出す。パラメータ作成部１２４は、マスタ鍵Ｓ、ｒ$_1$、およびｒ$_1$’から、パラメータ差分ΔＫ$_1$’を作成し、通信部１２３によりパラメータ差分ΔＫ$_1$’を第一の認証サーバ１００に送信する。

【００４３】

２．４．耐タンパデバイスの構成

図５は、耐タンパデバイス１４０の機能構成をブロック図として図示したものである。

耐タンパデバイス１４０は、通信部１４１、およびマスタ鍵保管部１４２、から構成される。

【００４４】

登録処理時には、通信部１４１によりクライアント端末１２０からマスタ鍵Ｓを受信し、マスタ鍵保管部１４２に格納する。

【００４５】

認証処理時、テンプレート共有処理時、テンプレート更新処理時には、クライアント端末１２０からの要求に応じて、通信部１４１によりマスタ鍵Ｓをクライアント端末１２０に出力する。

【００４６】

３．キャンセラブル指静脈生体認証システムにおける処理

次に、本実施形態のキャンセラブル指静脈生体認証システムにおいて行われる処理について説明する。説明する処理は、登録処理、テンプレート共有処理、認証処理およびテンプレート更新処理の４つである。

【００４７】

３．１．登録処理

図６は、本実施形態における、第一の認証サーバ１００での登録処理のフローを図示したものである。この登録処理は、例えば、ユーザから身分証明書が提示されるなどして登録に必要な準備が完了した後に実行される。

【００４８】

ステップＳ２０１で、第一の認証サーバ１００は、乱数ｒ$_1$を生成する。第一の認証サーバ１００は、乱数ｒ$_1$をクライアント端末１２０に送信する。

【００４９】

ステップＳ２０２で、クライアント端末１２０は、指静脈センサ１３０によってユーザから指静脈画像を取得する。

【００５０】

ステップＳ２０３で、クライアント端末１２０は、取得した指静脈画像から当該ユーザを特定することができる特徴量Ｆを抽出する。本実施形態では、特徴量の抽出方法は、例えば、下記文献１に記載の方法などによるものとし、詳細な説明は省略する。

（文献１）

Naoto Miura, Akio Nagasaka, and Takafumi Miyatake, “Feature extraction of finger-vein patterns based on repeated line tracking and it's application to personal identification”, Machine Vision and Applications, Vol.15, pp.194-203, 2004

【００５１】

ステップＳ２０４で、クライアント端末１２０は、マスタ鍵Ｓを生成する。本実施形態ではマスタ鍵生成の方法は、通常の乱数生成の方法によるものとするが、これに限定するものではない。

【００５２】

ステップＳ２０５で、クライアント端末１２０は、第一の認証サーバ１００から受信し

た乱数r_1とマスタ鍵Ｓとから、パラメータK_1を作成する。本実施形態ではパラメータK_1の作成方法は、乱数r_1とマスタ鍵Ｓとをビット連結し、ハッシュ関数を用いてそのハッシュ値をとる、という方法によるものとするが、これに限定するものではない。

【００５３】

ステップＳ２０６で、クライアント端末１２０は、パラメータK_1を用いて特徴量Ｆを変換する。本実施形態では、変換の方法は、例えば、下記文献２に記載の方法によるものとし、詳細な説明は省略する。変換後の特徴量（変換特徴量）K_1Ｆは、第一の認証サーバ１００に送信する。また、マスタ鍵Ｓは、耐タンパデバイス１４０に送信する。

（文献２）

比良田真史、高橋健太、三村昌弘、“画像マッチングに基づく生体認証に適用可能なキャンセラブルバイオメトリクスの提案”、2006-CSEC-34、pp.45-440、2006

【００５４】

ステップＳ２０７で、第一の認証サーバ１００は、乱数r_1と変換特徴量K_1Ｆとをまとめてテンプレート（r_1、K_1Ｆ）とし、テンプレート保管部１０５に登録する。その登録の際、登録を済ませたユーザのユーザ識別番号が決定される。ユーザ識別番号は、認証サーバが個人認証を行うときにクライアント端末１２０ａの入力部１２０から入力される情報であり、テンプレートデータベース（図３参照）の検索キーとして用いられる。テンプレートデータベースにおいて、ユーザ識別フィールド１０５ａには登録を済ませたユーザのユーザ識別番号が登録される。また、テンプレートフィールド１０５ｂには、そのユーザのテンプレートが登録される。

【００５５】

ステップＳ２０８で、耐タンパデバイス１４０は、クライアント端末１２０から受信したマスタ鍵Ｓを保存する。

【００５６】

クライアント端末１２０から第一の認証サーバ１００に送信される情報は変換特徴量K_1Ｆであり、パラメータK_1でも、特徴量Ｆでもない。第一の認証サーバ１００が何らかの原因により変換特徴量K_1Ｆを漏洩したとしても、特徴量Ｆそのものが漏洩したわけではないので、ユーザの元の生体情報は秘匿されている。また、第一の認証サーバ１００は変換特徴量K_1ＦだけからパラメータK_1や特徴量Ｆを求めることは不可能あり、第一の認証サーバ１００自身に対してもユーザの元の生体情報は秘匿されている。

【００５７】

３．２．テンプレート共有処理

図７は、本実施形態における、第一の認証サーバ１００から第二の認証サーバ１１０へのテンプレート共有処理のフローを図示したものである。このテンプレート共有処理は、例えば、第二の認証サーバ１１０から第一の認証サーバ１００に対してテンプレートの取得要求があったときに実行される。また、第二の認証サーバ１１０は、例えば、ユーザが第二の認証サーバ１１０が提供するサービスを利用するための入力（ユーザ識別番号などの入力）をクライアント端末１２０から行った場合に前記テンプレートの取得要求を実行する。

【００５８】

ステップＳ３０１で、第一の認証サーバ１００は、乱数ｒ’を生成する。第一の認証サーバ１００は、テンプレート保管部１０５において、クライアント端末１２０のユーザのユーザ識別番号を検索キーとしてテンプレートデータベースを検索し、検索キーのユーザ識別番号と、ユーザ識別番号フィールド１０５ａに登録されたユーザ識別番号とが一致した場合、テンプレートフィールド１０５ｂにおいて、そのユーザ識別番号に対応したテンプレート（r_1、K_1Ｆ）を読み出す。そして、読み出したテンプレート（r_1、K_1Ｆ）からr_1を読み出し、r_1とｒ’とをクライアント端末１２０に送信する。

【００５９】

ステップＳ３０２で、クライアント端末１２０は、耐タンパデバイス１４０からマスタ鍵Ｓを読み出し、第一の認証サーバ１００から受信したr_1、ｒ’とマスタ鍵Ｓからパラ

メータ差分ΔＫ$_1$を作成する。パラメータ差分ΔＫ$_1$の作成方法としては、例えば、次のような方法がある。まず、マスタ鍵Ｓとｒ$_1$とからパラメータＫ$_1$を作成する。これは、例えば、乱数ｒ$_1$とマスタ鍵Ｓとをビット連結し、ハッシュ関数を用いてそのハッシュ値をとる方法がある。また、マスタ鍵Ｓとｒ’とからパラメータＫ’を作成する。これは、例えば、乱数ｒ’とマスタ鍵Ｓとをビット連結し、ハッシュ関数を用いてそのハッシュ値をとる方法がある。ここで、Ｋ$_1$、Ｋ’、ΔＫ$_1$は画像（互いに直交するｘ軸とｙ軸とからなる２次元画像）と捉えることができるため、それぞれＫ$_1$（ｘ、ｙ）、Ｋ’（ｘ、ｙ）、ΔＫ$_1$（ｘ、ｙ）と表記できる。そして、ΔＫ$_1$（ｘ、ｙ）は、具体的には、

ΔＫ$_1$（ｘ、ｙ）＝Ｋ’（ｘ、ｙ）／Ｋ$_1$（ｘ、ｙ）

で求める。クライアント端末１２０は、作成したΔＫ$_1$を第一の認証サーバ１００に送信する。

【００６０】

ステップＳ３０３で、第一の認証サーバ１００は、一時テンプレート（ｒ’、Ｋ’Ｆ）を作成する。Ｋ’Ｆの作成方法は、例えば、次のような方法がある。ここで、Ｋ$_1$Ｆ、Ｋ’Ｆは画像（互いに直交するｘ軸とｙ軸とからなる２次元画像）と捉えられるため、それぞれＫ$_1$（ｘ、ｙ）Ｆ（ｘ、ｙ）、Ｋ’（ｘ、ｙ）Ｆ（ｘ、ｙ）と表記できる。そして、Ｋ’（ｘ、ｙ）Ｆ（ｘ、ｙ）は、具体的には、

Ｋ’（ｘ、ｙ）Ｆ（ｘ、ｙ）＝ΔＫ$_1$（ｘ、ｙ）×Ｋ$_1$（ｘ、ｙ）Ｆ（ｘ、ｙ）

で求められる。ステップＳ３０１で生成した乱数ｒ’とＫ’Ｆとをまとめて一時テンプレート（ｒ’、Ｋ’Ｆ）とし、第二の認証サーバ１１０に送信する。

【００６１】

ステップＳ３０４で、第二の認証サーバ１１０は、乱数ｒ$_2$を生成する。本実施形態では乱数生成は通常の方法によるものとするが、これに限定するものではない。その後、第一の認証サーバ１００から受信した一時テンプレート（ｒ’、Ｋ’Ｆ）からｒ’を読み出し、ｒ$_2$とｒ’をクライアント端末１２０に送信する。

【００６２】

ステップＳ３０５で、クライアント端末１２０は、第二の認証サーバ１１０から受信したｒ$_2$、ｒ’とマスタ鍵Ｓからパラメータ差分ΔＫ$_2$を作成する。パラメータ差分ΔＫ$_2$の作成方法としては、例えば、次のような方法がある。まず、マスタ鍵Ｓとｒ$_2$からパラメータＫ$_2$を作成する。これは、例えば、乱数ｒ$_2$とマスタ鍵Ｓとをビット連結し、ハッシュ関数を用いてそのハッシュ値をとる方法がある。また、マスタ鍵Ｓとｒ’とからパラメータＫ’を作成する。これは、例えば、乱数ｒ’とマスタ鍵Ｓとをビット連結し、ハッシュ関数を用いてそのハッシュ値をとる方法がある。ここで、Ｋ$_2$、Ｋ’、ΔＫ$_2$は画像（互いに直交するｘ軸とｙ軸とからなる２次元画像）と捉えることができるため、それぞれＫ$_2$（ｘ、ｙ）、Ｋ’（ｘ、ｙ）、ΔＫ$_2$（ｘ、ｙ）と表記できる。そして、ΔＫ$_2$（ｘ、ｙ）は、具体的には、

ΔＫ$_2$（ｘ、ｙ）＝Ｋ$_2$（ｘ、ｙ）／Ｋ’（ｘ、ｙ）

で求める。クライアント端末１２０は、作成したΔＫ$_2$を第二の認証サーバ１１０に送信する。

【００６３】

ステップＳ３０６で、第二の認証サーバ１１０は、一時テンプレート（ｒ’、Ｋ’Ｆ）のＫ’Ｆに対して、クライアント端末１２０から受信したΔＫ$_2$を用いて変換を実行し、Ｋ$_2$Ｆを作成する。変換の方法は、例えば、次のような方法がある。ここで、ΔＫ$_2$、Ｋ’Ｆ、Ｋ$_2$Ｆは画像（互いに直交するｘ軸とｙ軸とからなる２次元画像）と捉えることが

できるため、それぞれΔＫ$_2$（ｘ、ｙ）、Ｋ’（ｘ、ｙ）Ｆ（ｘ、ｙ）、Ｋ$_2$（ｘ、ｙ）Ｆ（ｘ、ｙ）と表記できる。そして、Ｋ$_2$（ｘ、ｙ）Ｆ（ｘ、ｙ）は、具体的には、

Ｋ$_2$（ｘ、ｙ）Ｆ（ｘ、ｙ）＝ΔＫ$_2$（ｘ、ｙ）×Ｋ’（ｘ、ｙ）Ｆ（ｘ、ｙ）

によって求める。

【００６４】

ステップＳ３０７で、第二の認証サーバ１１０は、乱数ｒ$_2$とＫ$_2$Ｆをまとめてテンプレート（ｒ$_2$、Ｋ$_2$Ｆ）として、テンプレート保管部１０５に登録する。テンプレートデータベースにおいて、ユーザ識別フィールド１０５ａには、テンプレート共有処理に関わったクライアント端末１２０のユーザのユーザ識別番号が登録される。また、テンプレートフィールド１０５ｂには、そのユーザのテンプレートが登録される。

【００６５】

これにより、第一の認証サーバ１００は、自身が管理するテンプレート（ｒ$_1$、Ｋ$_1$Ｆ）を秘匿したまま（つまり、（ｒ$_1$、Ｋ$_1$Ｆ）自体を第二の認証サーバ１１０に知られること無く）、第二の認証サーバ１１０にテンプレートを（ｒ$_2$、Ｋ$_2$Ｆ）として渡すことが可能なため、認証サーバ間でのテンプレート共有を安全に実現できる。また、クライアント端末１２０から認証サーバに送信される情報はパラメータＫ$_1$やＫ$_2$そのものではなく、その差分である。よって、パラメータを送信して、テンプレートの変換特徴量Ｋ$_1$Ｆ、Ｋ$_2$Ｆを構成する特徴量Ｆ自体が認証サーバに知られてしまうといった懸念もない。

【００６６】

３．３．認証処理

図８は、本実施形態における、第一の認証サーバ１００での認証処理のフローを図示したものである。この認証処理は、例えば、ユーザが第一の認証サーバ１００が提供するサービスを利用するための入力（ユーザ識別番号などの入力）をクライアント端末１２０から行った場合に実行される。

【００６７】

ステップＳ４０１で、クライアント端末１２０は、指静脈センサ１３０によってユーザの指静脈画像を取得する。

【００６８】

ステップＳ４０２で、クライアント端末１２０は、取得した指静脈画像から特徴量Ｇを抽出する。本実施形態では、特徴量の抽出方法は、例えば、文献１に記載の方法などによるものとし、詳細な説明は省略する。

【００６９】

ステップＳ４０３で、クライアント端末１２０は、第一の認証サーバ１００からｒ$_1$を受信し、マスタ鍵Ｓを耐タンパデバイス１４０から読み出し、パラメータＫ$_1$を作成する。

【００７０】

ここで第一の認証サーバ１００は、クライアント端末１２０にｒ$_1$を送信する場合には、以下の処理行う。すなわち、テンプレート保管部１０５において、クライアント端末１２０のユーザのユーザ識別番号を検索キーとしてテンプレートデータベースを検索し、検索キーのユーザ識別番号と、ユーザ識別番号フィールド１０５ａに登録されたユーザ識別番号とが一致した場合、テンプレートフィールド１０５ｂにおいて、そのユーザ識別番号に対応したテンプレート（ｒ$_1$、Ｋ$_1$Ｆ）を読み出す。そして、読み出したテンプレート（ｒ$_1$、Ｋ$_1$Ｆ）からｒ$_1$を読み出し、ｒ$_1$をクライアント端末１２０に送信する。

【００７１】

本実施形態では、パラメータＫ$_1$の作成方法は、例えば、乱数ｒ$_1$とマスタ鍵Ｓとをビット連結し、ハッシュ関数を用いてそのハッシュ値をとる方法によるものとするが、これに限定するものではない。

【００７２】

ステップＳ４０４で、クライアント端末１２０は、パラメータK_1を用いて特徴量Ｇを変換する。本実施形態では、変換の方法は、例えば、文献２に記載の方法によるものとし、詳細な説明は省略する。変換後の特徴量（変換特徴量）K_1Ｇを第一の認証サーバ１００に送信する。

【００７３】

ステップＳ４０５で、第一の認証サーバ１００は、受信したK_1Ｇとテンプレート（r_1、K_1Ｆ）のK_1Ｆとを照合し、本人か否かを判定する。本実施形態では、照合の方法は、例えば、文献２に記載の方法によるものとし、詳細な説明は省略する。従来の認証のように、認証を行うために一旦暗号化したものを復号化せず、特徴量を変換した状態で照合を行うことができる。

【００７４】

３．４．テンプレート更新処理

図９は、本実施形態における、第一の認証サーバ１００でのテンプレート更新処理のフローを図示したものである。このテンプレート更新処理は、例えば、第一の認証サーバ１００が、ユーザからユーザ識別番号などの入力があって、登録済みのテンプレートに含まれる変換特徴量を変更したいという要求を受けた場合に実行する。または、何らかの不測の事態により、登録済みのテンプレートが漏洩した場合に実行する。

【００７５】

ステップＳ５０１で、第一の認証サーバ１００は、乱数r_1’を生成する。本実施形態では、乱数生成は通常の方法によるものとするが、これに限定するものではない。第一の認証サーバ１００は、テンプレート保管部１０５において、クライアント端末１２０のユーザのユーザ識別番号を検索キーとしてテンプレートデータベースを検索し、検索キーのユーザ識別番号と、ユーザ識別番号フィールド１０５ａに登録されたユーザ識別番号とが一致した場合、テンプレートフィールド１０５ｂにおいて、そのユーザ識別番号に対応したテンプレート（r_1、K_1Ｆ）を読み出す。第一の認証サーバ１００は、r_1’とテンプレート（r_1、K_1Ｆ）から読み出したr_1をクライアント端末１２０に送信する。

【００７６】

ステップＳ５０２で、クライアント端末１２０は、耐タンパデバイス１４０から読み出したマスタ鍵Ｓ、r_1、およびr_1’から、パラメータ差分ΔK_1’を作成する。パラメータ差分ΔK_1’の作成方法としては、例えば、次のような方法がある。まず、マスタ鍵Ｓとr_1とからパラメータK_1を作成する。これは、例えば、乱数r_1とマスタ鍵Ｓとをビット連結し、ハッシュ関数を用いてそのハッシュ値をとる方法がある。また、マスタ鍵Ｓとr_1’とからパラメータK_1’を作成する。これは、例えば、乱数r_1’とマスタ鍵Ｓとをビット連結し、ハッシュ関数を用いてそのハッシュ値をとる方法がある。ここで、K_1、K_1’、ΔK_1’は画像（互いに直交するｘ軸とｙ軸とからなる２次元画像）と捉えることができるため、それぞれK_1（ｘ、ｙ）、K_1’（ｘ、ｙ）、ΔK_1’（ｘ、ｙ）と表記できる。そして、ΔK_1’（ｘ、ｙ）は、具体的には、

$$\Delta K_1'(x, y) = K_1'(x, y) / K_1(x, y)$$

で求める。クライアント端末１２０は、作成したΔK_1’を第一の認証サーバ１００に送信する。

【００７７】

ステップＳ５０３で、第一の認証サーバ１００は、受信したΔK_1’を用いて、テンプレート（r_1、K_1Ｆ）のK_1Ｆを変換して、新しい変換特徴量K_1’Ｆを作成する。変換方法は、例えば、次のような方法がある。ここで、K_1Ｆ、K_1’Ｆ、ΔK_1’は、画像（互いに直交するｘ軸とｙ軸とからなる２次元画像）と捉えることができるため、それぞれK_1（ｘ、ｙ）Ｆ（ｘ、ｙ）、K_1’（ｘ、ｙ）Ｆ（ｘ、ｙ）、ΔK_1’（ｘ、ｙ）と表記できる。そして、K_1’（ｘ、ｙ）Ｆ（ｘ、ｙ）は、具体的には、

$K_1'(x、y)F(x、y)=\Delta K_1'(x、y)\times K_1(x、y)F(x、y)$

で求められる。

【００７８】

ステップＳ５０４で、第一の認証サーバ１００は、r_1'とK_1'Ｆとをまとめて新しいテンプレート（r_1'、K_1'Ｆ）としてテンプレート保管部１０５において更新される。テンプレートデータベースにおいて、ユーザ識別フィールド１０５ａ内の、テンプレート更新処理に関わったユーザのユーザ識別番号を判別して、テンプレートフィールド１０５ｂにおいて、その判別したユーザの元のテンプレート（r_1、K_1Ｆ）に替えて、新しいテンプレート（r_1'、K_1'Ｆ）が登録される。元のテンプレート（r_1、K_1Ｆ）は破棄される。

【００７９】

これにより、元のテンプレートが漏洩しても、その漏洩の影響を抑えることができる。また、クライアント端末１２０から認証サーバに送信される情報はパラメータK_1やK_1'そのものではなく、その差分である。よって、パラメータを送信して、テンプレートの変換特徴量K_1ＦやK_1'Ｆを構成する特徴量Ｆ自体が認証サーバに知られてしまうといった懸念もない。

【００８０】

４．まとめ

本実施形態においては、複数の認証サーバを設置したキャンセラブル指静脈生体認証システムにおいて、認証サーバ間で安全にテンプレートを共有することにより、ユーザ及びサービスプロバイダにとっての登録に関する負担を軽減することができる。テンプレート共有処理によりテンプレートを受け取った認証サーバは、もはや登録処理を実行することはなく、登録窓口を設置する必要がなく、ユーザはその認証サーバに対して登録窓口に出向いて登録に必要となる手続を行う必要がなくなるからである。

【００８１】

また本実施形態においては、耐タンパデバイスに格納された単一のマスタ鍵と、認証サーバが管理する乱数とから、パラメータを作成することで、耐タンパデバイスに格納すべきデータは単一のマスタ鍵のみとなる。このため、認証サーバ毎にパラメータを格納していた場合と比べるとより少ないメモリ容量で済み、既存の耐タンパデバイスのメモリ容量で多数の認証サーバに対応可能となるメリットがある。

【００８２】

また、各ユーザの生体情報を認証サーバ間で共有することにより、クライアント端末に接続した指静脈センサを共有化することができ、それに伴うコストを削減することができる。

【００８３】

５．その他

なお、上述した形態は、本発明の生体認証システムを実施するための最良のものであるが、その実施形式はこれに限定する趣旨ではない。つまり、本発明の要旨を変更しない範囲内においてその実施形式を種々変形することは可能である。

【００８４】

５．１．認証サーバが３台以上の場合

本実施形態においては、認証サーバが２台設置された場合のシステムであるが、これが増えても構わない。またクライアント端末が複数台ある場合にも対応できる。

ここで、認証サーバの台数は、たとえ３台以上になったとしても、本発明の一般性は失われない。

【００８５】

例えば、テンプレート共有処理により、３台の認証サーバ間で一のユーザのテンプレートを共有する場合について説明する。既にテンプレートを登録済みの第一の認証サーバが第二の認証サーバ及び第三の認証サーバにテンプレートを渡す場合を採り上げる。この場

合、第二の認証サーバが第一の認証サーバからテンプレートを受け取り、第三の認証サーバも第一の認証サーバからテンプレートを受け取る、という第一のパターンと、第二の認証サーバが第一の認証サーバからテンプレートを受け取り、第三の認証サーバは第二の認証サーバからテンプレートを受け取る、という第二のパターンが想定される。

【００８６】

第一のパターンでは、第三の認証サーバが受け取るテンプレートは、一度のテンプレート共有処理によりテンプレートを受け取るのに対し、第二のパターンでは、第三の認証サーバが受け取るテンプレートは、二度のテンプレート共有処理を経てテンプレートを受け取る、という違いが生じる。しかし、本実施形態で行われるテンプレートの共有とは、テンプレートを受け取る認証サーバにとって専用のテンプレートを作成することを意味している。このため、第一のパターンであっても、第二のパターンであっても、第三の認証サーバが管理するテンプレートというのは、第三の認証サーバ自身が独自に作成したものである、という点で共通している。従って、第三の認証サーバが管理するテンプレートは第一の認証サーバにも、第二の認証サーバにも結局は知られることはない。この意味において、本発明の一般性が失われることはないということである。

【００８７】

５．２．パラメータについて

本実施形態では、クライアント端末において、特徴量を変換するパラメータを作成する際、マスタ鍵（例えば、乱数）と認証サーバから取得した乱数とをビット連結して、ハッシュ関数を用いてそのハッシュ値を取るものとした。しかし、ハッシュ関数のような、いわゆる一方向性関数として別の一方向性関数を用いて特徴量を変換し、その変換特徴量を元の特徴量に戻す、といった処理をできなくするようにしても良い。

【００８８】

５．３．耐タンパデバイスについて

本実施形態では、マスタ鍵を保管するために耐タンパデバイス１４０を用いたが、このようなデバイスが備える耐タンパ性を、論理的な手段によって高めても良いし、物理的な手段によって高めても良い。つまり、論理的な手段としては、逆アセンブラなどで簡単に解析できないようにする難読化技術などのソフトウェア的な技術を適用すればよい。また、物理的な手段としては、ＬＳＩ（Large Scale Integration Circuit）を解析するために保護層を剥がすと、内部の回路まで破壊されるようにするハードウェア的な技術を適用すればよい。

【００８９】

また、マスタ鍵は、耐タンパデバイス１４０に記憶させるのではなく、単に、ユーザ自身がパスワード（文字や数字、それらの組み合わせ等）として記憶していても良く、必ずしも耐タンパ性を備えたデバイスに格納させておく必要はない。ユーザは必要なときに、クライアント端末１２０の入力部１２０ａから、そのパスワードを入力すれば良い。

【産業上の利用可能性】

【００９０】

本発明は、生体情報をサーバに登録して照合を行う、任意の生体認証システムに対して適用可能である。例えば社内ネットワークにおける情報アクセス制御、インターネットバンキングシステムやＡＴＭ（Automated Teller Machine）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への適用が可能である。

【図面の簡単な説明】

【００９１】

【図１】本実施形態のキャンセラブル指静脈生体認証システムの構成をブロック図として図示したものである。

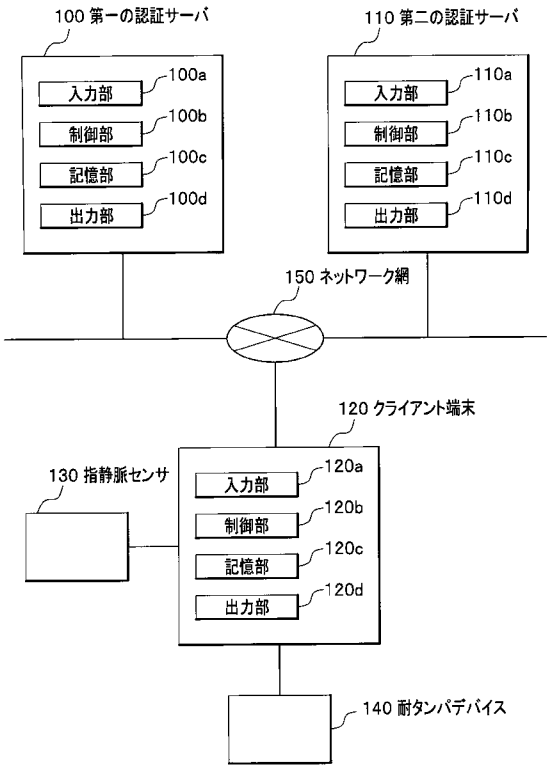
【図２】第一の認証サーバ１００の機能構成をブロック図として図示したものである。

【図３】テンプレート保管部１０５がテンプレートを保管する場合に用いるテンプレートデータベースのデータ構造を図示したものである。

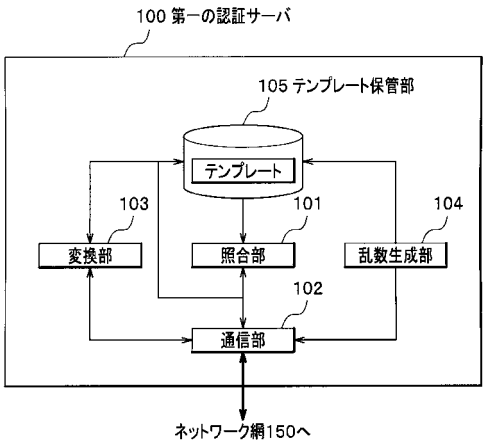
【図４】クライアント端末１２０の機能構成をブロック図として図示したものである。

【図５】耐タンパデバイス１４０の機能構成をブロック図として図示したものである。
【図６】本実施形態における、第一の認証サーバ１００での登録処理のフローを図示したものである。
【図７】本実施形態における、第一の認証サーバ１００から第二の認証サーバ１１０へのテンプレート共有処理のフローを図示したものである。
【図８】本実施形態における、第一の認証サーバ１００での認証処理のフローを図示したものである。
【図９】本実施形態における、第一の認証サーバ１００でのテンプレート更新処理のフローを図示したものである。
【符号の説明】
【００９２】
１００　　第一の認証サーバ
１１０　　第二の認証サーバ
１２０　　クライアント端末
１３０　　指静脈センサ
１４０　　耐タンパデバイス
１５０　　ネットワーク網

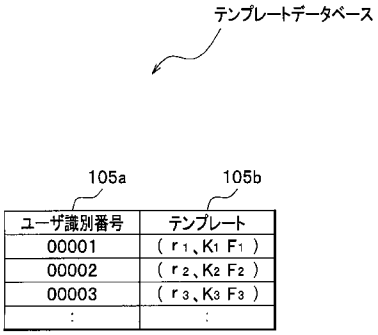
【図１】



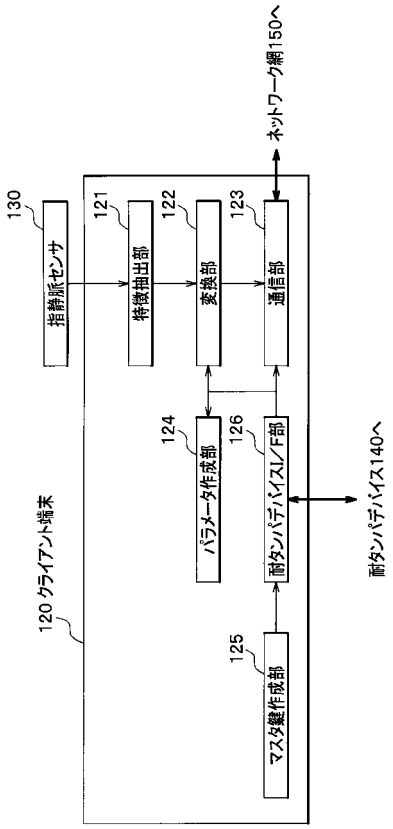
【図２】



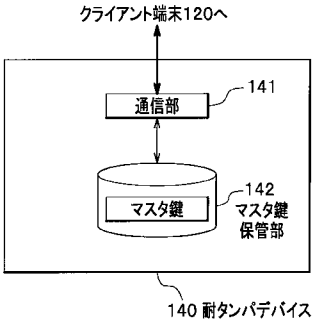
【図３】


テンプレートデータベース
105a
105b
ユーザ識別番号
テンプレート
00001
(r1、K1 F1)
00002
(r2、K2 F2)
00003
(r3、K3 F3)

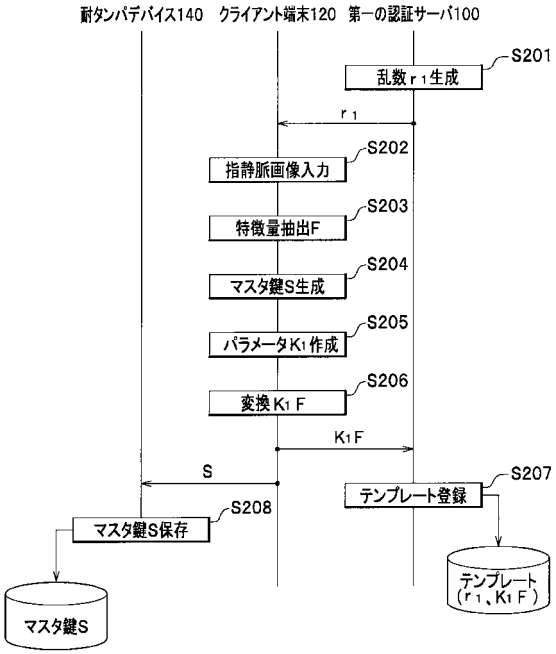
【図４】


ネットワーク網150へ
130
指静脈センサ
121
特徴抽出部
122
変換部
123
通信部
124
パラメータ作成部
126
耐タンパデバイスI/F部
耐タンパデバイス140へ
120 クライアント端末
125
マスタ鍵作成部

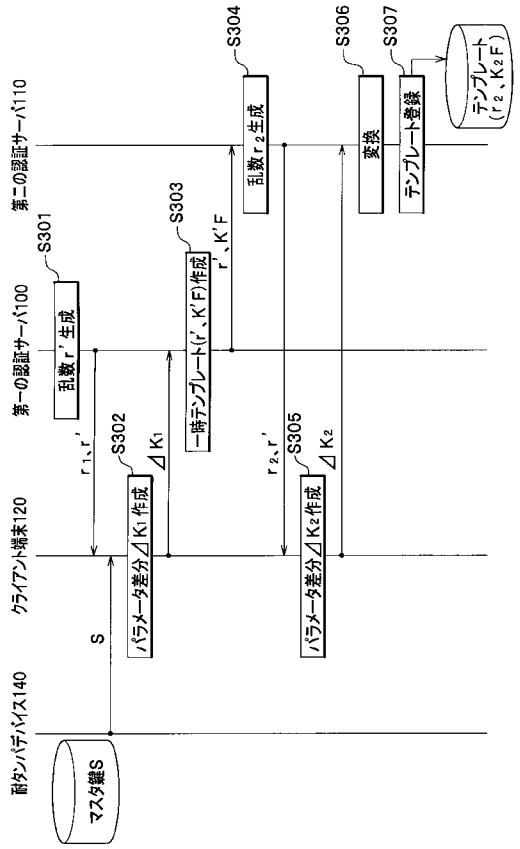
【図５】


クライアント端末120へ
通信部
141
マスタ鍵
142
マスタ鍵
保管部
140 耐タンパデバイス

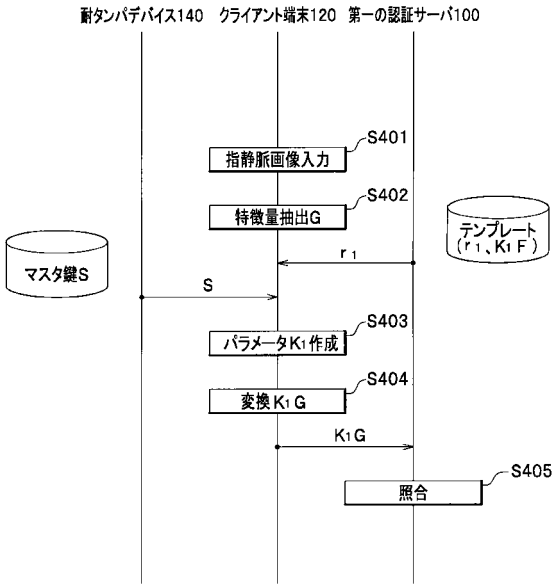
【図６】


耐タンパデバイス140
クライアント端末120
第一の認証サーバ100
S201
乱数r1生成
r1
S202
指静脈画像入力
S203
特徴量抽出F
S204
マスタ鍵S生成
S205
パラメータK1作成
S206
変換K1 F
K1F
S
S207
テンプレート登録
S208
マスタ鍵S保存
マスタ鍵S
テンプレート
(r1、K1 F)

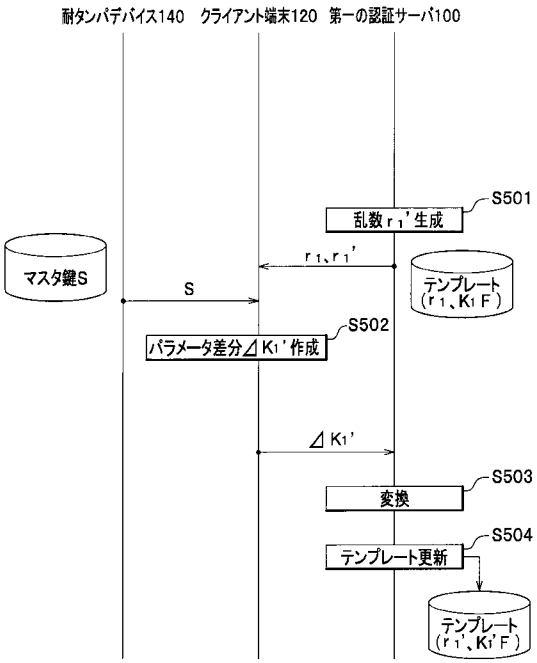
【図７】


第二の認証サーバ110
第一の認証サーバ100
クライアント端末120
耐タンパデバイス140
S301
乱数r'生成
S302
パラメータ差分⊿K1作成
S303
一時テンプレート(r'、K'F)作成
S304
乱数r2生成
S305
パラメータ差分⊿K2作成
S306
変換
S307
テンプレート登録
テンプレート(r2、K2F)
r1、r'
⊿K1
r'、K'F
r2、r'
⊿K2
S
マスタ鍵S

【図８】


耐タンパデバイス140
クライアント端末120
第一の認証サーバ100
S401
指静脈画像入力
S402
特徴量抽出G
テンプレート(r1、K1F)
マスタ鍵S
r1
S
S403
パラメータK1作成
S404
変換K1G
K1G
S405
照合

【図９】


耐タンパデバイス140
クライアント端末120
第一の認証サーバ100
S501
乱数r1'生成
マスタ鍵S
r1、r1'
テンプレート(r1、K1F)
S
S502
パラメータ差分⊿K1'作成
⊿K1'
S503
変換
S504
テンプレート更新
テンプレート(r1'、K1'F)

フロントページの続き

(56)参考文献　特開２００６－１５８８５１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２０
Ｇ０６Ｋ　１７／００
Ｇ０６Ｔ　７／００
Ｈ０４Ｌ　９／３２