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

特許第4114032号
(P4114032)

(45)発行日　平成20年7月9日(2008.7.9)　(24)登録日　平成20年4月25日(2008.4.25)

(51)Int.Cl.		F I		
H04L 9/32	(2006.01)	H04L	9/00	675B
G06K 19/10	(2006.01)	G06K	19/00	S
B42D 15/10	(2006.01)	H04L	9/00	673A
G06Q 10/00	(2006.01)	H04L	9/00	673C
G06K 17/00	(2006.01)	B42D	15/10	501L

請求項の数 3　(全 20 頁)　最終頁に続く

(21)出願番号　特願2000-292500 (P2000-292500)
(22)出願日　平成12年9月26日 (2000.9.26)
(65)公開番号　特開2002-101092 (P2002-101092A)
(43)公開日　平成14年4月5日 (2002.4.5)
審査請求日　平成17年1月5日 (2005.1.5)

(73)特許権者　000002369
セイコーエプソン株式会社
東京都新宿区西新宿２丁目４番１号
(74)代理人　100096703
弁理士　横井　俊之
(72)発明者　下里　秀人
長野県諏訪市大和３丁目３番５号　セイコーエプソン株式会社内
(72)発明者　牛山　祐一
長野県諏訪市大和３丁目３番５号　セイコーエプソン株式会社内
(72)発明者　最上　和人
長野県諏訪市大和３丁目３番５号　セイコーエプソン株式会社内

最終頁に続く

(54)【発明の名称】個人認証装置

(57)【特許請求の範囲】

【請求項１】

固有の画像データと情報データとを記憶するに際して、認証局にて固有の識別記号に対応させて管理される互いに対となる秘密鍵と公開鍵を二組利用し、一方の組の秘密鍵によって上記画像データと上記情報データとを暗号化した第一の暗号化データと、他方の組の秘密鍵によって同情報データと上記第一の暗号化データの改ざんを検出するための改ざん防止パラメータとを暗号化した第二の暗号化データとを記憶するＩＣカードから上記第一及び第二の暗号化データを読み取る読取手段と、

それぞれの組の識別記号を利用して上記認証局から上記公開鍵を取得するとともに、上記第一の暗号化データを対応する公開鍵で復号し上記情報データを抽出し、上記第二の暗号データを対応する公開鍵で復号し上記情報データと上記改ざん防止パラメータとを抽出し、抽出された上記改ざん防止パラメータを使用して上記第一の暗号化データに対する改ざんの有無を検出し、上記第一の暗号化データに対して改ざんが行なわれていない場合は、抽出されたそれぞれの情報データを突き合わせてデータの整合性を照合する復号照合手段と、

上記画像データを利用した本人認証の結果を取得する画像確認手段と、

データの整合性について照合した結果と本人認証の結果とを利用して個人認証を許可する許可手段とを具備することを特徴とする個人認証装置。

【請求項２】

上記請求項１に記載の個人認証装置において、

上記記憶媒体に記憶されたデータについては、一方の組の識別記号を他方の組の秘密鍵で暗号化してあり、
上記復号照合手段は、一方の組の識別記号にて上記認証局から上記公開鍵を取得し、
同公開鍵にて上記識別記号を暗号化したデータを復号し、
復号した識別記号にて上記認証局から上記公開鍵を取得して同公開鍵にて他方のデータを復号することを特徴とする個人認証装置。
【請求項３】
上記請求項１又は請求項２のいずれかに記載の個人認証装置において、
上記画像データは、人間の身体の画像を撮影したものであることを特徴とする個人認証装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、個人認証装置に関する。
【０００２】
【従来の技術】
近年、電子決済についての安全性を高めるため、各種の技術が考えられているが、これらはクレジットカードの決済データを改ざんされることなく信販会社に通知することを目的とするものである。
一方、クレジットカードの所持者が本当の所有者であるか否かは別問題である。すなわち、決済データが改ざんされないようにしても、現実のクレジットカードの所持者が本当の所有者でなければ意味はない。そして、従来は、クレジットカードの所持者が本当の所有者であるか否かはクレジットカードの裏面にされたサインと、伝票にされるサインの筆跡が一致するか否かで判断している。また、クレジットカードに本人の写真を刷り込んでおき、顔写真と所持者とを照合して一致するか否かを判断することも行われている。
【０００３】
【発明が解決しようとする課題】
上述した従来のクレジットカードでは、サインの筆跡を真似る練習をしてしまうと、クレジットカードの所持者を本当の所有者と区別できないという課題があった。
一方、写真は一見するとクレジットカードの所持者と本当の所有者とを区別できるようにも思われるが、もともと顔写真を入れ替えたクレジットカードを用意し、同じ磁気信号を書き込んでしまうことは困難ではない。
【０００４】
本発明は、上記課題にかんがみてなされたもので、電子決済などの前提として本人確認の安全性を高めることが可能な個人認証装置の提供を目的とする。
【０００５】
【課題を解決するための手段】
上記目的を達成するため、請求項１にかかる発明は、固有の画像データと情報データとを記憶するに際して、認証局にて固有の識別記号に対応させて管理される互いに対となる秘密鍵と公開鍵を二組利用し、一方の組の秘密鍵によって上記画像データと上記情報データとを暗号化した第一の暗号化データと、他方の組の秘密鍵によって同情報データと上記第一の暗号化データの改ざんを検出するための改ざん防止パラメータとを暗号化した第二の暗号化データとを記憶するＩＣカードから上記第一及び第二の暗号化データを読み取る読取手段と、それぞれの組の識別記号を利用して上記認証局から上記公開鍵を取得するとともに、上記第一の暗号化データを対応する公開鍵で復号し上記情報データを抽出し、上記第二の暗号データを対応する公開鍵で復号し上記情報データと上記改ざん防止パラメータとを抽出し、抽出された上記改ざん防止パラメータを使用して上記第一の暗号化データに対する改ざんの有無を検出し、上記第一の暗号化データに対して改ざんが行なわれていない場合は、抽出されたそれぞれの情報データを突き合わせてデータの整合性を照合する復号照合手段と、上記画像データを利用した本人認証の結果を取得する画像確認手段と、

データの整合性について照合した結果と本人認証の結果とを利用して個人認証を許可する許可手段とを具備する構成としてある。

【０００６】

上記のように構成した請求項１にかかる発明においては、記憶媒体に固有の画像データと固有の情報データとを記憶させておく。この際、単に記憶するのではなく、認証局にて固有の識別記号に対応させて管理される互いに対となる秘密鍵と公開鍵を二組利用し、一方の組の秘密鍵による暗号化と他方の組の秘密鍵による暗号化とを行ったデータをそれぞれ記憶している。従って、それぞれを復号化する際には秘密鍵と対になる公開鍵が必要であり、それらは識別記号に基づいて認証局から取得可能である。

【０００７】

一方、個人認証装置では、読取手段が上記記憶媒体から上記データを読み取る。また、復号照合手段はそれぞれの組の識別記号を利用して上記認証局から上記公開鍵を取得するとともに同公開鍵にて対応するデータを復号し、データの整合性を照合する。ここでは個別の公開鍵がないと暗号化されたデータを復号できない。そして、両者を復号できて初めて照合が可能となる。照合できなければ何らかの改ざんあるいは不正な利用と推測できる。また、画像確認手段では上記画像データを利用して本人認証を促し、その結果を取得する。そして、データの整合性について照合した結果と本人認証の結果とが得られた場合にだけ個人認証が確認できたものとして許可手段が許可を行なう。

【０００８】

このように、二組の秘密鍵と公開鍵とを利用することにより、安全性を向上させる手法は必ずしも個人認証装置においてのみ実現しうるものではなく、そのデータを記憶した記憶媒体としても実現可能である。このため、本発明は、固有の画像データと固有の情報データとを記憶するに際して、認証局にて固有の識別記号に対応させて管理される互いに対となる秘密鍵と公開鍵を二組利用し、一方の組の秘密鍵による暗号化と他方の組の秘密鍵による暗号化とを行ったデータを記憶する構成としてもよい。

【０００９】

従って、両者が対となって利用されるものとして、本発明は、固有の識別記号に対応させて互いに対となる秘密鍵と公開鍵とが認証局にて管理され、記憶媒体に画像データと情報データとを暗号化して記憶させる登録端末と、同記憶媒体から暗号化されたデータを取得し、同画像データと同情報データとを復号してデータの整合性を判断する個人認証端末とからなる個人認証システムであって、登録端末では、記憶媒体の所有者の身体を撮影した画像データを取得するとともに、同所有者に固有の情報データを取得し、当該所有者の秘密鍵と登録者の秘密鍵で別個に暗号化して上記所有者の記憶媒体に記憶させ、個人認証端末では、上記所有者と上記登録者の識別記号にて上記認証局からそれぞれの公開鍵を取得して上記暗号化したデータを復号するとともに、それぞれ復号化した上記情報データを照合し、上記画像データから画像を表示して認証操作を受け付ける構成としてもよい。

【００１０】

また、以上のような手法は必ずしも実体のある装置に限られる必要はなく、その方法としても機能することは容易に理解できる。このため、本発明は、固有の識別記号に対応させて互いに対となる秘密鍵と公開鍵とが認証局にて管理され、記憶媒体に画像データと情報データとを暗号化して記憶させる登録側と、同記憶媒体から暗号化されたデータを取得し、同画像データと同情報データとを復号してデータの整合性を判断する個人認証側とで実行する個人認証方法であって、登録側では、記憶媒体の所有者の身体を撮影した画像データを取得するとともに、同所有者に固有の情報データを取得し、当該所有者の秘密鍵と登録者の秘密鍵で別個に暗号化して上記所有者の記憶媒体に記憶させ、個人認証側では、上記所有者と上記登録者の識別記号にて上記認証局からそれぞれの公開鍵を取得して上記暗号化したデータを復号するとともに、それぞれ復号化した上記情報データを照合し、上記画像データから画像を表示して認証操作を受け付ける構成としてもよい。

【００１１】

すなわち、必ずしも実体のある装置に限らず、その方法としても有効であることに相違は

ない。
ところで、このような個人認証装置は単独で存在する場合もあるし、ある機器に組み込まれた状態で利用されることもあるなど、発明の思想としてはこれに限らず、各種の態様を含むものである。従って、ソフトウェアであったりハードウェアであったりするなど、適宜、変更可能である。
発明の思想の具現化例として個人認証方法を実現するソフトウェアとなる場合には、かかるソフトウェアを記録した記録媒体上においても当然に存在し、利用されるといわざるをえない。
【００１２】
その一例として、本発明は、固有の識別記号に対応させて互いに対となる秘密鍵と公開鍵とが認証局にて管理され、記憶媒体に画像データと情報データとを暗号化して記憶させる登録端末側プログラムと、同記憶媒体から暗号化されたデータを取得し、同画像データと同情報データとを復号してデータの整合性を判断する個人認証端末側プログラムをそれぞれのコンピュータにて実行させる個人認証プログラムを記憶した媒体であって、登録端末側プログラムでは、記憶媒体の所有者の身体を撮影した画像データを取得するとともに、同所有者に固有の情報データを取得する機能と、当該所有者の秘密鍵と登録者の秘密鍵で別個に暗号化して上記所有者の記憶媒体に記憶させる機能とを備え、個人認証端末側プログラムでは、上記所有者と上記登録者の識別記号にて上記認証局からそれぞれの公開鍵を取得して上記暗号化したデータを復号するとともに、それぞれ復号化した上記情報データを照合する機能と、上記画像データから画像を表示して認証操作を受け付ける機能とを実行させる構成としてもよい。
【００１３】
むろん、その記録媒体は、磁気記録媒体であってもよいし光磁気記録媒体であってもよいし、今後開発されるいかなる記録媒体においても全く同様に考えることができる。また、一次複製品、二次複製品などの複製段階については全く問う余地無く同等である。
さらに、一部がソフトウェアであって、一部がハードウェアで実現されている場合においても発明の思想において全く異なるものではなく、一部を記録媒体上に記憶しておいて必要に応じて適宜読み込まれるような形態のものとしてあってもよい。
【００１４】
本発明をソフトウェアで実現する場合、ハードウェアやオペレーティングシステムを利用する構成とすることも可能であるし、これらと切り離して実現することもできる。そして、実際にはオペレーティングシステムの介在のもとで実現するとしても、プログラムが媒体に記録されて流通される過程においては、このプログラムだけで本発明を実施できるものと理解することができる。
【００１５】
また、本発明をソフトウェアで実施する場合、発明がプログラムを記録した媒体として実現されるのみならず、本発明がプログラム自体として実現されるのは当然であり、プログラム自体も本発明に含まれる。
二組の秘密鍵と公開鍵を利用して安全性を高めるためには、各種の変形例が可能である。その一例として、請求項２にかかる発明は、上記請求項１に記載の個人認証装置において、上記記憶媒体に記憶されたデータについては、一方の組の識別記号を他方の組の秘密鍵で暗号化してあり、上記復号照合手段は、一方の組の識別記号にて上記認証局から上記公開鍵を取得し、同公開鍵にて上記識別記号を暗号化したデータを復号し、復号した識別記号にて上記認証局から上記公開鍵を取得して同公開鍵にて他方のデータを復号する構成としてある。
【００１６】
上記のように構成した請求項２にかかる発明においては、一方の組の識別記号を他方の組の秘密鍵で暗号化したデータが上記記憶媒体に記憶されている。そして、上記復号照合手段は、まず、一方の組の識別記号にて上記認証局から上記公開鍵を取得し、同公開鍵にて上記識別記号を暗号化したデータを復号することによって暗号化されている識別記号を取

得する。そして、取得した識別記号にて上記認証局から上記公開鍵を取得し、同公開鍵にて上記他方のデータを復号する。すなわち、最初に一つだけ識別記号が明らかになっていれば、それを使用して順次他のデータを復号していくことができる。

【００１７】

この応用パターンとして、本発明は、上記一方の組の識別記号を他方の組の秘密鍵で暗号化してある構成としてあり、上記登録端末では、上記所有者の秘密鍵で上記画像データと上記情報データと登録者の識別記号とを暗号化するとともに、上記登録者の秘密鍵で上記画像データと上記情報データとを暗号化し、上記個人認証端末では、上記所有者の識別記号にて上記認証局から同所有者の公開鍵を取得して上記登録者の識別記号を暗号化したデータを復号し、復号した上記登録者の識別記号にて上記認証局から同登録者の公開鍵を取得して残りの側のデータを復号する構成としてある。

【００１８】

次に、本発明は、上記記憶媒体に記憶されたデータについては、上記一方のデータの改ざん防止のパラメータを他方のデータに暗号化してあり、上記復号照合手段は、上記他方のデータから復号される上記改ざん防止のパラメータで上記一方のデータの改ざんを検出する構成としてある。

上記のように構成した発明においては、一方のデータの改ざん防止のパラメータを他方のデータに暗号化して上記記憶媒体に記憶してあるので、上記復号照合手段は、上記他方のデータから復号される上記改ざん防止のパラメータで上記一方のデータの改ざんを検出する。むろん、双方に改ざん防止パラメータを含めることは可能であるし、改ざん防止パラメータは暗号化された状態のデータについて行っても良いし、暗号化前のデータについて行なうようにしてもよい。

【００１９】

このように改ざん防止パラメータが他のデータに含まれていることにより、データに改ざんを加えれば容易に検出されることになる。

この応用パターンとして、本発明は、個人認証情報記憶媒体において、上記一方のデータの改ざん防止のパラメータを他方のデータに暗号化してある構成としてあり、本発明は、個人認証システムにおいて、上記登録端末では、上記所有者の秘密鍵と上記登録者の秘密鍵のいずれか一方で暗号化されたデータの改ざん防止パラメータを他方の暗号化の際に含めてあり、上記個人認証端末では、上記所有者の公開鍵と上記登録者の公開鍵のいずれか一方で復号化された改ざん防止パラメータで他方のデータの改ざんの有無を検出する構成としてもよい。

【００２０】

次に、画像データを扱うことから暗号化は電子透かし化で実現することもできる。すなわち、本願でいう暗号化は広く解し、電子透かし化も実質的には暗号化に含まれる。この一例として、本発明は、個人認証装置において、上記記憶媒体には、上記画像データに対して上記情報データを電子透かし化して暗号化を行なったデータを記憶してあり、上記復号照合手段は、透かし化された情報データを対応する公開鍵で抽出するとともに抽出の過程で画像データの改ざんを検出する構成としてもよい。

【００２１】

上記のように構成した発明においては、上記画像データに対して上記情報データを電子透かし化して暗号化を行ない、上記記憶媒体に記憶してある。そして、上記復号照合手段は、透かし化された情報データを対応する公開鍵で抽出するとともに抽出の過程で画像データの改ざんを検出する。

このように電子透かし化によれば、暗号化と改ざん防止を同時に実現できる。

この応用パターンとして、本発明は、個人認証情報記憶媒体において、上記画像データに対して上記情報データを電子透かし化して暗号化を行なったデータを記憶する構成としてあり、本発明は、記載の個人認証システムにおいて、上記登録端末では、上記登録者の秘密鍵で上記画像データに上記情報データを電子透かし化し、上記個人認証端末では、上記登録者の公開鍵で上記電子透かし化したデータから情報データを抽出する構成としてあ

る。
【００２２】
照合の手法は様々であり、その一例として、本発明は、個人認証装置において、上記記憶媒体に記憶されたデータについては、上記情報データをそれぞれの秘密鍵で個別に暗号化してあり、上記復号照合手段は、それぞれの秘密鍵で暗号化されたデータをそれぞれの公開鍵で復号して得られる情報データを突き合わせて照合する構成としてある。
【００２３】
上記のように構成した発明においては、上記復号照合手段が、それぞれ個別の秘密鍵で暗号化してあるデータをそれぞれの公開鍵で復号し、得られた情報データを突き合わせて照合する。
すなわち、個別に暗号化してあるので、一方だけを改ざんできたとしても他方についても改ざんできない限りは照合に失敗する。この場合、一致する場合に限らず、互いに対となって意味をなすような対応となれば照合できたと判断しても良い。
【００２４】
これと同様に、本発明は、個人認証情報記憶媒体において、上記情報データをそれぞれの秘密鍵で個別に暗号化してある構成としてある。
また、画像データは個人の認証に利用するものであるから、本発明は、個人認証装置において、上記画像データは、人間の身体の画像を撮影したものである構成としてある。
【００２５】
上記のように構成した発明においては、人間の身体の画像を撮影した画像データを記憶してあるので、データの復元や照合が行えたとしても表示される画像が本人と異なり、個人認証を正しく行える。また、画像を入れ替えるためには、暗号化の際の秘密鍵が必要であるが、これは実質的に不可能である。
これと同様に、本発明は、個人認証情報記憶媒体において、上記画像データは、人間の身体の画像を撮影したものである構成としてある。
【００２６】
この他、ＩＣカードへの登録を行う具体的な方法として、本発明は、固有の識別記号に対応させて互いに対となる秘密鍵と公開鍵とが認証局にて管理されており、所有者となる人物の特徴となる画像を表す画像データを取得するとともに、同所有者の所定の情報データを取得し、自己の秘密鍵で上記画像データと上記情報データを暗号化するとともに、同所有者の秘密鍵で自己の識別番号と上記情報データを暗号化してＩＣカードに記録して登録を行う構成とし、また、実際の個人認証時の方法として、本発明は、固有の識別記号に対応させて互いに対となる秘密鍵と公開鍵とが認証局にて管理されており、所有者の識別番号に基づいて上記認証局から公開鍵を取得し、同公開鍵にてＩＣカード内の一のデータを復号化して所有者の情報データと登録者の識別番号を抽出するとともに、同識別番号に基づいて上記認証局から公開鍵を取得し、同公開鍵にて他のデータを復号して所有者の情報データと画像データを復元し、データの改ざんの有無を検出して検出結果と画像データを利用可能とする構成としてもよい。
【００２７】
これらにおいては、登録現場あるいは決済現場で具体的に利用されることになる。
【００２８】
【発明の効果】
以上説明したように本発明は、二組の秘密鍵と公開鍵を利用して、画像データと情報データの改ざんを防止でき、極めて安全性の高い個人認証装置を提供することができる。
また、本発明によれば、識別記号を順次復元していくことができるので、複数の組の秘密鍵と公開鍵を利用する場合であっても、最初に必要なのは一つの識別記号だけで済み、多くの情報を覚えておく必要が無くなる。
【００２９】
さらに、本発明によれば、改ざん防止パラメータを含めることによってデータの改ざん自体を検出できるようになり、安全性を高めることができる。

さらに、本発明によれば、画像データに対して電子透かし化で情報データを含めることにより、暗号化を行えるとともに改ざん防止も可能となる。
さらに、本発明によれば、復元したデータ同士を突き合わせることにより、比較的容易に照合を行える。

【００３０】

さらに、請求項３にかかる発明によれば、身体の画像データを利用することによって目視による最終的な確認を容易に行うことができる。
さらに、本発明によれば、現場の実際の作業において、簡単かつ有効な個人認証の方法を提供することができる。

【００３１】

【発明の実施の形態】

以下、図面にもとづいて本発明の実施形態を説明する。本発明の個人認証システムでは、各個人が予め登録業者にて個人情報と画像をデータとしてＩＣカードに書き込んでおき、買い物などの際にこのＩＣカードを使用して本人の認証を行う。そして、本人認証後の決済などについては、既存および今後開発される各種の決済システムを利用することになるが、本明細書では認証までの段階について説明する。
図１は、本発明の一実施形態にかかる個人認証システムで買い物などの際に個人認証を利用するＰＯＳ端末をブロック図により示しており、図２は登録業者の端末装置をブロック図により示している。そして、図３は媒体となるＩＣカードの外観を示している。

【００３２】

同図において、ＰＯＳ端末１０は、制御本体１１と、各種の入力操作を行うコンソール１２と、入力情報と計算情報と後述する画像などを表示するディスプレイ１３と、ＩＣカード２０を接続するためのＩＣカードリーダ１４と、公衆電話網３０を介して外部の認証局４０と交信するためのモデム１５などを備えている。制御本体１１には、演算処理を実施するＣＰＵ１１ａと、プログラムやデータなどを記憶するＲＯＭ１１ｂと、ワークエリアなどに利用されるＲＡＭ１１ｃと、外部機器と電気的に接続するためのＩ／Ｏ１１ｄなどを備えている。

【００３３】

一方、登録業者の登録端末５０は、制御本体５１と、各種の入力操作を行うコンソール５２と、入力情報と計算情報と後述する画像などを表示するディスプレイ５３と、ＩＣカード２０を接続してデータの書き込みなどを行うためのＩＣカードリーダライタ５４と、画像を撮影して画像データを出力するデジタルカメラ（ＤＳＣ）５６などを備えている。同図には公衆電話網３０に接続するためのモデムを表示していないが、備えているものであっても良い。また、制御本体５１には、ＣＰＵ５１ａ～Ｉ／Ｏ５１ｄも備えている。

【００３４】

図４は上記ハードウェアを利用して個人認証を実現するにあたり、データ処理を概略的に示している。概略的には登録端末５０の側で画像データと個人情報とを二者に対応した二つの秘密鍵で暗号化してＩＣカード２０に書き込んでおき、ＰＯＳ端末１０の側でその二者に対応した二つの公開鍵で復号化する。このとき、本個人認証システムを利用すればデータの改ざんは不可能に近く、安全性の高さを保障できる。

【００３５】

二者の秘密鍵と公開鍵を利用する本発明の適用パターンは各種のものが考えられるが、本実施形態では、一つの秘密鍵で個人情報を画像データに透かしとして入れ込み、もう一つの秘密鍵は単独で個人情報の暗号化に利用される。そして、復元する際には対応する一つの公開鍵で透かしから個人情報を抽出するとともに、もう一つの公開鍵で個人情報を解読し、このように二つの経路で保存された個人情報を個別に解読した後、照合して改ざんの有無を判別する。これらの照合や改ざんのチェックは広い意味でのデータの整合性を判定するものといえる。

【００３６】

以下、具体的に各処理を表すフローチャートを参照して説明する。図５は登録業者におけ

る登録処理の内容をフローチャートにより示しており、図６はＰＯＳ端末での個人認証処理の内容をフローチャートにより示しており、図７は公開鍵を管理する認証局の照会処理の内容をフローチャートにより示している。
登録業者では、登録端末５０を利用して所有者の情報などを登録する作業を行う。ステップＳ１００では透かしを入れる画像データを取得する。画像データは一例として所有者の身体を表すものを利用できる。最も簡便なものは「顔」である。具体的にはデジタルカメラ５６を利用して顔写真を撮影し、デジタル化された画像データを作成する。そして、この画像データを直接または一時的にハードディスクなどに保存するなどし、ステップＳ１００にて同画像データを取得する。

【００３７】

ステップＳ１０２では個人情報データを取得する。個人情報データは氏名、住所、年齢などであるが、その使用用途によって適宜変更可能である。本実施形態の場合、個人情報は改ざんの有無を調べるために二つの別個の処理でＩＣカードに保存され、後に両者を個別に復元して照合するのに利用する。従って、氏名、住所、年齢などについては特別の意味を持っていない。ただし、個人情報データにはどの登録業者で登録されたかを表示するため、登録業者の識別記号を含めておく。この識別記号は認証局４０から公開鍵を取得するために必要となる。

【００３８】

ここで秘密鍵と公開鍵について簡単に説明する。秘密鍵と公開鍵は一対をなし、一方から他方を推定することはほとんど不可能に近いが両者は一義的な関係にある。一方を利用して暗号化されたものは他方を利用してのみ復号化が可能であり、これは暗号化した側の鍵を利用しても復号化することはできない。例えば、本人が秘密鍵を使って暗号化したものを誰かに配信するとする。この場合、予め公開鍵は相手に伝えておく。相手はこの公開鍵を利用して復号化することができる。第三者が本人の秘密鍵とともに既に配信した暗号化データを取得したとしても、これを復元することはできない。

【００３９】

認証局４０は、図８に示すような識別記号と公開鍵と秘密鍵とをテーブル状のデータベースとして備えており、識別記号に基づいて公開鍵を知らせる機能を有する。秘密鍵はデータベースとしては登録されているものの、通常は知らせることはない。同図に示す例として、登録業者の識別記号「ＡＡＡ０１２３４５」に対して公開鍵ＶＰと秘密鍵ＶＳが記録されており、また、所有者には識別記号「ＢＢＢ６７８９０１」に対して公開鍵ＯＰと秘密鍵ＯＳが記録されている。なお、公開鍵と秘密鍵は各種の方式があり、本明細書では詳しく触れない。また、この各鍵ＶＰ，ＶＳ，ＯＰ，ＯＳはその内容を表すものではなく、単なる符号にすぎない。

【００４０】

ステップＳ１０４では登録業者の秘密鍵ＶＳを取得する。この秘密鍵は自己のものであるため、上述した認証局４０に問合せる必要はない。ただし、この秘密鍵を利用する処理は重要な秘密処理であるため、例えばなんらかの役職あるいは資格をもった担当者だけが処理できるようなセキュリティ処理を組み込むことも可能である。
ステップＳ１０６では上述した画像データと個人情報データを登録業者の秘密鍵ＶＳを利用して電子透かし化処理を実施する。電子透かし化処理の具体的な方式は現在までに各種のものが提案されている。例えば、本願出願人による特開平１１－３４１２６８号公報にも、ＪＰＥＧ変換における８×８離散コサイン変換における６３番目の係数を利用して透かしビットを挿入する技術を開示している。６３番目は最高周波数の成分値であり、その値を変えても殆ど画像には影響を与えない。従って、この埋め込みビットを含めたままＪＰＥＧ展開しても肉眼で画像の変化を判断することは殆ど不可能となるという特性をもっている。本個人認証システムでの電子透かし化処理は、特にその方式を限定するものではないので、各種のものを採用可能である。

【００４１】

次に、ステップＳ１０８では所有者秘密鍵ＯＳを取得する。所有者秘密鍵ＯＳは所有者だ

けが管理するものであるから、コンソール５２から所有者自身で入力する。この場合、周りの人から操作状況を見にくいようにした独立のコンソールを用意しておき、このコンソールを用いて入力するようにしても良い。続いて、ステップＳ１１０では、この取得した所有者秘密鍵ＯＳを利用して個人情報データを暗号化する。この暗号化は所有者公開鍵ＯＰにて復号可能なものである。

【００４２】

最後のステップＳ１１２では登録業者の秘密鍵ＶＳを使用した電子透かし化処理を経て透かしを入れた画像データと、所有者公開鍵ＯＰを使用して暗号化した暗号化データをＩＣカード２０に対して書き込む。この結果、図４に示すように、ＩＣカード２０には、透かし入りの画像データと、暗号化データが保存されることになる。なお、ＩＣカード２０自体には登録業者識別記号と同様な後述する所有者識別記号が付与されて記録されているし、他の基本的なデータが記録されていることはいうまでもない。

【００４３】

一方、ＩＣカード２０を使用してＰＯＳ端末１０で個人認証する処理は図６に示すようになる。例えば、買い物の決済をする際、所有者はＰＯＳ端末１０のあるところへ商品を運び、このＰＯＳ端末１０のＩＣカードリーダ１４にＩＣカード２０を装着する。すると、ＰＯＳ端末１０では、以下の処理を実施する。なお、図９はＩＣカードとＰＯＳ端末と認証局との間でのデータのやりとりの概略を示している。

【００４４】

まず、ステップＳ２００では、ＩＣカード２０の所有者識別記号を取得する。ＩＣカード２０には上述したように所有者識別記号も記録されているので、ＩＣカードリーダ１４を介して読み込む。続くステップＳ２０２では、この所有者識別記号を使用して認証局４０に対応する公開鍵ＯＰを要求する。

認証局の処理は図７のフローチャートに示しており、ステップＳ３００にて公開鍵ＯＰの要求があるか否かを判断し、要求があればステップＳ３０２にて対象となる識別記号を取得する。認証局４０には図８に示すように識別記号と公開鍵ＯＰとを対応させた管理テーブルを有しており、ステップＳ３０４にて識別記号からデータベースを参照して公開鍵ＯＰを取得する。そして、取得した公開鍵ＯＰをステップＳ３０６にて送信する。なお、公開鍵ＯＰの要求については所定のセキュリティチェックが実施されているが、ここでは省略する。また、ステップＳ３００にて公開鍵ＯＰの要求がない場合には以上の処理を実施することなく終了し、図示しない他の処理を実施している。

【００４５】

図６のＰＯＳ端末１０の処理に戻ると、この間、ステップＳ２０４にて公開鍵ＯＰが受信されるのを待機しており、受信されるとステップＳ２０６にてＩＣカード２０内の暗号化データを取得するとともに、ステップＳ２０８では受信した所有者公開鍵ＯＰで上記暗号化データを復号して個人情報データを解読する。

この個人情報データには上述したように登録業者の識別記号も書き込まれている。従って、ステップＳ２１０ではこの登録業者の識別記号を取得し、認証局４０に対してこの登録業者識別記号を使用して対応する公開鍵ＶＰを要求する。認証局４０では、上述したように図７のフローチャートに従い、今度は登録業者の識別記号を使用してデータベースを参照し（ステップＳ３０４）、対応する公開鍵ＶＰを送信する（ステップＳ３０６）。一方、図６に示すＰＯＳ端末１０の側においては、ステップＳ２１２にて公開鍵ＶＰが受信されるのを待機し、公開鍵ＶＰが得られたらステップＳ２１４でＩＣカード２０から透かし入り画像データを取得するとともに、ステップＳ２１６にて得られた登録業者の公開鍵ＶＰを利用して透かしから個人情報データを抽出する。

【００４６】

この際、公開鍵ＶＰで透かしを抽出する過程でこの透かし入り画像データの改ざんの有無を判定できる。例えば、改ざんによって透かし自体が抽出されなくなることがある。また、透かしを抽出する過程で得られるハッシュ値と透かし入り画像データのハッシュ値とを比較しても透かし入り画像データに対する改ざんの有無を判定できる。この他、ハッシュ

値を秘密鍵で暗号化し、これを透かし化して組み込むことも可能である。この場合、透かしから暗号化されたハッシュ値を抽出し、公開鍵で復号化するとハッシュ値を得られるので、画像データの改ざんの有無を検出できる。

【００４７】

以上のようにして暗号化データと透かし入り画像データのそれぞれから個人情報が取り出される。これらは別個の秘密鍵ＯＳ，ＶＳで暗号化されているのであり、さらに、暗号化データを解読しなければ登録業者の識別記号を得ることができない。通常、所有者と登録業者とは殆ど関連性がないので、何の手がかりもなく外部から登録業者の公開鍵ＶＰを得るというのは可能性として殆ど考えられない。また、所有者は何らかの形で秘密鍵ＯＳを手元に管理しているはずなので、何らかの偶然によって秘密鍵ＯＳを盗取できてしまうかもしれないが、その場合でも登録業者の秘密鍵ＶＳまでは盗取できるとは考えられない。むろん、これらは可能性として０％でない限りありえるが、さらに使用者がＩＣカード２０を紛失したことを届け出るまでに全てを完結しなければならないという条件も加わるので、安全性が高いといえる。

【００４８】

ところで、この時点でＰＯＳ端末１０内には一時的に所有者と登録業者の識別記号および公開鍵ＯＰ，ＶＰが保持される。従って、極端な例としてこれらの識別記号および公開鍵ＯＰ，ＶＰを出力して悪用してしまうことが考えられる。しかしながら、この公開鍵ＯＰ，ＶＰを使用して個人情報データや画像データを作成したり暗号化した場合、これを復元するのに要するのは秘密鍵ＯＳ，ＶＳとなる。従って、これらの情報が得られたとしても、別のＰＯＳ端末１０でこのＩＣカード２０を使用したときには公開鍵ＯＰ，ＶＰが得られることになるが、公開鍵ＯＰ，ＶＰで暗号化したものを公開鍵ＯＰ，ＶＰで復号化することはできず、結局は使用できないことになる。

【００４９】

続く、ステップＳ２１８ではこのようにして別個に得られた個人情報データを照合するとともに、改ざんの有無をチェックする。照合した結果、両者が一致しなければ画像データも改ざんされている可能性が高い。また、上述したように透かし自体に画像の改ざんを検出する機能があればそれを利用することもできる。また、予め画像データについてのハッシュ値を求めておき、これを個人情報データとともに透かし化するようにしてもよい。そして、透かしを分離して元の画像データを求め、ハッシュ値を算出し、透かしとして保存されたときの値とずれがないかで改ざんの有無をチェックするようにしても良い。

【００５０】

ステップＳ２２０では透かし入り画像データの画像に基づいてディスプレイ１３に表示を行う。本実施例においては、透かし入り画像データに基づいて直接に画像データを展開して画像を復元することは可能であるため、透かしの抽出を待たずに画像を表示しても良い。

ステップＳ２２２では、上述した照合結果がＯＫであるか、あるいは改ざんがされていないか判断し、両者共にＯＫであればステップＳ２２４にてＰＯＳ端末１０の操作者からの画像確認操作を待機する。上述したようにステップＳ２２０で既に所有者の画像をディスプレイ１３に表示しており、ＰＯＳ端末１０の操作者は所有者の顔と照らし合わせて同一人物のように見えれば確認ＯＫの操作を行う。そして、ステップＳ２２６では画像についての本人確認がＯＫか否かを判断し、ＯＫであればステップＳ２２８にて以降の処理で参照できるように許可フラグをセットして本個人認証処理を終了する。これは画像データが改ざんされていないということを上述の処理を介して保障した上で、この画像データの顔の画像とこのＩＣカード２０の所有者が一致していれば個人認証が完了するということを意味する。

【００５１】

最終的に所持人の顔と画像の顔とが一致するか否かはＰＯＳ端末１０の操作者が判断することになるが、この判断から先については既存の認証と変わるところはなく、この段階までが従来の技術で安全性を保障できなかった部分である。例えば、クレジットカードで

あれば買い物伝票にサインをし、そのサインとカードのサインとが一致するかを店員が判断している。しかしながら、カードを盗取した窃盗者と店員が協力すれば、サインが一致したものとして決済してしまうことが可能である。だとすれば、店員の介在する場よりも以降のものについては安全性は変わらない。

【００５２】

一方、クレジットカードについては何よりもサインの練習さえすれば容易に買い物の場で決済ができてしまう。さらに、写真入りのカードであるとしても写真を改ざんしたカードを作り、これに同じ磁気情報を書き込んでしまえば改ざんの有無は分からない。従って、改ざんを絶対的に防止することによるメリットは計り知れない。

なお、上述した実施形態においては、ステップＳ２０６やステップＳ２１４がＩＣカード２０から暗号化データや透かし入り画像データを読み込んでいるので読取手段を構成する。また、ステップＳ２０８やステップＳ２１６で復号化や透かしからの抽出を行い、さらに、ステップＳ２１８にて照合と改ざんを行っており、これらによって復号照合手段を構成している。さらに、ステップＳ２２０にて画像を表示し、ステップＳ２２４にて画像の確認操作を受け付けており、これらの処理が画像確認手段を構成する。そして、これらの判断の結果によってステップＳ２２８にて許可フラグを設定するため、ステップＳ２２２とステップＳ２２６にて判断分岐処理を行っており、これらの処理が個人認証を許可する許可手段を構成している。

【００５３】

ところで、以上の実施形態においては、登録業者秘密鍵ＶＳで透かし化を行い、所有者秘密鍵ＯＳで暗号化を行っているが、広い意味での暗号化を異なる秘密鍵で行ない、復号化をそれぞれ対となる個別の公開鍵で行う対応は、各種の変形例も可能である。

図１０は変形例にかかる登録処理２をフローチャートにより示しており、図１１は対応する個人認証処理２をフローチャートにより示しており、図１２は暗号化・復号化の処理と対象とされるデータの対応を示している。

【００５４】

登録業者の側ではステップＳ１００にて画像データを取得し、ステップＳ１０２にて個人情報データを取得する点では先程の実施形態と同様である。しかしながら、ステップＳ１２０では電子透かし化処理するのでなく、画像データと個人情報データとを登録業者秘密鍵ＶＳで暗号化処理する。なお、この暗号化を第１の暗号化処理と呼び、暗号化されたデータを第１の暗号化データと呼ぶ。

次に、ステップＳ１２２ではこの暗号化データの改ざんを防止するためのパラメータを算出する。パラメータは各種の演算方式で演算することが可能であり、上述したハッシュ値を用いることも可能である。そして、ステップＳ１２４にてコンソール５２から所有者自身が所有者秘密鍵ＯＳを入力させて取得する。

【００５５】

そして、ステップＳ１２６にてこの所有者秘密鍵ＯＳを使用し、改ざん防止パラメータと個人情報データとを暗号化する。この暗号化は第２の暗号化処理と呼び、暗号化されたデータを第２の暗号化データと呼ぶ。なお、この個人情報データには登録業者の識別記号が含まれている。第２の暗号化後、ステップＳ１２８では第１の暗号化データと第２の暗号化データとをＩＣカード２０に書き込む。

一方、ＰＯＳ端末１０の側では、ステップＳ２４０にてＩＣカード２０から所有者識別記号を取得するとともに、ステップＳ２４２にてこの所有者識別記号を使用して認証局４０に対応する公開鍵ＯＰを要求する。認証局４０は先程と同様にして所定のセキュリティチェックをした上で所有者の公開鍵ＯＰを送信してくるので、ステップＳ２４６ではこの公開鍵ＯＰを使用してＩＣカード２０内の第２の暗号化データを復号する。

【００５６】

第２の暗号化データに含まれる個人情報データとして登録業者の識別記号も記録されているので、ステップＳ２４８ではこの登録業者の識別記号を使用して認証局４０に対応する公開鍵ＶＰを要求する。そして、認証局４０は先程と同様にして所定のセキュリティチェ

ックをした上で所有者の公開鍵ＶＰを送信してくるので、ステップＳ２５０ではこの公開鍵ＶＰを使用してＩＣカード２０内の第１の暗号化データを復号する。

【００５７】

第２の暗号化データを復号すると、改ざん防止パラメータと個人情報データと得られる。ステップＳ２５２では改ざん防止パラメータを使用して第１の暗号化データが改ざんされていないか判断する。上述したように所有者本人の顔の画像を改ざんされると従来の写真入りカードと同じ程度のセキュリティになってしまうが、このように画像データを暗号化する際の秘密鍵ＶＰは登録業者のものであり、その改ざんの有無を判断するためのパラメータは所有者の秘密鍵ＯＳで別個に暗号化されている。従って、改ざんの可能性は限りなく低いといえる。

【００５８】

ステップＳ２５４では改ざんのチェックの結果に基づいて分岐を行う。改ざんされていなければステップＳ２５６にてさらに両方の経路で暗号化された個人情報データを相互に照合する。照合の結果がＯＫであれば、第１の暗号化データを復号化して得られた画像データをステップＳ２６０にてディスプレイ１３上に表示する。

ディスプレイ１３上に所有者の顔の画像が表示されたら、ステップＳ２６２にてＰＯＳ端末１０の操作者からの画像確認操作を待機し、ＰＯＳ端末１０の操作者は所有者の顔と照らし合わせて同一人物のように見えれば確認ＯＫの操作を行う。そして、ステップＳ２６４では画像についての本人確認がＯＫか否かを判断し、ＯＫであればステップＳ２６６にて以降の処理で参照できるように許可フラグをセットして本個人認証処理を終了する。

【００５９】

この例では、画像データ自体を暗号化しており、透かし化していない点で先の例とは異なる。しかしながら、二者の秘密鍵と公開鍵の対を利用しており、かつ、少なくとも一方の対に関して復号化しないと、他方の対が誰の秘密鍵と公開鍵の対応によるものかすら分からない。従って、セキュリティは非常に高い。

さらに別の例として、図１３に示すように、画像データ自体を暗号化せず、改ざん防止パラメータを個人情報データとともに登録業者の秘密鍵ＶＳで第１の暗号化データに暗号化し、この第１の暗号化データについての改ざん防止パラメータを算出した上で所有者の秘密鍵ＯＳで個人情報データとともに第２の暗号化データに暗号化することも可能である。

【００６０】

この場合、まず、所有者の識別記号に基づいて所有者の公開鍵ＯＰを取得して第２の暗号化データを復号化し、解読された個人情報データに含まれる登録業者の識別記号に基づいて登録業者の公開鍵ＶＰを取得して第１の暗号化データを復号化する。このとき、第１の暗号化データ自体の改ざんを検出でき、さらに解読された画像データの改ざん防止パラメータに基づいて画像データの改ざんを検出できるため、結果として画像データの安全性はほぼ保障される。

【００６１】

一方、以上のような個人認証を利用した買い物の課金処理の例を図１４のフローチャートにより示している。

ステップＳ３００にて予め許可フラグをリセットしてから、ステップＳ３０２にて上述した個人認証処理を実行する。個人認証が行われて本人と確認された場合には許可フラグがセットされてくるため、ステップＳ３０４にてこの許可フラグに基づいて個人認証の結果を参照する。そして、許可されている場合にはステップＳ３０６にて所有者識別記号に対して課金情報を課すデータを送信する。ここではクレジットカードを想定しており、識別記号と売上金額などをクレジット会社に通知する。むろん、ここでの具体的な課金の手続きなどについては適宜変更可能である。

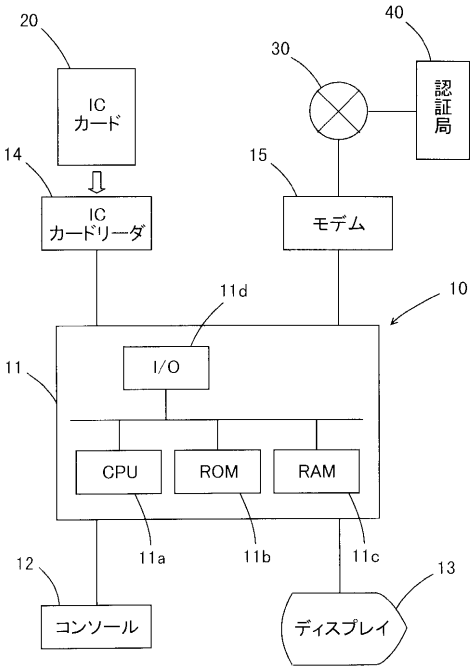
【００６２】

一方、ステップＳ３０８では送信した課金のデータに対する受理の有無を判断する。クレジット会社からそのＩＣカード２０に対する盗難などによってその時点で課金を受け付けないような場合もある。従って、個人認証はできたとしてもこの場合はステップＳ３１０

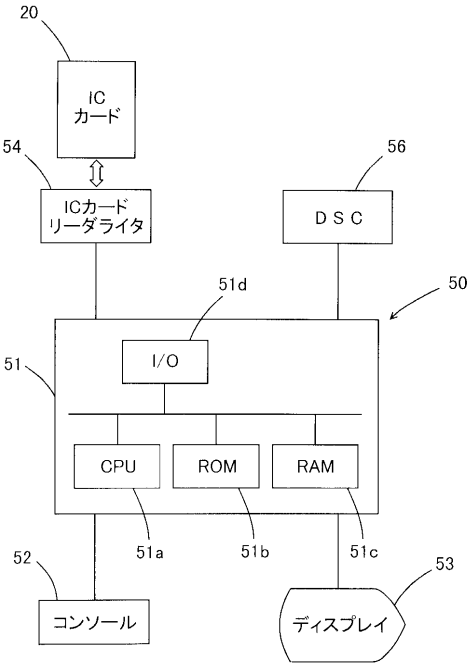
にて現金決済の処理を行う。なお、先に個人認証で許可が得られなかった場合もステップＳ３１０にて現金決済の処理を実行する。
ところで、画像データは本人確認のために利用され、上述した例では顔写真について説明した。図１５は買い物などの際にＰＯＳ端末１０のディスプレイ１３にはＩＣカード２０に記録されていた画像データに基づいて画像を表示された状態を示しており、ＰＯＳ端末１０の操作者は所持者の顔とディスプレイ１３に表示された顔の画像とを見比べて本人か否かを確認し、上述した画像確認操作を行うことになる。
【００６３】
画像を利用して本人を確認する他の手法として図１６には指紋を照合する例を示している。ディスプレイ１３は左右を分割して表示が行われるようにしてあり、所持者がＰＯＳ端末１０に備えられた指紋読み取りパッド１６に指を置くと、一方の領域に読み取られた指紋が表示される。そして、他方の領域には画像データとして記録されていた指紋を表示する。ＰＯＳ端末１０の操作者に判断させるのが困難な場合もあるが、その場合は両者をプログラムの処理で照合する指紋照合処理を実行させても良い。むろん、表示させるメリットもあり、プログラムによる処理では照合できなくても現実に並べられた指紋が肉眼で同一と判断できればＰＯＳ端末１０の操作者の判断を優先させることができるからである。
【００６４】
また、図１７は眼底写真で本人を確認する手法を示している。眼底写真も指紋と同様に絶対的な個別性を有しており、眼底写真撮影装置１７を使う点を除いてほぼ指紋と同様に判断することができる。
これまでディスプレイ１３はＰＯＳ端末１０に備えられていることを前提としているが、図１８に示すようにＩＣカード２０にディスプレイ２１を備えることも可能である。この応用例として例えばＰＤＡ端末のように予めディスプレイを備えている機器に対してＩＣカード２０と同様のデータを記憶させてもよい。また、携帯電話のディスプレイを利用するようにしてもよい。
【００６５】
携帯電話であると、課金を電話料金とともに課すことができて便利である。例えば、所持者の携帯電話に通話料の滞納が生じているのであれば、課金を許さないようにすることで、所持者の悪用を防止できる。また、使用期間が短ければ課金額を低額に設定することで被害を最小限とすることができるし、使用期間が短くても使用したい場合には予めデポジットを入金させておくことで不便さは解消しつつ不正使用を防止できる。
【００６６】
一方、商品を売る側についても電話の決済口座があることを条件とし、買い主から集金された金額はこの決済口座に払い込まれるものとすると、それまでの利用実績のある売り主だけがこのクレジットシステムを利用できる。一般に、携帯電話の課金は後払いであり、携帯電話の利用者は明細を確認してから振り込みの準備を行える。従って、不審な課金があればその時点でチェックできる。売り主はこのチェックを経てからしか振り込まれないから、悪意で課金の情報を作出した場合には振り込まれる前に発覚して金銭を回収できなくなる。
【００６７】
この意味では携帯電話に限らず、課金のシステムを備えた通信端末装置一般に利用可能である。
このように、所有者と登録業者はそれぞれ固有の識別記号を持ち、さらに各識別記号に対して秘密鍵と公開鍵を対応づけておき、所有者の秘密鍵で個人情報データと登録業者の識別記号を暗号化するとともに登録業者の秘密鍵で画像データと個人情報データとを電子透かし化してＩＣカード２０に記録し、個人認証する際には所有者の識別記号から公開鍵を取得して暗号化された個人情報と識別記号を復号化し、得られた識別記号で公開鍵を取得して電子透かしを入れた画像データから個人情報データを復元し、別個に得られた個人情報データを照合したり画像データの改ざんの有無を検出することにより、極めて安全性の高い個人認証システムを構築できる。

【図面の簡単な説明】
【図１】本発明の一実施形態にかかる個人認証装置を適用したＰＯＳ端末のブロック図である。
【図２】本発明の一実施形態にかかる個人認証装置を適用した登録端末のブロック図である。
【図３】ＩＣカードの外観図である。
【図４】データの暗号化・復号化の過程を示す模式図である。
【図５】登録処理を示すフローチャートである。
【図６】個人認証処理を示すフローチャートである。
【図７】認証局の公開鍵処理を示すフローチャートである。
【図８】認証局のデータベースの構造を示す図である。
【図９】ＩＣカードとＰＯＳ端末と認証局の間のデータの流れを示す図である。
【図１０】変形例にかかる登録処理を示すフローチャートである。
【図１１】変形例にかかる個人認証処理を示すフローチャートである。
【図１２】変形例にかかるデータの暗号化・復号化の過程を示す模式図である。
【図１３】他の変形例にかかるデータの暗号化・復号化の過程を示す模式図である。
【図１４】課金応用処理を示すフローチャートである。
【図１５】顔の画像データを利用する場合の適用例を示す模式図である。
【図１６】指紋の画像データを利用する場合の適用例を示す模式図である。
【図１７】眼底写真の画像データを利用する場合の適用例を示す模式図である。
【図１８】変形例にかかるＩＣカードの外観図である。
【符号の説明】
１０…ＰＯＳ端末
１１…制御本体
１２…コンソール
１３…ディスプレイ
１４…ＩＣカードリーダ
１５…モデム
１６…パッド
１７…眼底写真撮影装置
２０…ＩＣカード
２１…ディスプレイ
３０…公衆電話網
４０…認証局
５０…登録端末
５１…制御本体
５２…コンソール
５３…ディスプレイ
５４…ＩＣカードリーダライタ
５６…デジタルカメラ（ＤＳＣ）

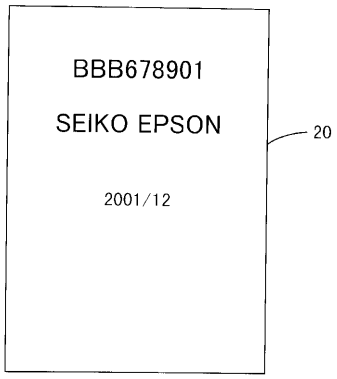
【図１】


20
IC
カード
14
IC
カードリーダ
30
40
認識
15
モデム
11d
10
11
I/O
CPU
ROM
RAM
11a
11b
11c
12
13
コンソール
ディスプレイ

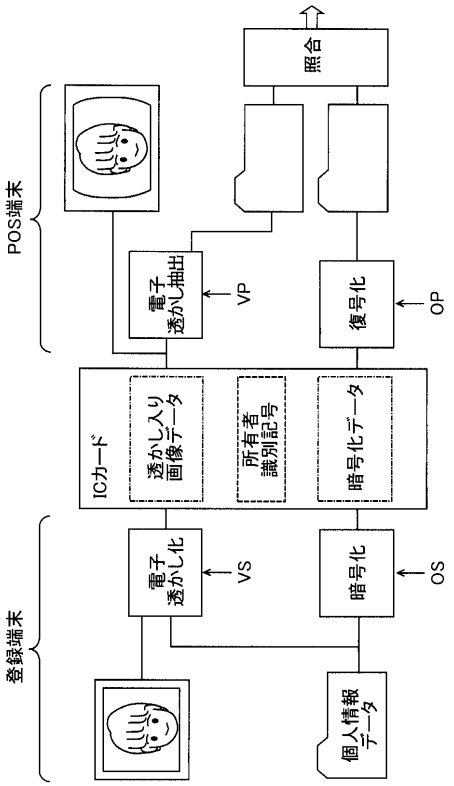
【図２】


20
IC
カード
54
ICカード
リーダライタ
56
DSC
51d
50
51
I/O
CPU
ROM
RAM
51a
51b
51c
52
53
コンソール
ディスプレイ

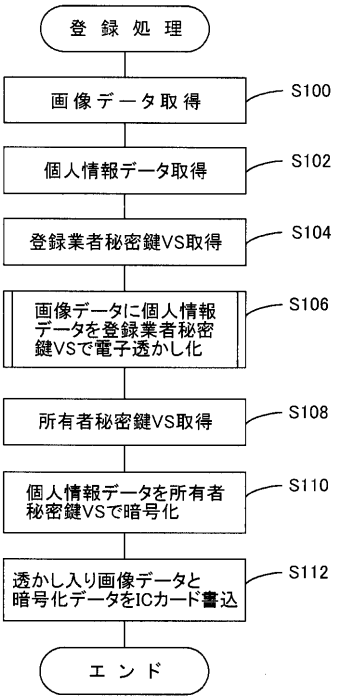
【図３】


BBB678901
SEIKO EPSON
2001/12
20

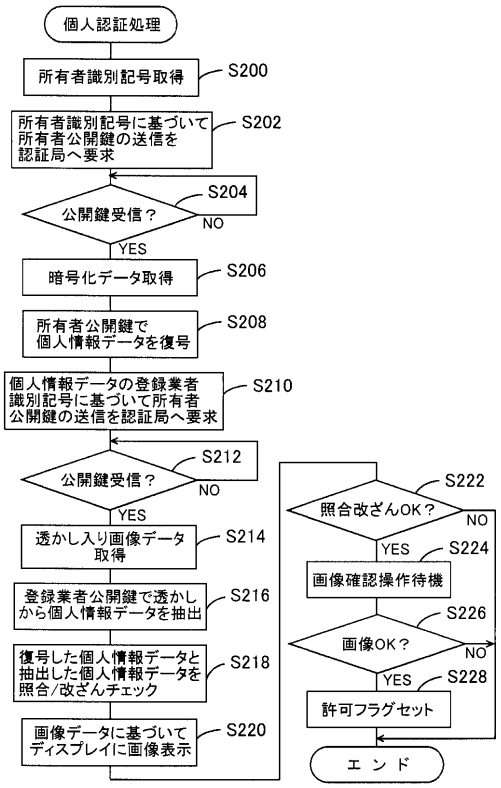
【図４】


照合
POS端末
電子
透かし抽出
VP
復号化
OP
ICカード
透かし入り
画像データ
所有者
識別記号
暗号化データ
登録端末
電子
透かし化
VS
暗号化
OS
個人情報
データ

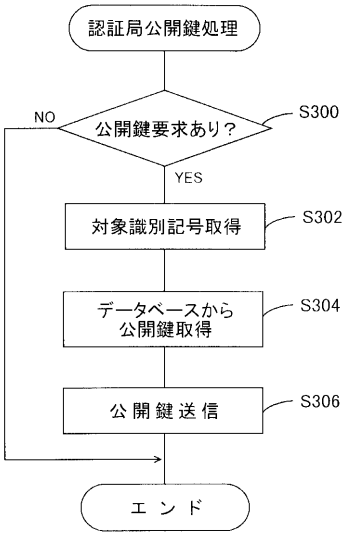
【図５】



【図６】



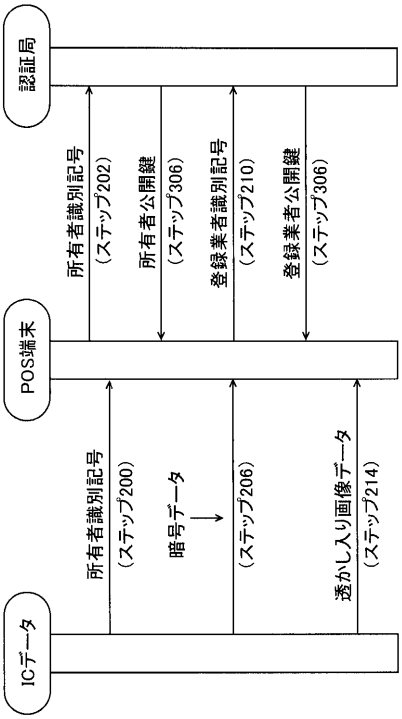
【図７】



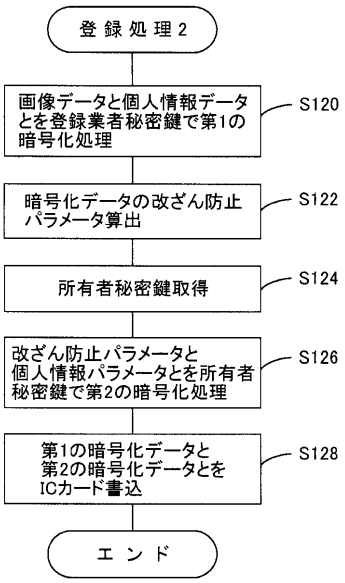
【図８】

識別記号	公開鍵	秘密鍵
⋮	⋮	⋮
BBB 678901（所有者）	OP	OS
⋮	⋮	⋮
AAA 012345（登録業者）	VP	VS
⋮	⋮	⋮

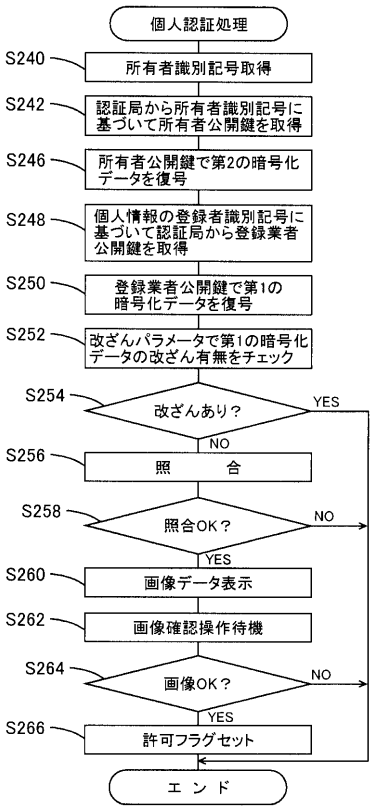
【図９】



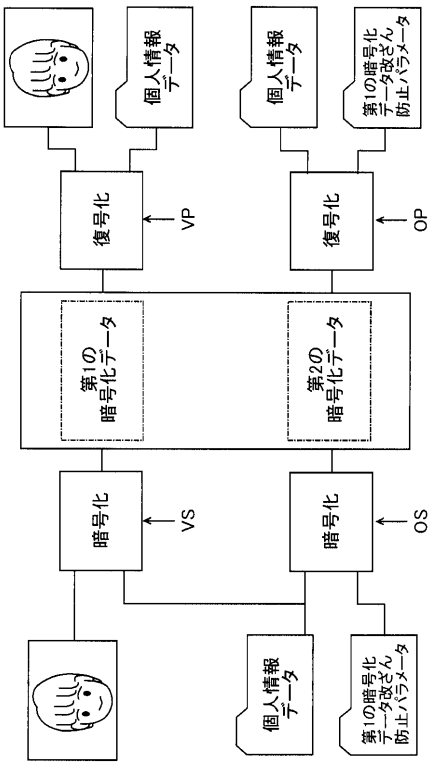
【図１０】



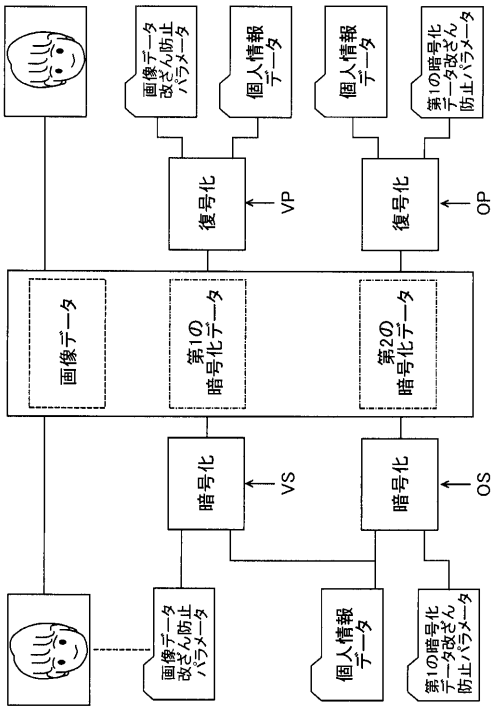
【図１１】



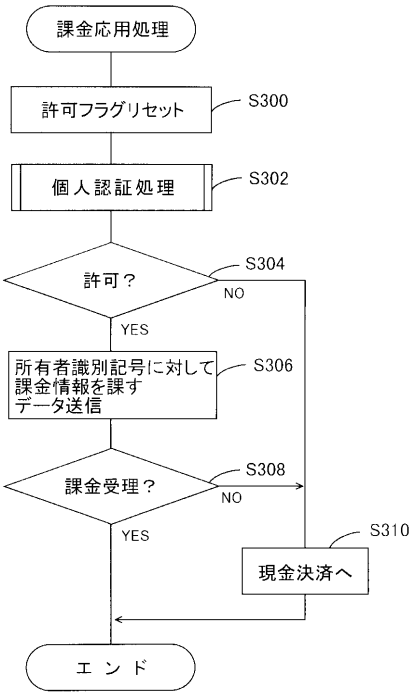
【図１２】



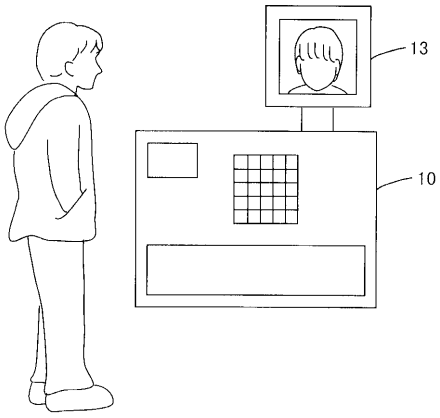
【図１３】



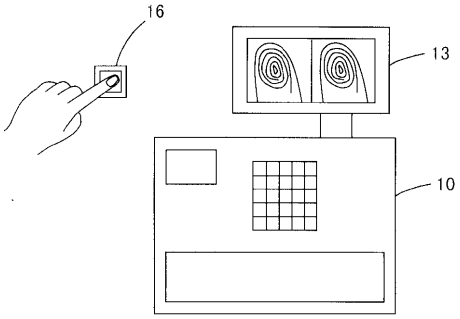
【図１４】



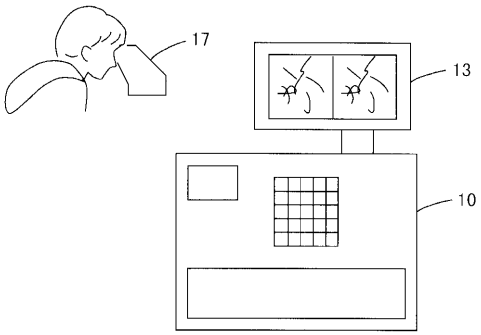
【図１５】



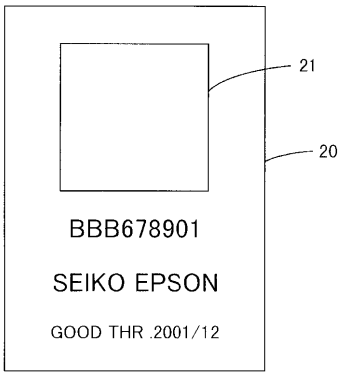
【図１６】



【図１７】



【図１８】



フロントページの続き

(51)Int.Cl.	FI		
	Ｂ４２Ｄ	15/10	５２１
	Ｇ０６Ｆ	17/60	５１０
	Ｇ０６Ｆ	17/60	５１２
	Ｇ０６Ｋ	17/00	Ｖ
	Ｈ０４Ｌ	9/00	６７３Ｅ

審査官　石田　信行

(56)参考文献　特開平１１－３２７４３８（ＪＰ，Ａ）
特開２０００－２１５１７１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 9/32
G06T 1/00