情報処理学会論文誌　Vol. 50　No. 9　2077–2087 (Sep. 2009)

Fuzzy Fingerprint Vault Schemeによるバイオメトリック暗号のロック情報作成手法

大木哲史[†1]　披田野清良[†2]
小松尚久[†2]　笠原正雄[†3]

バイオメトリック認証においてシステムに保管されている情報は，個人の生体情報であり，情報が漏洩した際に本人を特定される危険性がある．そこで本稿では，個人テンプレートを暗号化して保管するバイオメトリック暗号方式の一例として，個人テンプレートと提示したバイオメトリック情報から秘密情報を生成する方式である Fuzzy Vault Scheme を用い，秘密情報と秘密情報の取得に用いる個人テンプレートをシステムに保管された情報からは復元できない対策を施すとともに，本人のバイオメトリック情報を用いて秘密情報を生成可能とする手法を提案する．また提案手法の指紋照合への適用を提案し，秘密情報の復元可能性とテンプレート安全性についてシミュレーションを交え考察する．

A Locked-data Generating Method for Biometric Cryptosystem Using Fuzzy Fingerprint Vault Scheme

Tetsushi Ohki,[†1] Seira Hidano,[†2] Naohisa Komatsu[†2] and Masao Kasahara[†3]

Conventional biometric authentication systems simply store each user's template as is on the system. If registered templates are not properly protected, the risk arises of template leakage to a third party and impersonation using biometric data restored from a template. We propose a technique that encrypts and stores the user template and uses a "fuzzy vault scheme" to generate secret data from the user template and the query biometric data. It incorporates a measure to prevent the secret data and the user template used to obtain the secret data from being recovered from information stored in the system, and it enables the secret data to be generated from the user's biometric data. In this paper, we describe an application of our technique to fingerprint matching. We also describe simulations performed using this fingerprint matching system to examine the probability of secret data recovery and the level of secret data security.

1. Introduction

バイオメトリック認証は本人の意識に依存せずに安全性が確保でき，また記憶，所持の煩わしさから解放されるなどの利便性の面からも特長があり，入退室管理，ネットワークアクセスなどのアクセスコントロール，ネットワークバンキングなどのフローコントロール，またサーベランスシステムなどトラッキングへの展開が期待されているが，利用者，環境条件，運用条件，生体情報，バイオメトリクス装置といった様々な要素において脆弱性が存在しており，それぞれの脆弱性への対策が今後の展開への重要な課題となっている[1)]．

バイオメトリック認証では，指紋，顔，血管パターンといった個人の身体的特徴や筆跡，音声といった身体的特性などの個人に固有の情報を抽出し，登録者の属性などを加えて保管する（以下，個人テンプレート）．ネットワーク利用によりバイオメトリック認証がエンドユーザへ広く普及すると，テンプレートの保護がきわめて重要な対策の 1 つとなる．これはエンドユーザにはテンプレートを安全に管理する専門知識が必ずしも十分でないことに起因する．このようなエンドユーザにおける専門知識の不十分さによってバイオメトリック認証の普及が阻害されてはならない．こうした背景から，本稿ではバイオメトリック認証におけるテンプレート漏洩に着目して，その一対策を提案する．現在ヒルクライミングアタック[2)]などによるテンプレート漏洩への対策は，これまでにもいくつかの方式が提案されており，これらはテンプレート保護型バイオメトリック認証方式と呼ばれる．代表的な研究事例としてはテンプレート画像の幾何変形や相関性のあるハッシュ関数を用いてテンプレート画像を変換する手法である Cancelable Biometrics[3)–5)] や，ゼロ知識証明プロトコルを利用して生体情報をリモートサーバに提示することなく認証が可能な非対称生体認証方式[6)–8)] といったものがある．しかし，前者には幾何変形のパターンが限られるため秘匿性が必ずしもつねに十分達成できず，また変換パラメータの管理が必要になるという問題がある．さらに後者

†1 早稲田大学理工学研究所
Research Institute for Science and Engineering, Waseda University
†2 早稲田大学理工学術院
Faculty of Science and Engineering, Waseda University
†3 大阪学院大学情報学部
Faculty of Informatics, Osaka Gakuin University

では計算量や通信量が大きいという問題や，精度に関して十分な考察がなされていないという問題がある．このような問題から，いずれの研究も安全性と可用性を同時に満たす手法の実現には至っていない．そこで本稿では，個人テンプレートを暗号化して保管するバイオメトリック暗号方式の一例として，個人テンプレートと提示したバイオメトリック情報から秘密情報を生成する方式である Fuzzy Vault Scheme を用い，秘密情報と秘密情報の取得に用いる個人テンプレートをシステムに保管された情報からは復元できないように対策を施すとともに，本人のバイオメトリック情報を用いて秘密情報を生成可能とする手法を提案する．

Fuzzy Vault Scheme は，2002 年に Juels らによって提案された，任意の情報の組を用いて秘密の情報を秘匿する手法であり，登録，照合に用いる情報の組は大部分が一致すればよい点を特徴としている[9]．生体情報は不安定な情報であり，本人であっても毎回わずかに異なる情報が得られるが，Fuzzy Vault Scheme を用いることによりわずかに異なる情報であっても正しい情報を取得することが可能となるため，バイオメトリック情報を扱うのに適した手法といえる．

本手法では，秘密情報は登録したテンプレートと提示したバイオメトリック情報から生成される．このためテンプレートの安全性だけでなく秘密情報の秘匿性にも優れている点を特徴としている．また，秘密情報として秘密鍵を指定することができるため Challenge Handshake Authentication Protocol（CHAP）[10] などの認証プロトコルとの親和性が高い手法である．すなわち，サーバへ置いた公開鍵との検証を行い，復元した秘密鍵の正当性を検証することによって，クライアント認証とユーザ認証を同時に実現できる．また，テンプレートの形式を問わないため，指紋だけでなく様々なモダリティへの応用が可能である．本稿では，まず Fuzzy Vault Scheme の概要とバイオメトリック認証への応用について説明する．次いで提案手法の指紋照合への適用を提案する．さらに指紋照合方式に関しては秘密情報の復元可能性とテンプレートの安全性についてシミュレーションを交え考察する．

2. Fuzzy Vault Scheme を用いた Biometric Cryptosystem

Fuzzy Vault Scheme は，2002 年に Juels らによって提案された，任意の情報の組を用いてある情報を秘匿する手法である[9]．まず，ロック過程において秘匿したい秘密情報 S を任意の情報セット P を用いて解読不可能な状態に変換する．そして，アンロック過程において P と同じ形式の情報セット Q を与え，P と Q の大部分が一致すれば S を復元することができる．

Fuzzy Vault Scheme をバイオメトリック認証へ適用する際は，秘密情報 S を任意の情報

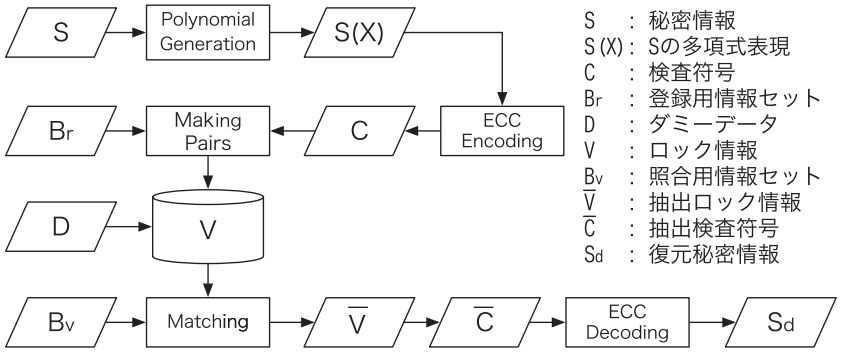

図 1　Fuzzy Vault Scheme を用いたバイオメトリック暗号
Fig. 1　Biometric Cryptosystem using Fuzzy Vault Scheme.

とし，ロック用情報セット B_r，アンロック用情報セット B_v にバイオメトリック情報を適用する．アンロック過程における秘密情報の復元には誤り訂正符号を用いる．Fuzzy Vault Scheme を用いたバイオメトリック暗号の概要を**図 1** に示す．

2.1　テンプレート情報の作成

2 を法とする拡大次数 m のガロア体 $GF(2^m)$ 上の k 個の情報からなる秘密情報 $S = \{S_1, S_2, \cdots, S_{k-1}, S_k\}$，$g$ 個の要素からなるロック用バイオメトリック情報 $B_r = \{B_{r_1}, B_{r_2}, \cdots, B_{r_{n-1}}, B_{r_g}\}$ を用意する．ここで，S の要素を各次数の係数とする多項式 $S(X)$ を作成する．

$$S(X) = S_1 + S_2X + \cdots + S_kX^{k-1}$$

以後，$S \rightarrow S(X)$ といった表記は $S(X)$ と同様に各要素を多項式表現したものとして扱う．$S(X)$ を情報符号と見なし，これを最大距離分離符号である Reed-Solomon 符号（以下，RS 符号）に符号化する．g 次の生成多項式 $G(X)$ を用いて $S(X)$ を符号化し，検査符号 $C = \{C_1, C_2, \ldots, C_i, \cdots, C_{g-1}, C_g\}$ を作成する．以上より，RS 符号により S を符号化した符号語 F を次式で表す．

$F = \{C_1, C_2, \cdots, C_g, S_1, S_2, \cdots, S_k\}$

$GF(2^m)$ 上の RS 符号における最大可能な符号長は $2^m - 1$ である．これに対し，本手法において符号 F の符号長を $k + g \leq 2^m - 1$ なる条件のもとに短縮して用いている．このため，本手法では最大可能な符号長を短縮して用いる．短縮された部分はすべて 0 シンボ

ルとして扱うことができ，通常復号法を短縮されていることを考慮せずに用いることができる．なお，このように符号長を生成多項式の周期より短くした符号は一般に擬巡回符号（quasi-cyclic codes）と呼ばれている．得られた情報 F のうち $S_1 \cdots S_k$ は削除し，C と B_r の間でペアを生成してテンプレート情報 T とする．

ここで，検査多項式を正しく復元するために参照番号 L を作成する．L_i は検査多項式上の要素 C_i を係数とする項の次数となる．したがって L は次式で表せる．

$$L = \{L_1, L_2, \cdots, L_i, \cdots, L_g \mid L_i = i\}$$

ロック用バイオメトリック情報 B_r，検査符号 C，参照番号 L の i 番目の要素をそれぞれ B_{r_i}，C_i，L_i とし，テンプレート情報 T を次式で表す．

$$T = \{T_1, T_2, \cdots, T_i, \cdots, T_{g-1}, T_g\}$$

$$T_i = \{B_{r_i}, C_i, L_i\}$$

2.2　ダミーデータの付加

Fuzzy Vault Scheme をバイオメトリック認証へ適用する際は，セキュリティ上ダミーデータの付加は必須である．ダミーデータを付加することで，テンプレート情報が漏洩した際に，成りすましやバイオメトリック情報の復元を困難とする．ロック情報 V が r 個のペアで構成されるとすれば，ダミーデータ D は次式で表せる．

$$D = \{D_1, D_2, \cdots, D_i, \cdots, D_{r-g-1}, D_{r-g}\}$$

$$D_i = \{\alpha_i, \beta_i, \gamma_i\}, \alpha_i \notin B_r, \beta_i \notin C, \gamma_i \in L$$

また，γ_i の値に偏りがある場合，ロック用バイオメトリック情報や検査記号が容易に特定される危険性が生じるため，γ_i は 1〜g の値が均等の確率で出現するように考慮する．テンプレート情報 T にダミーデータ D を加えてロック情報 V とする．セキュリティの観点からロック情報に含まれる各ペアをランダムにシャッフルした後にシステムへ保存する．

2.3　誤り訂正符号による秘密情報の復元

秘密情報を復元する際は，アンロック用バイオメトリック情報 B_v を提示する．アンロック時に n 個の要素が取得できるとすれば

$$B_v = \{B_{v_1}, B_{v_2}, \cdots, B_{v_{n-1}}, B_{v_n}\}$$

となる．そして，B_v とロック情報 V に含まれるバイオメトリック情報とでマッチングを行い，マッチしたペアを抽出ロック情報 $\bar{V}$ とする．マッチングにより t 個のペアが得られたとすると，抽出ロック情報は次のように表される．

$$\bar{V} = \{\bar{V}_1, \bar{V}_2, \cdots, \bar{V}_t\}$$

得られた抽出ロック情報 $\bar{V}$ に含まれる検査符号から抽出検査符号 $\bar{C}$ および抽出検査多項式 $\bar{C}(X)$ を作成する．得られた検査多項式 $\bar{C}(X)$ を誤り訂正復号器へ入力することで $S(X)$ が復元され，$S(X)$ の係数より S_d が生成される．ここで B_r と B_v の類似性が高ければ，$S = S_d$ となり，秘密情報 S が復元される．

2.3.1　秘密情報復元のための条件

ここで，ロック情報 V から正しい秘密情報 S を復元するための条件について述べる．g 個の検査符号 $C_1, C_2, \ldots, C_g$ を持つ誤り訂正符号の最小距離 d は $d = g + 1$ で与えられる．誤り訂正符号により S を復元するためには

$$\text{消失誤り数} + 2 \times \text{ピュア誤り数} + 1 \leq d \tag{1}$$

なる関係が成り立てばよい．ここで，マッチングによって取得した t 個の要素のうち m_t 個が S から生成した正しい検査符号を持つペアであるとする．秘密情報 S は消失誤りとしており，その要素数は k である．したがって，$g - m_t$ 個がピュア誤りと考えられるので

$$k + 2(g - m_t) + 1 \leq d \tag{2}$$

なる関係が得られる．これを m_t について解くと，

$$m_t \geq \frac{k + g}{2} \tag{3}$$

となる．ここではピュア誤りの個数を $g - m_t$ 個と定義しているが，本手法は参照番号 L により検査符号が検査多項式のどの項に対応するかを特定している．このためマッチングにより得られなかった項は消失誤りとして扱える．またダミーデータとの誤一致により取得された検査符号についてはピュア誤りとなる．消失誤りの個数（以下，消失数 e）はダミーデータとの誤一致数（以下，誤一致数 m_f）を用いて次のように表せる．

$$e = g - m_t - m_f \tag{4}$$

式 (4) を式 (1) に代入し，k について解くと次式が得られる．

$$k \leq m_t - m_f \tag{5}$$

以上より，一致数 m_t と誤一致数 m_f の差が秘密情報要素数 k より大きくなることが秘密情報復元の条件である．

2.3.2　ダミーデータとの誤一致による影響

アンロック時に，ダミーデータとの誤一致が発生した場合，対応する検査多項式の次数が同一の検査記号が複数得られることがある．この場合，次のような対策が考えられる．

(1)　一致した複数の検査記号から単一の検査記号を無作為に選択

(2)　該当する次数を消失誤りと判定

ここで，ピュア誤り数，消失誤り数，最小距離と，誤り訂正条件との関係は式 (1) によって

表せる．したがって，同一の次数に対して 3 つ以上の検査記号の候補が得られた場合，無作為に選択を行うよりも消失誤りとして扱うほうが，誤り訂正が可能となる確率が高いことが分かる．以上の理由から，本手法ではダミーデータとの誤一致により対応する検査多項式の次数が同一の検査記号が複数存在した場合，その次数は消失誤りとして扱うこととしている．

3. Fuzzy Fingerprint Vault Scheme

Fuzzy Vault Scheme のバイオメトリック認証への適用例として，指紋情報を用いて秘密情報を秘匿するバイオメトリック暗号について述べる．ロック過程では，提示された指紋から特徴点を取得し，秘密情報 S をロックする．アンロック過程では，提示された指紋から取得した複数の特徴点と，ロック過程において提示された特徴点を比較し，あらかじめ設定した割合の特徴点が一致すると秘密情報 S が復元可能となる．

3.1 円形エリアを用いた指紋特徴量の記述

指紋認証では，認証器へ指を置く際の位置ずれや角度ずれにより，正規ユーザが正しく認証されないことがある．また，マニューシャ情報として，特徴点の位置情報に座標情報を用いた場合，テンプレート情報がシステムから漏洩した際に，マニューシャ情報から元の指紋情報を推測される危険性が増大する[11]．これらの問題への対策として，円形エリアを用いて，位置ずれや角度ずれの影響を受けにくい指紋特徴量の記述を行う．本手法ではロック過程において取得されるマニューシャ情報を M_r，アンロック過程において取得されるマニューシャ情報を M_v とし，マニューシャ情報を次の 3 つのパラメータで構成する．

(1)　マニューシャが含まれるエリアを表す位置情報（以下，エリア情報 f）
　　各エリアは指紋の中心点を基準として指紋情報を複数分割して作成される．
(2)　隆線の端点，分岐点を表す値（以下，属性情報 a）
(3)　マニューシャの隆線ベクトルの角度
　　2π を 32 分割し，0 から 31 レベルで表現した値（以下，角度情報 θ）．したがって，1 レベルは 11.25 度に相当する．

マニューシャ情報 M の i 番目の要素は次式で表せる．

$$M = \{M_1, M_2, \cdots, M_i, \cdots, M_{g-1}, M_g\}$$
$$M_i = (f_i, a_i, \theta_i)$$

指紋画像を分割しエリアを作成する際，エリアの形状を正方形とした場合，各エリアにおいて中心から境界線までの距離が一定とならず，斜め方向への位置ずれ許容が大きくなる．

図 2　円形エリアの概要
Fig. 2　Generating of circular areas.

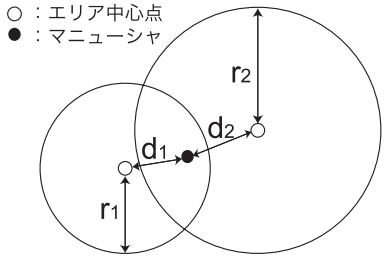

図 3　エリア重複部分のマニューシャ
Fig. 3　Minutiae of overlapped area.

そこで，位置ずれに対する揺らぎの許容範囲を均一にするために円形のエリアを用いることとした．以下，これを円形エリアとする．マニューシャは中心点に近いエリアに多く存在し，外縁に近づくほど少なくなる傾向がある．したがって**図 2** に示すように円の半径を中心ほど小さく，外縁ほど大きくなるようにエリアを設計する．本稿では予備実験（付録 A.2 参照）により各エリアに含まれるマニューシャ数が一定となるように各エリアの半径を設定した．

マッチングを行う際には，位置ずれによるエリア情報の差異を考慮して，一定範囲の誤差を許容したエリア情報の比較を行うこととする．アンロック用マニューシャが特定のエリアに含まれるかを判定する際は，円形エリアの中心からアンロック用マニューシャまでの距離を d，円形エリアの半径を r をとし，d/r を一致判定のパラメータとする．この値が閾値以下であればエリア情報が一致していると判定する．ただし，**図 3** に示すように，ロック過程においてエリアの重複領域にマニューシャが存在する場合，マニューシャを含む複数のエリアにおいて各々の d/r の値を求め，その値が最小となるエリアに属すると判定する．これにより，アンロック用指紋情報の位置情報の揺らぎに対応するだけではなく，円形エリアの重なりに存在するマニューシャへの対応を可能とする．

ダミーデータ付加時にはロック用マニューシャとダミーデータ，およびダミーデータどうしが一致しないようにダミーデータを付加する必要がある．この際のエリア一致判定に用いるパラメータ d/r をダミーデータ作成用閾値と定義する．また，アンロック用マニューシャとロック情報とのマッチング時にエリア一致判定に用いるパラメータ d/r を照合誤差許容閾値と定義する．

4. 指紋特徴を考慮したダミーデータ作成手法

秘密情報 S とロック用マニューシャ情報 M_r の安全性はダミーデータを付加することにより守られる．しかし，指紋情報はエリア，端点・分岐点の属性，角度といった各パラメータに相関関係があると考えられるため，単に乱数によりダミーデータを作成した場合攻撃者からの推測が容易となる危険性がある．そこで，指紋情報の特徴を考慮したダミーデータの作成手法を明らかにする必要がある．ダミーデータに求められる条件を以下に示す．

条件 1：正規ユーザが照合時に提示したマニューシャ情報と一致しにくい．

条件 2：ロック情報 V からダミーデータを特定できない．

条件 3：正規ユーザが登録時に提示したマニューシャ情報とダミーデータを判別できない．

条件 1 は，正規ユーザが認証した際に秘密情報 S を復元できない確率（以下，FRR）を低減させるために必要となる．アンロック用マニューシャ情報とダミーデータの一致数が多いほど，マッチングの際に得られる抽出検査符号 $\bar{C}$ にダミーの検査符号が多く含まれるため，秘密情報 S を正しく復元できる可能性が低減される．条件 2 は，ロック情報 V が漏洩した際に，不正に秘密情報 S を復元されたり，ロック情報から正規ユーザのロック用マニューシャ情報 M_r が取得されたりする可能性を低減させるために必要となる．したがって，ダミーデータはロック用マニューシャ情報 M_r と同様のデータ形式を持ち，一般的な指紋情報において頻出のマニューシャ情報を用いることが必要となる．

4.1 頻出角度を用いたダミー角度情報の作成

正規ユーザの同一マニューシャであってもロック時とアンロック時で取得される角度情報に取得誤差が生じる．この取得誤差の範囲内にある角度情報を持つマニューシャ情報をダミーデータとして付加しないことで，条件 1 を考慮する．

ここで，正規ユーザのロック用マニューシャとアンロック用マニューシャにおける角度情報の取得誤差について調査を行った．まず，20 個の要素からなるロック用マニューシャ情報 M_r を作成する．次に，M_r のすべてのマニューシャ情報 $M_{r_1} \sim M_{r_{20}}$ に対して，エリア情報および属性情報は変更せずに，角度情報を 1〜31 レベル回転させたマニューシャ情報をダミーデータとして付加し，ロック情報 V とする．したがってダミーデータ数は $20 \times 31 = 620$ となる．そして，作成したロック情報 V と正規ユーザのアンロック用マニューシャ情報 M_v との間でマッチングを行い，誤ってダミーデータと一致した場合，そのダミーデータと元のロック用マニューシャ情報の角度差を調査した．**図 4** は横軸にロック用マニューシャ情報とアンロック用マニューシャ情報の角度情報の取得誤差を表し，縦軸にその取得誤差における出現頻度を表した図である．角度情報の取得誤差はマッチングにおいてアンロック用マニューシャ情報 M_{v_1} が M_{r_1} を 1 レベル回転させたダミーデータと一致した場合，誤差 1 レベルとして算出した．図 4 より，角度情報の取得誤差は ±1 レベルが多いことが分かる．したがって，ロック用マニューシャ情報の角度情報に ±1 レベルの回転を加えた角度情報を持つダミーデータを付加しないことで，正規ユーザのアンロック用マニューシャ情報がダミーデータと一致する可能性を低減させることができる．ここで条件 2 の観点から，ダミーデータ推定の危険性を低下させるために，ダミーデータどうしも ±1 レベルの角度情報を持つものを付加しないこととする．また，**図 5** に示すように，アンロック時の隆線情報の微小な変化により分岐点として登録されているマニューシャが端点，端点として登録され

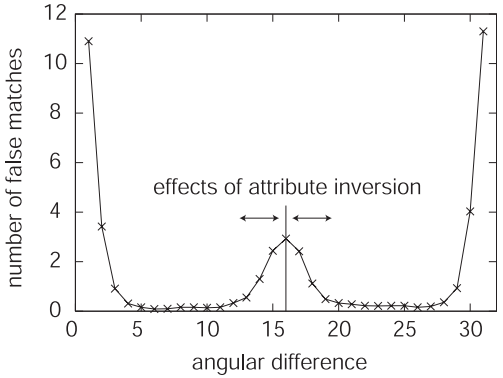

図 4　角度情報の取得誤差と出現頻度
Fig. 4　Number of false matches with dummy data versus angular difference.

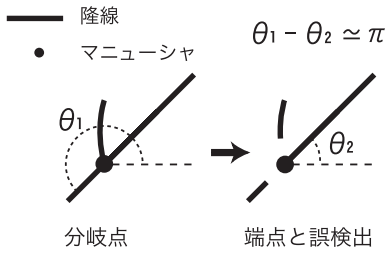

図 5　端点・分岐点属性の反転
Fig. 5　Attribute inversion.

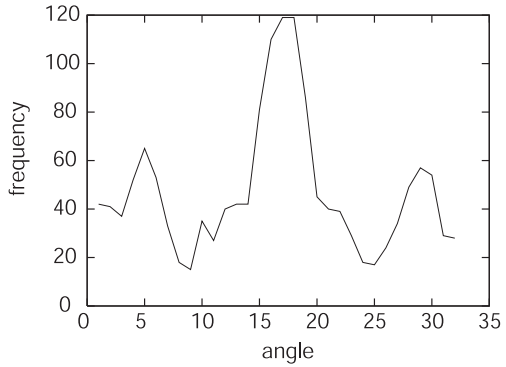

図 6　エリア情報・属性情報における角度情報の出現頻度例
Fig. 6　Frequency of appearance of angle level.

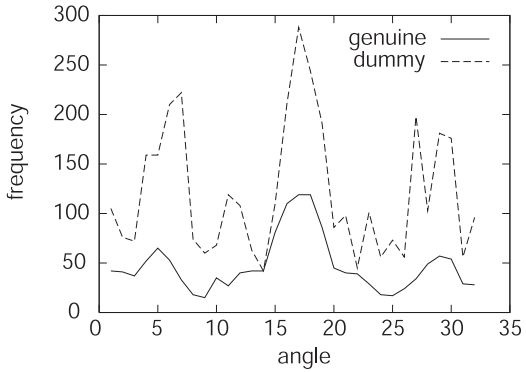

図 7　ダミーデータ付加の結果例
Fig. 7　Example of adding dummy data.

ているマニューシャが分岐点と誤判定されることがある．この場合，角度情報が 180 度異なるマニューシャとして検出される結果となるため（図 5 において $\theta_1 - \theta_2 \simeq \pi$）誤差 16 レベル付近に誤一致が見られる．

次に，条件 2 を考慮するために複数指紋に共通する角度情報について調査を行った．多数の指紋において出現頻度の高い角度情報をダミーデータに用いることで，他人が一致しやすいダミーデータを作成する．また，多数の指紋において出現頻度の低い角度情報をダミーデータに用いた場合，容易にダミーデータを推測される危険性が存在するため，出現頻度に応じたマニューシャの付加を行うことでより推測の困難なダミーデータを作成する．

一例として**図 6** にあるエリア情報と属性情報における角度情報の出現頻度を示す．調査用の指紋として 35 人の左右の人差し指，中指の指紋情報を各々5 回取得したものを用いた．図 6 より 8，9，24，25 レベルの角度を持つマニューシャは出現頻度が低い．したがって，このような角度を持つマニューシャを付加した場合，ダミーデータの推測が容易となることが分かる．

以上より，本提案では次のような手順でダミーデータを作成することとした．

(1)　多数の指紋から各エリア情報，属性情報における角度レベルの出現頻度を調査する．
(2)　エリア情報および属性情報はランダムに決定し，対応する角度レベルの出現頻度となるように角度情報を決定する．
(3)　決定したダミーデータがロック用マニューシャ情報，付加済みのダミーデータ，およびそれらの角度情報に ±1 レベルの回転を加えたマニューシャ情報と一致しなければダミーデータとして付加する．

図 7 は，図 6 と同じエリア情報，属性情報におけるダミーデータの角度情報の出現頻度である．一例として，調査用の指紋に図 6 で用いた指紋と同じものを用い，各指紋に対し 50 個のダミーデータを付加した．図 6 で示した角度情報の出現頻度に従ってダミーデータが付加されていることが分かる．

5. 安全性評価

バイオメトリック認証では，各人に固有な身体的特徴や身体的特性を用いて本人確認を行うため，生体情報の性質に起因したバイオメトリック認証特有の脆弱性が内在する．このため，一般的な IT システムにおける情報セキュリティの考え方を直接適用することができず，現状では情報セキュリティの観点に基づいたバイオメトリック認証の安全性に関する検討は十分に行われていない[12]．バイオメトリック暗号におけるリスク管理を行うためには，システムが脅威に対してどの程度セキュアであるかを示すことが必要である．バイオメトリック暗号の安全性評価項目は大きく分けて以下の 3 つに分類できる．

(1)　本人が秘密情報を復元できない確率と他人が秘密情報を復元する確率（FRR/FAR）
(2)　ロック情報から秘密情報を推定する困難性
(3)　ロック情報から生体情報を復元する困難性

表 1　シミュレーション諸元
Table 1　Simulation pecifications.

指紋データ	140 名 × 5 枚（登録 3 枚，照合 2 枚）
特徴点抽出アルゴリズム	NFIS2 [13]
テンプレート情報数 n	20 個
隆線方向の量子化レベル	32
エリアの大きさ/数	780 エリア
誤り訂正符号	$GF(2^8)$，検査符号数 $g = 20$ で符号化
ダミーデータ数	50，150，250 個
秘密情報要素数 k	4，5，6，7，8，9，10
ダミーデータ作成用閾値	2.3
照合誤差許容閾値	2.9

5.1　秘密情報復元率

秘密情報復元実験として，本人と他人の各々に対し，本人の秘密情報が正しく復元される確率（以下，復元率）の調査実験を行った．ロック時のテンプレート情報数 g を 20 個とし，ダミーデータ数が 50，150，250 個のときの復元率を調査した．本稿では，誤り訂正符号として $GF(2^8)$ ガロア拡大体上の Reed Solomon 符号を用いたが，一般に $GF(2^m)$ ガロア拡大体上の k 個のシンボルで構成される秘密情報の情報量は $m \times k$ bits となる．使用した指紋情報とその他のシミュレーション諸元を**表 1** に示す．

図 8 に，横軸を秘密情報要素数，縦軸を復元率とした秘密情報復元結果を示した．バイオメトリック認証では，一般的に本人拒否率（FRR）と他人受入率（FAR）で照合の精度を示すことが多いが，ここでは本人と他人の復元率に対応するために本人受入率と他人受入率を用いた．一例として $k = 6$，すなわち秘密情報量 48 $bits$，ダミーデータ数 150 の場合を見ると，本人復元率 98%以上，他人復元率 3%以下となっている．

また，比較対象として**図 9** に乱数によりダミーデータを作成した場合の照合結果を示す．本提案では，4 章において条件 1 を考慮したダミーデータを作成している．このため，図 8 では図 9 に比べ本人復元精度が大きく向上している．また，乱数によりダミーデータを作成すると指紋の外縁部など，照合に有効ではないダミーデータが付加される．このため，図 9 では図 8 に比べ他人がダミーデータをとる確率が若干低下している．

図 8 の結果から，秘密情報の復元精度とダミーデータ数，および秘密情報の復元精度と秘密情報要素数 k はトレードオフの関係にあることが分かる．2.3.1 項で述べたように，秘密情報が復元されるための条件は式 (5) で表すことができる．ダミーデータの個数が増加した場合，本人データとの一致数 m_t が減少し，同時にダミーデータとの誤一致数 m_f が増加する．このため式 (5) の右辺の値が減少し，秘密情報の復元率が低下する．また，秘密情報要素数 k が増加した場合，式 (5) の左辺の値が増加するため秘密情報の復元精度が低下する．

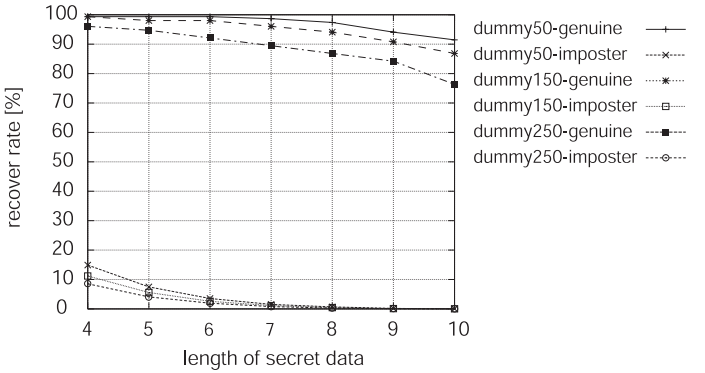

図 8　秘密情報復元率
Fig. 8　Simulation results.

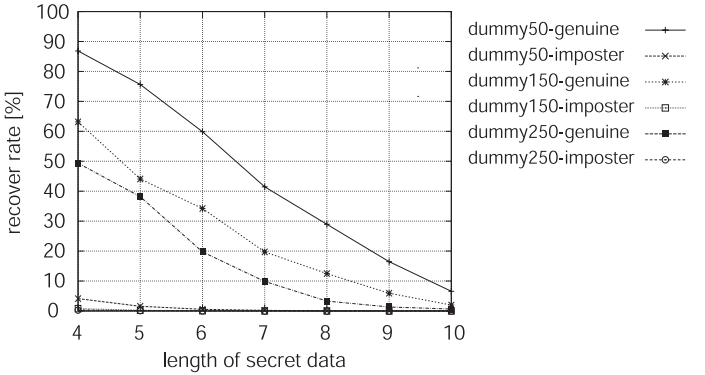

図 9　秘密情報復元率（ランダムダミーデータ付加）
Fig. 9　Simulation results (with random dummy data).

以上より，バイオメトリック暗号をシステムに応用する際は，想定されるリスクの程度や，運用条件により求められるセキュリティ強度が異なるため，パラメータ設定を適切に行う必要があるといえる．

5.2　推定エントロピーを用いた安全性評価

バイオメトリック暗号の安全性評価手法として，現在，前述の安全性評価項目 (3) の観点から，最小エントロピーを用いてロック情報に含まれる生体情報の安全性を定量化する試みが報告されている[14)–16)]．

しかし，攻撃者は生体情報を取得できなくても，ロック情報から無作為に検査符号を抽出し，それらの検査符号を用いて誤り訂正復号により秘密情報の復元を行い，復元された情報のパターンやその出現頻度などの統計的偏差から秘密情報を推定することが可能である．このため本稿では，安全性評価項目 (2) の観点から，ロック情報に含まれる生体情報の知識を持たない攻撃者により秘密情報を不正に推定される脅威に関して安全性評価を行う．ただし，秘密情報は図 8 で示した確率で復元され，誤り訂正復号に失敗した場合，空値または本人の秘密情報とは異なる情報が出力される．また，本人の秘密情報か否かを問わず，復元された情報のことを復元情報とする．以下に，復元情報の統計的偏差を利用した秘密情報推定攻撃の概要を述べる．

攻撃者が単一の復元情報のみから秘密情報を推定することは困難である．しかし，同一のロック情報から復元情報の取得を複数回試みると，各々の復元情報の出現頻度には偏差が生じる．このため，次のような攻撃手段が考えられる．ただし，秘密情報要素数 k，テンプレート情報要素数 g，ロック情報要素数 r が攻撃者にとって既知であるという条件下での攻撃を想定する．

(1)　ロック情報より無作為に k 個の検査符号を取得．
(2)　取得した検査符号を用いて誤り訂正により秘密情報を復元．
(3)　(1)，(2) の操作を複数回繰り返し，復元情報のパターンと復元確率の統計情報を作成．
(4)　復元情報が秘密情報である確率 ${}_gC_k/{}_rC_k$ を算出（以下，無作為復元確率 P_b とする）．
(5)　統計情報より，P_b と最も近似の確率で出現した復元情報のパターンから順に秘密情報として試行．

すなわち，秘密情報とは異なるパターンの復元情報は，ダミーデータとして無作為に生成した検査符号が取得された場合に復元されるため，それらの復元情報の出現確率が必ずしも P_b と一致しないという結果を利用する．その結果，総当たりで秘密情報の推定を行うより少ない試行回数で秘密情報の推定が可能となる．このような攻撃手段に対する安全性評価尺度として推定エントロピーを用いる．推定エントロピー $H_\infty(X)$ は式 (6) で定義される．

$$H_\infty(X) := -\sum_x P(X=x)\log_2 P(X=x) \tag{6}$$

ただし $P(X=x)$ は情報 X が値 x となる確率である．ここで，ロック情報から検査符号を取り出す場合，秘密情報要素数やロック情報要素数の増加にともない，検査符号の組合せ総数がきわめて大きくなるため，すべての組合せをシミュレートすることが困難である．したがって本稿ではロック情報から検査符号を取得する回数を N 回と限定し，N 個の標本から推定エントロピーを算出する．N 個の標本が独立分布であれば，推定エントロピー $H_\infty(X)$ は最大値 $\max H_\infty(X)$ となる．

$$\max H_\infty(X) = -\log_2 \frac{1}{N}$$

しかし，実験結果から得られる推定エントロピーは必ずしも $\max H_\infty(X)$ とは一致せず，エントロピーの減少がともなう．このとき，$\max H_\infty(X)$ からのエントロピーの減少率を estimated entropy loss H_{loss} を定義する．$\max H_\infty(X)$ は試行回数に依存するため，H_{loss} は $H_\infty(X)$ を $\max H_\infty(X)$ で正規化し式 (7) で定義する．

$$H_{loss} = \frac{\max H_\infty(X) - H_\infty(X)}{\max H_\infty(X)} \tag{7}$$

H_{loss} が 0 に近いほど復元結果が独立分布に近いことを示す．

ここで，ある人物のロック情報に対して上記の攻撃手段で復元情報の取得を 1×10^7 回試行し，得られた復元情報の分布から H_{loss} を算出した．調査用指紋として表 1 の指紋を用い，ダミーデータ数は 20，40，60，80，100 個と変化させて評価した．**図 10** に横軸をダミーデータ数，縦軸を H_{loss} として H_{loss} とダミーデータ数の関係を示す．なお，同図に最小二乗法から求めた近似曲線をあわせて示している．H_{loss} はダミーデータ数が少ないと最大で 30%程度となり，ダミーデータ数を増加させると 25%程度まで減少した．

H_{loss} は復元情報のパターンが独立分布にどの程度近いかを示す指標である．しかし，無作為復元確率 P_b が高い場合 H_{loss} がどんなに小さくても総当たりによる攻撃を容易に許してしまう危険性がある．したがって，安全性の評価にあたっては，無作為復元確率 P_b と H_{loss} の 2 点を同時に考慮する必要がある．

ここで，総当たり攻撃による秘密情報復元を行う場合に必要な試行回数を総当たり数 B_f とする．B_f の減少率は H_{loss} を用いて式 (8) で表すことができる．式 (8) より求めた B_f の減少率を**図 11** に示す．

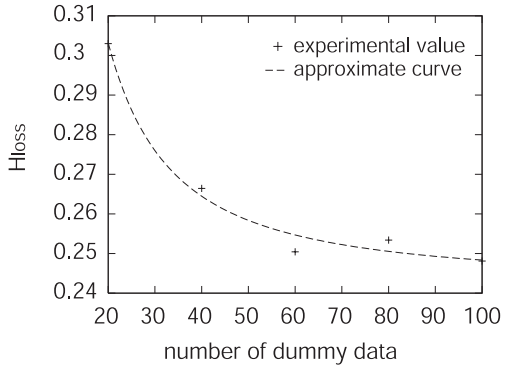

図 10　推定エントロピー減少率 H_{loss}
Fig. 10　Estimated Entropy Loss H_{loss}.

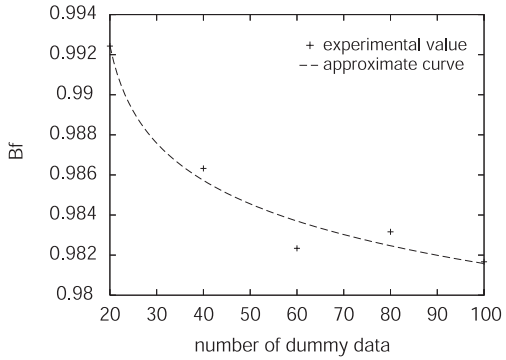

図 11　総当たり試行回数 B_f の減少率
Fig. 11　Rate of decrease in B_f.

$$\left(1 - \frac{1}{2^{(H_{loss} \times \max H_\infty(X))}}\right) \times 100 \ (\%) \tag{8}$$

式 (8) より H_{loss} が大きいほど総当たり攻撃に必要な攻撃回数が少なくなり，総当たり攻撃が容易となる．したがって，図 10 および式 (8) より，ダミーデータ数の増加によって H_{loss} が減少し，復元情報のパターンやその出現頻度などの統計情報を利用した秘密情報推定攻撃への耐性が高くなっているといえる．

6. ま と め

本稿では，バイオメトリック個人認証のシステムの構築においてテンプレートの安全性を確保することが重要であるとの認識から Fuzzy Vault Scheme を用いてテンプレートの安全性を高める一手法を提案した．そして指紋照合方式への適用を行い，指紋情報の特性を考慮したダミーデータの作成手法について述べた．次いで，秘密情報の要素数 k と検査符号の要素数 g を適切に設定することにより本人であれば高い確率で秘密情報を復元可能であることを確認した．また，バイオメトリック暗号の安全性評価手法の一例として推定エントロピーを用いた評価手法を提案し，ダミーデータ数の増加が秘密情報の推定攻撃対策として有効であることを確認した．本稿で提案した評価手法をもとに，秘密情報要素数やダミーデータ数，誤り訂正符号の構成方法とテンプレート安全性との関係を計算コストも考慮して明らかにしてくことが今後の課題である．

参 考 文 献

1) 社団法人日本自動認識システム協会：平成 15 年度基準認証研究開発事業，生体情報による個人識別技術（バイオメトリクス）を利用した社会基盤構築に関する標準化 (2004).
2) Soutar, C., Gilroy, R. and Stoianov, A.: Biometric System Performance and Security, *IEEE Auto. Identification Advanced Technol.*, pp.46–49 (1999).
3) Ratha, N., Connell, J. and Bolle, R.: Enhancing security and privacy in biometrics based authentication systems, *IBM Systems Journal 40*, pp.614–634 (2001).
4) 高橋健太，比良田真史：セキュアなリモート生体認証プロトコルの提案，暗号と情報セキュリティシンポジウム予稿集，SCIS2007 (2007).
5) 比良田真史，高橋健太，三村昌弘：画像マッチングに適用可能なキャンセラブル生体認証方式の脆弱性分析と安全性向上，暗号と情報セキュリティシンポジウム予稿集，SCIS2007 (2007).
6) 尾形わかは，菊池浩明，西垣正勝：リモートバイオメトリクスに有効な「近い」ことを示す零知識証明プロトコル，情報理論とその応用シンポジウム予稿集，SITA2006, pp.319–322 (2006).
7) 永井　慧，菊池浩明，尾形わかは，西垣正勝：ZeroBio—秘匿ニューラルネットワーク評価を用いた非対称指紋認証システムの開発と評価，情報処理学会論文誌，Vol.48, No.7, pp.2307–2318 (2007).
8) 坂下泰紀，柴田陽一，高橋健太，尾形わかは，菊池浩明，西垣正勝：ZKIP とほぼ同等の安全性を有する効率的なリモート生体認証の提案，暗号と情報セキュリティシンポジウム予稿集，SCIS2008 (2008).
9) Juels, A. and Sudan, M.: A fuzzy vault scheme, *Proc. IEEE Int. Symp. Inf. Theory*,

p.408 (2002).
10) The Internet Engineering Task Force: PPP Challenge Handshake Authentication Protocol (CHAP). http://www.ietf.org/rfc/rfc1994.txt
11) Shah, J.A., Ross, A. and Jain, A.K.: Can Fingerprints be Generated From Minutiae Points?, *Proc. Biometrics Symposium*, pp.9–10 (2005).
12) JAISA: Standarization of Public Infrastructure using Biometrics Authentication (2004).
13) National Institute of Standards and Technology: NIST fingerprint image software 2. http://fingerprint.nist.gov/nfis/
14) Dodis, Y., Reyzin, L. and Smith, A.: Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In Advances in Cryptology, *Proc. EUROCRYPT2004*, pp.523–540 (2004).
15) Tuyls, P. and Goseling, J.: Capacity and examples of template-protecting biometric authentication systems, *ECCV Workshop BioAW*, No.77 (2004).
16) Chang, E.-C., Shen, R. and Teo, F.W.: Finding the Original Point Set Hidden Among Chaff, *Proc. ASIACCS*, pp.182–188 (2006).

付　　録

A.1　提案手法における中心点の取得精度

指紋のマニューシャの位置を表すエリアは中心点を基準に作成しているため，中心点の取得誤差により，同一の位置にあるマニューシャが異なるエリア情報を持つマニューシャとして取得される可能性がある．このため，認証精度は中心点の取得精度に依存する．本手法では指紋中心点の取得に Wegstein らによって提案された R92 アルゴリズムを用いた NFIS2 の中心点自動取得プログラム[13] を利用している．

以下，NFIS2 の中心点自動取得プログラムによる中心点の取得精度に関して評価する．**図 12** に NFIS2 の中心点自動取得プログラムにおけるロック用指紋情報とアンロック用指紋情報における中心点の取得誤差を示す．横軸は中心点の取得誤差をピクセル数で表し，縦軸はその誤差の出現頻度を表す．取得誤差は 6 ピクセル近傍に集中し偏差が小さいことが分かる．ここで得た取得誤差を許容可能なエリアサイズを設定することで，中心点のずれによる精度劣化を抑えることができる．

A.2　円形エリアの作成手法

表 1 の指紋を用いて中心点からの距離が R 以下の領域に含まれるマニューシャの割合（以下，マニューシャ含有率）を求めた結果を**図 13** に示す．図 13 は横軸に中心点からの距離，縦軸にマニューシャ含有率を示したものであり，中心点からの距離 R が 150 ピクセル以内の領域に約 90%のマニューシャが含まれることが分かる．

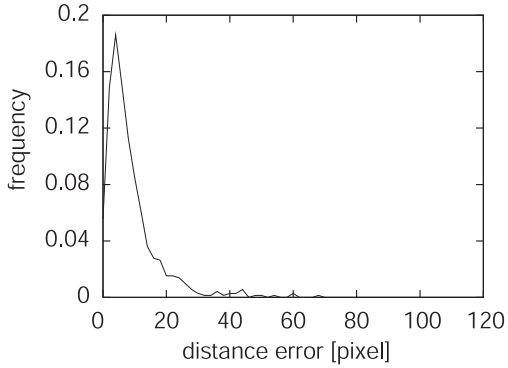

図 12　NFIS2 の中心点自動取得プログラムの中心点取得誤差
Fig. 12　Core detection differences for NFIS2 core detection algorithm.

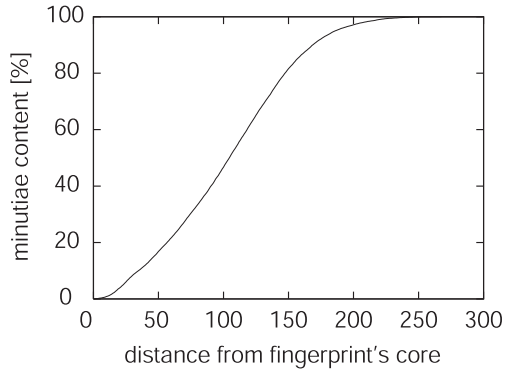

図 13　中心点からの距離とマニューシャ含有率の関係
Fig. 13　Relationship between distance from fingerprint's core and minutiae content.

ここで，注目するエリアにマニューシャが存在する確率をマニューシャ存在確率とする．本手法では図 13 に基づいて，中心点からの距離，エリアの半径を指定し，各エリアにおけるマニューシャ存在確率が一様となるようにエリア情報を作成した．**図 14** は表 1 の指紋における円形エリアのマニューシャ存在確率の分布である．図 14 において，マニューシャ

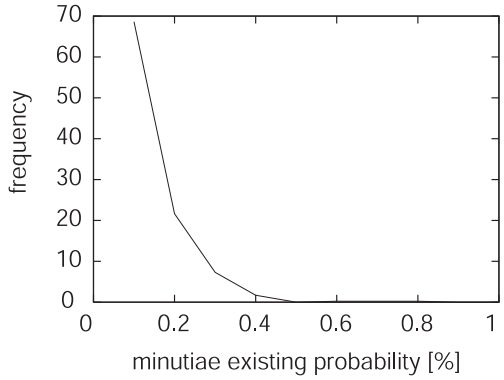

図 14　マニューシャ存在確率の分布
Fig. 14　Minutiae existing probability histogram.

存在確率の分散が小さいほど各エリアのマニューシャ存在確率が一様であるといえる．円形エリアを用いた場合，マニューシャ存在確率は 0.1 ～ 0.3% 付近に集中し，各エリアのマニューシャ存在確率がほぼ一様となっていることが分かる．

(平成 20 年 12 月 1 日受付)
(平成 21 年 6 月 4 日採録)

大木　哲史（正会員）

2002 年早稲田大学理工学部電子・情報通信学科卒業．2004 年同大学院理工学研究科修士課程修了．2007 年同大学理工学研究所嘱託研究員として現在に至る．バイオメトリクス等を用いた個人認証技術とネットワークへの応用に関する研究に従事．

披田野清良

2007 年早稲田大学理工学部コンピュータ・ネットワーク工学科卒業．2009 年同理工学術院基幹理工学研究科修士課程修了．同理工学術院博士後期課程在学中．バイオメトリック認証のテンプレート保護に関する研究に従事．

小松　尚久（正会員）

1979 年早稲田大学理工学部電子通信学科卒業．1981 年同大学院理工学研究科修士課程修了．同年 NTT に入社．1987 年早稲田大学理工学部助手．1989 年同専任講師．1996 年同教授．工学博士．セキュリティと品質を考慮したヒューマン/ネットワークインタフェースに関する研究に従事．特にバイオメトリック認証技術とその適用に興味を持つ．電子情報通信学会，画像電子学会，IEEE 各委員．

笠原　正雄（正会員）

1965 年大阪大学大学院工学研究科通信学専攻博士課程修了．工学博士．同年同大学工学部助手，1970 年同講師．1972 年同助教授．1987 年京都工芸繊維大学工芸学部教授．2000 年 4 月大阪学院大学情報学部教授として現在に至る．1967～1969 年米国ベル電話研究所客員研究員．情報理論，符号理論，ディジタル通信システム，情報セキュリティ，音声・画像符号化，技術倫理等の研究に従事．著書『情報技術の人間学』等．IEEE ライフフェロー．IEEESSIT 日本支部パストチェアマン．電子情報通信学会フェロー．電子情報通信学会名誉員，情報理論とその応用学会名誉会員，画像電子学会，映像情報メディア学会各会員，日本工学アカデミー会員等．