社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2006－CSEC－34 (59)
2006／7／21

画像マッチングに基づく生体認証に適用可能なキャンセラブルバイオメトリクスの提案

比良田真史† 高橋 健太† 三村 昌弘†

† (株) 日立製作所 システム開発研究所 〒215-0013 川崎市麻生区王禅寺 1099
E-mail: †{s-hirata,kenta,mmimura}@sdl.hitachi.co.jp

あらまし 生体認証において登録生体情報（テンプレート）の保護は重要である．個人が持つ生体情報の数は有限であるため自由に破棄・更新ができず，また生体情報は個人情報であるため漏洩時のリスクも大きい．これら課題への対策として，テンプレートを秘匿したまま認証を行うキャンセラブルバイオメトリクス技術が提案されている．本報告では，従来の画像マッチングに基づく生体認証に適用可能なキャンセラブルバイオメトリクスのアルゴリズムを提案する．また，実験により，提案方式は精度に影響を与えないことを示す．さらに，秘匿された特徴量の復元困難性を理論的に評価する．本研究により，画像マッチングに基づく生体認証に適用可能なキャンセラブルバイオメトリクスの実現への見通しつけた．

キーワード キャンセラブルバイオメトリクス，画像マッチング

A Proposal of Cancelable Biometircs for Image Matchig based biometrics

Shinji HIRATA†, Kenta TAKAHASHI†, and Masahiro MIMURA†

† Hitachi, Ltd., Systems Development Laboratory 1099, Ohzenji, Asao-ku, Kawasaki-shi, Kanagawa-ken, 215-0013, Japan
E-mail: †{s-hirata,kenta,mmimura}@sdl.hitachi.co.jp

Abstract It is important to protect biometric data (template) in biometric authentication systems. The risk due to exposure of biometric data is very high, because biometric data cannot be changed like a password and are kind of personal information. A model of "Cancelable Biometrics" has been proposed for the settlement with this problem. Biometric data is stored and verified in the transformed space in the model. In this paper, we propose a method for cancelable biometrics for image matching based biometrics and show experimentally that there exists no effect on the accuracy of verification . The probability of reproduction of original biometric data is also estimated theoretically. We have found a clue to realize a cancelable biometrics for image matching based biometrics.

Key words Cancelable biometrics, Image matching

1. はじめに

企業システムや行政システムのIT化に伴い，電子化された個人情報の保護が大きな課題となっている．特に生体情報は個人を特定し得る究極の個人情報とも言われており，生体認証システムの運用時には，登録生体情報（テンプレート）の厳格な管理が要求される．特に認証サーバ等のデータベースにテンプレートを保存する場合，システム管理者によるユーザ個人情報の持ち出しといった内部の不正を防ぐことは困難であり，プライバシの観点からユーザの心理的抵抗も大きい．また一人のユーザが認証に利用できる生体情報の数（例えば虹彩は2つ）には限りがあるため，一旦生体情報が漏洩すると，パスワードや鍵のように容易に破棄・更新することができない．以上の問題を解決するため，サーバに対して生体情報を秘匿しつつ認証を受けることが可能な，キャンセラブルバイオメトリクス[1]が提案されており，近年活発な研究・開発が行われている[2]～[4]．例えば文献[2]では2つの指紋画像を合成することによりキャンセラブル指紋認証を実現している．

本報告では，画像マッチングに基づく生体認証においてキャンセラブルバイオメトリクスを実現するアルゴリズムを提案する．以下，2章でキャンセラブルバイオメトリクスの概要を述べ，3章で画像マッチングに基づく生体認証に適用可能なキャンセラブルバイオメトリクスのアルゴリズムを提案し，精度保存性の実験的評価，復元困難性の理論的評価を行う．最後に，

5章で結論を述べる．

2. キャンセラブルバイオメトリクス

2.1 概　　要

本小節では，キャンセラブルバイオメトリクスの概要について述べる．

キャンセラブルバイオメトリクスは，2001年にRathaらによって初めて提案された，セキュリティとプライバシ強化型の生体認証モデルである．その概要を，ネットワークを介したサーバ・クライアント型の認証システムを例にとり，図1を用いて説明する．

ユーザ登録時，クライアントはユーザの生体情報を取得して特徴量 X を抽出する．次に，X を，パラメータ θ によって決まる関数 F_θ により変換し，変換特徴量 を $F_\theta(X)$ サーバに送信する．サーバはこれをテンプレートとして登録する．パラメータ θ はクライアントが保持し，サーバに対して秘匿する．

ユーザ認証時は，クライアントがユーザの生体情報を取得して特徴量 X' を抽出し，これを F_θ により変換して，変換特徴量 $F_\theta(X')$ をサーバに送信する．サーバは，テンプレート $F_\theta(X)$ と変換特徴量 $F_\theta(X')$ を照合し，照合値を計算する．サーバは元の特徴量 X，X' を知ることは出来ないが，X と X' の照合値を知ることは出来る．

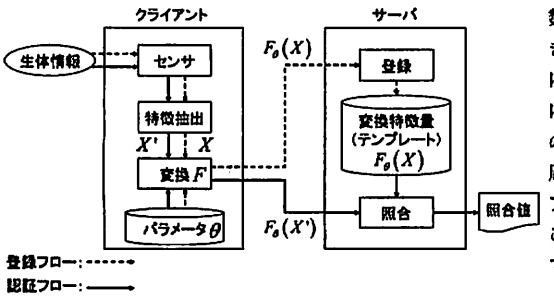

図1　キャンセラブルバイオメトリクスのモデル

このように，キャンセラブルバイオメトリクスは，生体情報を秘密の関数により変換した状態で登録および照合を行う．このため，サーバからテンプレートが漏洩したとしても，元の生体情報は秘匿されたままであり，偽造生体の作成に利用されるといったリスクが低減される．

なお，テンプレート保護のためにAES等の一般的なアルゴリズムで暗号化して保存し，認証時に復号化して照合する方法も考えられる．しかし，サーバ内に元の特徴量 X が存在してしまうため，悪意を持った管理者等による意図的な漏洩のリスクは残存する．キャンセラブルバイオメトリクスは，このような内部犯の対策としても有効である．

2.2 キャンセラブルバイオメトリクスの要件

本小節では，キャンセラブルバイオメトリクスの要件について述べる．

キャンセラブルバイオメトリクスを実現するためには，変換関数 を適切に設計することが重要である．具体的には，次の要件を満たす必要がある[3]．

（1）精度保存性

$F_\theta(X)$ と $F_\theta(X')$ から，照合値を正しく計算できること．一般に，変換後の状態で特徴量を照合すると誤差が生じ，変換を適用しない場合と比較して精度が劣化する可能性がある．変換による精度劣化が少ないことが重要である．

（2）復元困難性

θ を知らずに変換特徴量 $F_\theta(X)$ から元の特徴量 X を復元することが困難であること．復元が困難であるほど，テンプレート漏洩時のプライバシおよびセキュリティ上のリスクを低減できる．

3. 提案方式

3.1 相関不変ランダムフィルタリング

本小節では，画像マッチングに基づく生体認証においてキャンセラブルバイオメトリクスを実現するための変換として，相関不変ランダムフィルタリングを提案する．

まず，画像マッチングに基づく生体認証でキャンセラブルバイオメトリクスを実現するためのアプローチを説明する．照合値の計算が登録用と照合用2つの画像の相互相関関数の計算に帰着できるものとする．2つの画像を秘匿したまま相互相関関数を計算できれば，キャンセラブルバイオメトリクスを実現できる．2つの画像を秘匿したまま相互相関関数を計算するためには，フーリエ変換の畳み込みの性質が利用できる．この性質によれば，2つの画像の相互相関関数の計算は周波数空間上での掛け算に対応する（正しくは他方の画像は複素共役とする）．周波数空間上で，一方の画像には各成分にランダムな値を持つフィルタ $R(u,v)$ を掛け，他方の画像には $R^{-1}(u,v)$ を掛ける．これにより画像を秘匿できる．$R(u,v)R^{-1}(u,v)=1$ であるので，相互相関関数も正しく計算できる．

このアプローチに基づき，入力画像を秘匿したまま相互相関関数を計算可能とする変換を提案する．この変換を相関不変ランダムフィルタリングと呼ぶものとする．図2を用いて詳細を述べる．登録時には，登録用画像 $g(x,y)$ のフーリエ変換画像 $G(u,v)$ に対し，各成分がランダムな値を持つフィルタ $K(u,v)$ を掛ける．変換結果の $K(u,v)G(u,v)$ をサーバに登録する．認証時には，照合用画像 $f(x,y)$ のフーリエ変換画像の複素共役 $F^*(u,v)$ に対し $K^{-1}(u,v)$ を掛けて $K^{-1}(u,v)F^*(u,v)$ を生成し，$K(u,v)G(u,v)$ と積算する．$K^{-1}(u,v)F^*(u,v)K(u,v)G(u,v)=F^*(u,v)G(u,v)$ であるから，積算結果を逆フーリエ変換すると，$g(x,y)$ と $f(x,y)$ の相互相関関数 $w_{f,g}$ を求めることができる．これにより，$G(u,v)$ や $F(u,v)$ を秘匿したまま，つまり $f(x,y)$ や $g(x,y)$ を秘匿したまま，$f(x,y)$ と $g(x,y)$ の相互相関関数を計算することができる．

従来の画像マッチングに基づく生体認証アルゴリズムとしては例えば，[5]〜[8]がある．これら照合アルゴリズムの照合値の計算を相互相関関数の計算に帰着させたうえで相関不変ランダ

ムフィルタリングを適用することにより，キャンセラブルバイオメトリクスを実現することが可能である．

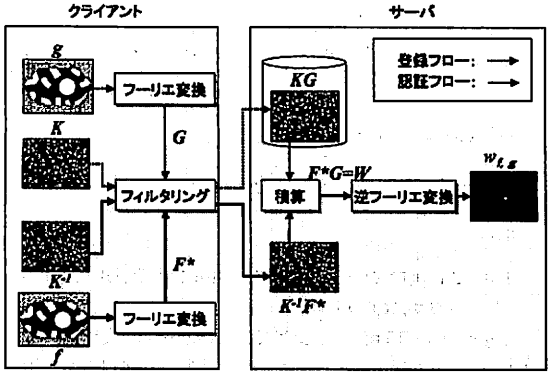

図 2　相関不変ランダムフィルタリングのフロー

3.2　あいまいビットを考慮した照合アルゴリズム

本小節では，画像マッチングに基づく生体認証アルゴリズムのうち特に，あいまいビットを考慮した照合アルゴリズムについて説明する．

あいまいビットを考慮した照合アルゴリズムとしては例えば，虹彩を用いた [9] や，静脈を用いた [10] などがある．これら照合アルゴリズムは，特徴部分と背景部分と信頼性の低い無効部分を定義することにより，通常の 2 値画像マッチングの照合と比較して認証精度を向上できるメリットがある．ここでは，あいまいビットを考慮した照合アルゴリズムの例として，以下のような 3 値画像マッチングの照合アルゴリズムを取り上げる．

登録用の 3 値画像を $g(x,y)$，照合用の 3 値画像を $f(x,y)$ とする．登録用の 3 値画像 $g(x,y)$ のサイズは $H_g \times W_g$，照合用の 3 値画像 $f(x,y)$ のサイズは $H_f \times W_f$ である．3 値画像の輝度値は，0,1,2 をとるものとする．0 は背景部分，2 は特徴部部分，1 は無効部分とする．

照合処理では，登録用の 3 値画像と照合用の 3 値画像を重ね合わせ，相違度 Rm を算出する．相違度 Rm は，両画像を相対的にずらしながら各ずれ位置 (p,q) での相違度 $Rm(p,q)$ を求め，その最小値とする．つまり，Rm は，

$$Rm = \min_{(p,q)\in S}\{Rm(p,q)\}$$

である．ただし，S は，ずれ位置 (p,q) の範囲全体の集合である．また，ずれ位置 (p,q) での相違度 $Rm(p,q)$ は，ずれ位置 (p,q) での両画像間で輝度値が異なるピクセル数 $Nm(p,q)$ と，登録用および照合用の 3 値画像の特徴部分の有効面積 $M(f,g)$ を用いて，以下のように定義する．

$$Rm(p,q) = \frac{Nm(p,q)}{M(f,g)} \qquad (1)$$

ここで，輝度値が異なるピクセルを数えるための関数 $\varphi(f(x,y,),g(x',y'))$ を，

$$\varphi(f(x,y,),g(x',y')) = \begin{cases} 1, & \text{if } |f(x,y)-g(x',y')| = 2 \\ 0, & \text{otherwise} \end{cases}$$

と定義すれば，$Nm(p,q)$ は，

$$Nm(p,q) = \sum_{(x,y)\in S(p,q)} \varphi(f(x,y,),g(x-p,y-q))$$

である．ただし，$S(p,q)$ は，ずれ位置 (p,q) で登録用 3 値画像 $g(x,y)$ と照合用 3 値画像 $f(x,y)$ とが重なる領域である．図 3 に，あるずれ位置 (p,q) で登録用 3 値画像 $g(x,y)$ と照合用 3 値画像 $f(x,y)$ が重なる様子，および $S(p,q)$ を示す．

このアルゴリズムに相関不変ランダムフィルタリングを適用することを考えた場合，相違度 $Rm(p,q)$ の計算を相互相関関数の計算に帰着させる必要がある．次の 3.3 節にて，相違度 $Rm(p,q)$ の計算が相互相関関数の計算に帰着できることを示す．

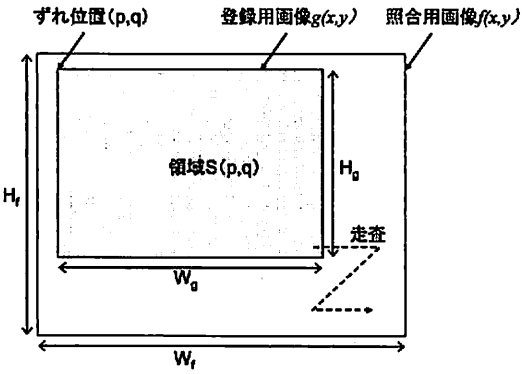

図 3　登録用と照合用の 3 値画像が重なる様子（模式図）

3.3　相違度 $Rm(p,q)$ の相互相関関数への帰着

本小節では，3.2 節で述べた 3 値画像マッチングのアルゴリズムに対し，相関不変ランダムフィルタリングを適用できるよう，相違度 $Rm(p,q)$ の計算式を式変形し，相互相関関数の計算に帰着できることを示す．

$Rm(p,q)$ は，式 (1) より，$Nm(p,q)$ と $M(f,g)$ から構成される．$M(f,g)$ は登録用と照合用の 3 値画像の有効面積のことであるから，この情報が漏れても元の特徴量の推測は困難であり，$M(f,g)$ を秘匿する必要は無いと考えられる．このため，$Nm(p,q)$ の計算を相互相関関数の計算に帰着させれば十分である．以下，$Nm(p,q)$ の式変形を行う．

まず，演算子 $\lfloor\ \rfloor$ を定義する．$\lfloor a \rfloor$ を実数 a を超えない最大の整数と定義する．これを用いれば，$\varphi(f(x,y,),g(x',y'))$ は，

$$\varphi(f(x,y,),g(x',y')) = \left\lfloor \frac{|f(x,y)-g(x',y')|}{2} \right\rfloor$$

である．$Nm(p,q)$ は，演算子 $\lfloor\ \rfloor$ を用いれば，

$$Nm(p,q)=\sum_{(x,y)\in S(p,q)}\lfloor\frac{f(x,y)}{2}\rfloor+\sum_{(x,y)\in S(p,q)}\lfloor\frac{g(x-p,y-q)}{2}\rfloor-\sum_{(x,y)\in S(p,q)}\lfloor\frac{f(x,y)g(x-p,y-q)}{2}\rfloor \quad (2)$$

となる.(証明は付録の1.を参照のこと.)

次に,$\hat{g}(x,y)$,$\hat{S}(p,q)$,$\hat{Nm}(p,q)$ を以下のように定義する.領域 $\hat{S}(p,q)$ は,領域 $S(p,q)$ を $f(x,y)$ のサイズに拡張したものと定義する.$\hat{g}(x,y)$ は,

$$\hat{g}(x,y)=\begin{cases}g(x,y), & \text{if } (x,y)\in S(p,q) \text{ かつ } (x,y)\notin \hat{S}(p,q)\\ 1, & \text{otherwise}\end{cases}$$

と定義する.$\hat{Nm}(p,q)$ は,

$$\hat{Nm}(p,q)=\sum_{(x,y)\in\hat{S}(p,q)}\lfloor\frac{f(x,y)}{2}\rfloor+\sum_{(x,y)\in\hat{S}(p,q)}\lfloor\frac{\hat{g}(x-p,y-q)}{2}\rfloor-\sum_{(x,y)\in\hat{S}(p,q)}\lfloor\frac{f(x,y)\hat{g}(x-p,y-q)}{2}\rfloor$$

と定義する.すると,

$$\sum_{(x,y)\in\hat{S}(p,q)}\lfloor\frac{\hat{g}(x-p,y-q)}{2}\rfloor=\sum_{(x,y)\in\hat{S}(p,q)}\lfloor\frac{g(x-p,y-q)}{2}\rfloor$$

であること,および $\hat{S}(p,q)$ 内であるが $S(p,q)$ には含まれない領域では,

$$\lfloor\frac{f(x,y)}{2}\rfloor=\lfloor\frac{f(x,y)\hat{g}(x-p,y-q)}{2}\rfloor$$

が成り立つことより,

$$Nm(p,q)=\hat{Nm}(p,q)$$

が成立する.したがって,$Nm(p,q)$ は次式となる.

$$Nm(p,q)=\sum_{(x,y)\in\hat{S}(p,q)}\lfloor\frac{f(x,y)}{2}\rfloor+\sum_{(x,y)\in\hat{S}(p,q)}\lfloor\frac{\hat{g}(x-p,y-q)}{2}\rfloor-\sum_{(x,y)\in\hat{S}(p,q)}\lfloor\frac{f(x,y)\hat{g}(x-p,y-q)}{2}\rfloor \quad (3)$$

また,$f'(x,y)$,$\hat{g}'(x,y)$ を次のように定義する.

$$f'(x,y)=f(x,y) \mod 2$$
$$\hat{g}'(x,y)=\hat{g}(x,y) \mod 2$$

$f(x,y)$ と $\hat{g}(x,y)$ の相互相関関数 $w_{f,\hat{g}}(p,q)$,$f'(x,y)$ と $\hat{g}'(x,y)$ の相互相関関数 $w_{f',\hat{g}'}(p,q)$ を次式で定義する.

$$w_{f,\hat{g}}(p,q)=\sum_{(x,y)\in\hat{S}(p,q)}f(x,y)\hat{g}(x-p,y-q)$$
$$w_{f',\hat{g}'}(p,q)=\sum_{(x,y)\in\hat{S}(p,q)}f'(x,y)\hat{g}'(x-p,y-q)$$

これにより,式(3)の第3項は,以下のように2つの相互相関関数の計算に帰着させることができる.

$$\sum_{(x,y)\in\hat{S}(p,q)}\lfloor\frac{f(x,y)\hat{g}(x-p,y-q)}{2}\rfloor=\frac{1}{2}\{w_{f,\hat{g}}(p,q)-w_{f',\hat{g}'(p,q)}\}$$

以上より,N_f,N_g を,

$$N_f=\sum_{(x,y)\in\hat{S}(p,q)}\lfloor\frac{f(x,y)}{2}\rfloor,\ N_g=\sum_{(x,y)\in\hat{S}(p,q)}\lfloor\frac{\hat{g}(x-p,y-q)}{2}\rfloor$$

と定義すれば,$Nm(p,q)$ は,

$$Nm(p,q)=N_f+N_g-\frac{1}{2}\{w_{f,\hat{g}}(p,q)-w_{f',\hat{g}'(p,q)}\} \quad (4)$$

となる.

3.4 3値画像マッチングにおけるキャンセラブルバイオメトリクスの実現方法

本小節では,相関不変ランダムフィルタリングを適用することにより,3.2節で述べた3値画像マッチングの照合アルゴリズムにおいてキャンセラブルバイオメトリクスを実現する方法について述べる.

式(4)の $Nm(p,q)$ の第1項,第2項は,登録用,照合用それぞれの3値画像の特徴部分のピクセル数のことであり,また $M(f,g)$ は登録用と照合用の3値画像の有効面積のことであるから,後の3.6節にて述べるように,これらの情報が漏れても元の特徴量の推測は困難と考えられる.そこで,式(4)の $Nm(p,q)$ の第3項のみに注目すれば十分である.以下,式(4)の第3項の計算に相関不変ランダムフィルタリングを適用することを考える.

$f(x,y)$,$f'(x,y)$,$\hat{g}(x,y)$,$\hat{g}'(x,y)$ のフーリエ変換をそれぞれ $F(u,v)$,$F'(u,v)$,$\hat{G}(u,v)$,$\hat{G}'(u,v)$ とする.また,$w_{f,\hat{g}}(p,q)$,$w_{f',\hat{g}'}(p,q)$ のフーリエ変換を $W_{F,\hat{G}}(u,v)$,$W_{F',\hat{G}'}(u,v)$ とすると,フーリエ変換の畳み込みの性質により,

$$W_{F,\hat{G}}(u,v)=F^*(u,v)\hat{G}(u,v)$$
$$W_{F',\hat{G}'}(u,v)=F'^*(u,v)\hat{G}'(u,v)$$

が成立する.これら $W_{F,\hat{G}}(u,v)$,$W_{F',\hat{G}'}(u,v)$ を逆フーリエ変換すれば,$w_{f,\hat{g}(p,q)}$,$w_{f',\hat{g}'(p,q)}$ が求められ,式(4)の $Nm(p,q)$ の第3項を計算できる.

$W_{F,\hat{G}}(u,v)$,$W_{F',\hat{G}'}(u,v)$ を保存したまま $F(u,v)$,$F'(u,v)$,$\hat{G}(u,v)$,$\hat{G}'(u,v)$ を秘匿する変換として相関不変ランダムフィルタリングを適用するには,以下のようにすれば良い.各成分が非ゼロのランダムな値を取るフィルタ $K(u,v)$,$K'(u,v)$ を作成する.$\hat{G}(u,v)$ に $K(u,v)$ を掛け,$\hat{G}'(u,v)$ に $K'(u,v)$ を掛け,これを登録用3値画像に対する変換とする.これにより $\hat{G}(u,v)$,$\hat{G}'(u,v)$ は秘匿される.また,各成分が $K(u,v)$,$K'(u,v)$ の逆数であるフィルタ $K^{-1}(u,v)$,$K'^{-1}(u,v)$ を作成する.$F^*(u,v)$ に $K^{-1}(u,v)$ を掛け,$F'^*(u,v)$ に $K'^{-1}(u,v)$ を掛け,これを照合用3値画像に対する変換とする.これにより $F^*(u,v)$,$F'^*(u,v)$ は秘匿される.ここで,

$$K^{-1}(u,v)F^*(u,v)\cdot K(u,v)\hat{G}(u,v)=F^*(u,v)\hat{G}(u,v)$$
$$K'^{-1}(u,v)F'^*(u,v)\cdot K'(u,v)\hat{G}'(u,v)=F'^*(u,v)\hat{G}'(u,v)$$

であるから，$W_{F,\hat{G}}(u,v)$，$W_{F',\hat{G}'}(u,v)$ は保存する．したがって，$W_{F,\hat{G}}(u,v)$，$W_{F',\hat{G}'}(u,v)$ を保存したまま $F(u,v)$，$F'(u,v)$，$\hat{G}(u,v)$，$\hat{G}'(u,v)$ を秘匿する変換となっている．

相違度 $Rm(p,q)$ を計算するには，$K(u,v)\hat{G}(u,v)$，$K'(u,v)\hat{G}'(u,v)$，$K^{-1}(u,v)F^*(u,v)$，$K'^{-1}(u,v)F'^*(u,v)$ のほかに，N_f と N_g が必要である．また，変換に用いるパラメータは登録時と認証時で異なり，登録時のパラメータを θ_e，認証時のパラメータを θ_v とすれば，

$$\theta_e = \{K(u,v), K'(u,v)\}$$
$$\theta_v = \{K^{-1}(u,v), K'^{-1}(u,v)\}$$

である．したがって，登録時にサーバに送信される変換特徴量 $F_{\theta_e}(X)$ は，

$$F_{\theta_e}(X) = \{K(u,v)\hat{G}(u,v), K'(u,v)\hat{G}'(u,v), N_g\}$$

となる．認証時にサーバに送信される変換特徴量 $F_{\theta_v}(X)$ は，

$$F_{\theta_v}(X) = \{K^{-1}(u,v)F^*(u,v), K'^{-1}(u,v)F'^*(u,v), N_f\}$$

となる．図 4 に登録時のフローを，図 5 に認証時のフローを示す．

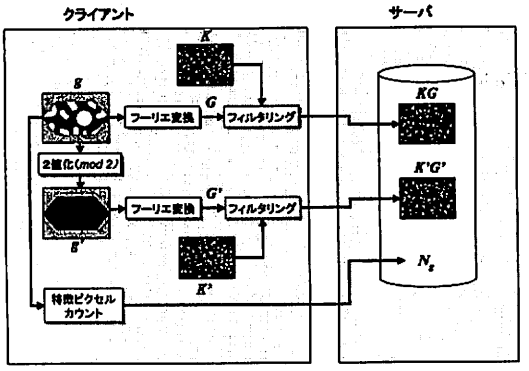

図 4　提案方式の登録時のフロー

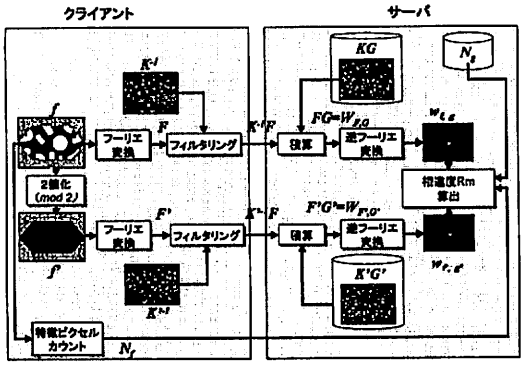

図 5　提案方式の認証時のフロー

3.5　精度保存性の実験的評価

本小節では，提案方式の精度保存性の実験的評価結果について述べる．ここでは，3.2 節で述べた 3 値画像マッチングの照合アルゴリズムを指静脈認証に適用する．指静脈認証と提案方式を適用したキャンセラブル指静脈認証とを PC 上で実装し，相違度 Rm の保存性を実験的に評価した．

実験には，登録用 426 指（各指 5 枚），照合用 426 指（各指 5 枚）の静脈画像を用いた．テンプレート作成に際しては各指 5 枚から最良な画像を選択した．テンプレートと照合用の全画像を用いて，同一指同士の照合 2130 件，異なる指同士の照合 905250 件，合計 907830 件の照合処理を行った．パラメータの各成分は，1 から 32767 までの整数からランダムに与えた．

実験の結果，全照合件数の 0.08% である 768 件で照合値に誤差があった．同一指同士の照合で誤差が生じたのは 1 件のみで，同一指同士の照合全件数に対する割合は 0.04% である．これより，誤差を生じている照合組み合わせの全てで照合値がしきい値を下回ってしまい本人拒否に含められるような最悪の場合でも，本人拒否率の劣化は 0.04% である．また，異なる指同士の照合で誤差が生じたのは 767 件で，異なる指同士の照合全件数に対する割合は 0.08% である．同様に，誤差を生じている照合組み合わせの全てで照合値がしきい値を上回ってしまい他人受入れに含められるような最悪の場合でも，他人受入れ率の劣化は 0.08% である．以上より，提案方式の適用による精度への影響は十分に小さく，精度保存性は高いと言える．なお，誤差の原因はフーリエ変換で生じる丸め誤差によるものと考えられる．

3.6　復元困難性の理論的評価

本小節では，提案方式の復元困難性を理論的に評価する．復元困難性とは，パラメータ θ を知らずに，変換特徴量 $F_\theta(X)$ から元の特徴量 X を復元することの困難さを指す．

攻撃者が変換特徴量 $F_{\theta_e}(X)$ のみ入手できると仮定した場合，元の特徴量 X を復元する方法として N_g からの復元が考えられる．以下，これについて元の特徴量 X を復元できる確率を見積もる．

特徴部分のピクセル数が N_g となる 3 値画像の候補数は，

$${}_{H_gW_g}C_{N_g} \times 2^{H_gW_g-N_g}$$

であるので，元の 3 値画像を復元できる確率 P は，

$$P = \frac{1}{{}_{H_gW_g}C_{N_g} \times 2^{H_gW_g-N_g}}$$

となる．ここでは H_g, W_g, N_g の値は例として $H_g = 200, W_g = 200, N_g = 20000$ とすると，

$$P = 3.97 \times 10^{-18060}$$

と見積もられる．これより，攻撃者が元の特徴量 X を復元できる確率は極めて小さいと言え，変換特徴量 $F_{\theta_e}(X)$ が漏洩しても偽造生体などによるなりすましのリスクは非常に低いと考えられる．

4. ま と め

画像マッチングに基づく生体認証に適用可能なキャンセラブルバイオメトリクスのアルゴリズム，およびこれを実現するための変換として相関不変ランダムフィルタリングを提案した．また，3値画像マッチングの照合アルゴリズムを指静脈認証に適用し，提案方式を実装し実験を行い，精度に影響を与えないことを示した．さらに，提案方式の復元困難性を理論的に評価し，復元が十分に困難であるとの見積もりを得，テンプレートが漏洩して偽造されるリスクが十分小さいことを示した．

本研究により，画像マッチングに基づく生体認証に適用可能なキャンセラブルバイオメトリクスの実現に見通しをつけた．

文　献

[1] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometric-based authentication systems," IBM System Journal, Vol.40, No.3, 2001.

[2] 森浩典, 鈴木裕之, 小尾高史, 山口雅浩, 大山永昭, "二つの個人識別情報を用いた相関演算によるキャンセラブルバイオメトリクス認証," 第53回応用物理学会関係連合講演会 講演予稿集, pp.1075, 2006.

[3] 高橋健太, 三村昌弘, "キャンセラブル指紋照合方式の提案," Computer Security Symposium 2005 論文集, pp.379-384, 2005.

[4] Marios Savvides, B.V.K. Vijayakumar, and Pradeep K.Khosla, "Authentication-Invariant Cancellable Biometric Filters for Illumination-Tolerant Face Verification," Proceedings fo SPIE, vol.5404, pp.156-163, 2004.

[5] 伊藤康一, 青木孝文, 樋口健雄, 中島寛, 小林孝次, "帯域制限位相限定相関法に基づく指紋照合アルゴリズム," 計測自動制御学会東北支部 第216回研究集会, 資料番号 216-15, 2004.

[6] Kazuyuki Miyazawa, Koichi Ito, Koji Kobayashi, Hiroshi Nkajima, "An Efficient Iris Recognition Algorithm Using Phase-Based Image Matching," IEEE International Conference on Image Processing, vol.2, pp.49-52, 2005.

[7] 宮武孝文, "静脈パターンを用いた個人認証," 光学, 33巻, 8号, 2004.

[8] Miyuki Kono, Hironori Ueki, and Shin-ichiro Umemura, "Near-infrared finger vein patterns for personal identification," Applied Optics, Vol.41, No.35, 2002.

[9] John Daugman, "How Iris Recognition Works," IEEE Transactions on Circuits and Systems for Video Technology, vol.14, No.1, pp.21-30, 2004.

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

付　録

1. 式(2)の証明

演算子 $\lfloor\ \rfloor$ を用いれば，$Nm(p,q)$ は，

$$Nm(p,q)=\sum_{(x,y)\in S(p,q)}\left\lfloor\frac{|f(x,y)-g(x-p,y-q)|}{2}\right\rfloor$$

である．

$$\left\lfloor\frac{|f(x,y)-g(x-p,y-q)|}{2}\right\rfloor=\left\lfloor\frac{|f(x,y)-g(x-p,y-q)|^2}{4}\right\rfloor$$

であるから，

$$Nm(p,q)=\sum_{(x,y)\in S(p,q)}\left\lfloor\frac{|f(x,y)-g(x-p,y-q)|^2}{4}\right\rfloor$$

である．ここで，

$$\left\lfloor\frac{|f(x,y)-g(x-p,y-q)|}{2}\right\rfloor^2$$
$$=\left\lfloor\frac{|f(x,y)-g(x-p,y-q)|^2}{4}\right\rfloor$$
$$=\left\lfloor\frac{|f(x,y)|^2}{4}\right\rfloor+\left\lfloor\frac{|g(x-p,y-q)|^2}{4}\right\rfloor-\left\lfloor\frac{2f(x,y)g(x-p,y-q)}{4}\right\rfloor$$

であり，また，

$$\left\lfloor\frac{|f(x,y)|^2}{4}\right\rfloor=\left\lfloor\frac{f(x,y)}{2}\right\rfloor$$
$$\left\lfloor\frac{|g(x-p,y-q)|^2}{4}\right\rfloor=\left\lfloor\frac{g(x-p,y-q)}{2}\right\rfloor$$
$$\left\lfloor\frac{2f(x,y)g(x-p,y-q)}{4}\right\rfloor=\left\lfloor\frac{f(x,y)g(x-p,y-q)}{2}\right\rfloor$$

であるから，

$$\begin{aligned}Nm(p,q)&=\sum_{(x,y)\in S(p,q)}\left\{\left\lfloor\frac{f(x,y)}{2}\right\rfloor+\left\lfloor\frac{g(x-p,y-q)}{2}\right\rfloor-\left\lfloor\frac{f(x,y)g(x-p,y-q)}{2}\right\rfloor\right\}\\&=\sum_{(x,y)\in S(p,q)}\left\lfloor\frac{f(x,y)}{2}\right\rfloor+\sum_{(x,y)\in S(p,q)}\left\lfloor\frac{g(x-p,y-q)}{2}\right\rfloor-\sum_{(x,y)\in S(p,q)}\left\lfloor\frac{f(x,y)g(x-p,y-q)}{2}\right\rfloor\end{aligned}$$

となる．(証明終わり)