光復号，照合のための指紋画像の最適暗号化技術

山崎光寛

現在，さまざまなところで情報のセキュリティー確保が必要とされている．セキュリティー技術としてはディジタル方式のものが主として用いられているが，より高度に大量データを取り扱う場合に，暗号，復号，照合に時間がかかり過ぎるという問題がある．このような問題を解決するひとつの方法として光を用いたセキュリティーシステムが考え出されている[1,2]．本稿では，パスポートやクレジットカードなどを想定し，これらに本人であることの証を画像暗号として記載する方法と，その復号，照合を光で行うシステムについて考える．特に，暗号化として二値化ホログラムを使うが，その復号化像をよりよく再生するための暗号化パターンの最適化について報告する．

1. セキュリティーシステム

クレジットカードなどに，使用する本人であることを特定するために，指紋画像を暗号化して記載することを考える．この暗号化したパターンを光で読みとり，復号化し，さらに本人であることを照合する全体のセキュリティーシステムの概念を図1に示した．このシステムは，(a) 暗号化，(b) 復号化，(c) 照合の3つの部分からなる．このうち，暗号化はほかの2つの部分とは切り離すことができるが，復号化と照合は通常同時に処理されるため，ひとつの装置として考える必要がある．暗号化はいわば登録であり，この部分での実時間性の要求は厳しいものではない．それに対し，復号化，照合はリアルタイムで行われる必要がある．

暗号化において，指紋（S）をランダム暗号化キーで暗号化（Z）し，これをカードに記載する．このカードを使うときには，カード上の暗号化パターンを読みとり，同じ暗号化キーを使い光で復号化を行う．この復号化されたパターンと使う人の指紋との照合を行い，カードの保持者とカードに記載されている指紋とが一致するかどうかを同定する．復号，照合は光を使うことによりきわめて高速に処理することができる．また，光による高速性を生かせば，暗号化キーを多数用意しておくこともでき，暗号化キーの検索も含めて高いセキュリティー性を確保することが可能になる．

静岡大学大学院理工学研究科システム工学専攻（〒432-8561 浜松市城北 3-5-1）
E-mail: tajohts@ipc.shizuoka.ac.jp

2. 暗号化パターンの最適化

光を用いた画像の復号化に適した暗号化の方法として，結合フーリエ変換を用いたホログラムを作成することを考える[2]．この方法では，指紋画像にランダム位相マスクをかけたものをひとつの画像とし，これとランダム暗号化キーとの結合フーリエ変換により，ホログラムを作成する．カードへの記載の容易さ，ほかの入出力機器との整合性を考え，ホログラムは振幅の正負に応じた白黒の二値化パターンとして記録する．実際に復号するときには，この二値を（0，π）の位相パターンとして処理する．ホログラムは，暗号化キーと同じランダムパターンで再生され，指紋画像が復号される．ただし，ホログラムの二値化のため，再生像の元に比べ画質が低下する．この復号化像は，参照する指紋との光結合相関によって処理され，本人であることを同定するために用いられる．

より高いセキュリティー性を維持するために，復号化像を元の画像に近いものにする必要がある．これは，ホログラムを最適化することによって達成できる．図1の方式では，ホログラムを作るのに光システムを用いることもできるが，暗号化は先にも述べたようにリアルタイムである必要はないため，ホログラムをディジタル的に計算機により作り，最適化することができる．ここでは，二値化したホログラムを初期値として，シミュレーテッドアニーリング[3]により，暗号化キーで再生したときに，元の指紋画像に限りなく近くなるように，二値化パターンの分布を最適化した．ただし，ホログラムは二値化したものであるため，アニーリングのプロセスで（0，1）パターン（または（0，π）の位相）を反転させており，通常の微小摂動を加えるという意味でのシミュレーテッドアニーリングの方法とは多少意味合いが異なっている．

図2は，ランダム暗号化キーをリファレンスとして，ホ

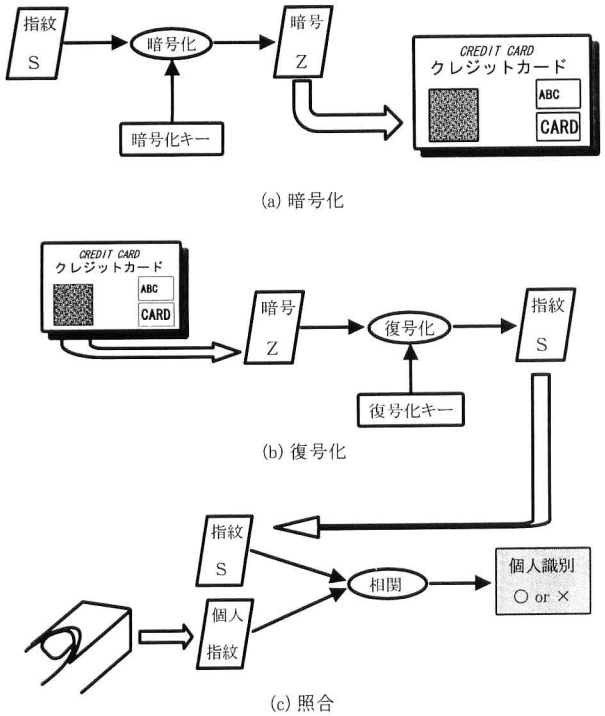

図1　セキュリティーシステムの概念．(a) 指紋画像の暗号化，(b) 復号化，(c) 照合．

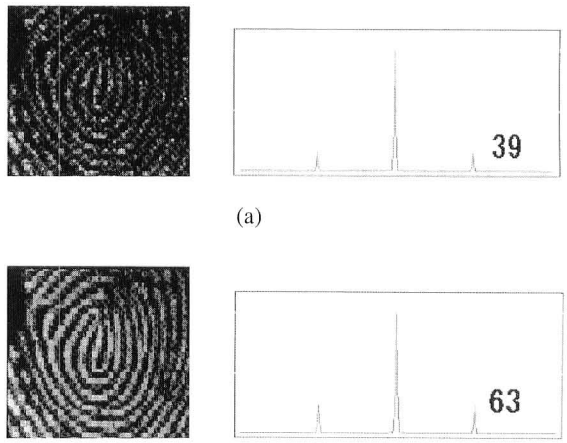

図2　暗号化ホログラムの最適化による復号化像．(a) 最適化前，(b) 最適化後．

ログラムを最適化したときの結果である．図2 (a) の指紋は，最適化する前の復号化画像である．暗号化に使った指紋画像の結合相関ピークの値が63であったのに対し，二値化によるホログラム再生の劣下のため，相関値は39に低下している．(b) は最適化されたホログラムの再生像であり，相関ピークの値も63と元と同じレベルまで回復している．指紋画像も元の画像と遜色ないほどに回復している．

指紋画像を暗号化し，それを復号，照合する光セキュリティーシステムの提案を行った．実際の用途を考え，二値化ホログラムを採用し，その最適化を行った．暗号化ホログラムの復号，照合は現状でも光を使って十分高速に処理できる．一方，ホログラムの最適化としてシミュレーテッドアニーリングを用いたが，この計算にはある程度の時間を要している．実際には，ホログラムあるいは暗号化キー自体がランダムであるため，アニーリングのプロセスは省略ができ，しかも収束はかなり早いことが確認できたが，より高精細な指紋画像の暗号化を考えると，最適化の方法にはまだ検討の余地がある．

光を用いたセキュリティーシステムとしてはいろいろと提案されているが，実際の使われ方に則した方法の提案と，それらを実証していくことが重要である．

文　　献

1) B. Javidi: "Securing information with optical technologies," Phys. Today, **50** (1997) 27-32.
2) H.-G. Yang and E.-S. Kim: "Practical image encryption scheme by real-valued data," Opt. Eng., **35** (1996) 2473-2478.
3) J. Ohtsubo and K. Nakajima: "Image recovery by simulated annealing with known Fourier modulus," Opt. Commun., **86** (1991) 265-270.

(2000年2月12日受理)