研究論文

Received March 11, 2003; Accepted November 17, 2003

光学 33, 1 (2004) 37-44

ICカード所持者認証を目的とした光暗号に基づく指紋照合

鈴木　裕之*・山谷　泰賀*・小尾　高史*・山口　雅浩*・大山　永昭**

*東京工業大学像情報工学研究施設　〒226-8503 横浜市緑区長津田町 4259
**東京工業大学フロンティア創造共同研究センター　〒226-8503 横浜市緑区長津田町 4259

Fingerprint Verification for Smart Card Holders Identification Based on Optical Image Encryption

Hiroyuki SUZUKI*, Taiga YAMAYA*, Takashi OBI*, Masahiro YAMAGUCHI* and Nagaaki OHYAMA**

*Imaging Science and Engineering Laboratory, Tokyo Institute of Technology, 4259 Nagatsuta, Midori-ku, Yokohama 226-8503
**Frontier Collaborative Research Center, Tokyo Institute of Technology, 4259 Nagatsuta, Midori-ku, Yokohama 226-8503

The fingerprint verification is more effective to identify the smart card holders compared with the conventional passcode verification. However, it is difficult to execute the operation of fingerprint verification in the embedded processor because of its computational burden and the shortage of the smart card performance. Then, we propose a hybrid card holder identification system, which consists of the conventional passcode verification with the smart card processor and the optical processing such as the optical fingerprint pattern matching and the optical recording-reproducing of the passcode, that are all based on the optical encryption-decryption method. The proposed method was evaluated using a computer simulation, and the result showed the feasibility of the smart card holder identification by the proposal system.

Key words: smart card, optical encryption, fingerprint verification, pattern matching

1. はじめに

近年，インターネットの普及により，さまざまなサービスがインターネット上の電子的な空間（サイバー空間）で行われるようになった．しかし，サイバー空間上でのサービスでは，悪意の第三者によるなりすましの危険があるため，サービスを提供される人や提供する人（もしくは組織・団体等）の正当性を保証する認証技術が重要となる．このようなネットワーク上での確実な認証を行うための手法として，ICカードを利用した認証技術の普及が進んでいる[1]．

ICカードは，内部データのアクセス管理機能により認証用の秘密鍵を読み出すことが不可能なことから，安全に鍵を保管することができるデバイスである．また，認証に必要な暗号化等の演算処理をカード内の独自プロセッサーによって行うことが可能であるため，安全な認証が実現される．しかし，ICカードによる認証では，秘密鍵を格納しているカード自体とサーバー間の認証に対しては相互の正当性を保証するが，ICカードを他人が拾った場合，拾い主が本人とみなされてしまうため，本人以外の人がカードを使えないように利用者を限定する仕組みを施す必要がある．現在のICカードでの利用者確認方法としては，パスフレーズや暗証番号の照合方式が主流であるが，登録したフレーズや暗証番号を忘れてしまうことや，容易に連想されるフレーズを用いることによる解読の容易さなどが問題となっている．このような問題に対して，情報を記憶する必要がなく，生涯不変，本人唯一の情報である身体的特徴（バイオメトリクス）を利用した認証方法が注目されている．

本研究では，正確性，利便性にすぐれ，現在最も普及しているバイオメトリクス認証である指紋認証[2]に着目した．従来の指紋認証方法としては，指紋画像のパターンマッチングを利用する方法[3]や，指紋の分岐や端点といった

E-mail: hiroyuki@isl.titech.ac.jp

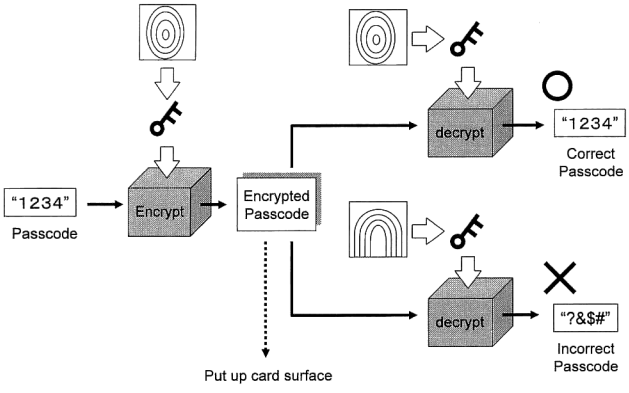

Fig. 1 The principle of the fingerprint verification to confirm the smart card holders. Only when the key made from own fingerprint is used in decryption, the correct passcode can be restored.

特徴点によるマッチングを利用する方法[4]が一般的であるが，指紋照合をICカード所持者の認証に適用する場合，いずれの方法も演算負荷の大きい画像処理が必要なため，演算能力がそれほど高くない現状のICカード内のプロセッサーで短時間に指紋照合を行うためには，処理する画像のサイズを小さくするなどの工夫が必要になる[5]．

そこで本研究では，演算負荷の大きい指紋照合は光学的な暗号化・復号化[6-8]の応用によるパターンマッチングで実装し，ICカード内ではパスコードの照合のみを行うハイブリッドな所持者確認システムを提案する．安全なICカードの所持者認証を実現するためには，不正プログラムが動作する危険性がないカード内での照合成否判定が必要になるが，これまでの光学的な指紋のパターンマッチングに関する研究[3]では，指紋画像の相関値によって照合成否の判定を行っており，これをICカード内で判定させた場合，高い相関値をICカードへ入力するだけで簡単に侵入されてしまうため，照合判定としては危険である．一方，カード内でのパスコード照合判定は，ある回数失敗したときのロック機能などにより，安全性の高い照合判定が可能である．本研究では，このパスコードを光暗号化手法で暗号化・復号化[6]し，そのときの暗号鍵を指紋から生成することで指紋のパターンマッチングを行い，本人の指紋で照合したときにのみ正しく復元されたパスコードを入力できるシステムを構築する．

本論文では，提案する認証システムの原理，特徴，認証手順などを説明し，今回のシステムで用いた認証用の鍵を指紋画像から生成する手法について述べる．また，提案システムの有効性を確認するために，指紋センサーを用いて実際に取得した指紋画像による計算機シミュレーションおよび指紋照合精度の評価を行った結果について報告する．

2. 提案システム

2.1 ハイブリッド認証システム

従来のICカードでは，暗証番号の照合により所持者の認証が行われる．利用者が入力した暗証番号はICカードに送られ，ICカード内部の機能により登録されている番号との一致を確認し，一致した場合にはカードが使用できるようになる．また，カードの紛失・盗難時の不正利用を防止するために，既定回数以上誤った番号を送るとカードはロックし，使用不可の状態になる仕組みが施されている．

提案するシステムは，暗証番号やパスコード照合によって所持者の確認を行う従来型のICカードの仕様を変更することなく実装する．指紋照合はICカード外部の演算により行うが，照合成否の判定はICカードのパスコード照合機能によりICカード内部で行う．基本的な所持者を確認する原理は次のようになる．Fig. 1に示すように指紋から生成した鍵を利用してパスコードを暗号化し，同様に指紋から生成した鍵でこの暗号化データを復号化する．このときの暗号化アルゴリズムとして，照合時に本人の指紋画像を入力したときのみ正しいパスコードが復元されるようなアルゴリズムを用いれば，正当な所持者のみがICカード内に正しいパスコードを入力することができる．また，暗号化されたパスコードをICカード表面に記録すれば，ICカード自身と登録指紋を結びつけられる．

しかし，一般的なディジタルデータの暗号技術では，暗号化・復号化に用いる鍵が1ビットでも間違っていると，正しく復号化できない．指紋画像をもとにして鍵を生成する場合，撮影環境や体調などにより多少の誤差が生じることから，完全に同一の鍵を毎回生成することは困難である．そこで，指紋画像から生成される鍵が多少違っても，本人であることが許容される暗号化手法が必要になる．このような要求に対して，本研究ではdouble random phase encodingによる光学的暗号化手法[6]を適用することを考えた．この光学的暗号化手法は，多少の誤差がある指紋画像から生成した鍵であっても正しい復号化画像が復元されるため，指紋照合に適用できると考えられる．

提案システムでは，暗号化データの記録のためにホログラムを利用することにより，記録されている暗号化データを読む際に特別な光学装置が必要となり，保存された暗号化データを読むことすら容易でないため，安全性の高い登録情報の保管が可能になる．また本システムでは，登録情報から指紋画像を復元することができないため，指紋画像の盗難や複製に対する安全性も高い．さらに，人間が記憶不可能な長いパスコードをICカードへ入力することも可

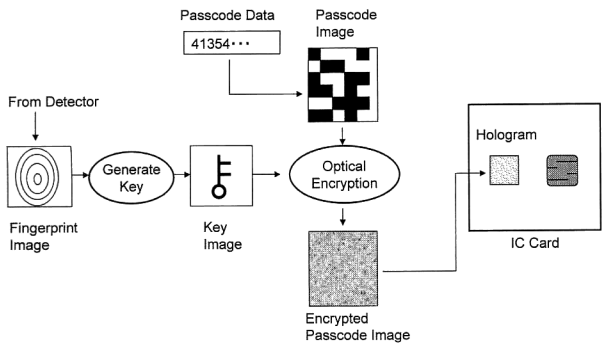

Fig. 2　Procedure of enrollment.

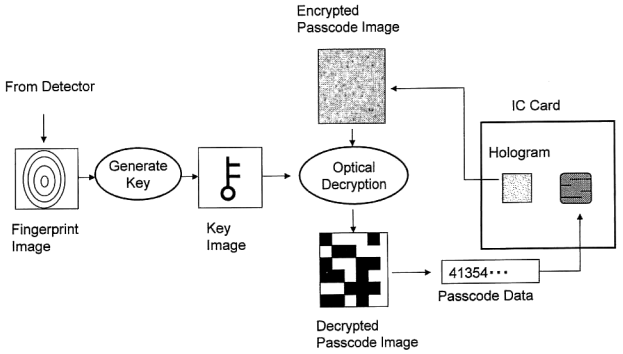

Fig. 3　Procedure of verification.

能であるため，利用者への負担を増やすことなくパスコード照合に対しての安全性も高められるシステムである．

具体的に認証を行う手順は以下のようになる．まず，パスコードをビットパターンとして画像化し，このパスコード画像を認証用のコードとして光暗号化する．そして，生成した複素振幅画像をホログラムとして記録し，このホログラムをICカードに貼りつける．これで所持者の登録が完了する（Fig. 2）．

所持者を確認する際には，ICカードに添付したホログラムに再生照明光を照射して得られる回折光に対して，確認者の指紋画像から生成した復号鍵を用いて復号化する．本人の指紋から生成した復号鍵が入力されていれば正しいパスコード画像が得られ，このパスコード画像をビット列に変換してICカードへ入力し，ICカード内でパスコードの照合を行うことで，所持者の確認が完了する（Fig. 3）．

2.2　光暗号化手法による指紋照合の原理

まず，光暗号化手法によってパスコード画像を暗号化する方法[6]を説明する（Fig. 4）．暗号化を行う元画像（ここではパスコード画像）$f(x,y)$ に対し，あるランダムパターン $R(x,y)$ を変調量とする位相変調を行い，これを $f_m(x,y)$ とする．そして，$f_m(x,y)$ をフーリエ変換し，フーリエ像 $F_m(u,v)$ に暗号鍵画像 $K_E(u,v)$ を位相物体として乗算することで，暗号化画像 $F_m(u,v)\exp\{jK_E(u,v)\}$ が生成される．

復号化の際は，ホログラムから再生した暗号化画像の共役像 $F_m^*(u,v)\exp\{-jK_E(u,v)\}$ に復号鍵画像 $K_D(u,v)$ を位相物体として乗算を行い，この画像 $F_m^*(u,v)\exp[-j\{K_E(u,v)-K_D(u,v)\}]$ をフーリエ変換すると，復号化画像 $f_r(x_d,y_d)$ が得られる．なお，文献6）をはじめとする従来の光暗号化の研究では，実空間での像を暗号化画像として定義しているが，フーリエ空間での像でも画像としては等価であるため，本論文ではフーリエ空間の像を暗号化画像として定義した．

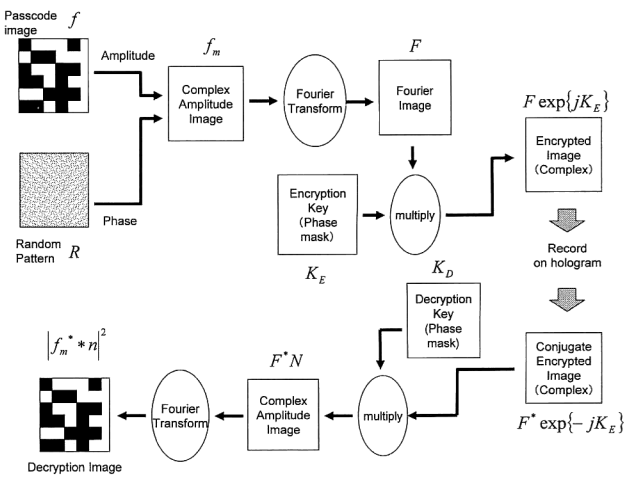

Fig. 4　Flow of optical encryption and decryption.

この光暗号化手法を利用して本人と他人を識別するためには，本人の指紋から生成した復号鍵で復号化した場合にはパスコード画像が正しく復元され，他人の指紋から生成した復号鍵では，パスコード画像がみえなくなることが要件となる．つまり，

$$\exp[-j\{K_E(u,v)-K_D(u,v)\}]=N(u,v) \quad (1)$$

とおき，$f_r(x_d,y_d)$ を

$$\begin{aligned} f_r(x_d,y_d) &= \Im[F_m^*(u,v)N(u,v)] \\ &= f_m^*(x_d,y_d) * n(x_d,y_d) \end{aligned} \quad (2)$$

（$n(x_d,y_d)=\Im[N(u,v)]$，$\Im[\ ]$ はフーリエ変換演算子を示す）

と表現したとき，この式（2）における本人識別に必要な条件は，

$$n(x_d,y_d)=\begin{cases}\delta(x_d-\alpha,y_d-\beta) & \text{（本人照合時）}\\ \text{random sequence} & \text{（他人照合時）}\end{cases} \quad (3)$$

である（$\delta(x_d,y_d)$ はDiracのデルタ関数，α，β は復号化画像の現れる座標を表す）．この式（3）を満たした場合，本人の指紋から生成した鍵を用いると，復号化画像は

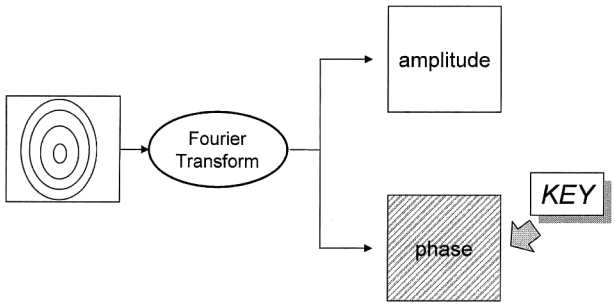

Fig. 5 Key generation method. The key image is the phase component of the Fourier-transformed fingerprint image.

$f_m^*(x_d-\alpha, y_d-\beta)$ となり正しいパスコード画像が復元され，他人の指紋から生成した鍵を用いたときは，復号化画像はランダム画像と元画像との畳み込み積分となる．また，

$$\mathfrak{F}[\exp\{-jK_E(u,\nu)\}]=g_E(x_d, y_d) \quad (4)$$

$$\mathfrak{F}[\exp\{-jK_D(u,\nu)\}]=g_D(x_d, y_d) \quad (5)$$

とおくと，$n(x_d, y_d)$ は

$$n(x_d, y_d)=g_E(x_d, y_d)\bigstar g_D(x_d, y_d) \quad (6)$$

（★ は相関演算を示す）

と記述できる．つまり光暗号化では，鍵画像から変換した $g_E(x_d, y_d)$ と $g_D(x_d, y_d)$ のパターンマッチングを行っており，パターンマッチングの出力結果と復元されるパスコードの再現精度を連動させることができる．よって，指紋画像から鍵画像を生成すれば，パスコードを出力とする指紋照合が実現できる．

2.3 暗号鍵の生成手法

2.3.1 鍵の要件

ここでは，本人と他人との識別性能，暗号化としての安全性という2つの面から，指紋画像を鍵画像へ変換する際に必要な要件を述べる．

まず，光暗号化を本人と他人の識別に用いるために必要な要件は，式（3）が近似的に成り立つことである．そのためには，登録時と同じ指紋を入力した場合には，指紋画像が多少異なったとしても，$n(x_d, y_d)$ に鋭いピークが現れる必要があり，また，登録時と異なる指紋を入力した場合には，たとえ指紋画像が似ていたとしても，$n(x_d, y_d)$ がランダムなパターンになる必要がある．ここで考慮すべき指紋画像撮影時の影響としては，位置ずれ，回転，形の歪み，画素値（濃度）のばらつき等である．ただし，提案システムでは照合時に登録指紋画像を参照することができないので，2つの指紋の相対位置のような相互関係の情報を利用しない鍵生成手法であることが条件になる．

次に，暗号化画像が高い暗号化強度を有するためには，光暗号化によって生成される暗号化画像が意味をもたない画像（理想的にはホワイトノイズ）になる必要がある．そのためには，暗号鍵がランダム画像（空間周波数成分の密度分布がほぼ均一）であること，画像としての空間分解能が十分に高いこと，および十分なビット数（画素数）を有することが必要になる．また，鍵のビット数が多ければ多いほど，暗号解読に対する安全性は高い．また，指紋の盗難や複製に対する安全性を考慮すると，指紋画像から暗号鍵への変換は，一方向性の不可逆変換であることが望ましい．

2.3.2 鍵生成手法

本論文では，上記の要件を考慮した暗号鍵生成の方法のひとつとして，指紋画像 $g(x', y')$（実数）をフーリエ変換した複素振幅画像

$$\mathfrak{F}[g(x', y')]=A_G(u,\nu)\exp\{jP_G(u,\nu)\} \quad (7)$$

の位相成分 $P_G(u,\nu)$ を光暗号の鍵とする（Fig. 5）．この手法を用いると，$n(x_d, y_d)$ が登録の際の指紋画像と照合の際の指紋画像との位相限定相関[9]となるため，本人の指紋画像同士では鋭いピークが現れ，本人と他人の場合はランダム系列に近い関数となり，式（3）が近似的に成立する．よって，この暗号鍵を用いた光暗号化手法では，登録時の指紋画像と照合時の指紋画像との位相限定相関によるパターンマッチングを行うことができ，また相関出力と元画像との畳み込み積分が復号化画像となる．このとき，暗号化画像がマッチトフィルターの役割を果たしている．

この鍵の大きな特徴は，指紋の平行な位置ずれに対して復号化画像が不変性を有することである．暗号化（登録時）と復号化（照合時）で撮影される指紋画像がシフトした場合，復号化のときの指紋画像 $g_s(x', y')$ は，暗号化のときの指紋画像 $g(x', y')$ を用いて

$$g_s(x', y')=g(x'+\Delta x, y'+\Delta y) \quad (8)$$

と書くことができる．これをフーリエ変換すると，

$$\mathfrak{F}[g_s(x', y')]=A_G(u,\nu)\exp[j\{P_G(u,\nu)+2\pi(u\Delta x+\nu\Delta y)\}] \quad (9)$$

となり，復号化の鍵 K_s は，暗号化のときの鍵 $K(=P_G(u,\nu))$ を用いて，

$$K_s(u,\nu)=P_G(u,\nu)+2\pi(u\Delta x+\nu\Delta y)=K+2\pi(u\Delta x+\nu\Delta y) \quad (10)$$

となる．よって，これらを式（2）の K_E，K_D にそれぞれ代入すると，復号化画像は，

$$\begin{aligned} f_r(x_d, y_d) &=\mathfrak{F}[F_m^*(u,\nu)N(u,\nu)] \\ &=\mathfrak{F}[F_m^*(u,\nu)\exp[j\{K(u,\nu)-K_s(u,\nu)\}]] \\ &=\mathfrak{F}[F_m^*(u,\nu)\exp[-j2\pi(u\Delta x+\nu\Delta y)]] \\ &=f_m^*(x_d-\Delta x, y_d-\Delta y) \end{aligned} \quad (11)$$

となり，指紋がシフトした分だけ復号化画像もシフトして再生される．

2.4 想定する光学系

Fig. 6 に，本システムを実現する光学系の例を示す．この光学系では，まず振幅変調素子としての LCD にパスコード画像を表示し，このフーリエ像を物体光としてホログラム面に照射する．また，位相変調素子としての LCD に表示した暗号鍵を参照光としてホログラム面に結像させ，2 つの光の干渉縞をホログラムに記録し，暗号化が行われる．復号化の際は，復号鍵を位相変調 LCD に表示し，これをホログラムに照射する．このとき再生される回折光のフーリエ像を観測することで，復号化されたビットパターンが得られる．

実際のシステムでは，IC カード表面にホログラムを貼りつけることを想定しているので，反射型のホログラムが必要になるが，Fig. 6 で示した光学系のホログラムの向きを変えることで反射型は実現できる．

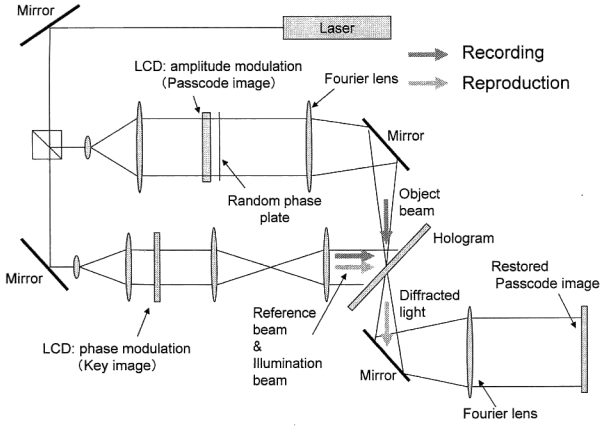

Fig. 6 Optical system for recording the encrypted image and reproducing the decrypted image.

3. 計算機シミュレーション

3.1 シミュレーション設定

記録するパスコード画像は，Fig. 7 の画像（8 ビット，256×256 ピクセル）を用いた．この画像は，“1234 ABCD” という文字列のコードを（0,1）のビット画像に変換したものである．

指紋画像は，静電容量方式の指紋センサー（NTT エレクトロニクス社製，指紋センサー LSI）によって，8 名の被験者（P1～P8）の人差し指をそれぞれ 6～10 枚ずつ取得した（枚数は Table 1 参照）．そして，各被験者のある 1 枚の指紋画像を登録用の指紋画像とし，残りの本人・他人のすべての画像を照合用の指紋として暗号化・復号化を行った．また，指紋センサーで取得される指紋画像サイズは 224×256，8 ビットグレースケール画像であるが，画像サイズを 256×256 へ拡張するために，まわりを画素値ゼロの画素で埋めて利用した．

なお，本論文で提案している指紋照合手法は，指紋のシフトに対して不変な照合結果を得られるように設計した照合手法である（2 章 3 節 2 項参照）が，実際の指紋照合では，指紋センサーの撮影範囲に収まる部分が一定でないため，シフト量が大きいと 2 つの指紋画像の共通部が少なくなり，照合精度が著しく劣化してしまう．この問題に対処する方法として，取得した指紋画像をディスプレイで確認し，目視で縦横約 50 ピクセル以上の位置ずれがあると判断した場合には，この指紋画像を評価対象からはずした．

システムの性能評価としては，まずパスコード画像の復

Table 1 The number of the fingerprint images that is used in simulation.

Experimental subject	P1	P2	P3	P4	P5	P6	P7	P8
Number of fingerprints	10	6	8	9	7	10	10	7

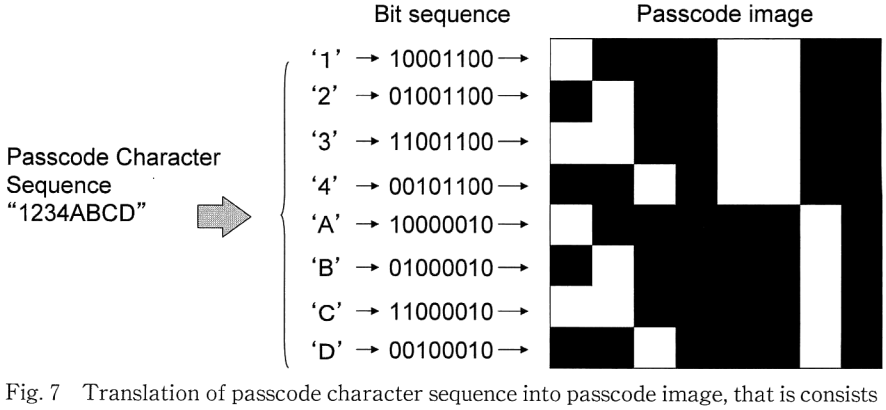

Fig. 7 Translation of passcode character sequence into passcode image, that is consists of binary bits; white and black bits show 1 and 0, respectively.

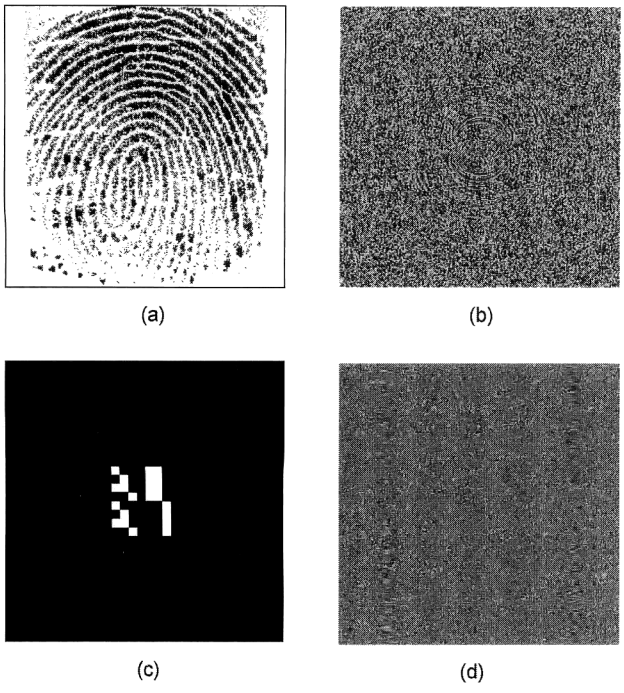

Fig. 8 Images used by computer simulation. (a) Fingerprint for enrollment, (b) Encryption key made from (a), (c) Original passcode image, (d) Hologram on which the encrypted image is recorded.

元具合を調べる方法として，復号化画像から変換されたコードのビットエラー率（bit error rate: BER）を求めた．BERは，以下の式で定義される．

$$\mathrm{BER}=\frac{N_{\mathrm{Error}}}{N_{\mathrm{PIN}}} \tag{12}$$

ここで，N_{PIN}はパスコードのビット数（ここでは8バイト＝64ビット），N_{Error}は復号化画像から抽出したパスコードのエラービット数である．また，BERがゼロとなる場合に照合成立とし，照合成立した指紋画像の枚数を数えることで本人排他率（false rejection rate: FRR）および他人許容率（false acceptance rate: FAR）を算出した．

なお，復元画像から実際にICカードへ入力するパスコードへの変換方法は，復号化画像からビットパターンの部分を切り出し，二値のビットパターンを8ビットの文字列へ復号することでパスコードが復元される．ただし，現段階ではビットパターンの位置検出方法については十分な検討を行っていないため，今回は暫定的な方法として，本来参照不可であるもとのパスコード画像を利用したビットパターンの切り出しを行った．具体的には，まず復号化画像ともとのパスコード画像との相関演算を行い，相関ピークの現れる座標を求め，この座標から復号化画像ともとのパスコード画像とのシフト量を算出する．シフト量が求まったら，ビットパターンが現れる部分の画像を切り出し，抽出したビットパターン画像に対して各ビットの平均画素値を計算する．この平均画素値がある閾値（今回は抽出したビットパターン部分全画素の平均画素値を閾値とした）より高いビットは“1”，低いビットは“0”として各ビットのバイナリー値を決定し，得られたバイナリー値を文字列として復号したものがパスコードとなる．

3.2 指紋画像の回転補正

本論文で提案した鍵生成手法では，指紋が平行移動しても正しいビットパターンが復元されるが，回転すると正しいビットパターンが得られない．しかし，平行移動と回転を同時に対処することは困難であるため，本稿ではこの問題を避ける手段として便宜的に，照合時に取得した指紋画像を少しずつ回転させて複数の照合用指紋画像を作成し，これらをすべて入力して得られたパスコードの中で最もBERが低いものを照合結果とした．回転角は，照合用の各指紋画像に対して0.2°間隔ずつ±10°の範囲で回転させ，計100枚の指紋画像を照合用の指紋画像とした．今回用いた回転補正手法では，回転角サンプリング間隔を細かくするにつれて本人排他率が改善（低下）していくが，この0.2°間隔という値は，回転角サンプリング間隔を徐々に細かくしながらシミュレーションを行ったときに，本人排他率が下限に達したときの値である．

3.3 暗号化・復号化シミュレーション結果

3.3.1 暗号化・復号化結果画像

登録の際に用いた指紋画像，生成した暗号鍵，記録したホログラムの例をFig. 8に示す．また，照合を行ったときの指紋画像，鍵画像，復号化画像の例をFig. 9に示す．この結果は，鍵画像Fig. 8(b)を使って登録（パスコードの暗号化）を行い，鍵画像Fig. 9(b)(e)を照合（復号化）に利用してシミュレーションを行った結果である．なお，Fig. 8(d)のホログラムは，光画像を仮定した複素振幅の暗号化画像に，入射角1°の平行光を照射したときにできる干渉縞を計算によって求めたホログラム画像である．この結果をみると，本人の指紋で照合したFig. 9(c)では，正しいパスコード画像が復元されており，登録時と照合時の指紋画像のシフト分だけビットパターンの位置もシフトして再生されていることが確認できる．この画像がノイズを多分に含んでいるのは，センサーによって制限される指紋の撮影範囲の違いがおもな原因であると考えられ，指紋の歪みや変形なども影響していると思われる．また，他人の指紋で照合したFig. 9(f)では，ランダムな画像になっており，もとのパスコード画像は復元されていないことが確認できる．これは，Fig. 8(b)とFig. 9(e)の差分がほぼランダム画像であるため，もとのパスコード画像にラン

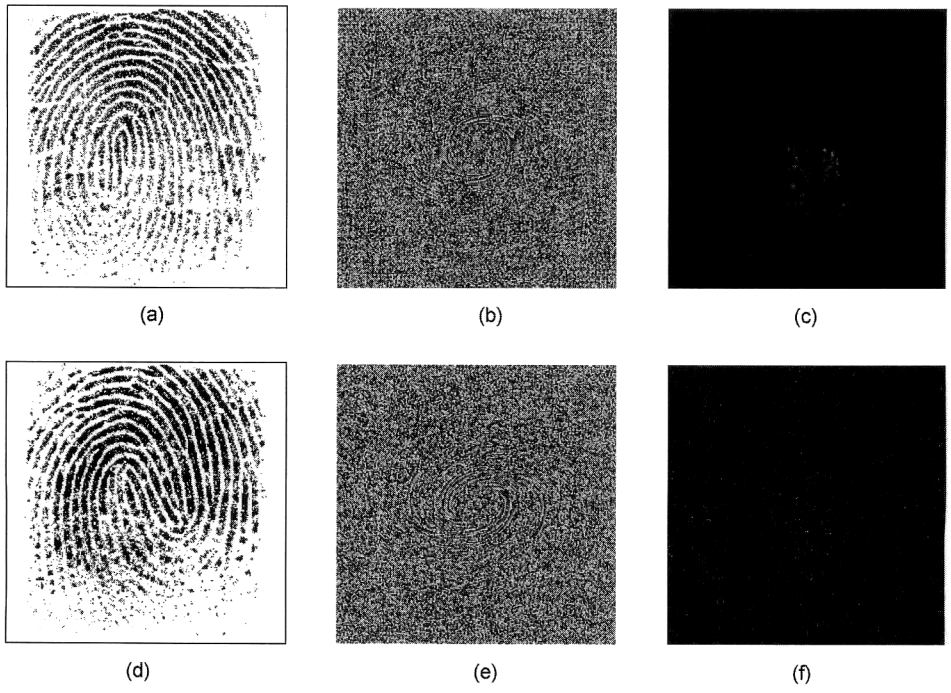

Fig. 9 Result images. It is confirmed that the correct passcode image is reconstructed using own fingerprint, and nothing appears using other's fingerprint. (a) Own fingerprint for verification, (b) Decryption key made from (a), (c) Decrypted image by (b), (d) Other's fingerprint for verification, (e) Decryption key made from (d), (f) Decrypted image by (e).

Fig. 10 This graph shows one sample of rotation angle vs. BER. In own fingerprint, BER goes down around a certain rotation degree.

ダム画像が畳み込み積分された結果である．

3.3.2 パスコード画像の復元評価および照合結果

まず，3章2節で述べた照合用指紋画像の回転角に対するパスコードのBERを調査した．Fig. 10は，本人と他人の照合用指紋画像1枚ずつについて，これらの画像を回転させた角度に対する復元されたパスコードのBERの関係を示している．この結果をみると，本人の指紋画像では，ある角度でBERが低い値をとり，他人の指紋画像では，どの角度でも高い値を保つことが確認できる．この傾向は，すべての被験者で同様であった．

他の指紋画像についても同様の処理を行い，8人の被験者から得られた平均BERの結果をTable 2に示す．また，FRR，FARを求めた結果をTable 3に示す．

この結果をみると，本人の指紋画像を入力した際の照合

Table 2　Bit error rate of all experimental testees.

Experimental subject	P1	P2	P3	P4	P5	P6	P7	P8	Average
BER (%) (own)	0.00	4.38	0.223	0.00	0.00	0.00	0.694	0.00	0.503
BER (%) (other's)	25.0	25.3	25.3	25.8	25.8	25.6	25.2	25.0	25.4

Table 3　False rejection rate (FRR) and false acceptance rate (FAR).

Experimental subject	P1	P2	P3	P4	P5	P6	P7	P8	Average
FRR (%)	0.00	60.0	14.3	0.00	0.00	0.00	33.3	0.00	11.9
FAR (%)	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

結果は個人差が大きく，完全に照合成立できる人とそうでない人に分かれた．今回の手法では，位置ずれおよび回転の影響は補正しているので，この原因は位置ずれや回転以外の要因（指紋の変形など）が影響していると考えられる．また，他人の指紋画像を入力した際には，完全に排他できることが確認できた．なお，完全なランダム画像から算出されるBERは50%になるはずだが，それより小さい値になっているのは，元画像と復号化画像との相関演算によってビットパターンの位置検出を行っているため，元画像に最も近いビットパターンが切り出されていること，および回転させた指紋画像によって得られる複数のBERの中から1つの照合結果を選ぶ際に，最もBERの小さいものを選択していることが原因である．

3.4 考　　察

今回の結果を既存の1対1の指紋照合システムと比較すると，FARについては十分に安全性の高い結果が得られたが，FRRはやや高い値になっている．この原因は，光暗号化手法による指紋のパターンマッチングにおける問題と復号化画像からビットパターンを抽出する精度の問題が考えられる．今回の照合では，相関演算による正確な位置検出を行っているため，後者の問題に大きな誤差があるとは考えにくい．よって，前者の問題が照合精度を劣化させる原因であると考えられる．この指紋照合手法を改善する方法としては，指紋を撮影する範囲の影響，指紋の歪みや傷等の変形，指紋画像の濃度分布の偏りなどを考慮したパターンマッチング手法などが考えられる．また，今回の回転補正にかかる計算時間が膨大であったので，高速に演算可能な回転不変手法の開発も必要になる．

4. ま　と　め

本稿では，指紋照合によるICカード所持者認証を安全かつ効率的に実現する手法として，光暗号化の鍵に指紋を適用して，指紋のパターンマッチングとパスコードの暗号化を組み合わせた認証手法を提案した．そして，実際の指紋画像でどの程度の照合精度が得られるかを調査するために，計算機シミュレーションを行った．その結果，この手法で所持者を認証可能であること，および照合精度として，本人を許容する能力に関しては既存の技術にはやや劣るが，他人を排他する能力については良好であることを確認した．

今回の論文では，認証を行う手法の検討のみを行ったが，今後は所持者認証システムを実現するために，指紋照合を行う光学系を構築し，復元されたパスコード画像を実際にICカードへ入力する実験を行う予定である．その際，光学系の実装方法や，実装と安全性の両方を考慮したパスコードのコーディング方法などを検討する．また，指紋照合精度の改善や，指紋の回転および大きな位置ずれに対して有効な指紋照合手法の検討も行う．

文　　献

1) 大山永昭："次世代ICカード元年"，エレクトロニクス，**46** (2001) 1-5.
2) 星野幸雄："指紋応用技術—(1) 指紋応用の歴史とシステム—"，画像電子学会誌，**31** (2002) 103-109.
3) 豊田晴義，吉田成浩，向坂直久，小林祐二，原　　勉："位相変調型空間光変調器を用いた光相関システム"，光学，**23** (1994) 315-320.
4) A. Jain: "On-line fingerprint verification," IEEE Trans. Pattern Anal. Machine Intell., **19** (1997) 302-314.
5) S. Ishida, M. Mimura and Y. Seto: "Development of personal authentication techniques using fingerprint matching embedded in smart cards," IEICE Trans. Inf. Syst., **E84-D** (2001) 812-818.
6) P. Refregier and B. Javidi: "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett., **20** (1995) 767-769.
7) B. Javidi and J. L. Horner: "Optical pattern recognition for validation and security verification," Opt. Eng., **33** (1994) 1752-1756.
8) B. Javidi and T. Nomura: "Securing information by use of digital holography," Opt. Lett., **25** (2000) 28-30.
9) J. L. Horner and P. D. Gianino: "Phase-only matched filtering," Appl. Opt., **23**, (1984) 812-816.