(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2012-226539
(P2012-226539A)
(43)公開日　平成24年11月15日(2012.11.15)

(51)Int.Cl.		F I			テーマコード（参考）
G06T 7/00	(2006.01)	G06T	7/00	510Z	5B043
G06F 21/20	(2006.01)	G06F	15/00	330G	5B285
H04L 9/32	(2006.01)	G06F	15/00	330F	5J104
		H04L	9/00	673D	
		H04L	9/00	673E	

審査請求 未請求　請求項の数 20　ＯＬ　（全 51 頁）

(21)出願番号　特願2011-93262(P2011-93262)
(22)出願日　平成23年4月19日(2011.4.19)

（特許庁注：以下のものは登録商標）
１．ＱＲコード

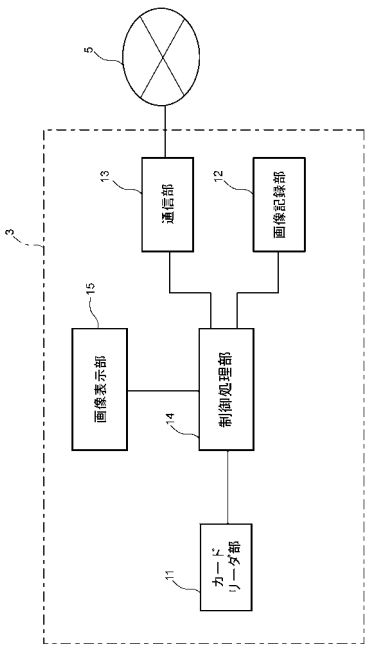
(71)出願人　506301140
公立大学法人会津大学
福島県会津若松市一箕町大字鶴賀字上居合９０番地
(74)代理人　100118094
弁理士　殿元　基城
(72)発明者　趙　強福
福島県会津若松市一箕町大字鶴賀字上居合９０番地　公立大学法人会津大学内
(72)発明者　謝　政勲
台湾彰化縣彰化市惠民莊２４號

Ｆターム(参考)　5B043 AA09　FA07

最終頁に続く

(54)【発明の名称】ホルダ認証システム、ホルダ認証端末、基底画像生成装置およびホルダであることの認証に利用される記録媒体

(57)【要約】
【課題】基底画像を用いた認証画像の生成処理においてセキュリティーを高めること。
【解決手段】ホルダ認証端末３は、画像の特徴を示すベクトルが互いに直交する複数の直交基底画像が変換行列により互いに非直交となる複数の非直交基底画像へと変換された基底画像集合と、ホルダの認証に用いられる認証画像を生成するために用いられる複数の非直交基底画像を、基底画像集合の中から特定するためのインデックス情報と、変換行列により変換される前の複数の直交基底画像からインデックス情報に基づいて複数の直交基底画像を特定し、特定された複数の直交基底画像と認証画像との内積により複数の直交基底画像のそれぞれに対応するようにして求められた係数の係数列に、変換行列の逆行列を積算することにより求められる新たな係数列の係数情報との３つの鍵情報を用いて認証画像を生成する。
【選択図】　図２



【特許請求の範囲】
【請求項１】
認証画像と該認証画像とは異なる互いに独立な複数の任意の画像とを線型部分空間の基底ベクトルとして直交化し、正規化することにより求められた互いに直交する複数の直交基底画像を、変換行列により互いに非直交となる複数の非直交基底画像へと変換させた基底画像集合を記録する端末記録手段を備えて、ホルダの認証に用いられる認証画像を生成するホルダ認証端末と、
ホルダの認証に用いられる認証画像を生成するために用いられる複数の非直交基底画像を、前記基底画像集合の中から特定するためのインデックス情報、または、前記変換行列により変換される前の前記複数の直交基底画像から前記インデックス情報に基づいて複数の直交基底画像を特定し、特定された複数の直交基底画像と前記認証画像との内積により求められた係数列に、前記変換行列の逆行列を積算することにより求められる新たな係数列の係数情報を記録可能なサーバ記録手段と、該サーバ記録手段に記録された前記インデックス情報または前記係数情報をネットワークを介して前記ホルダ認証端末に送信可能なサーバ通信手段とを備えたホルダ認証サーバと、
前記インデックス情報または前記係数情報のうち前記サーバ記録手段に記録されていない情報を記録する情報記録手段を備えて前記ホルダであることの認証に利用される記録媒体と
を有するホルダ認証システムであって、
前記ホルダ認証端末は、
前記ホルダ認証サーバの前記サーバ通信手段により送信された前記インデックス情報または前記係数情報を、前記ネットワークを介して取得して前記端末記録手段に記録するデータ通信手段と、
前記記録媒体の前記情報記録手段より前記インデックス情報または前記係数情報を取得して前記端末記録手段に記録するデータ取得手段と、
前記端末記録手段に記録される前記インデックス情報に基づいて、前記基底画像集合の中から前記複数の非直交基底画像を特定する基底画像特定手段と、
前記端末記録手段に記録される前記係数情報の新たな係数列に基づく、前記基底画像特定手段により特定された前記複数の非直交基底画像の線型結合を求めて前記認証画像を生成する認証画像生成手段と
を有することを特徴とするホルダ認証システム。
【請求項２】
前記記録媒体の前記情報記録手段には、ホルダを識別するための文字列情報Ｓと、変換関数Ｆ（Ｓ）により前記認証画像を生成するために用いられる基底画像の枚数ｒ（但しｒは自然数とする）に対応する数の数値からなる数列（u_1，u_2，・・・，u_r）に変換された該文字列情報Ｓのそれぞれの数値の逆数（１／u_1，１／u_2，・・・，１／u_r）が、前記係数情報の係数列のそれぞれの係数に積算されて重み付けが行われた係数情報とが記録され、
前記ホルダ認証サーバの前記サーバ記録手段には、前記インデックス情報と、前記変換関数Ｆ（Ｓ）とが記録され、
前記ホルダ認証サーバは、
前記サーバ記録手段に記録される前記変換関数Ｆ（Ｓ）に基づいて、前記文字列情報Ｓより求められた数列を第２の係数情報として算出する第２係数情報算出手段を有し、
前記ホルダ認証端末の前記データ取得手段は、前記記録媒体の前記情報記録手段より前記文字列情報Ｓと、前記重み付けが行われた係数情報とを取得して前記端末記録手段に記録し、
前記ホルダ認証端末の前記データ通信手段は、前記データ取得手段により取得された前記文字列情報Ｓを前記ホルダ認証サーバに送信し、
前記ホルダ認証サーバの前記サーバ通信手段は、前記データ通信手段により送信された前記文字列情報Ｓを取得し、

前記ホルダ認証サーバの前記第２係数情報算出手段は、前記サーバ通信手段によって取得した前記文字列情報Ｓと前記サーバ記録手段に記録される前記変換関数Ｆ（Ｓ）とに基づいて第２の係数情報を算出し、
前記ホルダ認証サーバの前記サーバ通信手段は、前記インデックス情報と、前記第２係数情報算出手段により算出された前記第２の係数情報とを前記ホルダ認証端末に送信し、
前記ホルダ認証端末の前記データ通信手段は、前記サーバ通信手段により送信された前記インデックス情報と、前記第２の係数情報とを受信して前記端末記録手段に記録し、
前記基底画像特定手段は、前記端末記録手段に記録される前記インデックス情報に基づいて、前記基底画像集合の中から前記複数の非直交基底画像を特定し、
前記認証画像生成手段は、前記端末記録手段に記録される前記重み付けが行われた係数情報の係数列と前記端末記録手段に記録される前記第２の係数情報の数列とにより算出された係数列とに基づく、前記基底画像特定手段により特定された前記複数の非直交基底画像の線型結合によって前記認証画像を生成すること
を特徴とする請求項１に記載のホルダ認証システム。
【請求項３】
前記基底画像集合は、前記複数の非直交基底画像が前記ホルダ認証端末毎に異なる置換変換テーブル情報に基づいて置換変換された状態で前記ホルダ認証端末のそれぞれの前記端末記録手段に記録され、
前記ホルダ認証サーバの前記サーバ記録手段には、前記ホルダ認証端末毎に異なる前記置換変換テーブル情報が記録され、
前記ホルダ認証サーバは、
前記ホルダ認証端末を識別するための端末情報により該当するホルダ認証端末の前記置換変換テーブル情報を前記サーバ記録手段より読み出し、読み出された前記置換変換テーブル情報に基づいて、前記インデックス情報を置換変換することにより、前記置換変換テーブル情報によって置換変換される前記基底画像集合の中から前記認証画像の生成に用いられる前記複数の非直交基底画像を求めるための第２インデックス情報を算出する第２インデックス情報算出手段を有し、
前記ホルダ認証端末の前記データ通信手段は、当該ホルダ認証端末の前記端末情報を前記ホルダ認証サーバに送信し、
前記ホルダ認証サーバの前記サーバ通信手段は、前記データ通信手段により送信された前記端末情報を取得し、
前記第２インデックス情報算出手段は、前記サーバ通信手段によって取得した前記端末情報に該当する前記置換変換テーブル情報に基づいて、前記第２インデックス情報を算出し、
前記ホルダ認証サーバの前記サーバ通信手段は、前記第２インデックス情報を前記ホルダ認証端末に送信し、
前記ホルダ認証端末の前記データ通信手段は、前記サーバ通信手段により送信された前記第２インデックス情報を受信して前記端末記録手段に記録し、
前記基底画像特定手段は、前記端末記録手段に記録される前記第２インデックス情報に基づいて、置換変換された前記基底画像集合の中から前記認証画像の生成に用いられる前記複数の非直交基底画像を特定する
ことを特徴とすることを特徴とする請求項１又は請求項２に記載のホルダ認証システム。
【請求項４】
認証画像と該認証画像とは異なる互いに独立な複数の任意の画像とを線型部分空間の基底ベクトルとして直交化し、正規化することにより求められた互いに直交する複数の直交基底画像を、変換行列により前記直交基底画像とは異なる複数の基底画像へと変換させた基底画像集合を記録する端末記録手段を備えて、ホルダの認証に用いられる認証画像を生成するホルダ認証端末と、
前記変換行列の逆行列が記録されると共に、ホルダの認証に用いられる認証画像を生成

するために用いられる複数の基底画像を、前記基底画像集合の中から特定するためのインデックス情報、または、前記変換行列により変換される前の前記複数の直交基底画像から前記インデックス情報に基づいて複数の直交基底画像を特定し、特定された複数の直交基底画像と前記認証画像との内積によって求められた係数列の係数情報を記録可能なサーバ記録手段と、該サーバ記録手段に記録された前記変換行列の逆行列と、前記インデックス情報または前記係数情報とをネットワークを介して前記ホルダ認証端末に送信可能なサーバ通信手段とを備えたホルダ認証サーバと、

前記インデックス情報または前記係数情報のうち前記サーバ記録手段に記録されていない情報を記録する情報記録手段を備えて前記ホルダであることの認証に利用される記録媒体と

を有するホルダ認証システムであって、

前記ホルダ認証端末は、

前記ホルダ認証サーバの前記サーバ通信手段により送信された前記逆行列と、前記インデックス情報または前記係数情報とを、前記ネットワークを介して取得して前記端末記録手段に記録するデータ通信手段と、

前記記録媒体の前記情報記録手段より前記インデックス情報または前記係数情報を取得して前記端末記録手段に記録するデータ取得手段と、

前記端末記録手段に記録される前記インデックス情報に基づいて、前記基底画像集合の中から前記複数の基底画像を特定する基底画像特定手段と、

前記基底画像特定手段により特定された前記複数の基底画像を前記端末記録手段に記録される前記逆行列を用いて複数の直交基底画像に変換し、前記端末記録手段に記録される前記係数情報の係数列に基づく、変換された前記複数の直交基底画像の線型結合を求めて前記認証画像を生成する認証画像生成手段と

を有することを特徴とするホルダ認証システム。

【請求項５】

前記記録媒体の前記情報記録手段には、ホルダを識別するための文字列情報Ｓと、変換関数Ｆ（Ｓ）により前記認証画像を生成するために用いられる基底画像の枚数ｒ（但しｒは自然数とする）に対応する数の数値からなる数列（u_1，u_2，・・・，u_r）に変換された該文字列情報Ｓのそれぞれの数値の逆数（１／u_1，１／u_2，・・・，１／u_r）が、前記係数情報の係数列のそれぞれの係数に積算されて重み付けが行われた係数情報とが記録され、

前記ホルダ認証サーバの前記サーバ記録手段には、前記逆行列と、前記インデックス情報と、前記変換関数Ｆ（Ｓ）とが記録され、

前記ホルダ認証サーバは、

前記サーバ記録手段に記録される前記変換関数Ｆ（Ｓ）に基づいて、前記文字列情報Ｓより求められた数列を第２の係数情報として算出する第２係数情報算出手段を有し、

前記ホルダ認証端末の前記データ取得手段は、前記記録媒体の前記情報記録手段より前記文字列情報Ｓと、前記重み付けが行われた係数情報とを取得して前記端末記録手段に記録し、

前記ホルダ認証端末の前記データ通信手段は、前記データ取得手段により取得された前記文字列情報Ｓを前記ホルダ認証サーバに送信し、

前記ホルダ認証サーバの前記サーバ通信手段は、前記データ通信手段により送信された前記文字列情報Ｓを取得し、

前記ホルダ認証サーバの前記第２係数情報算出手段は、前記サーバ通信手段によって取得した前記文字列情報Ｓと前記サーバ記録手段に記録される前記変換関数Ｆ（Ｓ）とに基づいて第２の係数情報を算出し、

前記ホルダ認証サーバの前記サーバ通信手段は、前記逆行列と、前記インデックス情報と、前記第２係数情報算出手段により算出された前記第２の係数情報とを前記ホルダ認証端末に送信し、

前記ホルダ認証端末の前記データ通信手段は、前記サーバ通信手段により送信された前

記逆行列と、前記インデックス情報と、前記第２の係数情報とを受信して前記端末記録手段に記録し、
前記基底画像特定手段は、前記端末記録手段に記録される前記インデックス情報に基づいて、前記基底画像集合の中から前記複数の基底画像を特定し、
前記認証画像生成手段は、前記基底画像特定手段により特定された前記複数の基底画像を前記端末記録手段に記録される前記逆行列を用いて複数の直交基底画像に変換し、前記端末記録手段に記録される前記重み付けが行われた係数情報の係数列と前記端末記録手段に記録される前記第２の係数情報の数列とにより算出された係数列に基づく、変換された前記複数の直交基底画像の線型結合を求めて前記認証画像を生成すること
を特徴とする請求項４に記載のホルダ認証システム。

【請求項６】
前記基底画像集合は、前記複数の基底画像が前記ホルダ認証端末毎に異なる置換変換テーブル情報に基づいて置換変換された状態で前記ホルダ認証端末のそれぞれの前記端末記録手段に記録され、
前記ホルダ認証サーバの前記サーバ記録手段には、前記ホルダ認証端末毎に異なる前記置換変換テーブル情報が記録され、
前記ホルダ認証サーバは、
前記ホルダ認証端末を識別するための端末情報により該当するホルダ認証端末の前記置換変換テーブル情報を前記サーバ記録手段より読み出し、読み出された前記置換変換テーブル情報に基づいて、前記インデックス情報を置換変換することにより、前記置換変換テーブル情報によって置換変換される前記基底画像集合の中から前記認証画像の生成に用いられる前記複数の基底画像を求めるための第２インデックス情報を算出する第２インデックス情報算出手段を有し、
前記ホルダ認証端末の前記データ通信手段は、当該ホルダ認証端末の前記端末情報を前記ホルダ認証サーバに送信し、
前記ホルダ認証サーバの前記サーバ通信手段は、前記データ通信手段により送信された前記端末情報を取得し、
前記第２インデックス情報算出手段は、前記サーバ通信手段によって取得した前記端末情報に該当する前記置換変換テーブル情報に基づいて、前記第２インデックス情報を算出し、
前記ホルダ認証サーバの前記サーバ通信手段は、前記第２インデックス情報を前記ホルダ認証端末に送信し、
前記ホルダ認証端末の前記データ通信手段は、前記サーバ通信手段により送信された前記第２インデックス情報を受信して前記端末記録手段に記録し、
前記基底画像特定手段は、前記端末記録手段に記録される前記第２インデックス情報に基づいて、置換変換された前記基底画像集合の中から前記認証画像の生成に用いられる前記複数の基底画像を特定する
ことを特徴とすることを特徴とする請求項４又は請求項５に記載のホルダ認証システム。

【請求項７】
ホルダの認証に用いられる認証画像とｒ－１枚（但しｒは２以上の自然数とする）の自然画像とに基づいて多画像モーフィング技術により生成されたモーフィング画像と、前記ｒ－１枚の自然画像とからなる複数の基底画像の基底画像集合を記録する端末記録手段を備えて、ホルダの認証に用いられる認証画像を生成するホルダ認証端末と、
前記認証画像とｒ－１枚の前記自然画像とのそれぞれの貢献度からなる貢献度情報、前記認証画像を生成するために用いられる複数の基底画像を、前記基底画像集合を構成する複数の基底画像の中から特定するためのインデックス情報、または、前記基底画像集合における全ての基底画像の特徴ベクトルからなる特徴ベクトル情報を記録可能なサーバ記録手段と、該サーバ記録手段に記録された前記貢献度情報、前記インデックス情報または前記特徴ベクトル情報を、ネットワークを介して前記ホルダ認証端末に送信可能なサーバ通

信手段とを備えたホルダ認証サーバと、
前記貢献度情報、前記インデックス情報または前記特徴ベクトル情報のうち前記サーバ記録手段に記録されていない情報を記録する情報記録手段を備えて前記ホルダであることの認証に利用される記録媒体と
を有するホルダ認証システムであって、
前記ホルダ認証端末は、
前記ホルダ認証サーバの前記サーバ通信手段により送信された前記貢献度情報、前記インデックス情報または前記特徴ベクトル情報を、前記ネットワークを介して取得して前記端末記録手段に記録するデータ通信手段と、
前記記録媒体の前記情報記録手段より前記貢献度情報、前記インデックス情報または前記特徴ベクトル情報を取得して前記端末記録手段に記録するデータ取得手段と、
前記端末記録手段に記録されるｒ－１枚の前記自然画像のそれぞれの特徴ベクトルが前記モーフィング画像の特徴ベクトルに一致するように、前記端末記録手段に記録されるｒ－１枚の前記自然画像のそれぞれを変形処理することにより、ｒ－１枚の前記自然画像の全てをそれぞれの変形画像に変形させる変形画像生成手段と、
前記端末記録手段に記録されるｒ－１枚の前記自然画像のそれぞれの特徴ベクトルに対して、前記端末記録手段に記録されるｒ－１枚の前記自然画像のそれぞれの貢献度に基づいて線型結合し、その結果を、前記モーフィング画像の特徴ベクトルから減算し、減算された前記特徴ベクトルを前記認証画像の貢献度で除算することにより、前記認証画像の特徴ベクトルを算出する認証画像特徴ベクトル算出手段と、
前記端末記録手段に記録されるｒ－１枚の前記自然画像のそれぞれの変形画像に対して、前記端末記録手段に記録されるｒ－１枚の前記自然画像のそれぞれの貢献度に基づいて線型結合し、その結果を、前記モーフィング画像から減算し、減算された前記モーフィング画像を前記認証画像の貢献度で除算することにより、認証変形画像を算出する認証変形画像算出手段と、
前記端末記録手段に記録される前記モーフィング画像の特徴ベクトルが、前記認証画像特徴ベクトル算出手段により算出された前記認証画像の特徴ベクトルに一致するように、前記認証変形画像算出手段により算出された前記認証変形画像をモーフィング処理することにより、前記認証変形画像を前記認証画像に変形させて前記認証画像を生成する認証画像モーフィング生成手段と
を有することを特徴とするホルダ認証システム。
【請求項８】
認証画像と該認証画像とは異なる互いに独立な複数の任意の画像とを線型部分空間の基底ベクトルとして直交化し、正規化することにより求められた互いに直交する複数の直交基底画像を、変換行列により互いに非直交となる複数の非直交基底画像へと変換させた基底画像集合と、
ホルダの認証に用いられる認証画像を生成するために用いられる複数の非直交基底画像を、前記基底画像集合の中から特定するためのインデックス情報と、
前記変換行列により変換される前の前記複数の直交基底画像から前記インデックス情報に基づいて複数の直交基底画像を特定し、特定された複数の直交基底画像と前記認証画像との内積により求められた係数列に、前記変換行列の逆行列を積算することにより求められる新たな係数列の係数情報と
の３つの鍵情報を記録する端末記録手段と、
該端末記録手段に記録される前記インデックス情報に基づいて、前記基底画像集合の中から前記複数の非直交基底画像を特定する基底画像特定手段と、
前記端末記録手段に記録される前記係数情報の新たな係数列に基づく、前記基底画像特定手段により特定された前記複数の非直交基底画像の線型結合を求めて前記認証画像を生成する認証画像生成手段と
を有することを特徴とするホルダ認証端末。
【請求項９】

前記端末記録手段は、
ホルダを識別するための文字列情報Ｓを前記認証画像を生成するために用いられる基底画像の枚数ｒ（但しｒは自然数とする）に対応する数の数値からなる数列（u_1，u_2，・・・，u_r）に変換する変換関数Ｆ（Ｓ）に基づいて求められた前記数列を第２の係数情報として記録すると共に、
前記係数情報の係数列のそれぞれの係数に対して、前記第２の係数情報をなす数列のそれぞれの数値の逆数（１／u_1，１／u_2，・・・，１／u_r）を積算することにより、各係数に重み付けが行われた係数列を重み付けが行われた係数情報として記録し、
前記認証画像生成手段は、前記端末記録手段に記録される前記重み付けが行われた係数情報の係数列と前記端末記録手段に記録される前記第２の係数情報の数列とにより算出された係数列とに基づく、前記基底画像特定手段により特定された前記複数の非直交基底画像の線型結合を求めて前記認証画像を生成すること
を特徴とする請求項８に記載のホルダ認証端末。
【請求項１０】
前記基底画像集合は、前記複数の非直交基底画像が置換変換テーブル情報に基づいて置換変換された状態で前記端末記録手段に記録され、
さらに、前記端末記録手段に、前記置換変換テーブル情報によって置換変換された前記基底画像集合の中から前記認証画像の生成に用いられる前記複数の非直交基底画像を求めるための第２インデックス情報が記録されており、
前記基底画像特定手段は、前記端末記録手段に記録される前記第２インデックス情報に基づいて、置換変換された前記基底画像集合の中から前記認証画像の生成に用いられる前記複数の非直交基底画像を特定する
ことを特徴とする請求項８又は請求項９に記載のホルダ認証端末。
【請求項１１】
認証画像と該認証画像とは異なる互いに独立な複数の任意の画像とを線型部分空間の基底ベクトルとして直交化し、正規化することにより求められた互いに直交する複数の直交基底画像を、当該直交基底画像とは異なる複数の基底画像へと変換する変換行列の逆行列と、
前記変換行列により変換された前記複数の基底画像からなる基底画像集合と、
ホルダの認証に用いられる認証画像を生成するために用いられる複数の基底画像を、前記基底画像集合を構成する複数の基底画像の中から特定するためのインデックス情報と、
前記変換行列により変換される前の前記複数の直交基底画像から前記インデックス情報に基づいて複数の直交基底画像を特定し、特定された複数の直交基底画像と前記認証画像との内積によって求められた係数列の係数情報と
の４つの鍵情報を記録する端末記録手段と、
該端末記録手段に記録される前記インデックス情報に基づいて、前記基底画像集合の中から前記複数の基底画像を特定する基底画像特定手段と、
前記基底画像特定手段により特定された前記複数の基底画像を前記端末記録手段に記録される前記逆行列を用いて複数の直交基底画像に変換し、前記端末記録手段に記録される前記係数情報の係数列に基づく、変換された前記複数の直交基底画像の線型結合を求めて前記認証画像を生成する認証画像生成手段と
を有することを特徴とするホルダ認証端末。
【請求項１２】
前記端末記録手段は、
ホルダを識別するための文字列情報Ｓを前記認証画像を生成するために用いられる基底画像の枚数ｒ（但しｒは自然数とする）に対応する数の数値からなる数列（u_1，u_2，・・・，u_r）に変換する変換関数Ｆ（Ｓ）に基づいて求められた前記数列を第２の係数情報として記録すると共に、
前記係数情報の係数列のそれぞれの係数に対して、前記第２の係数情報をなす数列のそれぞれの数値の逆数（１／u_1，１／u_2，・・・，１／u_r）を積算することにより、各係数

に重み付けが行われた係数列を重み付けが行われた係数情報として記録し、
前記認証画像生成手段は、前記基底画像特定手段により特定された前記複数の基底画像を前記端末記録手段に記録される前記逆行列を用いて複数の直交基底画像に変換し、前記端末記録手段に記録される前記重み付けが行われた係数情報の係数列と前記端末記録手段に記録される前記第２の係数情報の数列とにより算出された係数列に基づく、変換された前記複数の直交基底画像の線型結合を求めて前記認証画像を生成すること
を特徴とする請求項１１に記載のホルダ認証端末。
【請求項１３】
前記基底画像集合は、前記複数の基底画像が置換変換テーブル情報に基づいて置換変換された状態で前記端末記録手段に記録され、
さらに、前記端末記録手段に、前記置換変換テーブル情報によって置換変換された前記基底画像集合の中から前記認証画像の生成に用いられる前記複数の基底画像を求めるための第２インデックス情報が記録されており、
前記基底画像特定手段は、前記端末記録手段に記録される前記第２インデックス情報に基づいて、置換変換された前記基底画像集合の中から前記認証画像の生成に用いられる前記複数の基底画像を特定する
ことを特徴とする請求項１１又は請求項１２に記載のホルダ認証端末。
【請求項１４】
ホルダの認証に用いられる認証画像とｒ－１枚（但しｒは２以上の自然数とする）の自然画像とに基づいて多画像モーフィング技術により生成されたモーフィング画像と、前記ｒ－１枚の自然画像とからなる複数の基底画像の基底画像集合と、
前記認証画像とｒ－１枚の前記自然画像とのそれぞれの貢献度からなる貢献度情報と、
前記認証画像を生成するために用いられる複数の基底画像を、前記基底画像集合を構成する複数の基底画像の中から特定するためのインデックス情報と、
前記基底画像集合における全ての基底画像の特徴ベクトルからなる特徴ベクトル情報との４つの鍵情報を記録する端末記録手段と、
前記端末記録手段に記録されるｒ－１枚の前記自然画像のそれぞれの特徴ベクトルが前記モーフィング画像の特徴ベクトルに一致するように、前記端末記録手段に記録されるｒ－１枚の前記自然画像のそれぞれを変形処理することにより、ｒ－１枚の前記自然画像の全てをそれぞれの変形画像に変形させる変形画像生成手段と、
前記端末記録手段に記録されるｒ－１枚の前記自然画像のそれぞれの特徴ベクトルに対して、前記端末記録手段に記録されるｒ－１枚の前記自然画像のそれぞれの貢献度に基づいて線型結合し、その結果を、前記モーフィング画像の特徴ベクトルから減算し、減算された前記特徴ベクトルを前記認証画像の貢献度で除算することにより、前記認証画像の特徴ベクトルを算出する認証画像特徴ベクトル算出手段と、
前記端末記録手段に記録されるｒ－１枚の前記自然画像のそれぞれの変形画像に対して、前記端末記録手段に記録されるｒ－１枚の前記自然画像のそれぞれの貢献度に基づいて線型結合し、その結果を、前記モーフィング画像から減算し、減算された前記モーフィング画像を前記認証画像の貢献度で除算することにより、認証変形画像を算出する認証変形画像算出手段と、
前記端末記録手段に記録される前記モーフィング画像の特徴ベクトルが、前記認証画像特徴ベクトル算出手段により算出された前記認証画像の特徴ベクトルに一致するように、前記認証変形画像算出手段により算出された前記認証変形画像をモーフィング処理することにより、前記認証変形画像を前記認証画像に変形させて前記認証画像を生成する認証画像モーフィング生成手段と
を有することを特徴とするホルダ認証端末。
【請求項１５】
認証画像と該認証画像とは異なる互いに独立なｒ－１枚の任意の画像とが記録された画像記録手段と、
該画像記録手段に記録された前記認証画像と前記ｒ－１枚の任意の画像とを、線型部分

空間の基底ベクトルとして直交化し、正規化することによりｒ枚の基底画像を生成する基底画像生成手段と、
該基底画像生成手段により生成されたｒ枚の基底画像のそれぞれと前記認証画像との内積を算出することにより係数列をなす係数情報を求める係数情報算出手段と
を有し、
線型結合により前記認証画像を生成することが可能な前記ｒ枚の基底画像と前記係数情報とを求めることを特徴とする基底画像生成装置。
【請求項１６】
認証画像と該認証画像とは異なる互いに独立な複数の任意の画像とを線型部分空間の基底ベクトルとして直交化し、正規化することにより求められた互いに直交する複数の直交基底画像を、変換行列により互いに非直交となる複数の非直交基底画像へと変換させた基底画像集合と、
ホルダの認証に用いられる認証画像を生成するために用いられる複数の非直交基底画像を、前記基底画像集合の中から特定するためのインデックス情報と、
前記変換行列により変換される前の前記複数の直交基底画像から前記インデックス情報に基づいて複数の直交基底画像を特定し、特定された複数の直交基底画像と前記認証画像との内積により求められた係数列に、前記変換行列の逆行列を積算することにより求められる新たな係数列の係数情報と
の３つの鍵情報を用いて、
基底画像特定手段が、前記インデックス情報に基づいて、前記基底画像集合の中から前記複数の非直交基底画像を特定し、認証画像生成手段が、前記係数情報の新たな係数列に基づく、前記基底画像特定手段により特定された前記複数の非直交基底画像の線型結合を求めて前記認証画像を生成するホルダ認証端末において使用される
前記インデックス情報または前記係数情報の少なくとも一方を記録する情報記録手段を有すること
を特徴とするホルダであることの認証に利用される記録媒体。
【請求項１７】
認証画像と該認証画像とは異なる互いに独立な複数の任意の画像とを線型部分空間の基底ベクトルとして直交化し、正規化することにより求められた互いに直交する複数の直交基底画像を、変換行列により互いに非直交となる複数の非直交基底画像へと変換させた基底画像集合と、
ホルダの認証に用いられる認証画像を生成するために用いられる複数の非直交基底画像を、前記基底画像集合の中から特定するためのインデックス情報と、
ホルダを識別するための文字列情報Ｓを前記認証画像を生成するために用いられる基底画像の枚数ｒ（但しｒは自然数とする）に対応する数の数値からなる数列（u_1，u_2，・・・，u_r）に変換する変換関数Ｆ（Ｓ）に基づいて求められた前記数列からなる第２の係数情報と、
前記変換行列により変換される前の前記複数の直交基底画像から前記インデックス情報に基づいて前記複数の直交基底画像を特定し、特定された複数の直交基底画像と前記認証画像との内積により求められた係数列に、前記変換行列の逆行列を積算することにより求められる新たな係数列のそれぞれの係数に対して、前記第２の係数情報をなす数列のそれぞれの数値の逆数（１／u_1，１／u_2，・・・，１／u_r）を積算することにより、各係数に重み付けが行われた係数列からなる重み付けが行われた係数情報と
の４つの鍵情報を用いて、
基底画像特定手段が、前記変換行列により変換される前の前記複数の直交基底画像から前記インデックス情報に基づいて前記複数の直交基底画像を特定し、認証画像生成手段が、前記重み付けが行われた係数情報の係数列と前記第２の係数情報の数列とにより算出された係数列に基づく、前記基底画像特定手段により特定された前記複数の直交基底画像の線型結合を求めて前記認証画像を生成するホルダ認証端末おいて使用される
前記インデックス情報または前記重み付けが行われた係数情報の少なくとも一方を記録

する情報記録手段を有すること
を特徴とするホルダであることの認証に利用される記録媒体。
【請求項１８】
認証画像と該認証画像とは異なる互いに独立な複数の任意の画像とを線型部分空間の基底ベクトルとして直交化し、正規化することにより求められた互いに直交する複数の直交基底画像を、当該直交基底画像とは異なる複数の基底画像へと変換する変換行列の逆行列と、
前記変換行列により変換された前記複数の基底画像からなる基底画像集合と、
ホルダの認証に用いられる認証画像を生成するために用いられる複数の基底画像を、前記基底画像集合を構成する複数の基底画像の中から特定するためのインデックス情報と、
前記変換行列により変換される前の前記複数の直交基底画像から前記インデックス情報に基づいて複数の直交基底画像を特定し、特定された複数の直交基底画像と前記認証画像との内積によって求められた係数列の係数情報と
の４つの鍵情報を用いて、
基底画像特定手段が、前記インデックス情報に基づいて、前記基底画像集合の中から前記複数の基底画像を特定し、認証画像生成手段が、前記基底画像特定手段により特定された前記複数の基底画像を前記逆行列を用いて複数の直交基底画像に変換し、前記係数情報の係数列に基づく変換された前記複数の直交基底画像の線型結合を求めて前記認証画像を生成するホルダ認証端末おいて使用される
前記インデックス情報または前記係数情報の少なくとも一方を記録する情報記録手段を有すること
を特徴とするホルダであることの認証に利用される記録媒体。
【請求項１９】
認証画像と該認証画像とは異なる互いに独立な複数の任意の画像とを線型部分空間の基底ベクトルとして直交化し、正規化することにより求められた互いに直交する複数の直交基底画像を、当該直交基底画像とは異なる複数の基底画像へと変換する変換行列の逆行列と、
前記変換行列により変換された前記複数の基底画像からなる基底画像集合と、
ホルダの認証に用いられる認証画像を生成するために用いられる複数の基底画像を、前記基底画像集合を構成する複数の基底画像の中から特定するためのインデックス情報と、
ホルダを識別するための文字列情報Ｓを前記認証画像を生成するために用いられる基底画像の枚数ｒ（但しｒは自然数とする）に対応する数の数値からなる数列（u_1，u_2，・・・，u_r）に変換する変換関数Ｆ（Ｓ）に基づいて求められた前記数列からなる第２の係数情報と、
前記変換行列により変換される前の前記複数の直交基底画像から前記インデックス情報に基づいて前記複数の直交基底画像を特定し、特定された複数の直交基底画像と前記認証画像との内積によって求められた係数列のそれぞれの係数に対して、前記第２の係数情報をなす数列のそれぞれの数値の逆数（１／u_1，１／u_2，・・・，１／u_r）を積算することにより、各係数に重み付けが行われた係数列からなる重み付けが行われた係数情報とを用いて、
基底画像特定手段が、前記インデックス情報に基づいて、前記基底画像集合の中から前記複数の基底画像を特定し、認証画像生成手段が、前記基底画像特定手段により特定された前記複数の基底画像を前記逆行列を用いて前記複数の直交基底画像に変換し、前記重み付けが行われた係数情報の係数列と前記第２の係数情報の数列とにより算出された係数列に基づく、変換された前記複数の直交基底画像の線型結合を求めて前記認証画像を生成するホルダ認証端末おいて使用される
前記インデックス情報または前記重み付けが行われた係数情報の少なくとも一方を記録する情報記録手段を有する
ことを特徴とするホルダであることの認証に利用される記録媒体。
【請求項２０】

ホルダの認証に用いられる認証画像とｒ－１枚（但しｒは２以上の自然数とする）の自然画像とに基づいて多画像モーフィング技術により生成されたモーフィング画像と、前記ｒ－１枚の自然画像とからなる複数の基底画像の基底画像集合と、
前記認証画像とｒ－１枚の前記自然画像とのそれぞれの貢献度からなる貢献度情報と、
前記認証画像を生成するために用いられる複数の基底画像を、前記基底画像集合を構成する複数の基底画像の中から特定するためのインデックス情報と、
前記基底画像集合における全ての基底画像の特徴ベクトルからなる特徴ベクトル情報との４つの鍵情報を用いて、
変形画像生成手段が、ｒ－１枚の前記自然画像のそれぞれの特徴ベクトルが前記モーフィング画像の特徴ベクトルに一致するように、ｒ－１枚の前記自然画像のそれぞれを変形処理することにより、ｒ－１枚の前記自然画像の全てをそれぞれの変形画像に変形させ、
認証画像特徴ベクトル算出手段が、ｒ－１枚の前記自然画像のそれぞれの特徴ベクトルに対して、ｒ－１枚の前記自然画像のそれぞれの貢献度に基づいて線型結合し、その結果を、前記モーフィング画像の特徴ベクトルから減算し、減算された前記特徴ベクトルを前記認証画像の貢献度で除算することにより、前記認証画像の特徴ベクトルを算出し、
認証変形画像算出手段が、変形画像生成手段により変形されたｒ－１枚の前記自然画像のそれぞれの変形画像に対して、ｒ－１枚の前記自然画像のそれぞれの貢献度に基づいて線型結合し、その結果を、前記モーフィング画像から減算し、減算された前記モーフィング画像を前記認証画像の貢献度で除算することにより、認証変形画像を算出し、
認証画像モーフィング生成手段が、前記モーフィング画像の特徴ベクトルが前記認証画像特徴ベクトル算出手段により算出された前記認証画像の特徴ベクトルに一致するように、前記認証変形画像算出手段により算出された前記認証変形画像をモーフィング処理することにより、前記認証変形画像を前記認証画像に変形させて前記認証画像を生成するホルダ認証端末おいて使用される
前記貢献度情報、前記インデックス情報または前記特徴ベクトル情報のうち少なくとも一つを記録する情報記録手段を有する
ことを特徴とするホルダであることの認証に利用される記録媒体。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、ホルダ認証システム、ホルダ認証端末、基底画像生成装置およびホルダであることの認証に利用される記録媒体に関し、より詳細には、基底画像集合と、インデックス情報と、係数情報とに基づいて、所定のサービスなどを受けようとする使用者が、そのサービスを受けることが認められた正当（真正）の使用者（ホルダ）であるか否かの認証に用いられる認証画像を生成することが可能なホルダ認証システム、ホルダ認証端末、基底画像生成装置およびホルダであることの認証に利用される記録媒体に関する。

【背景技術】

【０００２】

従来より、２枚の画像から両方の画像の特徴を備えつつ違和感のない新たな画像を生成する技術としてモーフィング画像生成方法が知られている（例えば、特許文献１参照）。

【０００３】

このようなモーフィング技術を利用することにより、２枚の画像から、違和感のないモーフィング画像を生成することができる。例えば、２枚の画像が人間の顔の場合には、２枚の顔画像のそれぞれの特徴を備えながら、その２枚の顔画像とは異なる顔画像であって、見た目に違和感のない顔画像を生成することが可能となる。

【０００４】

さらに、近年では、このモーフィング技術を利用して、カード（例えば、クレジットカードなどのように、提示することによって一定のサービスなどを受けることが可能となるカード）を使用するユーザが、そのカードなどの正当な所有者（以下、ホルダという）であるか否かの判断を行う方法が提案されている（例えば、特許文献２参照）。

【０００５】
特許文献２に開示された方法では、ホルダを証明する認証画像と、認証画像とは異なる画像からなる目標画像とに基づいて、画像モーフィング技術を用いることによって、認証画像を目標画像に近づくように変形させた変形認証画像を生成する。そして、変形認証画像をカードに記録させる。
【０００６】
ホルダの認証を行う場合には、まず、カードに記録される変形認証画像を読み出す。そして、変形認証画像と、変形率と、目標画像と、変形認証画像の特徴的構成を部分的に定義した変形特徴情報（特徴ベクトル）と、目標画像の特徴ベクトルとに基づいて、逆モーフィング技術を用いてホルダ自身を証明する認証画像をカード認証端末が生成し、カード認証端末に設けられるディスプレイに認証画像を表示させる。このようにして生成された認証画像と、カードの使用者の顔とをオペレータが比較することにより、カードの使用者がホルダであるか否かの判断を行うことが可能となる。
【０００７】
しかしながら、特許文献２に示すように、カードに変形認証画像を記録させるためには、比較的容量の大きな記録手段（メモリなど）をカードに設ける必要が生じる。このため、一般的に流通しているクレジットカードなどでは、十分な記録容量を確保することが困難であるという問題があった。
【０００８】
このため、今日では、変形認証画像と目標画像とに基づいて、モーフィング技術により認証画像を生成するのではなく、基底画像集合（複数の画像により構成される基底画像の集まりを基底画像集とし、さらに複数の基底画像集の和集合を基底画像集合とする）と、基底画像集合の中から認証画像を生成するために用いられる基底画像集（複数の基底画像の集まり）を特定するためのインデックス情報と、基底画像集（複数の基底画像の集まり）に基づいて認証画像を生成するための係数情報（係数列）とに基づいて認証画像を生成する技術が特願２０１０－１４４３６８号において提案されている（この技術が提案されている特許出願を文献３とする）。
【０００９】
このように、３種類の情報（以下、認証画像の生成（合成）に用いられる情報を「鍵情報」とする）、つまり、基底画像集合（以下、１つめの鍵情報をＫｅｙ１で示す）と、インデックス情報（以下、２つめの鍵情報をＫｅｙ２で示す）と、係数情報（以下、３つめの鍵情報をＫｅｙ３で示す）とを用いて、認証画像を生成することにより、認証画像の生成を複数の鍵情報に基づいて行うことが可能となる。
【００１０】
ここで、Ｋｅｙ１の基底画像集合は、画像データの集合であるためデータ量が大きくなる傾向がある一方で、Ｋｅｙ２のインデックス情報、Ｋｅｙ３の係数情報は、データ量が少ない傾向がある。このため、データ量の大きい基底画像集合（Ｋｅｙ１）を、カード認証端末などの大容量記録媒体に予め記録させ、データ量の少ないインデックス情報（Ｋｅｙ２）や係数情報（Ｋｅｙ３）を、カードのメモリやネットワークを介して接続されるサーバの記録媒体などに記録させておくことにより、認証画像の生成に必要な情報の分散化が図れるとともに、メモリ容量の乏しいカード（例えば、磁気カードやＩＣカードなど）であっても、認証画像の生成に必要な情報を記録させておくことが可能になる。
【００１１】
ところで、文献３に示す認証画像の生成方法では、複数の基底画像（例えば顔写真）に基づいて認証画像を生成する処理を行っている。文献３に示す認証画像の生成方法では、認証画像を生成するために複数の基底画像を構成部分ごとに抽出するのではなく、複数の基底画像そのものを複数の画像パターンとして扱うことにより、統計的なパターン認識手段を適用してホルダの認証画像を生成している。このため、文献３に示すように、複数の基底画像そのものを複数の画像パターンとして扱って認証画像を生成する場合には、膨大な基底画像（顔写真）が必要になってしまうという問題が生じていた。

【００１２】
この問題を解決するために、文献３においては、主成分分析（ＰＣＡ：Principal Component Analysis）方法を用いて、認証画像の生成に利用される画像データのデータ量を低減させた上で、認証画像の生成処理を行っている。主成分分析方法とは、複数の画像の特徴を基準とした高次元の分布状態から、その分布状態をよく表現できる低次元の分布状態を示し得る基底画像を用いる方法である。具体的には、多数の顔写真、例えばＭ枚の顔写真（変数｛Ｚｍ｝｛ｍ＝１，２，・・・，Ｍ｝）に基づいて、情報の損失を最小限に抑えながら、顔写真をよく表現できる互いに直交なＮ（Ｎ＜Ｍ）個の基底画像｛b_N｝を求める方法である。

【００１３】
まず、Ｍ枚の顔写真のそれぞれを、各画像の特徴に基づくベクトルとして捉える。そして、Ｍ枚の顔写真より求められた平均画像を平均ベクトルとし、各画像を示すベクトルから平均ベクトルを差し引いたベクトルに基づいて、Ｍ次元の画像空間を構築する。基底画像を示すベクトルは、Ｍ次元の画像空間における主成分の軸を構成することになる。このＭ次元の空間にある任意の点ｐは、基底画像を示すベクトルの線型結合（一次結合）により近似的に求めることが可能となる。

【００１４】
具体的に、主軸のベクトルの集合をＢとし
Ｂ＝｛b_1，b_2，・・・，b_N｝
で表す。画像空間に存在する顔写真の画像ｐは、

【数１】

$$p=\sum_{i=1}^{N} w_i\, b_i+\varepsilon \quad \cdots式1$$

で表すことが可能となる。ここで、εは近似誤差（合成誤差、生成誤差）で、Ｗ＝｛w_1，w_2，w_3，・・・w_N｝は、基底画像に対応する係数の集合（係数列）である。Ｎ＝ＭあるいはＮが画像空間のランクに等しい場合、近似誤差εがゼロとなる。

【００１５】
基底画像は、上述したように、各画像の特徴を示す主軸となるベクトルであるため、基底画像に対応するベクトルを適切な係数で線型結合することによって、任意の画像（具体的には、ホルダの認証画像）を高い精度で生成することが可能となる。

【００１６】
なお、主成分分析方法により基底画像を求める場合には、各画像を示すベクトルから平均ベクトルを差し引いたベクトルに基づいて画像空間が構築される。つまり、各画像を示すベクトルに対して平均的な画像のベクトルを差し引くことによりセンタリングが行われる。このため、すべての画像の平均画像を求めて記憶する必要があるが、センターをなす平均画像を基底画像の１つと考えると、対応する係数を常に１とすることができる。

【００１７】
また、認証画像をｐとし、この認証画像ｐを最も精度よく生成することが可能な基底画像の集まり（基底画像集）をＢとする場合には、係数列w_iを、認証画像ｐと各基底画像b_iとの内積によって、簡単に求めることが可能である。
w_i ＝＜ｐ，b_i＞但し、ｉ＝１，２，３，…・・・式２

【００１８】
このように、文献３に示される認証画像の生成方法（Ｋｅｙ１～Ｋｅｙ３を用いて認証画像を生成する方法）を用いることにより、認証画像を生成するために利用する画像データとして複数の基底画像を用いることができるので、画像データのデータ量を低減させることが可能になる。さらに、認証画像の生成に必要な係数情報を、認証画像と基底画像との内積によって容易に求めることが可能となる。

【００１９】

さらに、文献３に示す方法では、上述したように、認証画像の生成に利用される複数の基底画像の集まり（基底画像集）をさらに複数グループ（例えばＫ組のグループ）だけ集めて基底画像集合を用いる。

【００２０】

基底画像集合をΩとすると、基底画像集合Ωは、

【数２】

$$\Omega=\{b_{11},b_{12},\cdots,b_{1N_1},b_{21},b_{22},\cdots,b_{2N_2},b_{31},b_{32},\cdots \cdots,b_{3N_3},\cdots,b_{K1},b_{K2},\cdots,b_{KN_K}\} \quad \cdots式３$$

で示される。

【００２１】

認証画像の生成処理に使用される基底画像集は、上述したように、基底画像集合の一部を構成する複数の基底画像であることから、基底画像集合の中から認証画像の生成処理に使用される基底画像を特定する情報が必要となる。このような情報として、例えば、基底画像集合を構成する各基底画像の順番を示した情報を用いることができる。この順番を示した情報が、上述したインデックス情報に該当するものである。

【００２２】

例えば、置換変換処理を行う前における第ｋグループの基底画像集の基底画像の順番は、インデックス情報によって、

【数３】

$$k_1,k_2,\cdots,k_{N_k} \quad \cdots式４$$

と示すことができる。

【００２３】

従って、生成処理に用いられる基底画像（例えば第ｋグループの基底画像集の基底画像）を基底画像集合より求める場合には、式４に示したインデックス情報を用いることにより、適切な基底画像を適切な順番で求めることができる。

【００２４】

文献３に記載の認証画像の生成方法では、多数の基底画像集の和集合である基底画像集合（Ｋｅｙ１）、インデックス情報（Ｋｅｙ２）、認証画像の生成処理に用いられる係数情報（係数列の情報：Ｋｅｙ３）として、具体的に、

【数４】

$$\text{Key1: } b_{11},b_{12},\cdots,b_{1N_1},b_{21},b_{22},\cdots \cdots,b_{2N_2},\cdots,b_{k1},b_{k2},\cdots,b_{KN_K}$$

【数５】

$$\text{Key2: } k_1,k_2,\ldots,k_{N_k}$$

【数６】

$$\text{Key3: } w_{k1},w_{k2},\cdots,w_{kN_k}$$

を用いて、認証画像の生成を行う。

【先行技術文献】

【特許文献】
【００２５】
【特許文献１】特開２００７－２１９２３０号公報
【特許文献２】特開２０１１－２９３８号公報
【発明の概要】
【発明が解決しようとする課題】
【００２６】
ところで、文献３に示された認証画像の生成方法では、多数の任意の画像を予め用意し、主成分分析法を用いることによって多数の基底画像を生成して認証画像の生成処理を行っている。このように多数の基底画像を用いて認証画像の生成を行うことにより、近似誤差（生成誤差、合成誤差）εの少ない違和感のない認証画像を生成することが可能となる。
【００２７】
しかしながら、１枚の認証画像を生成するために多数の基底画像を利用するため、認証画像の生成に用いられる係数情報のデータ量が大きくなるおそれがあった。このため、記録容量の少ないカード等においては、係数情報をカードに記録させることが困難になってしまう場合があるという問題があった。
【００２８】
さらに、認証画像の生成に用いられる基底画像は、認証画像毎（認証画像を利用するユーザ毎）に特化（最適化）し、近似誤差（生成誤差、合成誤差）εを最小に抑えることが好ましいが、文献３に示された技術では、すべての認証画像に共通の基底画像を求めているので、新しいユーザに対して、認証画像を精度よく生成することができなくなる恐れがあった。
【００２９】
一方で、主成分分析法により求められる基底画像は互いに直交であるため、簡単に解読されてしまうおそれがあるという問題があった。すなわち、第三者が、基底画像集合Ωにおいて、直交関係（同値関係）を定義すれば、任意の認証画像に対して、それを生成するための基底画像集合Ωの部分集合が特定されるおそれがあった。
【００３０】
さらに、文献３に示された認証画像の生成方法では、３種類の鍵情報を用いて認証画像の生成を行っているが、認証画像の生成処理におけるセキュリティー向上を目的として３種類の鍵情報だけでなく、さらにもう１つ鍵情報を加えて４種類の鍵情報とし、鍵情報の分散化を図ることが求められている。
【００３１】
本発明は、上記課題に鑑みてなされたものであり、基底画像を用いた認証画像の生成処理において、認証画像の生成に必要な基底画像をより効率的かつ効果的に算出し、また認証画像の生成に必要な係数情報のデータ量を低減させることができ、さらに、セキュリティーを高めることが可能なホルダ認証システム、ホルダ認証端末、基底画像生成装置およびホルダであることの認証に利用される記録媒体を提供することを課題とする。
【課題を解決するための手段】
【００３２】
上記課題を解決するために、本発明に係る第１のホルダ認証システムは、認証画像と該認証画像とは異なる互いに独立な複数の任意の画像とを線型部分空間の基底ベクトルとして直交化し、正規化することにより求められた互いに直交する複数の直交基底画像を、変換行列により互いに非直交となる複数の非直交基底画像へと変換させた基底画像集合を記録する端末記録手段を備えて、ホルダの認証に用いられる認証画像を生成するホルダ認証端末と、ホルダの認証に用いられる認証画像を生成するために用いられる複数の非直交基底画像を、前記基底画像集合の中から特定するためのインデックス情報、または、前記変換行列により変換される前の前記複数の直交基底画像から前記インデックス情報に基づいて複数の直交基底画像を特定し、特定された複数の直交基底画像と前記認証画像との内積

により求められた係数列に、前記変換行列の逆行列を積算することにより求められる新たな係数列の係数情報を記録可能なサーバ記録手段と、該サーバ記録手段に記録された前記インデックス情報または前記係数情報をネットワークを介して前記ホルダ認証端末に送信可能なサーバ通信手段とを備えたホルダ認証サーバと、前記インデックス情報または前記係数情報のうち前記サーバ記録手段に記録されていない情報を記録する情報記録手段を備えて前記ホルダであることの認証に利用される記録媒体とを有するホルダ認証システムであって、前記ホルダ認証端末は、前記ホルダ認証サーバの前記サーバ通信手段により送信された前記インデックス情報または前記係数情報を、前記ネットワークを介して取得して前記端末記録手段に記録するデータ通信手段と、前記記録媒体の前記情報記録手段より前記インデックス情報または前記係数情報を取得して前記端末記録手段に記録するデータ取得手段と、前記端末記録手段に記録される前記インデックス情報に基づいて、前記基底画像集合の中から前記複数の非直交基底画像を特定する基底画像特定手段と、前記端末記録手段に記録される前記係数情報の新たな係数列に基づく、前記基底画像特定手段により特定された前記複数の非直交基底画像の線型結合を求めて前記認証画像を生成する認証画像生成手段とを有することを特徴とする。

【００３３】

また、本発明に係る第１のホルダ認証端末は、認証画像と該認証画像とは異なる互いに独立な複数の任意の画像とを線型部分空間の基底ベクトルとして直交化し、正規化することにより求められた互いに直交する複数の直交基底画像を、変換行列により互いに非直交となる複数の非直交基底画像へと変換させた基底画像集合と、ホルダの認証に用いられる認証画像を生成するために用いられる複数の非直交基底画像を、前記基底画像集合の中から特定するためのインデックス情報と、前記変換行列により変換される前の前記複数の直交基底画像から前記インデックス情報に基づいて複数の直交基底画像を特定し、特定された複数の直交基底画像と前記認証画像との内積により求められた係数列に、前記変換行列の逆行列を積算することにより求められる新たな係数列の係数情報との３つの鍵情報を記録する端末記録手段と、該端末記録手段に記録される前記インデックス情報に基づいて、前記基底画像集合の中から前記複数の非直交基底画像を特定する基底画像特定手段と、前記端末記録手段に記録される前記係数情報の新たな係数列に基づく、前記基底画像特定手段により特定された前記複数の非直交基底画像の線型結合を求めて前記認証画像を生成する認証画像生成手段とを有することを特徴とする。

【００３４】

さらに、本発明に係るホルダであることの認証に利用される第１の記録媒体は、認証画像と該認証画像とは異なる互いに独立な複数の任意の画像とを線型部分空間の基底ベクトルとして直交化し、正規化することにより求められた互いに直交する複数の直交基底画像を、変換行列により互いに非直交となる複数の非直交基底画像へと変換させた基底画像集合と、ホルダの認証に用いられる認証画像を生成するために用いられる複数の非直交基底画像を、前記基底画像集合の中から特定するためのインデックス情報と、前記変換行列により変換される前の前記複数の直交基底画像から前記インデックス情報に基づいて複数の直交基底画像を特定し、特定された複数の直交基底画像と前記認証画像との内積により求められた係数列に、前記変換行列の逆行列を積算することにより求められる新たな係数列の係数情報との３つの鍵情報を用いて、基底画像特定手段が、前記インデックス情報に基づいて、前記基底画像集合の中から前記複数の非直交基底画像を特定し、認証画像生成手段が、前記係数情報の新たな係数列に基づく、前記基底画像特定手段により特定された前記複数の非直交基底画像の線型結合を求めて前記認証画像を生成するホルダ認証端末において使用される前記インデックス情報または前記係数情報の少なくとも一方を記録する情報記録手段を有することを特徴とする。

【００３５】

従来より知られている認証画像の生成方法では、画像の特徴を示すベクトルが互いに直交する複数の直交基底画像からなる基底画像集合と、ホルダの認証に用いられる認証画像を生成するために用いる複数の直交基底画像を基底画像集合の中から特定するためのイン

デックス情報と、インデックス情報に基づいて基底画像集合から特定された複数の直交基底画像のそれぞれと認証画像との内積により求められる係数列の係数情報との３つの鍵情報を用いて、認証画像の生成を行っていた。

【００３６】

しかしながら、基底画像集合として複数の直交基底画像をそのまま用いると、係数情報が認証画像と各基底画像との内積により簡単に求められるという利点がある一方で、基底画像は互いに直交であるため、簡単に解読されてしまうおそれがあるという問題があった。例えば、第三者が、直交関係（同値関係）を基底画像集合Ωに定義すれば、任意の認証画像に対して、それを生成するための基底画像集合Ωの部分集合が特定されるおそれがあるという問題があった。

【００３７】

本発明に係る第１のホルダ認証システム、第１のホルダ認証端末およびホルダであることの認証に利用される第１の記録媒体では、複数の直交基底画像からなる基底画像集合に代えて、変換行列により互いに非直交となる複数の非直交基底画像へと変換された基底画像集合を用いることにより、認証画像の生成処理を行うことを特徴とする。このように、複数の非直交基底画像からなる基底画像集合を用いることにより、直交基底画像のように第三者によって簡単に基底画像が解読されてしまうことを防止することが可能となる。

【００３８】

ここで、ホルダとは、一定のサービスの提供などを受けることが認められた正当な（真性の）なユーザ（使用者）を意味し、例えば、クレジットカードによる商品購入サービスをユーザが受けようとする場合には、クレジットカード会社によりクレジットカードの利用を認められた者が該当し、一般的にクレジットカードの正当な所有者が該当することになる。

【００３９】

また、ホルダの認証に用いられる認証画像とは、ホルダの顔写真が一般的に用いられる。ただし、ホルダの認証に用いられる認証画像は、必ずしも顔写真だけには限定されず、ホルダを認証可能なデータであればどのような情報であってもよい。つまり、認証画像は、必ずしも人間の視覚により確認できる画像データだけには限定されず、機械的な判断装置により判断することが可能となるパスワード、サイン、指紋（視覚的に判断できる指紋画像だけでなく、視覚的に判断することが困難な指紋の特徴ベクトル情報も含む）、静脈パターン情報などであってよい。

【００４０】

さらに、ホルダであることの認証に利用される記録媒体とは、クレジットカードのようにカード形状をなすものはもちろんのこと、携帯電話（フィーチャーフォン(Feature phone)やスマートフォンなどを含む）、ＰＤＡ（Personal Digital Assistant、Personal Data Assistance）、タブレット端末、携帯用コンピュータなどのように、ユーザが個別に所持して使用する携帯情報機器などであって、必ずしもカード形状を呈しないものであっても、ホルダであることの認証に利用される記録媒体に含まれる。

【００４１】

また、ホルダであることの認証に利用される記録媒体の情報記録手段は、メモリなどのように電子データを記録可能な媒体だけには限定されない。例えば、ホルダであることの認証に利用される記録媒体がカードである場合において、カードの表面にバーコード、ＱＲコード、認証コード番号などが印刷など（記録）されている場合であっても、所定の情報をカードに付帯することが可能であることから、情報記録手段を備えるものと判断することが可能となる。

【００４２】

さらに、ホルダ認証サーバは、ネットワークを介してホルダ認証端末に接続され、ホルダ認証端末において認証画像の生成に必要な鍵情報を記録するものであれば、必ずしもクライアントとサーバとの関係をなすものには限定されない。例えば、ホルダ認証サーバが他のホルダ認証端末として機能するものであって、ホルダ認証サーバと、ホルダ認証端末

とが、Peer to Peer（ピアトゥピア）の関係により接続されるものであってもよい。この場合には、一のホルダ認証端末が、他のホルダ認証端末の鍵情報を所有し、必要に応じてネットワークを介して鍵情報の送受信を行うことによって、ホルダ認証端末で認証画像の生成処理を行うことが可能となる。

【００４３】

また、本発明に係る第２のホルダ認証システムは、認証画像と該認証画像とは異なる互いに独立な複数の任意の画像とを線型部分空間の基底ベクトルとして直交化し、正規化することにより求められた互いに直交する複数の直交基底画像を、変換行列により前記直交基底画像とは異なる複数の基底画像へと変換させた基底画像集合を記録する端末記録手段を備えて、ホルダの認証に用いられる認証画像を生成するホルダ認証端末と、前記変換行列の逆行列が記録されると共に、ホルダの認証に用いられる認証画像を生成するために用いられる複数の基底画像を、前記基底画像集合の中から特定するためのインデックス情報、または、前記変換行列により変換される前の前記複数の直交基底画像から前記インデックス情報に基づいて複数の直交基底画像を特定し、特定された複数の直交基底画像と前記認証画像との内積によって求められた係数列の係数情報を記録可能なサーバ記録手段と、該サーバ記録手段に記録された前記変換行列の逆行列と、前記インデックス情報または前記係数情報とをネットワークを介して前記ホルダ認証端末に送信可能なサーバ通信手段とを備えたホルダ認証サーバと、前記インデックス情報または前記係数情報のうち前記サーバ記録手段に記録されていない情報を記録する情報記録手段を備えて前記ホルダであることの認証に利用される記録媒体とを有するホルダ認証システムであって、前記ホルダ認証端末は、前記ホルダ認証サーバの前記サーバ通信手段により送信された前記逆行列と、前記インデックス情報または前記係数情報とを、前記ネットワークを介して取得して前記端末記録手段に記録するデータ通信手段と、前記記録媒体の前記情報記録手段より前記インデックス情報または前記係数情報を取得して前記端末記録手段に記録するデータ取得手段と、前記端末記録手段に記録される前記インデックス情報に基づいて、前記基底画像集合の中から前記複数の基底画像を特定する基底画像特定手段と、前記基底画像特定手段により特定された前記複数の基底画像を前記端末記録手段に記録される前記逆行列を用いて複数の直交基底画像に変換し、前記端末記録手段に記録される前記係数情報の係数列に基づく、変換された前記複数の直交基底画像の線型結合を求めて前記認証画像を生成する認証画像生成手段とを有することを特徴とする。

【００４４】

さらに、本発明に係る第２のホルダ認証端末は、認証画像と該認証画像とは異なる互いに独立な複数の任意の画像とを線型部分空間の基底ベクトルとして直交化し、正規化することにより求められた互いに直交する複数の直交基底画像を、当該直交基底画像とは異なる複数の基底画像へと変換する変換行列の逆行列と、前記変換行列により変換された前記複数の基底画像からなる基底画像集合と、ホルダの認証に用いられる認証画像を生成するために用いられる複数の基底画像を、前記基底画像集合を構成する複数の基底画像の中から特定するためのインデックス情報と、前記変換行列により変換される前の前記複数の直交基底画像から前記インデックス情報に基づいて複数の直交基底画像を特定し、特定された複数の直交基底画像と前記認証画像との内積によって求められた係数列の係数情報との４つの鍵情報を記録する端末記録手段と、該端末記録手段に記録される前記インデックス情報に基づいて、前記基底画像集合の中から前記複数の基底画像を特定する基底画像特定手段と、前記基底画像特定手段により特定された前記複数の基底画像を前記端末記録手段に記録される前記逆行列を用いて複数の直交基底画像に変換し、前記端末記録手段に記録される前記係数情報の係数列に基づく、変換された前記複数の直交基底画像の線型結合を求めて前記認証画像を生成する認証画像生成手段とを有することを特徴とする。

【００４５】

また、本発明に係るホルダであることの認証に利用される第２の記録媒体は、認証画像と該認証画像とは異なる互いに独立な複数の任意の画像とを線型部分空間の基底ベクトルとして直交化し、正規化することにより求められた互いに直交する複数の直交基底画像を

、当該直交基底画像とは異なる複数の基底画像へと変換する変換行列の逆行列と、前記変換行列により変換された前記複数の基底画像からなる基底画像集合と、ホルダの認証に用いられる認証画像を生成するために用いられる複数の基底画像を、前記基底画像集合を構成する複数の基底画像の中から特定するためのインデックス情報と、前記変換行列により変換される前の前記複数の直交基底画像から前記インデックス情報に基づいて複数の直交基底画像を特定し、特定された複数の直交基底画像と前記認証画像との内積によって求められた係数列の係数情報との４つの鍵情報を用いて、基底画像特定手段が、前記インデックス情報に基づいて、前記基底画像集合の中から前記複数の基底画像を特定し、認証画像生成手段が、前記基底画像特定手段により特定された前記複数の基底画像を前記逆行列を用いて複数の直交基底画像に変換し、前記係数情報の係数列に基づく変換された前記複数の直交基底画像の線型結合を求めて前記認証画像を生成するホルダ認証端末おいて使用される前記インデックス情報または前記係数情報の少なくとも一方を記録する情報記録手段を有することを特徴とする。

【００４６】

本発明に係る第２のホルダ認証システム、第２のホルダ認証端末およびホルダであることの認証に利用される第２の記録媒体によれば、認証画像を生成するために必要な鍵情報として、基底画像集合、インデックス情報および係数情報の３種類だけではなく、さらに変換行列の逆行列を加えた４種類とすることが可能となる。このように鍵情報の数が増加することにより、従来のように３種類の鍵情報を用いて認証画像の生成を行う場合に比べてセキュリティーを高めることが可能となる。

【００４７】

さらに、本発明に係る第２のホルダ認証システムでは、４種類の鍵情報を、ホルダ認証端末、ホルダ認証サーバおよび記録媒体に分散させることができるので、認証画像の生成のために必要とされる鍵情報の全て揃えることが困難となる。このため、容易に認証画像の生成が行われてしまうことを防止することができ、認証画像の生成処理におけるセキュリティーを高めることが可能となる。

【００４８】

また、上述した第１のホルダ認証システムにおいて、前記記録媒体の前記情報記録手段には、ホルダを識別するための文字列情報Ｓと、変換関数Ｆ（Ｓ）により前記認証画像を生成するために用いられる基底画像の枚数ｒ（但しｒは自然数とする）に対応する数の数値からなる数列（u_1，u_2，・・・，u_r）に変換された該文字列情報Ｓのそれぞれの数値の逆数（１／u_1，１／u_2，・・・，１／u_r）が、前記係数情報の係数列のそれぞれの係数に積算されて重み付けが行われた係数情報とが記録され、前記ホルダ認証サーバの前記サーバ記録手段には、前記インデックス情報と、前記変換関数Ｆ（Ｓ）とが記録され、前記ホルダ認証サーバは、前記サーバ記録手段に記録される前記変換関数Ｆ（Ｓ）に基づいて、前記文字列情報Ｓより求められた数列を第２の係数情報として算出する第２係数情報算出手段を有し、前記ホルダ認証端末の前記データ取得手段は、前記記録媒体の前記情報記録手段より前記文字列情報Ｓと、前記重み付けが行われた係数情報とを取得して前記端末記録手段に記録し、前記ホルダ認証端末の前記データ通信手段は、前記データ取得手段により取得された前記文字列情報Ｓを前記ホルダ認証サーバに送信し、前記ホルダ認証サーバの前記サーバ通信手段は、前記データ通信手段により送信された前記文字列情報Ｓを取得し、前記ホルダ認証サーバの前記第２係数情報算出手段は、前記サーバ通信手段によって取得した前記文字列情報Ｓと前記サーバ記録手段に記録される前記変換関数Ｆ（Ｓ）とに基づいて第２の係数情報を算出し、前記ホルダ認証サーバの前記サーバ通信手段は、前記インデックス情報と、前記第２係数情報算出手段により算出された前記第２の係数情報とを前記ホルダ認証端末に送信し、前記ホルダ認証端末の前記データ通信手段は、前記サーバ通信手段により送信された前記インデックス情報と、前記第２の係数情報とを受信して前記端末記録手段に記録し、前記基底画像特定手段は、前記端末記録手段に記録される前記インデックス情報に基づいて、前記基底画像集合の中から前記複数の非直交基底画像を特定し、前記認証画像生成手段は、前記端末記録手段に記録される前記重み付け

が行われた係数情報の係数列と前記端末記録手段に記録される前記第２の係数情報の数列とにより算出された係数列とに基づく、前記基底画像特定手段により特定された前記複数の非直交基底画像の線型結合によって前記認証画像を生成するものであってもよい。

【００４９】

また、上述した第２のホルダ認証システムにおいて、前記記録媒体の前記情報記録手段には、ホルダを識別するための文字列情報Ｓと、変換関数Ｆ（Ｓ）により前記認証画像を生成するために用いられる基底画像の枚数ｒ（但しｒは自然数とする）に対応する数の数値からなる数列（u_1，u_2，・・・，u_r）に変換された該文字列情報Ｓのそれぞれの数値の逆数（１／u_1，１／u_2，・・・，１／u_r）が、前記係数情報の係数列のそれぞれの係数に積算されて重み付けが行われた係数情報とが記録され、前記ホルダ認証サーバの前記サーバ記録手段には、前記逆行列と、前記インデックス情報と、前記変換関数Ｆ（Ｓ）とが記録され、前記ホルダ認証サーバは、前記サーバ記録手段に記録される前記変換関数Ｆ（Ｓ）に基づいて、前記文字列情報Ｓより求められた数列を第２の係数情報として算出する第２係数情報算出手段を有し、前記ホルダ認証端末の前記データ取得手段は、前記記録媒体の前記情報記録手段より前記文字列情報Ｓと、前記重み付けが行われた係数情報とを取得して前記端末記録手段に記録し、前記ホルダ認証端末の前記データ通信手段は、前記データ取得手段により取得された前記文字列情報Ｓを前記ホルダ認証サーバに送信し、前記ホルダ認証サーバの前記サーバ通信手段は、前記データ通信手段により送信された前記文字列情報Ｓを取得し、前記ホルダ認証サーバの前記第２係数情報算出手段は、前記サーバ通信手段によって取得した前記文字列情報Ｓと前記サーバ記録手段に記録される前記変換関数Ｆ（Ｓ）とに基づいて第２の係数情報を算出し、前記ホルダ認証サーバの前記サーバ通信手段は、前記逆行列と、前記インデックス情報と、前記第２係数情報算出手段により算出された前記第２の係数情報とを前記ホルダ認証端末に送信し、前記ホルダ認証端末の前記データ通信手段は、前記サーバ通信手段により送信された前記逆行列と、前記インデックス情報と、前記第２の係数情報とを受信して前記端末記録手段に記録し、前記基底画像特定手段は、前記端末記録手段に記録される前記インデックス情報に基づいて、前記基底画像集合の中から前記複数の基底画像を特定し、前記認証画像生成手段は、前記基底画像特定手段により特定された前記複数の基底画像を前記端末記録手段に記録される前記逆行列を用いて複数の直交基底画像に変換し、前記端末記録手段に記録される前記重み付けが行われた係数情報の係数列と前記端末記録手段に記録される前記第２の係数情報の数列とにより算出された係数列に基づく、変換された前記複数の直交基底画像の線型結合を求めて前記認証画像を生成するものであってもよい。

【００５０】

さらに、上述した第２のホルダ認証端末において、前記端末記録手段は、ホルダを識別するための文字列情報Ｓを前記認証画像を生成するために用いられる基底画像の枚数ｒ（但しｒは自然数とする）に対応する数の数値からなる数列（u_1，u_2，・・・，u_r）に変換する変換関数Ｆ（Ｓ）に基づいて求められた前記数列を第２の係数情報として記録すると共に、前記係数情報の係数列のそれぞれの係数に対して、前記第２の係数情報をなす数列のそれぞれの数値の逆数（１／u_1，１／u_2，・・・，１／u_r）を積算することにより、各係数に重み付けが行われた係数列を重み付けが行われた係数情報として記録し、前記認証画像生成手段は、前記端末記録手段に記録される前記重み付けが行われた係数情報の係数列と前記端末記録手段に記録される前記第２の係数情報の数列とにより算出された係数列とに基づく、前記基底画像特定手段により特定された前記複数の非直交基底画像の線型結合を求めて前記認証画像を生成するものであってもよい。

【００５１】

さらに、上述した第２のホルダ認証端末において、前記端末記録手段は、ホルダを識別するための文字列情報Ｓを前記認証画像を生成するために用いられる基底画像の枚数ｒ（但しｒは自然数とする）に対応する数の数値からなる数列（u_1，u_2，・・・，u_r）に変換する変換関数Ｆ（Ｓ）に基づいて求められた前記数列を第２の係数情報として記録すると共に、前記係数情報の係数列のそれぞれの係数に対して、前記第２の係数情報をなす数列

のそれぞれの数値の逆数（１／u_1，１／u_2，・・・，１／u_r）を積算することにより、各係数に重み付けが行われた係数列を重み付けが行われた係数情報として記録し、前記認証画像生成手段は、前記基底画像特定手段により特定された前記複数の基底画像を前記端末記録手段に記録される前記逆行列を用いて複数の直交基底画像に変換し、前記端末記録手段に記録される前記重み付けが行われた係数情報の係数列と前記端末記録手段に記録される前記第２の係数情報の数列とにより算出された係数列に基づく、変換された前記複数の直交基底画像の線型結合を求めて前記認証画像を生成するものであってもよい。

【００５２】

また、本発明に係るホルダであることの認証に利用される第３の記録媒体は、認証画像と該認証画像とは異なる互いに独立な複数の任意の画像とを線型部分空間の基底ベクトルとして直交化し、正規化することにより求められた互いに直交する複数の直交基底画像を、変換行列により互いに非直交となる複数の非直交基底画像へと変換させた基底画像集合と、ホルダの認証に用いられる認証画像を生成するために用いられる複数の非直交基底画像を、前記基底画像集合の中から特定するためのインデックス情報と、ホルダを識別するための文字列情報Ｓを前記認証画像を生成するために用いられる基底画像の枚数ｒ（但しｒは自然数とする）に対応する数の数値からなる数列（u_1，u_2，・・・，u_r）に変換する変換関数Ｆ（Ｓ）に基づいて求められた前記数列からなる第２の係数情報と、前記変換行列により変換される前の前記複数の直交基底画像から前記インデックス情報に基づいて前記複数の直交基底画像を特定し、特定された複数の直交基底画像と前記認証画像との内積により求められた係数列に、前記変換行列の逆行列を積算することにより求められる新たな係数列のそれぞれの係数に対して、前記第２の係数情報をなす数列のそれぞれの数値の逆数（１／u_1，１／u_2，・・・，１／u_r）を積算することにより、各係数に重み付けが行われた係数列からなる重み付けが行われた係数情報との４つの鍵情報を用いて、基底画像特定手段が、前記変換行列により変換される前の前記複数の直交基底画像から前記インデックス情報に基づいて前記複数の直交基底画像を特定し、認証画像生成手段が、前記重み付けが行われた係数情報の係数列と前記第２の係数情報の数列とにより算出された係数列に基づく、前記基底画像特定手段により特定された前記複数の直交基底画像の線型結合を求めて前記認証画像を生成するホルダ認証端末おいて使用される前記インデックス情報または前記重み付けが行われた係数情報の少なくとも一方を記録する情報記録手段を有することを特徴とする。

【００５３】

さらに、本発明に係るホルダであることの認証に利用される第４の記録媒体は、認証画像と該認証画像とは異なる互いに独立な複数の任意の画像とを線型部分空間の基底ベクトルとして直交化し、正規化することにより求められた互いに直交する複数の直交基底画像を、当該直交基底画像とは異なる複数の基底画像へと変換する変換行列の逆行列と、前記変換行列により変換された前記複数の基底画像からなる基底画像集合と、ホルダの認証に用いられる認証画像を生成するために用いられる複数の基底画像を、前記基底画像集合を構成する複数の基底画像の中から特定するためのインデックス情報と、ホルダを識別するための文字列情報Ｓを前記認証画像を生成するために用いられる基底画像の枚数ｒ（但しｒは自然数とする）に対応する数の数値からなる数列（u_1，u_2，・・・，u_r）に変換する変換関数Ｆ（Ｓ）に基づいて求められた前記数列からなる第２の係数情報と、前記変換行列により変換される前の前記複数の直交基底画像から前記インデックス情報に基づいて前記複数の直交基底画像を特定し、特定された複数の直交基底画像と前記認証画像との内積によって求められた係数列のそれぞれの係数に対して、前記第２の係数情報をなす数列のそれぞれの数値の逆数（１／u_1，１／u_2，・・・，１／u_r）を積算することにより、各係数に重み付けが行われた係数列からなる重み付けが行われた係数情報とを用いて、基底画像特定手段が、前記インデックス情報に基づいて、前記基底画像集合の中から前記複数の基底画像を特定し、認証画像生成手段が、前記基底画像特定手段により特定された前記複数の基底画像を前記逆行列を用いて前記複数の直交基底画像に変換し、前記重み付けが行われた係数情報の係数列と前記第２の係数情報の数列とにより算出された係数列に基づく

、変換された前記複数の直交基底画像の線型結合を求めて前記認証画像を生成するホルダ認証端末おいて使用される前記インデックス情報または前記重み付けが行われた係数情報の少なくとも一方を記録する情報記録手段を有することを特徴とする。

【００５４】

上述したように、本発明に係る第１および第２のホルダ認証システム、第１および第２のホルダ認証端末、本発明に係るホルダであることの認証に利用される第３の記録媒体および第４の記録媒体では、変換関数Ｆ（Ｓ）に基づいて、ホルダを識別するための文字列情報Ｓが数列で示された第２の係数情報を算出するとともに、第２の係数情報を利用して重み付けが行われた係数情報を算出することによって、認証画像の生成に必要とされる鍵情報の一部を、第２の係数情報および重み付けが行われた係数情報に置き換えることが可能となる。このため、鍵情報を従来に比べて複雑にすることができ、認証画像の生成処理におけるセキュリティーを高めることが可能となる。

【００５５】

さらに、第２の係数情報および重み付けが行われた係数情報は、文字列情報Ｓと変換関数Ｆ（Ｓ）とにより算出することができる。このため、文字列情報Ｓを記録媒体の情報記録手段に記録させ、変換関数Ｆ（Ｓ）をホルダ認証サーバのサーバ記録手段に記録させることにより、鍵情報を分散させることができるので、セキュリティーを高めることができる。

【００５６】

また、上述した第１のホルダ認証システムにおいて、前記基底画像集合は、前記複数の非直交基底画像が前記ホルダ認証端末毎に異なる置換変換テーブル情報に基づいて置換変換された状態で前記ホルダ認証端末のそれぞれの前記端末記録手段に記録され、前記ホルダ認証サーバの前記サーバ記録手段には、前記ホルダ認証端末毎に異なる前記置換変換テーブル情報が記録され、前記ホルダ認証サーバは、前記ホルダ認証端末を識別するための端末情報により該当するホルダ認証端末の前記置換変換テーブル情報を前記サーバ記録手段より読み出し、読み出された前記置換変換テーブル情報に基づいて、前記インデックス情報を置換変換することにより、前記置換変換テーブル情報によって置換変換される前記基底画像集合の中から前記認証画像の生成に用いられる前記複数の非直交基底画像を求めるための第２インデックス情報を算出する第２インデックス情報算出手段を有し、前記ホルダ認証端末の前記データ通信手段は、当該ホルダ認証端末の前記端末情報を前記ホルダ認証サーバに送信し、前記ホルダ認証サーバの前記サーバ通信手段は、前記データ通信手段により送信された前記端末情報を取得し、前記第２インデックス情報算出手段は、前記サーバ通信手段によって取得した前記端末情報に該当する前記置換変換テーブル情報に基づいて、前記第２インデックス情報を算出し、前記ホルダ認証サーバの前記サーバ通信手段は、前記第２インデックス情報を前記ホルダ認証端末に送信し、前記ホルダ認証端末の前記データ通信手段は、前記サーバ通信手段により送信された前記第２インデックス情報を受信して前記端末記録手段に記録し、前記基底画像特定手段は、前記端末記録手段に記録される前記第２インデックス情報に基づいて、置換変換された前記基底画像集合の中から前記認証画像の生成に用いられる前記複数の非直交基底画像を特定するものであってもよい。

【００５７】

さらに、上述した第２のホルダ認証システムにおいて、前記基底画像集合は、前記複数の基底画像が前記ホルダ認証端末毎に異なる置換変換テーブル情報に基づいて置換変換された状態で前記ホルダ認証端末のそれぞれの前記端末記録手段に記録され、前記ホルダ認証サーバの前記サーバ記録手段には、前記ホルダ認証端末毎に異なる前記置換変換テーブル情報が記録され、前記ホルダ認証サーバは、前記ホルダ認証端末を識別するための端末情報により該当するホルダ認証端末の前記置換変換テーブル情報を前記サーバ記録手段より読み出し、読み出された前記置換変換テーブル情報に基づいて、前記インデックス情報を置換変換することにより、前記置換変換テーブル情報によって置換変換される前記基底画像集合の中から前記認証画像の生成に用いられる前記複数の基底画像を求めるための第

２インデックス情報を算出する第２インデックス情報算出手段を有し、前記ホルダ認証端末の前記データ通信手段は、当該ホルダ認証端末の前記端末情報を前記ホルダ認証サーバに送信し、前記ホルダ認証サーバの前記サーバ通信手段は、前記データ通信手段により送信された前記端末情報を取得し、前記第２インデックス情報算出手段は、前記サーバ通信手段によって取得した前記端末情報に該当する前記置換変換テーブル情報に基づいて、前記第２インデックス情報を算出し、前記ホルダ認証サーバの前記サーバ通信手段は、前記第２インデックス情報を前記ホルダ認証端末に送信し、前記ホルダ認証端末の前記データ通信手段は、前記サーバ通信手段により送信された前記第２インデックス情報を受信して前記端末記録手段に記録し、前記基底画像特定手段は、前記端末記録手段に記録される前記第２インデックス情報に基づいて、置換変換された前記基底画像集合の中から前記認証画像の生成に用いられる前記複数の基底画像を特定するものであってもよい。

【００５８】

また、上述した第１のホルダ認証端末において、前記基底画像集合は、前記複数の非直交基底画像が置換変換テーブル情報に基づいて置換変換された状態で前記端末記録手段に記録され、さらに、前記端末記録手段に、前記置換変換テーブル情報によって置換変換された前記基底画像集合の中から前記認証画像の生成に用いられる前記複数の非直交基底画像を求めるための第２インデックス情報が記録されており、前記基底画像特定手段は、前記端末記録手段に記録される前記第２インデックス情報に基づいて、置換変換された前記基底画像集合の中から前記認証画像の生成に用いられる前記複数の非直交基底画像を特定するものであってもよい。

【００５９】

さらに、上述した第２のホルダ認証端末において、前記基底画像集合は、前記複数の基底画像が置換変換テーブル情報に基づいて置換変換された状態で前記端末記録手段に記録され、さらに、前記端末記録手段に、前記置換変換テーブル情報によって置換変換された前記基底画像集合の中から前記認証画像の生成に用いられる前記複数の基底画像を求めるための第２インデックス情報が記録されており、前記基底画像特定手段は、前記端末記録手段に記録される前記第２インデックス情報に基づいて、置換変換された前記基底画像集合の中から前記認証画像の生成に用いられる前記複数の基底画像を特定するものであってもよい。

【００６０】

上述したように、本発明に係る第１および第２のホルダ認証システム、第１および第２のホルダ認証端末では、基底画像集合の基底画像が置換変換テーブル情報によって置換変換されているので、インデックス情報を第三者が取得しても、基底画像集合から認証画像の生成に用いられる基底画像を求めることが困難となる。このため、認証画像の生成に用いられる基底画像が第三者により簡単に解読されてしまうことを防止することができ、セキュリティーを高めることが可能となる。

【００６１】

さらに、置換変換テーブル情報が認証画像の生成に用いられる鍵情報に加えられることになるので、鍵情報の数が増加することにより、認証画像の生成処理におけるセキュリティーを高めることが可能となる。

【００６２】

また、本発明に係る第３のホルダ認証システムは、ホルダの認証に用いられる認証画像とｒ－１枚（但しｒは２以上の自然数とする）の自然画像とに基づいて多画像モーフィング技術により生成されたモーフィング画像と、前記ｒ－１枚の自然画像とからなる複数の基底画像の基底画像集合を記録する端末記録手段を備えて、ホルダの認証に用いられる認証画像を生成するホルダ認証端末と、前記認証画像とｒ－１枚の前記自然画像とのそれぞれの貢献度からなる貢献度情報、前記認証画像を生成するために用いられる複数の基底画像を、前記基底画像集合を構成する複数の基底画像の中から特定するためのインデックス情報、または、前記基底画像集合における全ての基底画像の特徴ベクトルからなる特徴ベクトル情報を記録可能なサーバ記録手段と、該サーバ記録手段に記録された前記貢献度情

報、前記インデックス情報または前記特徴ベクトル情報を、ネットワークを介して前記ホルダ認証端末に送信可能なサーバ通信手段とを備えたホルダ認証サーバと、前記貢献度情報、前記インデックス情報または前記特徴ベクトル情報のうち前記サーバ記録手段に記録されていない情報を記録する情報記録手段を備えて前記ホルダであることの認証に利用される記録媒体とを有するホルダ認証システムであって、前記ホルダ認証端末は、前記ホルダ認証サーバの前記サーバ通信手段により送信された前記貢献度情報、前記インデックス情報または前記特徴ベクトル情報を、前記ネットワークを介して取得して前記端末記録手段に記録するデータ通信手段と、前記記録媒体の前記情報記録手段より前記貢献度情報、前記インデックス情報または前記特徴ベクトル情報を取得して前記端末記録手段に記録するデータ取得手段と、前記端末記録手段に記録されるｒ－１枚の前記自然画像のそれぞれの特徴ベクトルが前記モーフィング画像の特徴ベクトルに一致するように、前記端末記録手段に記録されるｒ－１枚の前記自然画像のそれぞれを変形処理することにより、ｒ－１枚の前記自然画像の全てをそれぞれの変形画像に変形させる変形画像生成手段と、前記端末記録手段に記録されるｒ－１枚の前記自然画像のそれぞれの特徴ベクトルに対して、前記端末記録手段に記録されるｒ－１枚の前記自然画像のそれぞれの貢献度に基づいて線型結合し、その結果を、前記モーフィング画像の特徴ベクトルから減算し、減算された前記特徴ベクトルを前記認証画像の貢献度で除算することにより、前記認証画像の特徴ベクトルを算出する認証画像特徴ベクトル算出手段と、前記端末記録手段に記録されるｒ－１枚の前記自然画像のそれぞれの変形画像に対して、前記端末記録手段に記録されるｒ－１枚の前記自然画像のそれぞれの貢献度に基づいて線型結合し、その結果を、前記モーフィング画像から減算し、減算された前記モーフィング画像を前記認証画像の貢献度で除算することにより、認証変形画像を算出する認証変形画像算出手段と、前記端末記録手段に記録される前記モーフィング画像の特徴ベクトルが、前記認証画像特徴ベクトル算出手段により算出された前記認証画像の特徴ベクトルに一致するように、前記認証変形画像算出手段により算出された前記認証変形画像をモーフィング処理することにより、前記認証変形画像を前記認証画像に変形させて前記認証画像を生成する認証画像モーフィング生成手段とを有することを特徴とする。

【００６３】

さらに、本発明に係る第３のホルダ認証端末は、ホルダの認証に用いられる認証画像とｒ－１枚（但しｒは２以上の自然数とする）の自然画像とに基づいて多画像モーフィング技術により生成されたモーフィング画像と、前記ｒ－１枚の自然画像とからなる複数の基底画像の基底画像集合と、前記認証画像とｒ－１枚の前記自然画像とのそれぞれの貢献度からなる貢献度情報と、前記認証画像を生成するために用いられる複数の基底画像を、前記基底画像集合を構成する複数の基底画像の中から特定するためのインデックス情報と、前記基底画像集合における全ての基底画像の特徴ベクトルからなる特徴ベクトル情報との４つの鍵情報を記録する端末記録手段と、前記端末記録手段に記録されるｒ－１枚の前記自然画像のそれぞれの特徴ベクトルが前記モーフィング画像の特徴ベクトルに一致するように、前記端末記録手段に記録されるｒ－１枚の前記自然画像のそれぞれを変形処理することにより、ｒ－１枚の前記自然画像の全てをそれぞれの変形画像に変形させる変形画像生成手段と、前記端末記録手段に記録されるｒ－１枚の前記自然画像のそれぞれの特徴ベクトルに対して、前記端末記録手段に記録されるｒ－１枚の前記自然画像のそれぞれの貢献度に基づいて線型結合し、その結果を、前記モーフィング画像の特徴ベクトルから減算し、減算された前記特徴ベクトルを前記認証画像の貢献度で除算することにより、前記認証画像の特徴ベクトルを算出する認証画像特徴ベクトル算出手段と、前記端末記録手段に記録されるｒ－１枚の前記自然画像のそれぞれの変形画像に対して、前記端末記録手段に記録されるｒ－１枚の前記自然画像のそれぞれの貢献度に基づいて線型結合し、その結果を、前記モーフィング画像から減算し、減算された前記モーフィング画像を前記認証画像の貢献度で除算することにより、認証変形画像を算出する認証変形画像算出手段と、前記端末記録手段に記録される前記モーフィング画像の特徴ベクトルが、前記認証画像特徴ベクトル算出手段により算出された前記認証画像の特徴ベクトルに一致するように、前記認

証変形画像算出手段により算出された前記認証変形画像をモーフィング処理することにより、前記認証変形画像を前記認証画像に変形させて前記認証画像を生成する認証画像モーフィング生成手段とを有することを特徴とする。

【００６４】

さらに、本発明に係るホルダであることの認証に利用される第５の記録媒体は、ホルダの認証に用いられる認証画像とｒ－１枚（但しｒは２以上の自然数とする）の自然画像とに基づいて多画像モーフィング技術により生成されたモーフィング画像と、前記ｒ－１枚の自然画像とからなる複数の基底画像の基底画像集合と、前記認証画像とｒ－１枚の前記自然画像とのそれぞれの貢献度からなる貢献度情報と、前記認証画像を生成するために用いられる複数の基底画像を、前記基底画像集合を構成する複数の基底画像の中から特定するためのインデックス情報と、前記基底画像集合における全ての基底画像の特徴ベクトルからなる特徴ベクトル情報との４つの鍵情報を用いて、変形画像生成手段が、ｒ－１枚の前記自然画像のそれぞれの特徴ベクトルが前記モーフィング画像の特徴ベクトルに一致するように、ｒ－１枚の前記自然画像のそれぞれを変形処理することにより、ｒ－１枚の前記自然画像の全てをそれぞれの変形画像に変形させ、認証画像特徴ベクトル算出手段が、ｒ－１枚の前記自然画像のそれぞれの特徴ベクトルに対して、ｒ－１枚の前記自然画像のそれぞれの貢献度に基づいて線型結合し、その結果を、前記モーフィング画像の特徴ベクトルから減算し、減算された前記特徴ベクトルを前記認証画像の貢献度で除算することにより、前記認証画像の特徴ベクトルを算出し、認証変形画像算出手段が、変形画像生成手段により変形されたｒ－１枚の前記自然画像のそれぞれの変形画像に対して、ｒ－１枚の前記自然画像のそれぞれの貢献度に基づいて線型結合し、その結果を、前記モーフィング画像から減算し、減算された前記モーフィング画像を前記認証画像の貢献度で除算することにより、認証変形画像を算出し、認証画像モーフィング生成手段が、前記モーフィング画像の特徴ベクトルが前記認証画像特徴ベクトル算出手段により算出された前記認証画像の特徴ベクトルに一致するように、前記認証変形画像算出手段により算出された前記認証変形画像をモーフィング処理することにより、前記認証変形画像を前記認証画像に変形させて前記認証画像を生成するホルダ認証端末おいて使用される前記貢献度情報、前記インデックス情報または前記特徴ベクトル情報のうち少なくとも一つを記録する情報記録手段を有することを特徴とする。

【００６５】

本発明に係る第３のホルダ認証システム、第３のホルダ認証端末およびホルダであることの認証に利用される第５の記録媒体では、多画像モーフィング技術を応用することによって、認証画像の生成処理を行うことができる。ここで、多画像モーフィング技術を利用することにより、認証画像の生成処理に用いられる基底画像集合に自然画像を利用することが可能となる。基底画像集合を構成する画像として自然画像を用いることにより、不自然な画像を用いる場合に比べて第三者による基底画像集合の攻撃を回避することができ、認証画像の生成処理におけるセキュリティーを高めることが可能となる。

【００６６】

また、本発明に係る基底画像生成装置は、認証画像と該認証画像とは異なる互いに独立なｒ－１枚の任意の画像とが記録された画像記録手段と、該画像記録手段に記録された前記認証画像と前記ｒ－１枚の任意の画像とを、線型部分空間の基底ベクトルとして直交化し、正規化することによりｒ枚の基底画像を生成する基底画像生成手段と、該基底画像生成手段により生成されたｒ枚の基底画像のそれぞれと前記認証画像との内積を算出することにより係数列をなす係数情報を求める係数情報算出手段とを有し、線型結合により前記認証画像を生成することが可能な前記ｒ枚の基底画像と前記係数情報とを求めることを特徴とする。

【００６７】

本発明に係る基底画像生成装置では、認証画像と該認証画像とは異なる互いに独立なｒ－１枚の任意の画像とに基づいてｒ枚の基底画像を生成する。この処理において、ｒ枚の基底画像を算出するために認証画像が用いられるため、ｒ枚の基底画像に認証画像の特徴

が分散されて含まれることになる。このため、求められた基底画像を用いて、認証画像の生成処理を行う場合には、従来の基底画像よりも少ない枚数ｒの基底画像を用いて精度の高い認証画像を生成することが可能となる。

【００６８】

また、係数情報をなす係数列は、各基底画像と認証画像との内積により求められるので、基底画像の枚数ｒが少ない場合には、求められる係数の数も少なくなり、結果として、係数情報のデータ量を少なくすることが可能となる。さらに、認証画像の追加に伴って、認証画像の生成に必要な基底画像だけを生成し、基底画像集合に追加するので、既存のユーザの情報に悪影響を与えることはない。また、基底画像集合の更新や削除も簡単となる。

【発明の効果】

【００６９】

本発明に係るホルダ認証システム、ホルダ認証端末およびホルダであることの認証に利用される記録媒体によれば、複数の直交基底画像からなる基底画像集合に代えて、変換行列により互いに非直交となる複数の非直交基底画像へと変換された基底画像集合を用いることにより、認証画像の生成処理を行うことができる。このように、複数の非直交基底画像からなる基底画像集合を用いることにより、直交基底画像のように第三者によって簡単に基底画像が解読されてしまうことを防止することが可能となる

【００７０】

また、本発明に係るホルダ認証システム、ホルダ認証端末およびホルダであることの認証に利用される記録媒体では、多画像モーフィング技術を応用することによって、認証画像の生成処理を行うことができる。ここで、多画像モーフィング技術を利用することにより、認証画像の生成処理に用いられる基底画像集合に自然画像を利用することが可能となる。基底画像集合を構成する画像として自然画像を用いることにより、不自然な画像を用いる場合に比べて第三者による基底画像集合の攻撃を回避することができ、認証画像の生成処理におけるセキュリティーを高めることが可能となる。

【００７１】

さらに、本発明に係る基底画像生成装置は、認証画像と該認証画像とは異なる互いに独立なｒ－１枚の任意の画像とに基づいてｒ枚の基底画像を生成する。このように、ｒ枚の基底画像を算出するために認証画像が用いられるため、ｒ枚の基底画像に認証画像の特徴が分散されて含まれることになる。このため、求められた基底画像を用いて、認証画像の生成処理を行う場合には、従来の基底画像よりも少ない枚数ｒの基底画像を用いて精度の高い認証画像を生成することが可能となる。

【００７２】

また、本発明に係る基底画像生成装置では、係数情報をなす係数列が、各基底画像と認証画像との内積により求められるので、基底画像の枚数ｒが少ない場合には、求められる係数の数も少なくなり、結果として、係数情報のデータ量を少なくすることが可能となる。さらに、認証画像の追加に伴って、認証画像の生成に必要な基底画像だけを生成し、基底画像集合に追加するので、既存のユーザの情報に悪影響を与えることはない。また、基底画像集合の更新や削除も簡単となる。

【図面の簡単な説明】

【００７３】

【図１】実施の形態に係るホルダ認証システムの概略構成を示したブロック図である。

【図２】実施の形態に係る端末の概略構成を示したブロック図である。

【図３】実施の形態に係るサーバの概略構成を示したブロック図である。

【図４】実施の形態に係るサーバの制御部が、基底画像と係数情報とに基づいて、認証画像を生成する処理を示したフローチャートである。

【図５】実施の形態に係る端末の制御処理部が、認証画像を生成する処理手順を示したフローチャートである。

【図６】実施の形態に係る端末の制御処理部が、自然画像Ｉと自然画像I_2，I_3，・・・

，I_rとに基づいて、自然画像I_1を求める逆モーフィング処理を示したフローチャートである。

【発明を実施するための形態】

【００７４】

以下、本発明に係るホルダ認証システムの一例を、図面を用いて詳細に説明する。なお、［背景技術］において既に説明した事項については、本実施の形態において重複した説明を省略するものとする。

【００７５】

［ホルダ認証システムの全体構成］

図１は、本実施の形態に係るホルダ認証システムの概略構成を示したブロック図である。本実施の形態に係るホルダ認証システム１は、サーバ（ホルダ認証サーバ、基底画像生成装置）２と、端末（ホルダ認証端末）３と、ホルダであることの認証に利用される記録媒体により概略構成されている。本実施の形態に係るホルダ認証システム１では、ホルダであることの認証に利用される記録媒体の一例として、クレジットカード（ＩＣカード）４を用いて説明を行う。

【００７６】

但し、ホルダであることの認証に利用される記録媒体は、クレジットカードだけには限定されない。所定のサービスなどを受けようとする場合に、使用者がサービスの提供を受けることが認められる者であることを証明するために用いられる媒体であって、例えば、サービス提供者などから提示等することが求められる物品（例えば、携帯物）などであれば、どのような形状・形態をなすものであってもよい。

【００７７】

例えば、ホルダであることの認証に利用される記録媒体には、会社の社員証、大学などの学生証、住民基本台帳カード、定期券やプリペイドカードなどに利用される非接触式ＩＣカードなどのようなカード形状を呈するものが含まれ、さらに、携帯電話（フィーチャーフォン(Feature phone)やスマートフォンなどを含む）、ＰＤＡ（Personal Digital Assistant、Personal Data Assistance）、タブレット端末、携帯用コンピュータなどのように、ユーザが個別に所持して使用する携帯情報機器などであって、必ずしもカード形状を呈しないものであっても、ホルダであることの認証に利用される記録媒体に含まれる。

【００７８】

また、ホルダであることの認証に利用される記録媒体は、必ずしもホルダの所有物には限定されず、サービス提供者などから貸与されたもの（例えば、返却が求められる会員証（学生所や社員証など））であってもよい。

【００７９】

図１に示すように、サーバ２と端末３とは、ネットワーク５を介して接続されている。サーバ２と端末３とは、認証画像の生成処理に必要なデータ（例えば、既に説明したＫｅｙ１～Ｋｅｙ３など）や、クレジットカード４の正当性を判断するための情報（カード情報）などの送受信を、ネットワーク５を介して行う。このネットワーク５は、専用回線であってもよく、またインターネットなどの公開された通信回線であってもよい。

【００８０】

サーバ２と端末３とのデータの送受信には、そのデータ内容が簡単に第三者に漏洩しないように、暗号化技術を用いることが多い。暗号化技術としてさまざまな方法を用いることができるが、本実施の形態に係るホルダ認証システム１では、データの暗号化を行うために、さらに、サーバ２および端末３の正当性判断を行うために、公開鍵暗号方式を採用する。

【００８１】

公開鍵暗号方式では、データの暗号化に使用する鍵と復号化に使用する鍵とが分離されており、暗号化に使った鍵と同じ鍵では復号化を行うことができず、片方の鍵からもう一方の鍵を割り出すことも容易にできない仕組みになっている。鍵の持ち主は復号化に用いる鍵のみを他人に知られないように管理し（復号化する鍵＝秘密鍵）、暗号化に用いる鍵

は広く公開することが可能となっている（暗号化する鍵＝公開鍵）。なお、公開鍵は必ずしも公開する必要はなく、使用方法に応じて公開しない方法を用いることも可能である。データを暗号化して送受信する場合、送信者は、受信者が公開している公開鍵を入手してデータの暗号化を行った後にデータの送信を行う。暗号化されたデータは受信者の持つ秘密鍵でしか復号化できないため、途中で第三者に傍受されても中身を解読されることはなく、情報漏洩を防止することが可能となる。

【００８２】

なお、本実施の形態に係る端末３とサーバ２とのデータの送受信では、上述した公開鍵暗号方式を用いるが、暗号化の方法は公開鍵暗号方式には限定されず、他の暗号化方式を採用するものであってもよい。例えば、暗号化に用いる鍵と復号化に用いる鍵とが同一の鍵となる共通鍵暗号方式であってもよい。共通鍵暗号方式を採用する場合であっても、鍵情報の管理を徹底することにより、データの漏洩を抑制することが可能である。

【００８３】

なお、上述した暗号化方式は、クレジットカード４に記録された情報が第三者に盗み取られて内容が簡単に漏洩してしまうことを防止するため、クレジットカード４に記録させる情報に暗号化を行うときにも利用することが可能である。例えば、クレジットカード４を発行する前に、情報の暗号化を行った後に、暗号化された情報をクレジットカード４に記録させる。このように暗号化された情報をクレジットカード４に記録させることにより、第三者がクレジットカード４に記録される情報を盗み取った場合であっても、簡単にその内容を知ることが困難となる。

【００８４】

クレジットカード４に記録される情報の中身を確認する必要が生じた場合には、後述するようにクレジットカード４と端末３との相互認証が行われ、さらに端末３とサーバ２との相互認証とによりクレジットカード４および端末３の正当性が認められた後に、サーバ２が端末３の公開鍵を用いて、クレジットカード４に記録される情報を復号化するための復号化鍵を暗号化し、暗号化された復号化鍵を端末３に送る。

【００８５】

端末３では、サーバ２からの復号化鍵を受信して、サーバ２で使用した公開鍵に対応する秘密鍵で、取得した復号化鍵の復号化を行い、この復号化された復号化鍵を用いることにより、クレジットカード４から読み出した情報の復号化を行うことが可能となる。

【００８６】

クレジットカード４には、認証画像を生成するために必要な情報（例えば、Ｋｅｙ２（インデックス情報）やＫｅｙ３（係数情報）など）の情報を記録することが可能な記録部（情報記録手段）９が設けられている。記録部９は、一般的なメモリにより構成されており、一定量のデータを記録することが可能となっている。本実施の形態においては、記録部９に、認証画像の生成に必要とされるＫｅｙ２（インデックス情報）やＫｅｙ３（係数情報）が記録される。

【００８７】

なお、クレジットカード４の記録部９は必ずしも一般的なメモリなどには限定されない。例えば、クレジットカード４の表面にバーコード、ＱＲコード、識別番号などが印刷（記録）されている場合には、これらの印刷情報に基づいてＫｅｙ２（インデックス情報）やＫｅｙ３（係数情報）を記録することができるので、実質的に記録部９を備えているものと判断することができる。

【００８８】

［端末の構成］

端末３は、図２に示すように、カードリーダ部（データ取得手段）１１と、画像記録部（端末記録手段）１２と、通信部（データ通信手段）１３と、制御処理部（基底画像特定手段、認証画像生成手段、変形画像生成手段、認証画像特徴ベクトル算出手段、認証変形画像算出手段、認証画像モーフィング生成手段）１４と、画像表示部１５とを有している。

【００８９】
カードリーダ部１１は、クレジットカード４の記録部９に記録されるデータ（上述したＫｅｙ２（インデックス情報）やＫｅｙ３（係数情報）などの情報）を読み取る機能を有している。また、カードリーダ部１１は、クレジットカード４に記録されるデータを読み取るだけでなく、クレジットカード４に対して必要な情報を入力することが可能となっている。ＩＣカード型のクレジットカードでは、入力された情報に基づいて情報の認証処理を行うことが可能となっており、カードリーダ部１１で、クレジットカード（ＩＣカード）から認証結果を読み取ることによって、クレジットカード４と端末３との認証を行うことが可能になっている。
【００９０】
画像記録部１２は、ハードディスクやＳＳＤ（Solid State Drive）などの一般的な記憶装置により構成されている。画像記録部１２には、サーバ２より取得する基底画像集合（複数の基底画像集（Ｋｅｙ１））などを記録することが可能となっている。通信部１３は、一般的なネットワークインターフェイスカード（ＬＡＮ（Local Area Network）カード）などにより構成されており、サーバ２とのデータの送受信などに使用される。
【００９１】
制御処理部１４は、端末３におけるさまざまな処理を行う機能を有しており、演算処理を行うＣＰＵ（Central Processing Unit）、ホルダの認証処理に関するプログラム等を記録するＲＯＭ（Read-Only Memory）、ワークエリアとして利用されるＲＡＭ（Random Access Memory ：情報記録手段）等により構成されている。このＲＡＭは、カードリーダ部１１においてクレジットカード４より読み取ったデータなどを一時的に記録することが可能となっている。
【００９２】
制御処理部１４は、Ｋｅｙ１（基底画像集合）、Ｋｅｙ２（インデックス情報）、Ｋｅｙ３（係数情報）の情報などに基づいて、認証画像の生成を行う役割を有している。また、本実施の形態に係るクレジットカード４は、ＩＣカード型のクレジットカードであるため、制御処理部１４は、カードリーダ部１１を操作することにより、クレジットカード４と端末３との認証処理を、クレジットカードに行わせる役割を有している。なお、クレジットカード４としてＩＣカードではなく磁気カードが用いられている場合、制御処理部１４は、通信部１３を介してサーバ２にカード情報を送信し、サーバ２より返信された認証情報を、通信部１３を介して取得することによって、磁気カードの認証処理を行う。
【００９３】
また、制御処理部１４は、端末３を識別することが可能な認証情報を、通信部１３を介してサーバ２に送信すると共に、送信した端末３の認証情報に対するサーバ２からの返信認証結果を、通信部１３を介して受信することによって、端末３とサーバ２との認証処理を行う機能を有している。なお、制御処理部１４は、サーバ２との情報の送受信処理において、上述した公開鍵暗号方式を用いて暗号化・復号化処理を行う役割も有している。
【００９４】
画像表示部１５は、液晶ディスプレイやＣＲＴディスプレイなどで構成され、制御処理部１４により生成された認証画像をオペレータに視認させる役割を有している。画像表示部１５に表示される認証画像は、Ｋｅｙ１～Ｋｅｙ３の情報に基づいて復元された認証画像であって、クレジットカードの登録時に申請されたホルダの顔写真とほぼ同じ写真であると判断できる（近似誤差（合成誤差、生成誤差）εが許容範囲に収まる場合）。オペレータは、画像表示部１５に表示される顔写真と実際のクレジットカード４の使用者の顔とを比較することによりホルダの認証を行うことが可能となる。
【００９５】
なお、画像表示部１５に表示される認証画像は、オペレータだけが視認可能なように表示させることが望ましい。このため、画像表示部１５を見る角度によって視認できるか否かを切り替えることが可能な表示技術などを用いることも可能である。さらに、認証画像は平面的なもの（２Ｄ写真）には限定されないため、認証画像を立体画像（３Ｄ写真）と

し、画像表示部１５を肉眼で立体画像を立体視することが可能なディスプレイとすることにより、ホルダの認証精度を向上させることが可能である。

【００９６】

なお、本実施の形態に係る端末３では、端末３のそれぞれに画像記録部１２が設けられ、各端末３のそれぞれの画像記録部１２に基底画像を記録する構成としたが、画像記録部１２は必ずしも全ての端末３のそれぞれに設ける必要はない。例えば、店舗に多数の端末３が設けられる場合には、画像記録部１２に該当する記録手段を備えるローカルサーバを設けて、ローカルサーバと各端末３とをＬＡＮなどで接続させる構成とすることができる。ローカルサーバの記録手段にまとめて複数の基底画像を記録し、各端末３においてＬＡＮを介して認証画像の生成に必要な基底画像を読み出すことにより、各端末３のそれぞれに画像記録部１２を設けることなく、端末３の制御処理部１４で認証画像の生成処理を行うことが可能となる。

【００９７】

［サーバの構成］

サーバ２は、図３に示すように、通信部（サーバ通信手段）２０と、制御部（第２係数情報算出手段、重み付け係数情報算出手段、基底画像生成手段、係数情報算出手段、第２インデックス情報算出手段）２１と、端末情報記録部（サーバ記録手段）２２と、基底画像記録部（サーバ記録手段、画像記録手段）２３と、ホルダ情報記録部（サーバ記録手段）２４とを有している。

【００９８】

通信部２０は、ネットワーク５を介して接続される端末３と、データの送受信を行う機能を有している。なお、図１において、ネットワーク５を介してサーバ２に接続された端末３は、便宜上２台しか示されていないが、サーバ２に接続される端末３の数は、２台に限定されるものではなく、一般には、複数台の端末３が接続されることになる。

【００９９】

端末情報記録部２２、基底画像記録部２３およびホルダ情報記録部２４は、端末３の画像記録部１２と同様に、ハードディスクやＳＳＤ（Solid State Drive）などの一般的な記録装置により構成されている。

【０１００】

端末情報記録部２２には、ネットワーク５を介して接続される端末３に関する情報が記録されている。この端末情報記録部２２に記録される端末３毎の情報を利用することにより、サーバ２では端末３の認証を行うことが可能となっている。端末３毎の情報（以下、端末情報という）とは、例えば、端末のＩＤ（識別番号情報）、端末の種類、端末の使用者または管理者に関する情報、端末の設置場所に関する情報などである。

【０１０１】

また、端末情報記録部２２には、サーバ２と端末３との間で情報の送受信を行う場合において、送信する情報を暗号化し、あるいは暗号化された情報を復号化するときに用いられる端末３毎の公開鍵が記録されている。サーバ２から端末３に対して情報を暗号化して送信する場合には、該当する端末３の公開鍵を用いて情報の暗号化を行うことにより、対応する秘密鍵を有する正当な端末３のみで情報の復号化が可能となる。

【０１０２】

なお、ネットワーク５を通じて容易に該当する端末３の公開鍵を取得することができる状況である場合には、端末情報記録部２２で常に端末３毎の公開鍵を記録させておくのではなく、ネットワーク５を介して取得した公開鍵を一時的に端末情報記録部２２に記録して、暗号化処理を行うようにしてもよい。

【０１０３】

基底画像記録部２３には、多数の基底画像により構成される基底画像集合が記録されている。基底画像集合は、複数の基底画像により構成される基底画像集がグループ毎に整列された状態（基底画像が決められた順番で配置された状態）で記録される。

【０１０４】

なお、基底画像集合は、多数の基底画像により構成されている。この多数の基底画像は、ホルダを認証するための画像と任意の複数の画像によって求められる。ここで、ホルダを認証するための画像とは、本実施の形態に係るホルダ認証システム１を用いて認証を行うホルダの顔写真がその一例として該当する。ホルダを認証するための画像は、端末３の制御処理部１４による認証画像の生成処理により生成される認証画像と等しい画像となる。本説明では、ホルダを認証するための画像を、認証画像ｐとする。

【０１０５】

図４は、認証画像ｐと、任意の画像p_1，p_2，p_3，...，p_{r-1}（但し、各任意の画像は互いに独立であるとする）とに基づいて、基底画像b_1，b_2，b_3，...，b_rと、認証画像ｐを生成するための係数列（係数情報）とを求める処理を示したフローチャートである。

【０１０６】

本実施の形態に係るホルダ認証システム１では、制御部２１によって、図４に示したフローチャートの処理が行われるものとする。また、本実施の形態においては、認証画像ｐと予め認証画像とは異なる複数の任意の画像p_1，p_2，p_3，...，p_{r-1}が基底画像記録部２３に記録されているものとする。

【０１０７】

制御部２１は、まず、認証画像ｐと任意の画像p_1，p_2，p_3，...，p_{r-1}を基底画像記録部２３から読み出す（ステップＳ．１）。次に、制御部２１は、認証画像ｐと任意の画像p_1，p_2，p_3，...，p_{r-1}とからなるｒ枚の画像を、線型部分空間の基底ベクトルとして既存の直交化方法を用いて直交化し、正規化して正規直交基底ベクトルとなるｒ枚の基底画像b_1，b_2，b_3，...，b_rを算出する（ステップＳ．２）。このようにして算出された基底画像に基づく基底画像集合が、本実施の形態に係るホルダ認証システム１における認証画像の生成処理の鍵情報の１つとして利用されることになる。

【０１０８】

この処理において、ｒ枚の基底画像を算出するために、認証画像ｐが用いられているため、基底画像b_1，b_2，b_3，...，b_rに認証画像ｐの特徴が分散されて含まれることになる。このため、算出された基底画像b_1，b_2，b_3，...，b_rを用いて、認証画像ｐの生成処理を行うことにより、従来の基底画像よりも少ない枚数の基底画像を用いて精度の高い認証画像を生成することが可能となる。

【０１０９】

その後、制御部２１は、求められた各基底画像b_iに基づいて認証画像ｐを求める場合に用いる係数w_iを、

$w_i = <p, b_i>$　（但し、$<p, b_i>$は、ｐとb_iとの内積を示す）

の関係式から求める（ステップＳ．３）。

【０１１０】

そして、制御部２１は、求められた基底画像b_1，b_2，b_3，...，b_rと係数w_1，w_2，w_3，...，w_rとに基づいて認証画像ｐを生成する（ステップＳ．４）。ここで、上述したように、各基底画像b_iと認証画像ｐとの内積により係数w_iが求められるので、基底画像b_1，b_2，b_3，...，b_rが少ない場合には、求められる係数w_iの数も少なくなり、係数情報のデータ量が少なくなる。本実施の形態に係るホルダ認証システム１では、例えば、基底画像が２～３枚程度であっても、精度の高い認証画像を生成することが可能となる。

【０１１１】

そして、制御部２１は、求められた基底画像集と係数列とにより認証画像ｐが生成されることを確認した後に、処理を終了する。この処理において生成された基底画像集は、基底画像記録部２３に記録される。また、係数列は係数情報として、サーバ２のホルダ情報記録部２４あるいは、クレジットカード４の記録部９に記録される。制御部２１が図４に示した処理を行うことにより、制御部２１は、本発明に係る基底画像生成装置として機能することになる。

【０１１２】
図４のフローチャートに示すように、認証画像ｐを生成するための基底画像を求めるためには、任意の画像p_1，p_2，p_3，...，p_{r-1}を予め用意する必要が生ずる。任意の画像p_1，p_2，p_3，...，p_{r-1}を用意する方法として、
１）認証画像ｐと違う画像をランダムに生成することにより、任意の画像p_1，p_2，p_3，...，p_{r-1}を用意する。
２）予め多数の自然画像（例えば人間の顔画像）を集めて、集められた自然画像の集合からランダムに画像を選んで任意の画像p_1，p_2，p_3，...，p_{r-1}を用意する。
３）自然画像集合の中の一部の画像を用いて、多画像モーフィング（MIBM: Multiple Image Based Morphing）法（多画像モーフィング技術）により新たに擬似画像集合を作成し、作成された擬似画像集合の中からランダムに擬似画像を抽出することにより、任意の画像p_1，p_2，p_3，...，p_{r-1}を用意する。
などの方法を採用することができる。
【０１１３】
上述した１）の方法で任意の画像p_1，p_2，p_3，...，p_{r-1}を用意することは簡単で実装しやすいが、この方法で用意された任意の画像p_1，p_2，p_3，...，p_{r-1}は、基底画像b_1，b_2，...，b_rから推測される可能性があるため、セキュリティー確保の観点からあまり好ましい方法とはいえない。
【０１１４】
また、上述した２）の方法も、任意の画像の用意が簡単で実装しやすいが、自然画像を用いるために実在の顔画像などが必要となるため、プライバシー保護の観点から採用することが容易でなかった。
【０１１５】
上述した３）の方法は、擬似画像集合からランダムに抽出される画像は擬似画像であって、実在する人の顔写真など（自然画像）でないため、プライバシー保護の観点からも問題が生じにくく、さらに多数の任意の画像を生成しやすいので、任意の画像を用意するために最適な方法であるといえる。
【０１１６】
なお、３）の方法で利用される多画像モーフィング法は、多数の基本画像とそれぞれの画像における貢献度と、それぞれの画像の特徴ベクトルとを用いて、各基本画像とは異なる画像であるが、それぞれの基本画像の貢献度を反映した違和感のない画像を生成する技術である。この多画像モーフィング法については、特願２０１１－０２４３３３号に詳細に開示されている。
【０１１７】
また、基底画像記録部２３に記録される基底画像集合は、制御部２１により、一定期間毎に基底画像の削除・追加・更新などが行われる場合があり、この基底画像の更新などに伴って、認証画像の生成精度の向上などを図ることも可能となっている。
【０１１８】
ここで、従来の方法で生成された基底画像は、１枚の認証画像の生成に多数の基底画像を用いていたため、基底画像の一部が複数人の認証画像の生成処理に利用される場合があった。このような場合に、認証画像ｐの生成に利用されなくなった基底画像を基底画像記録部２３から削除する必要が生ずるが、ある認証画像の生成に使用されなくなった基底画像であっても、他の認証画像の生成に利用されている場合も存在するため、安易に基底画像を削除することができない。このような認証画像の削除・追加・更新が、認証画像の追加・減少に応じて行われるため、それらの作業負担が膨大なものであった。
【０１１９】
しかしながら、上述したように認証画像ｐとｒ－１枚の任意の画像とに基づいてｒ枚の基底画像を生成する場合には、１枚の認証画像ｐの生成に必要とされる基底画像の枚数を少なくすることができる。このため、基底画像の削除・追加・変更処理を行うべき基底画像の枚数を少なくし、処理負担を低減することができる。特に、生成される基底画像には

、認証画像ｐの特徴が分散されて含まれることになる。このため、各基底画像は特定の認証画像ｐにだけ使用されることが好ましく、特定の認証画像ｐが利用されなくなった場合には、該当する基底画像のみを削除すればよくなるので、処理負担の軽減を実現することが可能となる。

【０１２０】

さらに、１枚の認証画像の生成に必要な基底画像の枚数を従来に比べて大幅に低減させることができるので、認証画像が増加しても、認証画像の増加に伴う基底画像の増加を、従来に比べて抑制することが可能となる。

【０１２１】

なお、基底画像記録部２３に記録される基底画像集合の更新などが行われる場合には、制御部２１が、基底画像記録部２３に記録された基底画像集合を端末３のＩＤ情報（識別番号情報）などに基づいて置換変換テーブル（置換変換テーブル情報）を用いて置換変換処理し、置換変換処理が行われた基底画像集合は、該当する端末３に配信されることになる。

【０１２２】

ホルダ情報記録部２４には、ホルダのＩＤ情報や、クレジットカード４の種類や、ホルダの個人情報（住所、氏名など）などのホルダに関するさまざまな情報が記録されている。このため、サーバ２の制御部２１では、端末３から受信したカードを特定するための情報（カード情報）と、ホルダ情報記録部２４に記録されるホルダに関する情報と基づいて、クレジットカード４の種類やホルダの特定などを行うことが可能となっている。

【０１２３】

また、クレジットカード４の記録部９に記録された情報を暗号化した場合において、暗号化されたクレジットカード４の情報を復号化させるために用いる復号化鍵が、ホルダ情報記録部２４に記録されている。例えば、クレジットカード４にＫｅｙ２やＫｅｙ３の情報が記録され、セキュリティー向上のためにＫｅｙ２やＫｅｙ３の情報が暗号化されている場合に、クレジットカード４と相互認証が認められた端末３は、サーバ２に対してクレジットカード４に記録された情報の復号化を行うための復号化鍵を要求することができる。端末３では、サーバ２より送信されたクレジットカード４の復号化鍵を用いることにより、Ｋｅｙ２やＫｅｙ３の情報の復号化を行うことが可能となる。

【０１２４】

さらに、ホルダ情報記録部２４には、必要に応じて、Ｋｅｙ２やＫｅｙ３などの情報を記録することが可能となっている。Ｋｅｙ２およびＫｅｙ３は、ホルダ毎に異なる情報であり、ホルダに関する情報に関連した情報となる。このため、サーバ２では、端末３からの要求に応じて、カード情報により求められたホルダのＫｅｙ２やＫｅｙ３の情報を、端末３の公開鍵を用いて暗号化して、端末３へ送信することができる。

【０１２５】

本実施の形態に係るホルダ認証システム１では、制御部２１が、一定期間毎に、サーバ２から端末３に対して基底画像集合を配信する構成となっている。端末３では、認証画像の生成を行う場合に、サーバ２より配信された基底画像集合の中から認証画像の生成に用いられる基底画像を特定する必要が生ずる。この基底画像を特定するときに、インデックス情報（Ｋｅｙ２）が使用される。

【０１２６】

このようにして構成されるホルダ認証システム１において、ユーザがクレジットカード４を、端末３を操作するオペレータに提示することにより、端末３の制御処理部１４においてホルダの認証画像を生成して画像表示部１５に表示させることが可能となり、オペレータは画像表示部１５に表示される認証画像と、クレジットカード４の使用者（ユーザ）の顔とを比較することによって、クレジットカード４の使用者がホルダであるか否かの判断を行うことが可能となる。

【０１２７】

［認証画像の生成処理］

次に、端末３の制御処理部１４においてホルダの認証画像を生成する処理について説明する。既に説明したように、ホルダの認証画像をｐとすると、認証画像ｐは、複数の基底画像b_iと、認証画像ｐの生成に用いられる基底画像を基底画像集合の中から特定するためのインデックス情報（インデックス集合）Ｊ（ｐ）（但し、認証画像の生成に用いられるインデックス情報Ｊ（ｐ）は、全てのインデックス情報Ｉ＝｛１，２，・・・，Ｎ｝の一部をなす）と、各基底画像における係数情報（係数列）w_iとに基づいて、

【数７】

$$p=\sum_{i\in J(p)} w_i\, b_i \quad \cdots式5$$

に基づいて求められる。

【０１２８】

つまり、認証画像を生成するためには、原則として

（１）認証画像の生成処理に用いられる基底画像集合（Ｋｅｙ１）

（２）認証画像の生成処理に必要な基底画像を特定するためのインデックス情報（Ｋｅｙ２）

（３）認証画像の生成処理を行うために用いられる係数情報（Ｋｅｙ３）

の３つの鍵情報が必要とされる。

【０１２９】

Ｋｅｙ３の係数情報における係数の数は、生成する認証画像毎に異なる数に設定されていてもよいし、どのような認証画像を生成する場合であっても、同じ数に設定されるものであってもよい。係数情報は、データ量が非常に小さいので、クレジットカード４の記録部９に記録することが可能である。

【０１３０】

また、Ｋｅｙ２で示されるインデックス情報も係数情報と同じようにデータ量が小さいので、クレジットカード４の記録部９に記録することができる。但し、インデックス情報（Ｋｅｙ２）または係数情報（Ｋｅｙ３）は、必ずしも、クレジットカード４の記録部９だけに記録されるのではなく、サーバ２のホルダ情報記録部２４などに記録することも可能である。できるだけ、認証画像の生成に必要とされる情報（Ｋｅｙ１～Ｋｅｙ３）を、クレジットカード４、端末３、サーバ２のそれぞれに分散させて管理することによって、セキュリティーを高めることが可能となる。

【０１３１】

また、Ｋｅｙ１で示される基底画像集合は、認証画像ｐと任意の複数の画像とに基づいて複数の基底画像を生成することにより、１枚の認証画像ｐを生成に必要とされる基底画像の枚数を少なくすることができる。しかしながら、もともと画像データは、インデックス情報や係数情報よりもデータ量が大きいため、クレジットカード４の記録部９に記録させることは困難となる場合が多い。このため、サーバ２の基底画像記録部２３あるいは端末３の画像記録部１２に記録させることになる。

【０１３２】

但し、基底画像集合をサーバ２に記録させておく場合、認証画像を生成するたびに、基底画像集合をサーバ２から端末３へとダウンロードさせる必要が生ずる。このように頻繁に基底画像集合をダウンロードさせると、通信負担が増すと共にダウンロード時間が必要となり、円滑な認証画像の生成処理が困難となる場合がある。このため、基底画像集合は、予め端末３の画像記録部１２に記録させておき、定期的にサーバ２から端末３へ一部の基底画像をダウンロードさせることによって基底画像の変更を行うような構成とすることが望ましい。

【０１３３】

なお、認証画像の生成に用いられる基底画像集（複数の基底画像）が端末３に依存する場合には、Ｋｅｙ２で示されるインデックス情報を、サーバ２の端末情報記録部２２に保

存させておき、必要に応じてダウンロードさせる構成とすることが好ましい。基底画像集合を端末３の画像記録部１２に保存する場合において、インデックス情報を端末３に記録させておくと、端末３に記録されるインデックス情報と基底画像集合とに基づいて、認証画像の生成に用いる基底画像が容易に特定される可能性が高くなってしまう。このため、インデックス情報と、基底画像集合とをそれぞれ異なる場所（例えば、端末３とサーバ２と）に保存しておくことにより、認証画像の生成に用いられる情報を分散させることができるので、セキュリティーを高めることができる。

【０１３４】

図５は、端末３の制御処理部１４が、認証画像を生成する処理手順を示したフローチャートである。図５に示すフローチャートでは、端末３にあらかじめ基底画像集合（Ｋｅｙ１）が記録され、サーバ２にインデックス情報（Ｋｅｙ２）が記録され、クレジットカード４に係数情報（Ｋｅｙ３）が記録される場合における認証画像の生成処理を示しており、端末３は、ＲＯＭに記録されたプログラムに従ってこの生成処理を実行する。

【０１３５】

また、クレジットカード４に記録される情報（カード情報やＫｅｙ３の情報）は、第三者に内容が知られてしまうとカード偽造が行われる可能性が高くなるため、あらかじめ暗号化処理されているものとする。また、クレジットカード４に記録された情報を復号化するための復号化鍵は、サーバ２に記録されるものとする。端末３でクレジットカード４の情報を復号化するためには、クレジットカード４と端末３との認証が認められた後に、端末３が、クレジットカード４から情報を取得し、さらに、端末３とサーバ２との認証が認められた後に、端末３が、サーバ２からクレジットカード４の復号化鍵を取得する必要が生ずる。このように、サーバ２にクレジットカード４の復号化鍵を記録しておくことにより、容易なカード情報の復号化が抑制され、クレジットカード４に関する情報のセキュリティーを高めることが可能となる。

【０１３６】

制御処理部１４は、まず、クレジットカード４との認証処理を行う（ステップＳ．２１）。制御処理部１４は、クレジットカード４に対して、認証に必要となる情報を送ることにより、ＩＣカードの演算処理機能を利用してクレジットカード４側で端末３とクレジットカード４との相互認証を判断させ、クレジットカード４より返信された認証結果に基づいて、端末３で認証結果の判断を行う。

【０１３７】

クレジットカード４の認証結果を取得した端末３の制御処理部１４では、取得した認証結果に基づいてクレジットカード４が正当であるかどうかを判断する（ステップＳ．２２）。認証結果が正当でないと判断した場合（ステップＳ．２２においてＮｏの場合）、制御処理部１４は、クレジットカード４が不正であると判断して、クレジットカード４が不正使用である旨のメッセージを、画像表示部１５などに表示させてオペレータに警告を行い（ステップＳ．２３）、クレジットカード４の認証処理を終了する。このように、クレジットカード４の正当性の判断を行うことによって、クレジットカード４の不正使用を防止することができる。

【０１３８】

一方で、認証結果が正当であると判断できた場合（ステップＳ．２２においてＹｅｓの場合）、制御処理部１４は、カードリーダ部１１を介してクレジットカード４にアクセスし、クレジットカード４の記録部９に記録される係数情報（Ｋｅｙ３）と、カードに関する情報（カード情報）とを取得する（ステップＳ．２４）。クレジットカード４では、ステップＳ．２１に示した認証処理において、端末３が正当である旨の認証が行われた場合にのみ、係数情報（Ｋｅｙ３）とカード情報との読み出しを許可する。一方で、ステップＳ．２１に示した認証処理において、端末３が正当でないと判断された場合、クレジットカード４では、制御処理部１４による係数情報（Ｋｅｙ３）およびカード情報の要求を断ることにより、認証画像の生成処理に必要なデータ等が不正にアクセスされてしまうことを防止する。

【０１３９】
次に、制御処理部１４は、端末情報とカード情報とを、サーバ２の公開鍵を用いて暗号化をしてから、サーバ２へ送信する（ステップＳ．２５）。サーバ２では、自己の秘密鍵を用いて、サーバ２の公開鍵で暗号化された情報（端末情報とカード情報）を復号化する。
【０１４０】
サーバ２の公開鍵で暗号化された情報が、端末３からサーバ２に対して送信されるため、公開鍵に対応する秘密鍵を持たないサーバ２では、暗号化された情報の復号化を行うことができない。しかしながら、公開鍵に対応する秘密鍵を備えた正当なサーバ２では、自己の秘密鍵によって、端末３から送信された情報の復号化が可能である。このように、正当なサーバ２でなければ、端末３から送信された情報の復号化が行われないため、第三者に端末情報とカード情報とが漏洩してしまうことを防止することができる。
【０１４１】
サーバ２では、復号化した端末情報に基づいて、端末３の認証処理を行うとともに、カード情報に基づいて、クレジットカード４の認証処理を行う。端末３およびクレジットカード４の認証処理により、端末３およびクレジットカード４が正当であると判断された場合、サーバ２は、カード情報に基づいて対応するホルダの情報をホルダ情報記録部２４から抽出する。そして、サーバ２は、抽出されたホルダ情報に基づいて、ホルダの認証画像を生成するために必要なインデックス情報（Ｋｅｙ２）を求めるとともに、ホルダの情報に基づいて、クレジットカード４に記録された係数情報（Ｋｅｙ３）を復号化するための鍵情報を求める。
【０１４２】
そして、サーバ２の制御部（第２インデックス情報算出手段）２１では、認証処理において特定された端末３のＩＤ情報などに基づく置換変換テーブルにより、インデックス情報の置換変換処理を行う。このため、基底画像集合の配置順序が置換変換処理された後に端末３へ配信される場合であっても、置換変換処理されたインデックス情報（第２インデックス情報）を参照することにより、認証画像の生成処理に必要とされる基底画像を特定することが可能となる。
【０１４３】
その後、サーバ２では、置換変換処理されたインデックス情報（Ｋｅｙ２）と、係数情報（Ｋｅｙ３）を復号化するための鍵情報とを、端末３の公開鍵で暗号化してから、端末３へ送信する。
【０１４４】
端末３では、サーバ２によって送信された暗号化された情報を受信し（ステップＳ．２６）、受信した情報を端末３の秘密鍵で復号化することにより、インデックス情報と係数情報の鍵情報とを取得する（ステップＳ．２７）。そして、端末３では、取得した係数情報の鍵情報に基づいて、クレジットカード４より読み出した係数情報（Ｋｅｙ３）の復号化処理を行う（ステップＳ．２８）。また、端末３では、置換変換処理されたインデックス情報に基づいて、認証画像の生成処理に必要とされる基底画像の特定を行う（ステップＳ．２９）。この処理により、端末３の制御処理部１４は、本発明に係る基底画像特定手段に該当することになる。
【０１４５】
このように、端末３は、係数情報の復号化処理を行うことにより、認証画像の生成処理に必要とされる係数情報を求めることができ、さらに、置換変換処理されたインデックス情報に基づいて、認証画像の生成処理に必要とされる基底画像を求めることができる。そして、端末３は、求められた係数情報を用いて基底画像の線型結合を求めることにより、認証画像の生成処理を行う（ステップＳ．３０）。この処理において、端末３の制御処理部１４は、本発明に係る認証画像生成手段に該当することになる。
【０１４６】
その後、端末３では、生成された認証画像を、画像表示部１５に表示させ（ステップＳ

．３１）、オペレータにホルダの認証画像を提供する。

【０１４７】

オペレータでは、画像表示部１５に表示されたホルダの認証画像と、クレジットカード４の使用者（ユーザ）の顔とを比較することにより、クレジットカード４の使用者が真正の所有者であるホルダであるかどうかを目視により確認することができる。また、認証画像によりカード使用者がホルダであるか否かを、オペレータが肉眼で直接的に判断できるため、ホルダの髪型や服装などが認証画像と異なっている場合であっても、総合的な判断によって、ホルダの認証を行うことができ、クレジットカード４の安全性をより高めることが可能となる。

【０１４８】

なお、図５に示したフローチャートでは、端末３にあらかじめ基底画像集合（Ｋｅｙ１）が記録され、サーバ２にインデックス情報（Ｋｅｙ２）が記録され、クレジットカード４に係数情報（Ｋｅｙ３）が記録される場合において、端末３で認証画像を生成する処理内容を示したが、サーバ２に係数情報（Ｋｅｙ３）が記録され、クレジットカード４にインデックス情報（Ｋｅｙ２）が記録される場合や、クレジットカード４にインデックス情報（Ｋｅｙ２）と係数情報（Ｋｅｙ３）とが記録され、サーバ２には、Ｋｅｙ１～Ｋｅｙ３のいずれも記録されない場合や、サーバ２にインデックス情報（Ｋｅｙ２）と係数情報（Ｋｅｙ３）とが記録され、クレジットカード４には、Ｋｅｙ１～Ｋｅｙ３のいずれも記録されない場合においても、同様に、端末３が基底画像集合（Ｋｅｙ１）と、インデックス情報（Ｋｅｙ２）と、係数情報（Ｋｅｙ３）とを、サーバ２およびクレジットカード４から取得することにより、認証画像を生成することが可能である。

【０１４９】

［基底画像の非直交化］

上述したように、認証画像の生成には、基底画像集合（Ｋｅｙ１）と、インデックス情報（Ｋｅｙ２）と、係数情報（Ｋｅｙ３）とが用いられる。基底画像は、認証画像の生成に用いられる複数の任意の画像を線型部分空間の基底ベクトルとして既存の直交化方法を用いて直交化し、正規化することにより求められるものである。ここで、基底画像は互いに直交であるため容易に解読されるおそれがある。

【０１５０】

つまり、第三者が、基底画像集合Ωに、直交関係（同値関係）を定義することにより、任意の認証画像ｐに対して、その認証画像を生成する基底画像集合Ωの部分集合を特定することが可能となる。従って、直交基底画像を利用することはセキュリティーを確保する上で好ましいことではなかった。

【０１５１】

このため、正規直交画像である基底画像に代えて、非直交の基底画像（非直交基底画像）を認証画像の生成処理に利用することについて説明する。

【０１５２】

まず、説明を簡単にするために、認証画像ｐを生成するためのインデックス情報（インデックス集合）を、Ｊ（ｐ）＝｛１，２，・・・，ｒ｝とする。また、非直交の基底画像（非直交基底画像）の集合を［c_1，c_2，・・・，c_r］とし、正規直交画像である基底画像を、［b_1，b_2，・・・，b_r］とすると、非直交基底画像は、

【数８】

$$[c_1 c_2 \cdots c_r]=[b_1\ b_2 \cdots b_r]\begin{bmatrix}\varphi_{11} & \varphi_{21} & \cdots & \varphi_{r1}\\ \varphi_{12} & \varphi_{22} & \cdots & \varphi_{r2}\\ \vdots & \vdots & \cdots & \vdots\\ \varphi_{1r} & \varphi_{2r} & \cdots & \varphi_{rr}\end{bmatrix}=[b_1\ b_2 \cdots b_r]\Phi$$

…式６

で示すことが可能となる。

【０１５３】

ここで、変換行列Φの要素は、［c_1，c_2，・・・，c_r］が互いに独立になるように適切に設定される、このような設定により、認証画像ｐは、

【数９】

$$p=[b_1\ b_2\cdots b_r]\begin{bmatrix}w_1\\w_2\\\vdots\\w_r\end{bmatrix}=[c_1c_2\cdots c_r]\Phi^{-1}\begin{bmatrix}w_1\\w_2\\\vdots\\w_r\end{bmatrix}$$

$$=[c_1c_2\cdots c_r]\begin{bmatrix}w'_1\\w'_2\\\vdots\\w'_r\end{bmatrix}\quad\cdots式7$$

のようにして生成することが可能となる。

【０１５４】

この式７より認証画像ｐは、非直交基底画像の集合である［c_1，c_2，・・・，c_r］と、新しい係数情報［w'_1，w'_2，・・・，w'_r］とにより求めることができる。

【０１５５】

従って、複数の非直交基底画像集を非直交基底画像集合として、この非直交基底画像集合の中から認証画像ｐを生成するために用いる非直交基底画像を求めるインデックス情報をＫｅｙ２として用いることにより

（１）認証画像の生成処理に用いられる非直交基底画像集合（Ｋｅｙ１）

（２）認証画像の生成処理に必要な非直交基底画像を特定するためのインデックス情報（Ｋｅｙ２）

（３）認証画像の生成処理を行うために用いられる新しい係数情報（Ｋｅｙ３）

の３つの鍵情報を新たな認証画像の生成に必要な情報とすることができる。

【０１５６】

このようにして、互いに直交する直交基底画像集合をＫｅｙ１に用いるのではなく、非直交基底画像集合をＫｅｙ１として用いることにより、基底画像集合（Ｋｅｙ１）の解読が困難となり、ホルダ認証システム１における認証画像の生成処理のセキュリティーを従来よりも高めることができる。

【０１５７】

［基底画像の置換変換処理］

基底画像集合を構成する基底画像は、基底画像集合における各基底画像の順番を置換変換（シャッフル）してから端末３の画像記録部１２やローカルサーバの記録手段に記録させることにより、ホルダ認証システム１における認証画像の生成処理のセキュリティーを高めることが可能となる。このように、基底画像を置換変換するためには置換変換テーブル（置換変換テーブル情報）などを、認証画像を生成するために必要な鍵情報として追加することになる。

【０１５８】

つまり、

（１）認証画像の生成処理に用いられる基底画像集合（Ｋｅｙ１）

（２）認証画像の生成処理に用いられるインデックス情報（Ｋｅｙ２）

（３）認証画像の生成処理に用いられる係数情報（Ｋｅｙ３）

（４）置換変換された基底画像から、置換変換前の順番の基底画像を求めるための置換変換テーブル（置換変換テーブル情報）
の４つの鍵情報が、認証画像の生成に必要となる。このように生成に必要な情報を多くすることにより、情報の分散化が可能となり、セキュリティーを高めることが可能となる。

【０１５９】
なお、置換変換を行う場合、インデックス情報は、置換変換に応じてその情報が変化する可能性があるため、サーバ２の制御部２１においてインデックス情報を置換変換テーブルで置換変換した状態（第２インデックス情報）で、端末３に提供されることが望ましい。このため、インデックス情報は、クレジットカード４ではなくサーバ２に記録しておくことが好ましい。

【０１６０】
例えば、基底画像集合を端末３の画像記録部１２に記録させ、インデックス情報をサーバ２のホルダ情報記録部２４に記録させ、係数情報をクレジットカード４の記録部９に記録させ、置換変換テーブル（置換変換テーブル情報）をサーバ２の端末情報記録部２２などに記録させておくことにより、認証画像の生成に必要となる情報の分散化を行うことが可能となる。

【０１６１】
［基底画像の線型変換処理］
次に基底画像を線型変換することにより、認証画像の生成に必要な鍵情報を追加する方法について説明を行う。

【０１６２】
認証画像ｐの生成に用いられる基底画像を$b_1, b_2, \cdots, b_r$とすると、$b_1, b_2, \cdots, b_r$から式８に示すような別の基底画像$d_1, d_2, \cdots, d_r$を求めることができる。

【数１０】

$$[d_1 d_2 \cdots d_r]=[b_1\ b_2 \cdots b_r]\begin{bmatrix}\Psi_{11} & \Psi_{21} & \cdots & \Psi_{r1}\\ \Psi_{12} & \Psi_{22} & \cdots & \Psi_{r2}\\ \vdots & \vdots & \cdots & \vdots\\ \Psi_{1r} & \Psi_{2r} & \cdots & \Psi_{rr}\end{bmatrix}=[b_1\ b_2 \cdots b_r]\Psi \quad \cdots式８$$

従って、認証画像ｐは式９を用いて、

【数１１】

$$p=[b_1\ b_2 \cdots b_r]\begin{bmatrix}w_1\\ w_2\\ \vdots\\ w_r\end{bmatrix}=[d_1 d_2 \cdots d_r]\Psi^{-1}\begin{bmatrix}w_1\\ w_2\\ \vdots\\ w_r\end{bmatrix} \quad \cdots式９$$

で求めることが可能となる。但し、Ψ^{-1}は変換行列Ψの逆行列を示している。

【０１６３】
このように基底画像集［$b_1, b_2, \cdots, b_r$］を、新しい基底画像集［$d_1, d_2, \cdots, d_r$］と変換行列Ψの逆行列であるΨ^{-1}とで求めることが可能となるため、従来より用いられていた基底画像集合を新しい基底画像集合と逆行列Ψ^{-1}とに分割することが可能となる。

【０１６４】
従って、認証画像の生成処理に必要な鍵情報は、
（１）認証画像の生成処理に用いられる新たな基底画像集合（Ｋｅｙ１）
（２）認証画像の生成処理に用いられるインデックス情報（Ｋｅｙ２）
（３）認証画像の生成処理に用いられる係数情報（Ｋｅｙ３）
（４）逆行列Ψ^{-1}の情報
の４つとなり、認証画像の生成処理に必要な情報数を多くすることにより、情報の分散化が可能となり、セキュリティーを高めることが可能となる。
【０１６５】
なお、逆行列Ψ^{-1}は、サーバ２に保存（記録）しておくことが望ましい。線型変換を行う前の基底画像集合は、もともと端末３毎に異なった、端末３に依存する基底画像であるといえる。このため、線型変換された新しい基底画像集合および逆行列Ψ^{-1}の情報は端末３に依存するものである。従って、新しい基底画像集合を定期的にサーバ２から端末３に配信して端末３の画像記録部１２に記録させておくと共に、端末３に依存する逆行列Ψ^{-1}の情報は、サーバ２の端末情報記録部２２に記録させておくことが好ましい。
【０１６６】
また、サーバにおける負担を軽減するために、一般的な行列（逆行列Ψ^{-1}）ではなく、座標の回転と平行移動などを用いて逆行列Ψ^{-1}に該当する情報を設定することもできる。変換行列を座標の回転と平行移動により示す場合には、逆行列Ψ^{-1}をそのまま使う場合に比べて少ないパラメータ（例えば回転角度など）で同様の情報を表すことができ、データ量の低減を図ることが可能となる。
【０１６７】
［ホルダを特定するための情報等に基づく係数情報の決定処理］
次に、認証画像の生成処理に用いられる係数情報（Ｋｅｙ３）を、ホルダを特定するための情報やクレジットカード４がホルダの所有する本物（真正）のクレジットカードであることを特定するための情報（以下、ホルダ特定情報とする。：本発明に係るホルダを識別するための文字列情報Ｓ）に基づいて決定する場合について説明を行う。ホルダ特定情報とは、例えばクレジットカードのカード番号情報や社員証の社員番号情報などがその一例として該当する。
【０１６８】
上述したように、係数情報は、認証画像と基底画像との内積により求められる。しかしながら、係数情報は、このような内積により求められた値をそのまま利用するものには限定されず、ホルダ特定情報を用いてこの値を変形させて利用するものであってもよい。
【０１６９】
一般的に、ホルダ特定情報は、数字あるいは文字が複数組み合わされて構成されている。このホルダ情報の文字列（文字列情報）をＳとすると、文字列Ｓ（文字列情報Ｓ）を数列［u_1，u_2，・・・，u_r］に変換する関数（この関数を変換関数Ｆ（Ｓ）とする）を適切に定義することができれば、認証画像ｐは、次式のようにして生成することが可能となる。
【数１２】

$$p=\left[\frac{w_1 b_1}{u_1}\ \frac{w_2 b_2}{u_2}\cdots\frac{w_r b_r}{u_r}\right]\begin{bmatrix}u_1\\u_2\\\vdots\\u_r\end{bmatrix}\quad\cdots式１０$$

【０１７０】
ここで、式１０に示されるb_1，b_2，・・・，b_rは各基底画像を示している。従って

、認証画像ｐを生成するためには、文字列Ｓがわかればよい。例えば、一般的なクレジットカードには、ホルダ特定情報としてクレジットカード番号が示されている。従って、クレジットカード４の表面に示されるクレジットカード番号を文字列Ｓとして用いることにより、クレジットカード４の記録部９に係数情報そのものを記載する必要がなくなる。従って、記録部９として十分なデータ記録容量を持たないクレジットカード４はもちろんのこと、記録部９そのものが備えられていないカードであっても、カード表面などに番号等が記載されていれば、認証画像ｐを生成することが可能となる。

【０１７１】

例えば、文字列Ｓが「２４５３９９８７４４５３」で示されるような１２桁の文字列であり、認証画像ｐの生成処理に利用される基底画像の枚数ｒが「３」（ｒ＝３）である場合には、文字列Ｓを４桁の数字の集まりであると考えることにより、文字列Ｓを３組の数字の組み合わせとすることができる。３組の数字の組み合わせを正規化することにより、式１０に示した認証画像ｐの生成処理における係数情報として利用することができる。

【０１７２】

文字列Ｓ＝「２４５３９９８７４４５３」を変換関数Ｆ（Ｓ）に適用することにより、式１０に示される数列［u_1，u_2，・・・，u_r］に変換する場合の一例について説明する。

【０１７３】

まず、文字列Ｓを４桁の数字の組み合わせとして、x_1，x_2，x_3の３組の数字を求める。

x_1＝２４５３，x_2＝９９８７，x_3＝４４５３

そしてx_1，x_2，x_3の和をＳＵＭとして求める。

ＳＵＭ＝x_1＋x_2＋x_3＝１６８９３

【０１７４】

そして、求められたＳＵＭに示すx_1，x_2，x_3の割合を求めることにより、u_1，u_2，u_3の値を算出する。

u_1＝x_1／ＳＵＭ＝０．１４５２

u_2＝x_2／ＳＵＭ＝０．５９１２

u_3＝x_3／ＳＵＭ＝０．２６３６

従って、ホルダ特定情報の文字列Ｓに基づいてu_1，u_2，u_3を求めることが可能となる。このようにして求められる数列［u_1，u_2，・・・，u_r］を第２の係数情報という。

【０１７５】

文字列Ｓの各要素を２進数で表現することができれば、文字列Ｓの要素が、漢字であっても、ローマ字であっても、数字であっても、端末３の制御処理部１４およびサーバ２の制御部２１における処理判断においては同じように処理を行うことが可能である。従って文字列Ｓは、ホルダやホルダの所有物であることが特定可能な文字列であれば、どのような文字列（例えば、会員番号、電話番号、住所など）であってもよい。また、変換関数Ｆ（Ｓ）を実装するために様々な方法を利用することが可能であり、文字列Ｓを変換関数Ｆ（Ｓ）に適用することにより、数列［u_1，u_2，・・・，u_r］（第２の係数情報）を求めること（変換すること）ができる関数式であればどのようなものであってもよい。上述したようなx_1，x_2，x_3およびＳＵＭを求める関係式は、あくまでも一例にすぎない。

【０１７６】

また、式１０は、式１や式５に示した従来の認証画像ｐの生成に用いられる数式との違いにより、２種類の解釈の仕方が生じる。１つめは、基底画像b_1，b_2，・・・，b_rをスケーリングすることにより変化させたものとする解釈である。つまり、基底画像b_iにw_i／u_iを積算したもの（スケーリングしたもの）を新たな基底画像とする考え方である。この考え方の場合には、認証画像ｐを生成するための鍵情報の数は３つであるが、

（１）認証画像の生成処理に用いられる新たな基底画像集合（スケーリングされた新しい基底画像の集合）（Ｋｅｙ１）

（２）認証画像の生成処理に用いられるインデックス情報（Ｋｅｙ２）
（３）認証画像の生成処理に用いられる第２の係数情報（u_1，u_2，・・・，u_r）（Ｋｅｙ３）
の３種類となる。

【０１７７】
一方で、もう１つの解釈は、新しい鍵要素として

【数１３】

$$\left[\frac{w_1}{u_1}\frac{w_2}{u_2}\cdots\frac{w_r}{u_r}\right]$$

（以下、重み付けされた係数情報という）が加えられて、認証画像ｐの生成処理が行われると考える解釈である。［w_1，w_2，・・・，w_r］は、既に説明したように基底画像と認証画像との内積により求められた係数情報である。重み付けされた係数情報は、この係数情報のそれぞれの数値に対して、第２の係数情報の逆数［１／u_1，１／u_2，・・・，１／u_r］が積算されたものである。つまり、係数情報の係数列のそれぞれの数値に対して、第２の係数情報の逆数［１／u_1，１／u_2，・・・，１／u_r］の重み付けがなされたものとなる。

【０１７８】
このことから、認証画像ｐを生成するための鍵情報は、
（１）認証画像の生成処理に用いられる基底画像集合（Ｋｅｙ１）
（２）認証画像の生成処理に用いられるインデックス情報（Ｋｅｙ２）
（３）認証画像の生成処理に用いられる重み付けされた係数情報（Ｋｅｙ３）
（４）認証画像の生成処理に用いられる第２の係数情報（u_1，u_2，・・・，u_r）
の４種類となる。

【０１７９】
１つの認証画像ｐを生成するためには、複数枚の基底画像が必要となることから、異なる認証画像ｐの生成処理において、一部の基底画像を共通して使用する場合（基底画像のシェアリング）も考えられる。さらに、基底画像をスケーリングすると基底画像の自然さが損なわれるおそれがあるため、できるだけ基底画像そのものをスケーリングなどすることなくそのまま利用することが好ましい。従って、重み付けされた係数情報を新しい鍵情報として、認証画像ｐの生成処理に利用する考え方が好ましいと考える。

【０１８０】
なお、第２の係数情報は、ホルダ特定情報の文字列Ｓに基づいて求められる情報であり、ホルダに依存するため、クレジットカード４や端末３ではなく、サーバ２のホルダ情報記録部２４などに記録しておくことが好ましい。

【０１８１】
しかしながら、第２の係数情報は、変換関数Ｆ（Ｓ）に基づいて文字列Ｓにより算出される係数列である。従って、クレジットカード４に文字列Ｓだけを記録し、第２の係数情報をサーバ２のホルダ情報記録部２４に記録する場合には、サーバ２の制御部２１が、ネットワーク５を介して文字列Ｓを取得し、取得された文字列Ｓに基づいて第２の係数情報と重み付けされた係数情報とを算出することになる。このため、サーバ２には、変換関数Ｆ（Ｓ）が記録され、制御部２１が取得された文字列Ｓから変換関数Ｆ（Ｓ）を用いて第２の係数情報と重み付けされた係数情報とを算出する構成とすることができる。この点で、サーバ２の制御部２１は、本発明に係る第２係数情報算出手段および重み付け係数情報算出手段として機能することになる。

【０１８２】
また、サーバ２の制御部２１が、取得された文字列Ｓから変換関数Ｆ（Ｓ）を用いて第２の係数情報を算出する場合や、第２の係数情報そのものがサーバ２のホルダ情報記録部２４に記録される場合には、鍵情報の分散化を図るために、重み付けされた係数情報（Ｋ

ｅｙ３）をサーバ２以外の場所に記録させることが好ましい。このように、重み付けされた係数情報（Ｋｅｙ３）をサーバ２以外の場所に記録させる場合には、重み付けされた係数情報（Ｋｅｙ３）を、クレジットカード４の記録部９に記録させることも可能である。

【０１８３】

［多画像モーフィング法に基づく画像の生成処理と再構成処理］

上述した認証画像ｐを生成するために用いられる基底画像は、画像の特徴を基準とした高次元の分布状態から、主成分分析方法を用いてその分布状態をよく表現できる低次元の分布状態を示し得る画像であり、必ずしも「自然な」画像ではない。この不自然さから基底画像集合は、悪意のある第三者から攻撃の対象となるおそれがある。このため、基底画像そのものに暗号化を施したり、端末依存性を付与したりすることにより、第三者からの攻撃に対する対応を図っているが、万が一のことを考えて攻撃の対象にならないように、基底画像を「自然な」画像とすることが望まれている。基底画像を自然化する処理は、一種のステガノグラフィーにより解決することができる。このような基底画像の自然化処理を目的として、多画像モーフィング（MIBM: Multiple Image Based Morphing）法を用いることができる。

【０１８４】

多画像モーフィング法とは、複数の自然画像（原画像）をモーフィング処理により求める目標画像の特徴ベクトルと同じ特徴ベクトルを備えた変形画像へと変形処理（ワーピング処理）し、変形された全ての変形画像を、予め原画像毎に設定された貢献度に応じて合成することにより、違和感のない自然な画像からなる目標画像を生成する方法である。

【０１８５】

このような多画像モーフィング法を利用する場合には、各変形画像を基底画像の代わりに用い、貢献度を係数情報の代わりに用いることにより、目標画像(認証画像)を生成することが可能となる。変形画像は、自然画像をワーピング処理により変形させた不自然な画像であるから、それらを直接に基底画像集合Ωに保存しない。基底画像集合Ωに保存するのは、変形する前の自然画像である。認証画像を生成する際に、これらの自然画像を変形してから使用すればよい。多画像モーフィング技術については、特願２０１１－０２４３３３号に詳細に記載されている。

【０１８６】

多画像モーフィング法を用いることによって、例えばｒ枚の自然画像I_1，I_2，・・・，I_rから自然画像Ｉを生成することが可能となる。また、この多画像モーフィング法を応用すること（逆モーフィング法を用いること）によって、ｒ枚の自然画像I_1，I_2，・・・，I_rのうちのｒ－１枚のいずれかの自然画像と自然画像Ｉとに基づいて、残りの自然画像を再構成することが可能である。例えば、自然画像Ｉと自然画像I_2，I_3，・・・，I_rとに基づいて、自然画像I_1を求めることができる。

【０１８７】

図６は、自然画像Ｉと自然画像I_2，I_3，・・・，I_rとに基づいて、自然画像I_1を求める逆モーフィング処理を示したフローチャートである。本実施の形態に係るホルダ認証システム１では、端末３の制御処理部１４が、画像記録部１２に記録される自然画像（基底画像）に基づいて逆モーフィング処理を行う。

【０１８８】

まず、制御処理部１４は、自然画像Ｉの特徴ベクトルＦと、自然画像I_iの特徴ベクトルF_i（但しｉ＝２，３，・・・ｒ）と、自然画像I_iとに基づいて、下記の式１１に示すように変形画像$I^{w}{}_i$を求める。ここで制御処理部１４は、自然画像I_iの特徴ベクトルF_i（但しｉ＝２，３，・・・ｒ）が、自然画像Ｉの特徴ベクトルＦと一致するように、自然画像I_iを変形処理することによって、自然画像I_iの全てを変形画像$I^{w}{}_i$に変形させる。つまり、制御処理部１４は、自然画像I_1を復元するために必要な画像を全て変形画像に変形する処理を行う（ステップＳ．４１）。この処理において、制御処理部１４は、本発明に係る変形画像生成手段に該当する処理を行うことになる。

【数１４】

$$I_i^W = warping(I_i, F_i, F), i = 2,3,..., r \quad \cdots式１１$$

式１１において関数warping（Ｉ$_i$，Ｆ$_i$，Ｆ）は、自然画像Ｉ$_i$と、特徴ベクトルＦ，Ｆ$_i$（ｉ＝２，３，・・・ｒ）とに基づいて変形画像Ｉ$^w{}_i$を生成する関数を示している。

【０１８９】

次に、制御処理部１４は、自然画像Ｉの特徴ベクトルＦと、自然画像Ｉ$_i$の特徴ベクトルＦ$_i$（ｉ＝２，３，・・・ｒ）とに基づいて、下記の式１２に示すように、自然画像Ｉ$_1$の特徴ベクトルＦ$_1$を求める。つまり、復元対象となる自然画像Ｉ$_1$の特徴ベクトルＦ$_1$を求める処理を行う（ステップＳ．４２）。

【数１５】

$$F_1 = (F - \sum_{i=2}^{r} w_i F_i)/w_1 \quad \cdots式１２$$

但し、ｗ$_1$，ｗ$_2$，・・・，ｗ$_r$は、自然画像Ｉを求めるときに使用される各自然画像の貢献度（合成係数と見なされる数）である。

【０１９０】

この処理で制御処理部１４は、自然画像Ｉ$_i$の特徴ベクトルＦ$_i$（ｉ＝２，３，・・・ｒ）に対して、自然画像Ｉ$_i$の貢献度ｗ$_i$の値を元に、線型結合をし、その結果を、自然画像Ｉの特徴ベクトルＦから減算し、減算された特徴ベクトルを自然画像Ｉ$_1$の貢献度ｗ$_1$の値で除算することにより、自然画像Ｉ$_1$の特徴ベクトルＦ$_1$を算出する。この処理において、制御処理部１４は、本発明に係る認証画像特徴ベクトル算出手段に該当する処理を行うことになる。

【０１９１】

そして、制御処理部１４は、上述した処理により求められた、変形画像Ｉ$^w{}_i$（ｉ＝２，３，・・・ｒ）と、貢献度ｗ$_i$（ｉ＝２，３，・・・ｒ）と、自然画像Ｉとを利用して、式１３に示すように、変形画像Ｉ$^w{}_1$を求める。つまり、復元対象である自然画像Ｉ$_1$の変形画像Ｉ$^w{}_1$を求める処理を行う（ステップＳ．４３）。

【数１６】

$$I_1^W = (I - \sum_{i=2}^{r} w_i I_i^W)/w_1 \quad \cdots式１３$$

【０１９２】

この処理で制御処理部１４は、自然画像Ｉ$_i$の変形画像Ｉ$^w{}_i$に対して、自然画像Ｉ$_i$の貢献度ｗ$_i$の値を元に、線型結合し、その結果を、自然画像Ｉから減算し、減算された画像を自然画像Ｉ$_1$の貢献度ｗ$_1$の値で除算することにより、自然画像Ｉ$_1$の変形画像Ｉ$^w{}_1$を算出する。この処理において、制御処理部１４は、本発明に係る認証変形画像算出手段に該当することになる。

【０１９３】

最後に、制御処理部１４は、上述した関数warpingを利用して、復元対象である自然画像Ｉ$_1$を、式１４に示すようにして求めて（ステップＳ．４４）処理を終了する。

【数１７】

$$I_1 = warping(I_1^W, F, F_1) \quad \cdots式１４$$

【０１９４】

この処理で制御処理部１４は、自然画像Ｉの特徴ベクトルＦが、自然画像Ｉ$_1$の特徴ベ

クトルF_1と一致するように、変形画像$I^{w}{}_1$にモーフィング処理を施すことによって、変形画像$I^{w}{}_1$を自然画像I_1に変形させる。この処理において、制御処理部１４は、本発明に係る認証画像モーフィング生成手段に該当することになる。

【０１９５】

上述した多画像の逆モーフィング技術（法）を利用して、自然画像I_1を認証画像とし、自然画像Ｉと自然画像I_2，I_3，・・・，I_rとを基底画像集合とすると、認証画像を生成するために必要な鍵情報を、

（１）認証画像の生成処理に用いられる基底画像集合（自然画像Ｉと自然画像I_2，I_3，・・・，I_r：Ｋｅｙ１）

（２）認証画像の生成処理に用いられるインデックス情報（Ｋｅｙ２）

（３）認証画像の生成処理に用いられる貢献度（合成係数w_1，w_2，・・・，w_r：Ｋｅｙ３）

（４）各基底画像における特徴ベクトル（Ｆ，F_2，・・・，F_r：Ｋｅｙ４）

の４種類で示すことが可能となる。

【０１９６】

この４種類の鍵情報を用いることにより、基底画像集合を構成する基底画像を自然画像とすることができるため、ホルダ認証システム１における認証画像の生成処理のセキュリティーを高めることが可能となる。

【０１９７】

具体的に、認証画像の生成処理に、上述した多画像の逆モーフィング法を用いる場合には、自然画像（自然な画像あるいは自然に見える画像を意味する）を複数枚（例えばＬ枚）用意して、基底画像集合Ωを構成する基底画像として端末３の画像記録部１２に記録しておく。端末３の制御処理部１４は、任意の認証画像ｐに対して基底画像集合Ωからｒ－１枚の自然画像b_1，b_2，・・・，b_{r-1}（但し、ｒ＜Ｌ）を任意に選択し、認証画像ｐとｒ－１枚の自然画像b_1，b_2，・・・，b_{r-1}とを利用して、変形画像Ｉを作成する。この変形画像Ｉは自然画像となる。そして、作成された変形画像Ｉだけを基底画像集合Ωに追加すれば、変形画像Ｉとｒ－１枚の自然画像b_1，b_2，・・・，b_{r-1}とを利用して、認証画像ｐを生成することができる。

【０１９８】

従って、多画像の逆モーフィング法を利用することによって、基底画像集合Ωを構成する画像を自然画像にすることができるだけでなく、基底画像集合Ωのデータ量を抑制することが可能となる。基底画像集合Ωの画像数は、はじめの自然画像Ｌ枚に対して変形画像が加えられた合計の枚数となる（但し、自然画像の枚数Ｌは変形画像の枚数よりも遙かに少ない枚数となる）ため、少ない基底画像集合のデータ量により効率的に認証画像を生成することが可能となる。ただし、この方法を用いる場合には、認証画像を復元するために必要とされる計算量が多少増加してしまう傾向がある。

【０１９９】

なお、認証画像を生成するために用いられる各基底画像の特徴ベクトル（Ｋｅｙ４）は、数十バイト～数百バイト程度のデータ量にしかならないため、クレジットカード４の記録部９に記録させることができ、またサーバ２に記録させた場合であっても、データの通信負担が増加されることがない。

【０２００】

［基底画像の圧縮処理］

上述したが多画像の逆モーフィング法を用いる場合に、認証画像の生成に用いられる基底画像集合の基底画像数を低減させることが可能であるが、それ以外の方法を用いる場合には、１枚の認証画像を生成するために複数枚（既に説明した基底画像集ではｒ枚、このｒ枚は、認証画像毎に変更することも可能であるが、説明の便宜上ここでは一律にｒ枚必要であるとする）の基底画像が必要となる。

【０２０１】

従って、本実施の形態に係るホルダ認証システム１を利用するユーザ（ホルダ）がＭ人

いるとすると、それぞれのユーザがクレジットカード４のホルダであるか否かの認証に用いる認証画像もＭ枚生成する必要が生ずる。単純に１枚の認証画像にｒ枚の基底画像が必要とすれば、Ｍ枚の認証画像を生成するためには、Ｍ枚の認証画像×ｒ枚の基底画像でＮ枚（＝Ｍ×ｒ）となり、基底画像集合のデータ量が非常に大きくなってしまう。

【０２０２】

基底画像集合のデータ量が大きい場合、端末３にＬＡＮ等で接続されたローカルサーバが存在し、ローカルサーバの記録手段に記録された基底画像集合を各端末３で共通して利用する場合には、データ量の増大を吸収することもできるが、システム全体のポータビリティが損なわれるおそれがあった。このため、基底画像そのものの圧縮を図ることにより基底画像集合のデータ量低減が求められている。基底画像を圧縮するために、既存の画像圧縮技術を利用することもできるが、より効率的な方法を用いることもできる。

【０２０３】

まず、任意のＭ枚の認証画像を一つのグループにまとめる。そして、認証画像を生成するr枚の基底画像を求めて、認証画像の生成に用いられる基底画像を、Ｍ枚の認証画像間で共通の基底画像によりシェアリングすることで、認証画像の生成に必要な基底画像の数をＮ（=ｒ×Ｍ）枚ではなく、Ｍ枚（ただし、ｒ＜Ｍ）とすることができる。もちろん、認証画像の生成に用いられる基底画像の枚数rは、認証画像毎に固定であってもよく、また可変でもよい。

【０２０４】

さらに、Ｍ枚の認証画像を生成するために必要な基底画像を求める場合に、主成分分析（ＰＣＡ：Principal Component Analysis）方法を用いてデータ量の低減を図ったうえで、認証画像の生成処理を行う方法を採用することもできる。主成分分析法を利用する場合には、ｒ－１枚の基底画像（Eigen-faceともいう）と一枚の平均画像（Mean Face）とが求められる。なお、ｒの数が小さいときには、平均画像から元の画像を推定することが可能となるので、主成分分析法をあまり勧められない。また、他の方法を用いることによりデータ量の低減を図ることも可能である。

【０２０５】

また、上述した多画像の逆モーフィング技術を用いる場合には、基底画像数をおよそＭ枚（厳密にはＭ＋α枚）となるので、基底画像を認証画像においてシェアリングする方法を使用する必要性は低い。また、多画像の逆モーフィング技術を用いる場合には、基底画像として自然画像を用いることができるので、基底画像の画素間の相関性が高く、従来の画像圧縮方法（例えばＪＰＥＧなど）を利用することによってデータ量を大幅に減らすことができる。

【０２０６】

［認証画像の種類について］

本実施の形態に係るホルダ認証システム１の説明においては、認証画像として、通常、写真（２次元画像でもあっても、３次元画像であってもよい）を用いた場合を想定して説明を行った。しかしながら、オペレータによる目視の認証処理ではなく、機械的な認証（以下、自動認証という）が可能な場合（つまり、自動認証を行う装置などが設けられている場合）には、必ずしも認証に用いるデータを認証画像として視認可能な画像にする必要がない。このため、パスワード、サイン、指紋、静脈パターンなどを認証画像に該当する認証データ（認証情報）として用いることができる。

【０２０７】

即ち、クレジットカード４などを使用する使用者が真正のホルダであるかを判断するための認証データ（認証情報）として、画像データに限らず、どんな「データ」であっても利用することが可能である。このような場合、認証データ（認証情報）の生成に用いられる情報（基底ベクトル）は、既に説明した基底画像とまったく同じようにして求めることができる。但し、生成された認証データ（認証情報）を認証するためには、人の目ではなく、機械による自動認証となる。ここで重要なのは、認証データ（認証情報）がクレジットカード４などに保存されていないことである。従って、第三者は認証データ（認証情報

）をクレジットカード４などから解読したり、真似したり、改ざんしたりすることができない。

【０２０８】

また、認証データに基づいて使用者の認証を行うための別の方法として、オンラインで使用者の認証データ（認証情報）を取得する必要がある。認証過程はおよそ以下の通りとなる

ステップ１：　使用者の認証データ（認証情報）を取得する。

ステップ２：　ホルダの認証データ（認証情報）を生成する。

ステップ３：　以上の２つステップにより得られたそれぞれの認証データ（認証情報）を照合する。

【０２０９】

例えば、カードに指紋検出手段（例えば、エプソンの薄型指紋センサー（日本経済新聞夕刊（２００６年７月２４日発行）参照））が設けられている場合に、使用者がカードを使用するときには、その指紋がオンラインで読み取られ、端末に送られる。端末３は、クレジットカード４、端末３、サーバ２からの情報に基づき、ホルダの指紋情報を生成すれば、カードの使用者の指紋とホルダの指紋とを照合することによってホルダの認証を行うことができる。この場合には、オペレータの「目視」による認証は必要がない。

【０２１０】

従来、ホルダの指紋情報はカードの中に保存されるので、その情報が一旦解読されれば、第三者がそれを自分のものに置き換えることができる。第三者が指紋の置き換えがなされたカードを使用する場合には、オンラインで読み取った指紋とカードにある指紋とは一致するので、指紋がオンラインで読み取られても困らない。実際、ＩＣカードに記録される情報を暗号化しても数分で解読可能であることが、ドイツのハッカーグループによって実証されている（２００８年）。従って、上述したエプソンの指紋センサーのみでは不正使用を防ぐことができない。

【０２１１】

本実施の形態に係るホルダ認証システム１の認証画像を認証データとして用いることにより、ホルダの指紋情報をクレジットカード４に保存する必要がなく、ホルダの指紋情報がクレジットカード４を合法的に使用するときだけ生成することが可能となる。従って、本実施の形態に係るホルダ認証システム１の構成と、上述したエプソンの指紋センサーなどの既存技術と併用することによって、はじめて真正の使用者（ホルダ）を保護することができる。

【０２１２】

なお、上述した指紋情報とは、指紋を示す画像そのものであってもよいし、指紋の「特徴ベクトル」であってもよい。後者の場合、基底ベクトル集合のデータ量は小さく、より実装しやすいという利点が存在する。もちろん、指紋だけではなく、他の生体情報も使用することができる。例えば、カメラを用いることにより、画像の自動認証を行うことが可能である。タブレット状の情報端末などを利用することにより、サインに基づくオンライン自動認証を行うこともできる。このような方法を用いることにより、ＡＴＭ（自動現金預払機）などにおいて、人間のオペレータがいなくても、高い認証精度でホルダの確認を行うことが可能となる。

【０２１３】

以上、本発明に係るホルダ認証システムの一例としてホルダ認証システム１を示し、図面を用いて詳細に説明したが、本発明に係るホルダ認証システムは上述した実施の形態に記載した内容に限定されるものではない。いわゆる当業者であれば、特許請求の範囲に記載された範疇内において、各種の変更例または修正例に想到し得ることは明らかであり、それらについても当然に本発明の技術的範囲に属するものと了解される。

【０２１４】

例えば、本実施の形態に係るホルダ認証システム１では、サーバ２の制御部２１が、認証画像（ホルダを認証するための画像）と任意の複数の画像とに基づいて複数の基底画像

を生成する処理を行う場合について説明を行った。しかしながら、認証画像と任意の複数の画像とに基づいて複数の基底画像を生成する処理は、必ずしもサーバ２の制御部２１において行われる構成には限定されない。例えば、サーバ２、端末３とは異なる手段として、認証画像と任意の複数の画像とに基づいて複数の基底画像を生成する基底画像生成装置を設けて、この基底画像生成装置において生成された基底画像が、サーバ２の基底画像記録部２３に記録され、生成された係数情報が、サーバ２のホルダ情報記録部２４やクレジットカード４の記録部９などに記録される構成とすることも可能である。

【０２１５】

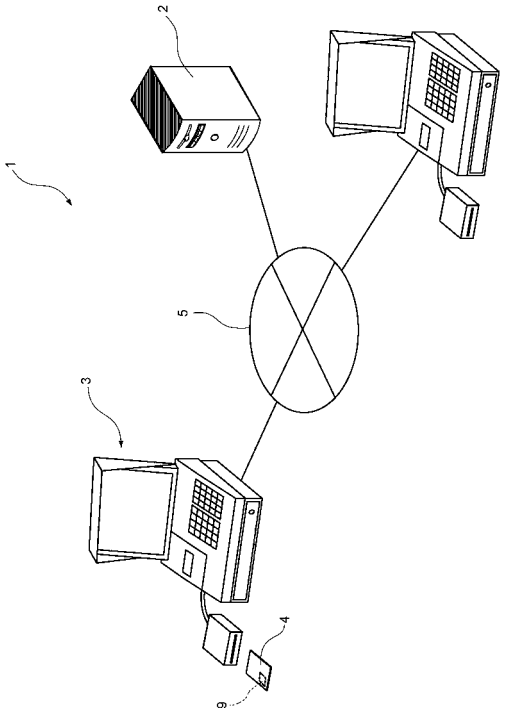
また、本実施の形態に係るホルダ認証システム１では、端末３とサーバ２とが、クライアント－サーバ方式で接続される構成について説明を行ったが、端末３とサーバ２との接続方式は、必ずしもクライアント－サーバ方式には限定されず、いわゆるPeer to Peer（ピアトゥピア）方式により接続されるものであってもよい。サーバ２は、ネットワークを介して端末３に接続され、端末３において認証画像の生成に必要な鍵情報を記録するものであればよい。例えば、サーバ２が他の端末３として機能し、一の端末３が、他の端末３の鍵情報を所有して、必要に応じてネットワークを介して互いに鍵情報の送受信を行う構成にすることによって、各端末３で認証画像の生成処理に必要な鍵情報を分散させることができる。ネットワークに接続される端末３の数が増えれば増えるほど、鍵情報をより広範囲に分散させることが可能となる。

【符号の説明】

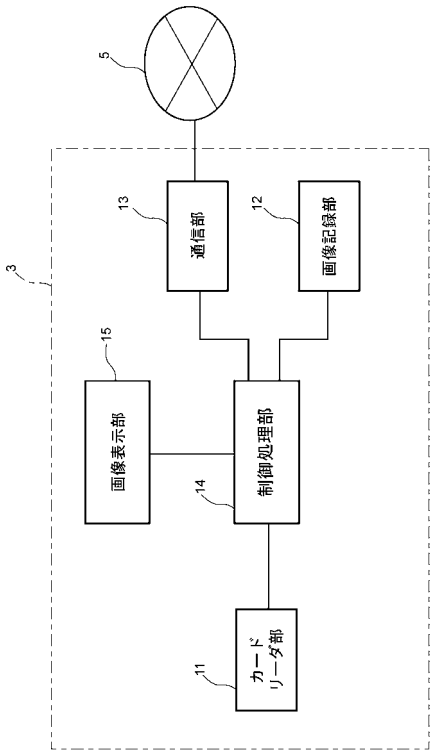
【０２１６】

１　…ホルダ認証システム
２　…サーバ（ホルダ認証サーバ、基底画像生成装置）
３　…端末（ホルダ認証端末）
４　…クレジットカード（ホルダであることの認証に利用される記録媒体）
５　…ネットワーク
９　…（クレジットカードの）記録部（情報記録手段）
１１　…（端末の）カードリーダ部（データ取得手段）
１２　…（端末の）画像記録部（端末記録手段）
１３　…（端末の）通信部（データ通信手段）
１４　…（端末の）制御処理部（基底画像特定手段、認証画像生成手段、変形画像生成手段、認証画像特徴ベクトル算出手段、認証変形画像算出手段、認証画像モーフィング生成手段）
１５　…（端末の）画像表示部
２０　…（サーバの）通信部（サーバ通信手段）
２１　…（サーバの）制御部（第２係数情報算出手段、重み付け係数情報算出手段、基底画像生成手段、係数情報算出手段、第２インデックス情報算出手段）
２２　…（サーバの）端末情報記録部（サーバ記録手段）
２３　…（サーバの）基底画像記録部（サーバ記録手段、画像記録手段）
２４　…（サーバの）ホルダ情報記録部（サーバ記録手段）

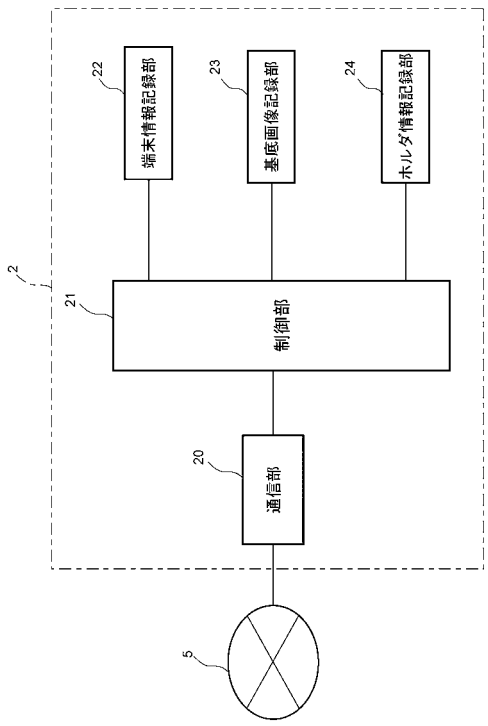
【図１】


1
2
3
4
5
9

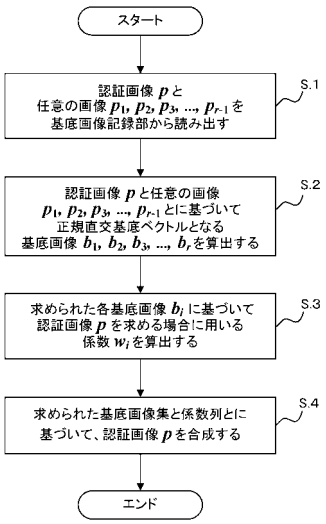
【図２】


5
3
13
通信部
12
画像記録部
15
画像表示部
制御処理部
14
11
カード
リーダ部

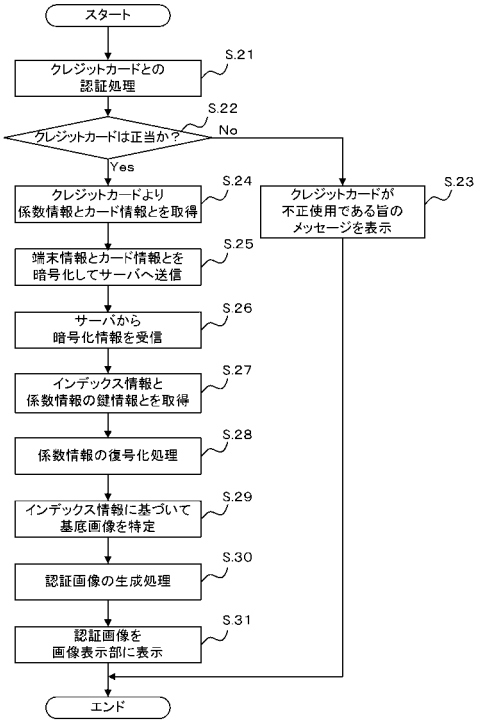
【図３】


22
端末情報記録部
23
基底画像記録部
24
ホルダ情報記録部
2
21
制御部
20
通信部
5

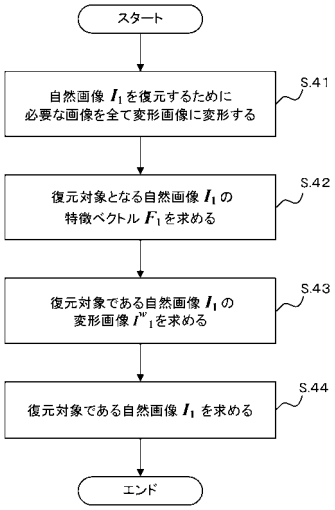
【図４】


スタート
認証画像 p と
任意の画像 $p_1, p_2, p_3, \ldots, p_{r-1}$ を
基底画像記録部から読み出す
S.1
認証画像 p と任意の画像
$p_1, p_2, p_3, \ldots, p_{r-1}$ とに基づいて
正規直交基底ベクトルとなる
基底画像 $b_1, b_2, b_3, \ldots, b_r$ を算出する
S.2
求められた各基底画像 b_i に基づいて
認証画像 p を求める場合に用いる
係数 w_i を算出する
S.3
求められた基底画像集と係数列とに
基づいて、認証画像 p を合成する
S.4
エンド

【図５】


スタート
クレジットカードとの
認証処理
S.21
クレジットカードは正当か？
S.22
No
Yes
クレジットカードより
係数情報とカード情報とを取得
S.24
クレジットカードが
不正使用である旨の
メッセージを表示
S.23
端末情報とカード情報とを
暗号化してサーバへ送信
S.25
サーバから
暗号化情報を受信
S.26
インデックス情報と
係数情報の鍵情報とを取得
S.27
係数情報の復号化処理
S.28
インデックス情報に基づいて
基底画像を特定
S.29
認証画像の生成処理
S.30
認証画像を
画像表示部に表示
S.31
エンド

【図６】


スタート
自然画像 I_1 を復元するために
必要な画像を全て変形画像に変形する
S.41
復元対象となる自然画像 I_1 の
特徴ベクトル F_1 を求める
S.42
復元対象である自然画像 I_1 の
変形画像 $I^w{}_1$ を求める
S.43
復元対象である自然画像 I_1 を求める
S.44
エンド

フロントページの続き

Ｆターム(参考) 5B285 AA01 AA04 BA01 BA08 CA42 CA43 CB02 CB06 CB07 CB14
CB15 CB16 CB24 CB44 CB52 CB55 CB56 CB62 CB63 CB64
CB73 CB74 CB75 CB76 DA05 DA08
5J104 AA07 AA16 AA32 EA04 EA19 JA21 KA01 KA16 NA02 NA33
NA37 NA38 PA07