誤り訂正を導入した統計的 AD 変換による複数の特徴量からの生体鍵生成

柴田陽一[†] 宮木孝[††]
水野忠則[†††] 西垣正勝[†††]

生体情報から暗号に用いる鍵を生成する方式の 1 つとして，統計的 AD 変換が提案されている．本論文では，複数の生体特徴量から暗号鍵を生成することにより統計的 AD 変換の精度の改善を図る．一般的に本人拒否率と他人受入率はトレードオフの関係にあるが，複数の特徴量を組み合わせる場合には，各々の特徴量ごとの本人拒否率を低く抑えることが肝要である．本人拒否率の低減には誤り訂正の導入が有効であることに鑑み，複数の特徴量を用いた生体鍵生成方式として，Fuzzy Commitment を用いた統計的 AD 変換の改良方式を提案し，方式の有効性を検証する．

Key Generation from Multiple Biometric Features Using Statistical A/D Conversion with Error Correction

Yoichi Shibata,[†] Takashi Miyaki,[††] Tadanori Mizuno[†††] and Masakatsu Nishigaki[†††]

The statistical A/D conversion is an effective scheme to convert biometric information to a cryptographic key. This paper proposes to improve the accuracy of biometric key generation with statistical A/D conversion by using multiple biometric features. Here, in using multiple biometric features, it is important to keep FRR low at A/D conversion of each feature, and error correction is an efficient solution for the purpose. Therefore, this paper studies to combine Fuzzy Commitment with statistical A/D conversion to achieve an accurate key generation from multiple biometric features.

1. はじめに

ネットワーク社会においては非対面の通信相手を認証するための技術が不可欠であり，現在までに様々な認証プロトコルが提案されている[1)]．これらは，共通鍵暗号系の秘密鍵（前もって共有しておいた秘密情報）または公開鍵暗号系の秘密鍵（前もって登録しておいた公開鍵に対応する秘密情報）によってオンライン認証を実現するものであり，その安全性が暗号学的に証明されているということが大きな特徴である．ただし，その安全性を実効的なものにするためには，ユーザに秘密鍵の厳重な管理徹底が要求されることになる．

一方，生体情報による本人認証[2)]は，認証のために新たな情報を記憶したり専用デバイスを持ち歩いたりする必要がなく，ユーザの利便性が高い．したがって，生体情報を秘密鍵として用いることができれば，各種認証プロトコルにおける利便性の問題を克服することが可能となると期待される．具体的には，暗号技術を基盤とした認証プロトコルに「生体情報から秘密鍵を生成する」方式を加えることにより，ユーザは秘密鍵の管理から解放されることになるであろう．

しかし，DNA を除くほとんどの生体情報はアナログデータであるため，一般に，その読み取り時に人的および外的要因によって何らかの誤差（指のゆがみ，ゴミの付着など）が混入することが避けられない．生体情報における特徴量（たとえば，特定領域の隆線の角度など）をしきい値で量子化してやることにより，読み取り誤差によって生じた量子化誤差未満の変動についてはこれを除去することが可能であるが，しきい値付近のデータが読み取り誤差によって変動してしまうと，量子化の結果が異なってしまうことになる．す

† 静岡大学大学院理工学研究科
Graduate School of Science and Engineering, Shizuoka University
†† 三菱電機エンジニアリング株式会社
Mitsubishi Electric Engineering Company Limited
††† 静岡大学創造科学技術大学院
Graduate School of Science and Technology, Shizuoka University

なわち，生体情報をつねに一意で固有な値として取得することは難しい．

このような状況の中で，生体情報を暗号化鍵に変換する「生体鍵生成」技術の研究開発が進められている[3)~5)]．これらは，登録時に 1 つの生体情報を複数回取得して読み取り時の変動を推測しておくことにより，生体情報の変動を統計学的に補償した形で量子化する方法であり，指紋[3)]，手書きの署名[4)]，顔画像[5)]からそれぞれ 50〜100 ビット程度の鍵が生成可能であったとの報告がなされている．しかし，各方式の本人拒否率および他人受入率を実用レベルでゼロに抑えることは達成されておらず，読み取り誤差を完全に吸収することは現実的に非常に難しい課題であることが分かる．

この「生体情報の変動によって精度が悪化する」という問題の克服は，生体鍵生成に限らず，生体認証においても重要な課題である．これに対し，生体認証の分野では，近年，複数の特徴量を用いることによって認証精度の改善を図る「アンサンブルモデルの生体認証方式[6)]」が注目を集めている．そこで本論文では，このアイデアを生体鍵生成に応用することを検討する．指紋認証においてアンサンブルモデルの適用が効果的に機能することが文献 7) で確認されていることに鑑み，本論文では，指紋からの生体鍵生成を報告している文献 3) の統計的 AD 変換手法に焦点を当てる．すなわち，指紋に含まれる複数の特徴量を利用することによって統計的 AD 変換の精度改善を試みる．

一般的に本人拒否率と他人受入率はトレードオフの関係にあるが，複数の特徴量を組み合わせる場合には，各々の特徴量ごとの本人拒否率を低く抑えることが肝要である．そこで本論文では，特徴量から生成される生体鍵の誤り訂正を行うために，生体情報の誤り訂正方式として知られている Fuzzy Commitment[8)] を導入し，1 つの生体情報から抽出した複数種類の特徴量を用いる生体鍵生成手法を提案する．生体情報として指紋を用いた実験を行い，従来方式よりも精度が向上することを示す．

2. 統計的 AD 変換

統計的 AD 変換[3)] は，正規ユーザの生体情報の特徴量の平均や標準偏差が，不特定多数の生体情報の特徴量の平均や標準偏差と異なるという統計的な性質に基づき，ユーザ各々の生体情報をリアルタイムでつねに一意なユニーク ID に変換することができる技術である．本章では，生体情報として指紋を例にとり，その方式を概説する．

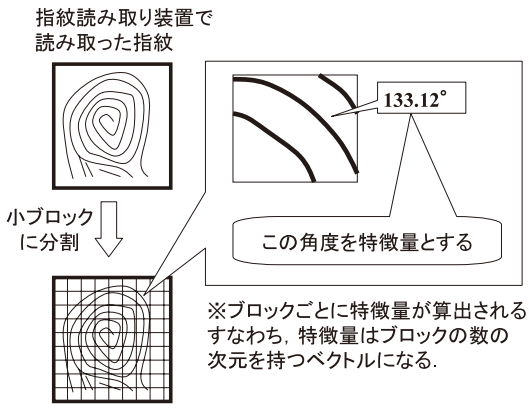

図 1 指紋の特徴量
Fig. 1 A feature vector of fingerprint.

2.1 指紋の特徴量

指紋の特徴量としては，様々な候補が考えられるが，ここでは指紋を小さなブロック（文献 3) では 100 ブロック）に分割し，各ブロック内の隆線の傾きを特徴量とする（**図 1** 参照）．

2.2 指紋の登録（登録フェーズ）

(1) 正規ユーザの指紋を複数回（文献 3) では 10 回）読み取る．同一の生体情報であるが，読み取り誤差が混入するため，異なったデータが得られる．

(2) 複数個の指紋データのそれぞれについて，指紋の各小ブロックの隆線の傾きを特徴量として算出する．以降の処理は，各小ブロックごとに行われる．

(3) 算出された特徴量の統計を測り，正規ユーザの指紋の特徴量の平均 μ と標準偏差 σ を計算する．

(4) 統計的な性質から（特徴量の誤差が正規分布に従っていると仮定すると），正規ユーザの指紋であれば指紋の特徴量は区間 $[\mu-3\sigma, \mu+3\sigma)$ の中に（約 99.7%の確率で）収まることが期待できるため，正規ユーザの特徴量の許可範囲を $[\mu-3\sigma, \mu+3\sigma)$ の区間であるとする．そして，特徴量空間におけるその他の区間を許可範囲と同じ大きさに分割する（**図 2** 参照）．

(5) 分割されたすべての区間に対して，それぞれ乱数 ID_i（$i=0,1,2,\cdots$）を割り当てる（**図 3** 参照）．各区間の境界 $\{\mu\pm3\sigma, \mu\pm9\sigma, \mu\pm15\sigma, \cdots\}$ と各区間の乱数 ID_i（$i=0,1,2,\cdots$）のみを記憶する．この情報を「スケール」と呼ぶ．

2.3 指紋からの ID 抽出（鍵生成フェーズ）

(1) 指紋を読み取り，特徴量を算出する．

(2) 特徴量が含まれる区間に割り当てられた乱数が

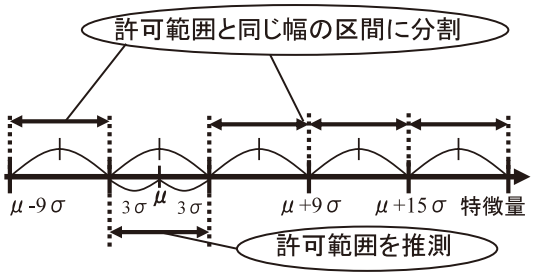

図 2 許可範囲の決定と他の区間の分割
Fig. 2 Determination of authentic region and division of feature space.

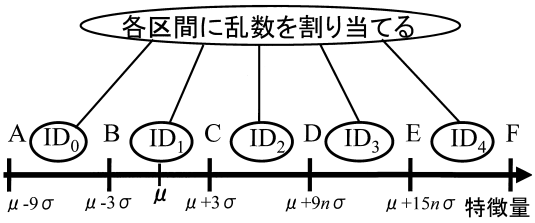

図 3 各区間への乱数の割当て
Fig. 3 Assignment of a random number to each region.

ID となる．すべての小ブロックから抽出された乱数を連結し，これをハッシュ化したものが生体鍵となる．

登録時に 1 つの生体情報から何度もデータを読み取って統計量を算出することにより，その生体情報に対する読み取り誤差の混入の期待値を測定している．このため，正規ユーザの生体情報であれば，ID 抽出時に算出された特徴量はかなりの高確率で許可範囲の中に入る．すなわち，正規ユーザの ID は高確率で同じ値となる．なお，同じ生体情報から複数のデータを読み取る必要があるのは登録時のみであり，ID 抽出時にはそのつどデータを 1 回読み取るだけであることに注意されたい．

2.4 精度に関する考察

上記の例では特徴量の誤差が正規分布に従っていると仮定したが，実際にはその保証はない．そこで，変数としてセキュリティパラメータ n を設定して，許可範囲を $[\mu - n\sigma, \mu + n\sigma)$ とし，本人拒否率と他人受入率を勘案して n を調節することとする．通常，本人拒否率と他人受入率はトレードオフの関係にあるので，両者を満足する n の決定は難しいであろう．そこで，本方式では，本人拒否率を改善するために n を用い，他人受入率は特徴量の次元を増加させることにより調整する方策をとる．すなわち，まず，本人拒否率が十分小さくなるまでセキュリティパラメータ n の値（つまり，許可範囲）を大きくする．そして，他人受入率を減らすためには，十分な数の特徴量を用意する．

文献 3) では，指紋を小ブロックに分割しているため，各小ブロックからの ID の数だけ特徴量が得られることとなる．ある 1 つの小ブロックだけを見た場合には正しい ID が得られる者は正規ユーザ以外にも多数存在するが，全体の ID が正しく得られる者は高い確率で正規ユーザのみとなる．ただし，文献 3) の評価実験においては，本人拒否率と他人受入率を実用レベルでゼロに抑えることは達成されていない．精度向上のためには，指紋の隆線の角度という情報だけでは不十分で，他の特徴量を追加する必要があると思われる．

3. 複数特徴量の統計的 AD 変換

3.1 アンサンブルモデルの適用

生体認証の分野では，近年，複数の特徴量を用いることによって認証精度の改善を図る方式が注目を集めている．複数の特徴量を用いた生体認証方式は，異なる生体情報の特徴量を利用する「マルチモーダルモデル」と，1 つの生体情報の中の異なる特徴量を利用する「アンサンブルモデル」に大別される[6]．ここで，統計的 AD 変換においては登録時に各生体情報ごとに複数回の生体情報を入力してもらう必要があることを考慮すると，統計的 AD 変換の改良には，生体情報のスキャニングの回数を増加させることなく精度向上を果たすことができるアンサンブルモデルのアプローチが適していると考える．

そこで本論文では，指紋に含まれる「隆線の角度」以外の特徴量を追加することによって統計的 AD 変換の精度改善を試みる．生体鍵生成にアンサンブルモデルを適用した例は，著者らが確認した限り現時点までに報告されていない．

指紋の中の複数種類の特徴量から生体鍵を生成するにあたっては，各特徴量の個別の本人拒否率を十分ゼロに近づけることが肝要である．今，特徴量 A のみを用いて統計的 AD 変換により生体鍵を生成した際の本人拒否率，他人受入率を $\mathrm{FRR_A}$，$\mathrm{FAR_A}$ とし，特徴量 B のみを用いた生体鍵生成の本人拒否率，他人受入率を $\mathrm{FRR_B}$，$\mathrm{FAR_B}$ としよう．ここでは議論を簡単にするため，特徴量 A と B が独立である場合を考えてみる．特徴量 A と B の両方を用いて統計的 AD 変換により生体鍵を生成した際の本人拒否率，他人受入率は，それぞれ $\mathrm{FRR_A} + \mathrm{FRR_B} - \mathrm{FRR_A} \times \mathrm{FRR_B}$，$\mathrm{FAR_A} \times \mathrm{FAR_B}$ となる．すなわち，複数の特徴量を重ね合わせることによって精度向上が見込めるのは，他人受入率のみである．本人拒否率に対しては，個別の本人拒否率を十分小さくしておく必要がある．この性

質は，特徴量 A と B が完全には独立でない場合においても（完全に従属でない限り）成り立つ．

3.2 誤り訂正の導入

一般的に本人拒否率と他人受入率はトレードオフの関係にあるが，複数の特徴量を組み合わせる場合には，上述のとおり，各々の特徴量ごとの本人拒否率を低く抑えることが肝要である．本人拒否率の低下は「読み取りのたびに生体情報が変動する」ことが大きな要因となるため，統計的 AD 変換では，登録フェーズにおいて指紋を複数回（文献 3) では 10 回）取得して生体情報の変動を推測することによって，鍵生成フェーズで混入しうる読み取り誤差を補償しようとしている．しかし，たかだか 10 回のサンプルから指紋の変動を完全に推測することは不可能であるので，（セキュリティパラメータ n の値をある程度大きくして）本人の許可範囲 $[\mu - n\sigma, \mu + n\sigma)$ を広げるだけでは十分な本人拒否率を得ることは難しいと予想される．

そこで本論文では，各特徴量の本人拒否率をさらに低減させるために，誤り訂正の導入を検討する．一般には，誤り訂正の導入は本人拒否率を改善する一方で他人受入率を悪化させてしまうため[9]，生体認証への誤り訂正の導入がつねに効果を発揮するとは限らない．しかし，各特徴量ごとに本人拒否率を低下させることを優先すればよいアンサンブルモデルによる生体鍵生成に対しては，誤り訂正の導入は有効なアプローチといえる．

ここで，統計的 AD 変換が許可範囲 $[\mu - n\sigma, \mu + n\sigma)$ を設けることによって個々の特徴量の変動を吸収しようとしているのに対し，誤り訂正の目的は各特徴量から抽出された ID を連結した「全体の ID」の誤りを訂正することにあるということに注意されたい．すなわち，鍵生成フェーズにおいていくつかの特徴量の値が許可範囲を外れてしまい，一部の特徴量からの ID 抽出が誤ったとしても，誤りの数が誤り訂正可能範囲内であれば，誤り訂正することにより正しい「全体の ID」を得ることができる．

3.3 Fuzzy Commitment

統計的 AD 変換に誤り訂正を導入するにあたり，本論文では，生体情報に対する誤り訂正方式として知られている Fuzzy Commitment[8] を用いることとした．

Fuzzy Commitment は登録データから補助情報を作成し，その補助情報を用いて，（登録データとはわずかに異なる）認証データから登録データを（誤り訂正により）復元する方式である．

3.3.1 登録フェーズ

(1) 登録データ D を取得する．
(2) m ビット誤り訂正符号の中から 1 つの符号 R をランダムに選ぶ．なお，今回は Reed-Solomon 符号を用いた．
(3) $F(D) = D \oplus R$ を計算し，$F(D)$ を補助情報として記憶する．ここで，$\oplus$ は排他的論理和である．

3.3.2 認証フェーズ

(1) 認証データ D' を取得する．
(2) 保存されている補助情報 $F(D)$ を使って，$S = D' \oplus F(D)$ を計算する．
(3) S に対して誤り訂正を行う．これにより得られる符号を S' とする．
(4) $D'' = F(D) \oplus S'$ を出力する．

D と D' のハミング距離が m ビット以内であれば，$D'' = D$ である．その理由は以下のとおりである．$S = D' \oplus F(D) = D' \oplus D \oplus R$ であるので，D と D' のハミング距離と S と R のハミング距離は等しい．したがって，D と D' のハミング距離 d が m ビット以内であった場合には，S（R からハミング距離 d だけ離れたデータ）に対して誤り訂正を行うことにより，R が復元できる．つまり，$S' = R$ となる．よって，D'' は $F(D) \oplus S' = D \oplus R \oplus R = D$ となる．

4. 複数の特徴量からの生体鍵生成

実際に複数の特徴量を用いて統計的 AD 変換によって生体鍵生成を行う．本来であれば，できるだけ多くの特徴量を用意するべきであるが，本論文は本方式のコンセプトの提案に焦点を当てているため，ここでは指紋の隆線の傾き[3] と周波数成分の係数という 2 つの特徴量を使用したシステムを構築する．各々の特徴量から統計的 AD 変換によって得られる ID のそれぞれに対して Fuzzy Commitment による誤り訂正を行ったうえで，その 2 つの ID を結合することにより生体鍵を生成する．これによって，それぞれの特徴量から生成される ID の本人拒否率を低減させ，かつ，全体で他人受入率も低下させることができる．

4.1 指紋の特徴量

4.1.1 指紋の隆線に基づく特徴量

今回は Veridicom 社の 5th Sense☆という指紋読み取り装置を使用して，指紋画像を取得する．指紋画像は 300×300 画素のモノクロ画像として得られる．本論文では，この指紋画像を小さなブロックに分割し，各ブロックにおける隆線の角度を特徴量とする．なお，各ブロックの隆線の角度の抽出に関しては，基本的に

☆ 5th Sense は Veridicom 社の登録商標です．

文献 10) の 2.4 節で述べられている方法を採用した．抽出手順は以下のとおりである．

(1) 対象画像抽出処理
指紋画像に対して輝度の正規化を行ったうえで，指紋画像を小さなブロックに分割する．本方式では 1 ブロックのサイズを 16×16 画素，ブロック数を 8×8 個とした．すなわち，300×300 画素の指紋画像の中の中央の 128×128 画素を使用する．

(2) 特徴抽出処理
すべての画素 (u,v) に Sobel 演算子を適用し，各画素の x 勾配 $\partial_x(u,v)$ と y 勾配 $\partial_y(u,v)$ を得る．

(3) ブロック化処理
各ブロックごとに (2) で得た $\partial_x(u,v)$ と $\partial_y(u,v)$ を使って，以下の計算を行い，$\theta(p,q)$ を得る．なお，$\sum_{u=p-8}^{p+8}\sum_{v=q-8}^{q+8}$ は第 (p,q) ブロックに含まれる 16×16 画素における和を意味する．$\theta(p,q)$ がブロック (p,q) における隆線の角度である．

$$V_x(p,q)=\sum_{u=p-8}^{p+8}\sum_{v=q-8}^{q+8}\left\{\partial_x^2(u,v)-\partial_y^2(u,v)\right\}$$

$$V_y(p,q)=\sum_{u=p-8}^{p+8}\sum_{v=q-8}^{q+8}2\partial_x(u,v)\,\partial_y(u,v)$$

$$\theta(p,q)=\frac{1}{2}\tan^{-1}\left(\frac{V_y(p,q)}{V_x(p,q)}\right)$$

(4) ブロック間平滑化処理
(3) で求めた $\theta(p,q)$ には突発的なノイズによって局所的な誤差が生じている可能性がある．そこで，周囲 2 近傍ブロックの隆線の角度の情報を用いて誤差を吸収する．
i) 以下の計算により，$\Phi_x(p,q)$ と $\Phi_y(p,q)$ を求める．

$$\Phi_x(p,q)=\cos(2\theta(p,q))$$
$$\Phi_y(p,q)=\sin(2\theta(p,q))$$

ii) 求めた $\Phi_x(p,q)$ と $\Phi_y(p,q)$ に対して，5×5 ブロックの low-pass フィルタをかけ，誤差の吸収を試みる．その結果である $\Phi'_x(p,q)$ と $\Phi'_y(p,q)$ から，以下の計算によって誤差吸収後の隆線の角度 $V(p,q)$ を求める．

$$V(p,q)=\frac{1}{2}\tan^{-1}\left(\frac{\Phi'_y(p,q)}{\Phi'_x(p,q)}\right)$$

iii) この $V(p,q)$ がブロック (p,q) の特徴量となる．

(5) ベクトル化処理
$j=8p+q+1$ の変換により，8×8 ブロックの各特徴量 $V(p,q)$ からの特徴量ベクトル $\boldsymbol{V}=\{V_j\,|\,1\leqq j\leqq 64\}$ が得られる．

ただし，実際には，この前処理として，指紋読み取り時の位置ズレ（平行移動，回転移動）を補正する処理が加わる．今回は，指紋データのマニューシャの位置を利用して位置補正を行った．位置補正の詳細は脚注☆に示したとおりであるが，明らかに位置補正に失敗している指紋画像も散見された．位置補正アルゴリズムの改良は本論文のスコープから外れるため，ここでは，これらの指紋画像に対しては手動で再補正を行った．

また，読み取り時の位置ズレあるいはかすれなどのために，隆線が検出されないブロックが発生することがある（以降，このブロックを空白ブロックと呼ぶ）．本方式では空白ブロックの検出を行い，空白ブロックが検出された指紋画像に対しては，登録フェーズにおいて 4.2.1 項の手順 (5) で示す例外処理を施すことにする．

4.1.2 指紋の周波数成分による特徴量

4.1.1 項と同様の方法で得られた指紋画像を 2 次元 DCT 変換で周波数成分に変換し，その周波数成分から特徴量を得る．抽出手順は以下のとおりである．

(1) 対象画像抽出処理
指紋画像の中心から 128×128 画素を切り取る．

(2) 特徴抽出処理
切り取った画像に 2 次元 DCT 変換を施し，128×128 個の周波数成分 $W(r,s)$ を得る．

(3) ブロック化処理
指紋を取得する際，毎回の指の置き方の違いによって隆線の幅が伸縮し，本来の周波数成分の振幅の分布が変動することになる．そこで，周波数空間をある程度の大きさにブロック化してブロック内の振幅値を平均することによって，

☆ 具体的な位置補正のアルゴリズムは以下のとおり．
1. 登録フェーズにて 10 枚の指紋画像が入力された時点で，その中の 1 枚を基準画像として選ぶ．
2. 登録フェーズにおいては，マニューシャの位置情報および角度情報を用いて，基準画像のマニューシャと残りの 9 枚の指紋画像のマニューシャの相対位置が最小になるように 9 枚の指紋画像の位置をそれぞれ調整する．
3. スケールを作成した時点で，基準画像のマニューシャの位置情報のみをスケールに記録しておく．また，スケールには無効ブロック（4.2.1 項の手順 (5) を参照）の位置も記録する．
4. 鍵生成フェーズにおいては，指紋画像が入力されるたびに，マニューシャの位置情報のみを用いて，基準画像のマニューシャと入力画像のマニューシャの相対位置が最小になるように入力画像の位置をそれぞれ調整する．

ブロック内における振幅の変動を吸収する．また，今回，実験で用いた指紋読取装置にはオートゲインコントロール機能が用いられている影響で，取得した指紋画像に縞模様状のノイズが発生することがある．ブロック内を平均化することは，ある特定の周波数に乗ってくるノイズをブロック内に分散させる効果も期待できる．

i) (2) で得られた $W(r,s)$ のうちの $1 \leqq r, s \leqq 125$ の成分を，5×5 成分ごとに 25×25 個のブロックに分割し，以下の式により周波数成分の平均値を計算する．

$$\varphi(l,m) = \frac{1}{25} \sum_{r=5l}^{5l+4} \sum_{s=5m}^{5m+4} W(r,s)$$

なお，$\sum_{r=5l}^{5l+4} \sum_{s=5m}^{5m+4}$ は第 (l,m) ブロックに含まれる 5×5 成分における和を意味する．$\varphi(l,m)$ がブロック (l,m) における周波数成分の平均である．

ii) $W(r,s)$ の $r=0$ または $s=0$ の成分に関連する低周波成分ブロック（$l=0$ または $m=0$ となる $\varphi(l,m)$）には，隆線の模様に含まれる周波数帯よりも低い周波数成分が多く含まれているため，これを除く．また，サンプリング定理より隆線の模様に含まれる最高調波の 2 倍以上の成分は無意味であることから，高周波成分（$l+m \geq 13$ となる $\varphi(l,m)$）を除く．この結果，ブロックの数は 25×25 個から 90 個になる．

(4) ベクトル化処理

90 ブロックの周波数成分 $\varphi(l,m)$ が特徴量ベクトル $\boldsymbol{U} = \{U_k \,|\, 1 \leqq k \leqq 90\}$ となる．

4.1.3 各特徴量の特性

指紋を指紋読取装置で読み取った際に生じるノイズとしては以下のものが考えられる．

(1) 指紋画像の位置ズレ（平行移動，回転移動）

(2) 指の置き方の不良もしくはスキャナに付着したゴミなどによる指紋画像の欠落

(3) 指の置き方のゆがみによる指紋画像の変形

(1) のノイズに対しては，本方式では，指紋画像の位置補正を行っているため，隆線の傾きに基づく特徴量 $\boldsymbol{V}$ も周波数成分に基づく特徴量 $\boldsymbol{U}$ も，大きな悪影響を受けないと考えられる．これに対し，(2) のノイズは，欠落領域の隆線が欠損することになるため，特徴量 $\boldsymbol{V}$ を劣化させる原因となる．しかし，指紋画像の大部分が残っていれば，指紋としての特徴は依然として周波数成分に現れる．よって，画像欠落の周波数領域における影響が，統計的 AD 変換や誤り訂正によって吸収できる程度の大きさである限り，正しく鍵生成が行える．すなわち，特徴量 $\boldsymbol{U}$ は (2) のノイズにある程度ロバストである．一方，(3) のノイズは，隆線の幅を伸縮させることに通じるため，特徴量 $\boldsymbol{U}$ を劣化させる原因となる．しかし，隆線の傾きを局所的に歪ませるほどのゆがみでなければ，特徴量 $\boldsymbol{V}$ への影響は少ない．以上のことから，今回採用した 2 つの特徴量 $\boldsymbol{U}$ と $\boldsymbol{V}$ は（完全に独立ではないであろうが）互いに補い合う関係となっており，併用するに適した特徴量であると考えられる．

4.2 各特徴量を用いての統計的 AD 変換

隆線の傾きに基づく特徴量 $\boldsymbol{V}$ と周波数成分に基づく特徴量 $\boldsymbol{U}$ を用いて統計的 AD 変換によって生体鍵を生成するための具体的なアルゴリズムを説明する．

4.2.1 指紋の登録（登録フェーズ）

(1) 正規ユーザの指紋を 10 回読み取る．

(2) 複数個の指紋データのそれぞれについて，隆線の傾きに基づく特徴量 $\boldsymbol{V} = \{V_j \,|\, 1 \leqq j \leqq 64\}$，および，周波数成分に基づく特徴量 $\boldsymbol{U} = \{U_k \,|\, 1 \leqq k \leqq 90\}$ を求める．

(3) V_j の平均 μ_j と標準偏差 σ_j を計算する．同様に，U_k の，平均 μ_k と標準偏差 σ_k を計算する．ただし，U_k に対しては，実際に指紋の周波数成分の統計的 AD 変換を行うという予備実験を実施したところ，許可範囲 $[\mu_k - n_k\sigma_k, \mu_k + n_k\sigma_k)$ が極端に小さくなってしまう周波数ブロックが存在する場合があることが分かった．そこで，このような許可範囲に関しては，周囲の近傍ブロックの周波数成分の情報を用いて，これを伸張してやることで当該許可範囲からの ID 生成の精度を向上させる．今回は，各ブロックの標準偏差に対して周辺ブロックとの平滑化を行うことによって，これを行う．具体的には，各ブロックの標準偏差 σ_k（$1 \leqq k \leqq 90$）に対して，周波数平面上で 5×5 ブロックのガウスフィルタをかけ，σ_k を平滑化する．ただし，この結果，標準偏差が元の値より小さくなってしまうブロックの値は変更しない．以後，σ_k（$1 \leqq k \leqq 90$）はブロック間平滑化が施された標準偏差であるとする．

(4) V_j の許可範囲を $[\mu_j - n_j\sigma_j, \mu_j + n_j\sigma_j)$ の区間に設定し，スケールを生成する．同様に，U_k の許可範囲を $[\mu_k - n_k\sigma_k, \mu_k + n_k\sigma_k)$ の区間に設定し，スケールを生成する（n_j，n_k は統計的 AD 変換におけるセキュリティパラメータである）．

(5) 隆線の傾きに基づく特徴量 $\boldsymbol{V} = \{V_j \,|\, 1 \leqq j \leqq 64\}$ においては，$n_j\sigma_j$ の値（スケールの幅）が 90° 以上となったブロックからは ID 抽出を行わないこと（無効ブロック）とする．また，登録用の指紋画像中に空白ブロックが存在した場合，空白ブロックは統計解析の対象から除外される．ただし，登録用の指紋画像 10 枚のうち，3 枚以上の指紋画像で同じブロックが空白ブロックとなった場合には当該ブロックを無効ブロックとする．

(6) m^V ビット誤り訂正符号の中から任意の符号 R^V をランダムに選ぶ．同様に，m^U ビット誤り訂正符号の中から任意の符号 R^U をランダムに選ぶ（m^V，m^U は Fuzzy Commitment における誤り訂正強度のパラメータである）．

(7) 補助情報 $F(ID^V) = ID^V \oplus R^V$ を計算し，$F(ID^V)$ を，スケールとともに記憶する．同様に，補助情報 $F(ID^U) = ID^U \oplus R^U$ を計算し，$F(ID^U)$ を，スケールとともに記憶する．

以上の処理により，すべての特徴量に対するスケールおよび $F(ID^V)$ と $F(ID^U)$ が登録情報として記憶されることになる．

4.2.2 指紋からの ID 抽出（鍵生成フェーズ）

(1) 指紋を読み取り，特徴量を算出する．

(2) すべての特徴量に対して，記憶されている各々のスケールを用いて，特徴量の値が含まれる区間に割り当てられた乱数を抽出する．隆線の傾きに基づく特徴量から抽出された乱数を連結することにより $ID^{V\prime}$ を得る．同様に，周波数成分に基づく特徴量から抽出された乱数を連結することにより $ID^{U\prime}$ を得る．ここで，指紋を指紋読取装置で読み取った際に生じるノイズのために，$ID^{V\prime}$ および $ID^{U\prime}$ は，登録フェーズにおける ID^V および ID^U と異なりうる．

(3) 記憶されている補助情報 $F(ID^V)$，$F(ID^U)$ を使い，$ID^{V\prime}$ および $ID^{U\prime}$ に対して，Fuzzy Commitment による誤り訂正を行う．訂正結果を $ID^{V\prime\prime}$，$ID^{U\prime\prime}$ とする．$ID^{V\prime}$ および $ID^{U\prime}$ の誤りがそれぞれ m^V ビット以内，m^U ビット以内であれば，ID^V，ID^U が復元される．

(4) $ID = (ID^{V\prime\prime} \,||\, ID^{U\prime\prime})$ のハッシュ値が生成鍵である．ここで，‘||’ は連結を表す．

4.3 パラメータの調整

3.1 節に示したように，本方式においては，「各特徴量から生成される ID に関する本人拒否率をそれぞれ独立に十分小さくしたうえで，これらを重ね合わせる」という方策によって，全体の本人拒否率を低く保ちながら，全体の他人受入率の低減を達成するというアプローチとなる．

このため，本方式によれば，パラメータ（セキュリティパラメータ n や誤り訂正強度 m）の調整については，各特徴量ごとに独立に，かつ，単一の指標（本人拒否率のみ）を用いて実施することが可能である．一般的に，本人拒否率と他人受入率はトレードオフの関係にあるため，これらパラメータの適正な調整は容易ではない．特徴量が複数ある場合には，特徴量の組み合わせ方によっても本人拒否率と他人受入率のバランスが変わるため，パラメータの調整はさらに困難となる．よって，各特徴量ごとに独立に，かつ，本人拒否率の低減のみを狙ってパラメータの値を調整・決定することができる本方式は，実用的であると考えられる．

なお，パラメータを調整するための具体的な方法としては，以下の 2 つのアプローチが考えられる．

- アプローチ 1：

(1) 特徴量 $\boldsymbol{V}$ に関するパラメータ n^V および m^V を調整し，特徴量 $\boldsymbol{V}$ から生成される ID^V に関する「本人拒否率」が十分小さくなるように，n^V，m^V の値を決定する．

(2) 特徴量 $\boldsymbol{U}$ に関するパラメータ n^U および m^U を調整し，特徴量 $\boldsymbol{U}$ から生成される ID^U に関する「本人拒否率」が十分小さくなるように，n^U，m^U の値を決定する．

- アプローチ 2：

(1) 特徴量 $\boldsymbol{V}$ に関するパラメータ n^V および m^V を調整し，特徴量 $\boldsymbol{V}$ から生成される ID^V に関しては，「本人拒否率と他人受入率」がともに十分小さくなるように，n^V，m^V の値を決定する．

(2) 特徴量 $\boldsymbol{U}$ に関するパラメータ n^U および m^U を調整し，特徴量 $\boldsymbol{U}$ から生成される ID^U に関する「本人拒否率」が十分小さくなるように，n^U，m^U の値を決定する．

アプローチ 1 がすべての特徴量を等しく扱う方法であるのに対し，アプローチ 2 は「ある 1 つの特徴量（$\boldsymbol{V}$）をベースとして，まずはベースとなる特徴量（$\boldsymbol{V}$）に対して本人拒否率と他人受入率の両者を満足するようにパラメータを調整しておき，他の特徴量（$\boldsymbol{U}$）についてはベースとなる特徴量（$\boldsymbol{V}$）の精度をさらに高めるために使用する」というタイプの方法となる．なお，上記の例では，特徴量 $\boldsymbol{V}$ をベースとした記述となっているが，特徴量 $\boldsymbol{U}$ をベースとしてもかまわない．

5. 精度評価実験

5.1 実験内容

4.1 節で示した 2 つの特徴量を用い，実際に指紋から生体鍵を生成する．今回の実験では以下について検証する．

(1) FRR（本人拒否率）：指 α が登録されている場合に α の指紋から本来抽出されるべき生体鍵が抽出されない確率．

(2) FAR（他人受入率）：指 α が登録されている場合に α 以外の指の指紋から α と同一の生体鍵が抽出されてしまう確率．

(3) FRR＋FAR：精度評価の目安として，FRR と FAR の和を用いる☆．

なお，文献 3) では生成された生体鍵の（みかけの）ビット長を算出していたが，実際に重要となるのは生体鍵のエントロピ（実効ビット長）である．生体鍵のエントロピは「本人と他人の相違度」であるため，他人受入率の逆数により測ることができると考えられる．また，本論文の主題は統計的 AD 変換の精度向上にあることからも，今回は生体鍵の（みかけの）ビット長については評価対象から除外した．

実験に先立ち，本学の男子学生 8 人を被験者として，各人の左右の手のそれぞれから人差し指と中指の指紋画像を採取し，各指ごとにそれぞれ 40 枚，合計 1280 枚（8 人 × 4 指 × 40 枚）の指紋画像を採取した．以下では，32 本の指（8 人 × 4 指）を指 1〜指 32 と呼ぶことにする．

実験手順を以下に示す．

(1) 指 1 の指紋画像 40 枚のうち，先に採取したものから 10 枚抜き出し，それらを登録用の指紋画像とする．そして，残りの指紋画像 30 枚を評価用の指紋画像とする．

(2) 指 1 の登録用の 10 枚の指紋画像から，4.1 節の方法により 2 種類の特徴量 $\boldsymbol{V} = \{V_j \,|\, 1 \leqq j \leqq 64\}$ および $\boldsymbol{U} = \{U_k \,|\, 1 \leqq k \leqq 90\}$ を算出し，4.2.1 項の方法によりそれぞれの特徴量に対するスケールを作成する．ただし，セキュリティパラメータ n_j，n_k の影響を測るため，同一特徴量においては一律の値 n^V と n^U を用いることとしたうえで，n^V については 3.0 から 6.0 まで，n^U については 4.0 から 7.0 まで 1.0 刻みで変更し，各々の場合のスケールを作成した．したがって，$\boldsymbol{V}$ と $\boldsymbol{U}$ のそれぞれに 4 種類のスケールが生成されることになる．

(3) 4.2.1 項の方法に従い，$\boldsymbol{V}$ と $\boldsymbol{U}$ のそれぞれに対する補助情報 $F(ID^V)$，$F(ID^U)$ を作成する．ここで，補助情報を作成するにあたり，ID^V，ID^U のそれぞれに対する誤り訂正強度 m^V，m^U を設定する必要があるが，実際には適切な誤り訂正強度（ID^V 抽出および ID^U 抽出における本人拒否率を可能な限りゼロに近づけるために必要となる誤り訂正強度）を事前に求めることは容易ではない．そこで，今回の実験では，m^V を 5 から 9，m^U を 4 から 8 まで 1 ずつ変化させて，それぞれ 5 種類の $F(ID^V)$，$F(ID^U)$ を生成した．

(4) 作成したスケールと補助情報を用いて，指 1 の評価用の 30 枚の指紋画像から生体鍵を生成し，指 1 に対する FRR を求める．すなわち，FRR は「30 枚中，誤って異なる生体鍵が生成されてしまう指紋画像数」の割合となる．ただし，4.1.1 項の脚注で示した位置合わせを行った時点で空白ブロックが検知された指紋画像に対しては，指紋の再入力を促すという対処が可能であるということに鑑み，今回の実験では評価の対象から除外することとし，その割合を別途，本人の指紋に対する取得失敗率 FTAR として算出する．また，実際には指紋から抽出された ID のハッシュ値が生体鍵となるが，本実験の本質は指紋から一意な ID が生成可能であるかを検証することにあるため，ID が一致するかどうかを評価することとした．

(5) 作成したスケールと補助情報を用いて，指 1 以外の指（指 2〜指 32）の評価用の指紋画像 930 枚（31 指 × 30 枚）から生体鍵を生成し，指 1 に対する FAR を求める．すなわち，FAR は「930 枚中，誤って正しい生体鍵が生成されてしまう指紋画像数」の割合となる．手順 (4) と同様に，FTAR については別途算出し，また，ID を評価対象とする．

(6) 指 2 から指 32 に対して，手順 (1)〜(5) を繰り返す．最後に，すべての指の FRR，FAR，FTAR の平均を算出する．

☆ 生体認証の精度評価の目安には，一般的に EER（Equal Error Rate）が用いられる．しかし，本論文の実験では変動させているパラメータ（n^V，m^V，n^U，m^U）が離散値であるため，FAR と FRR のクロスポイントを適切に求めることが難しい状態であった．そこで今回は，統計的パターン認識における識別能力の限界の指標となるベイズ誤り確率が生体認証においては（本人と他人の認証の機会が等しいという条件では）「FRR + FAR」の最小値であることに鑑みて，EER に代わる評価指標として，「FRR + FAR」を使用することとした．

表 1 様々な n を用いた ID 抽出結果
Table 1 Experimental results of ID extraction using various values of n.

n^V	n^U	4	5	6	7
3	FRR [%]	4.73	2.14	1.91	1.91
	FAR [%]	0.17	0.26	0.32	0.34
	FRR+FAR [%]	4.90	2.40	2.23	2.26
4	FRR [%]	3.49	0.90	0.68	0.68
	FAR [%]	0.35	0.55	0.67	0.75
	FRR+FAR [%]	3.84	1.45	1.34	1.42
5	FRR [%]	3.27	0.56	0.34	0.34
	FAR [%]	1.44	2.16	2.66	2.96
	FRR+FAR [%]	4.70	2.73	3.00	3.30
6	FRR [%]	3.27	0.56	0.34	0.34
	FAR [%]	1.73	2.58	3.16	3.51
	FRR+FAR [%]	5.00	3.14	3.50	3.85

セキュリティパラメータ n^V，n^U の影響を分析するため，**表 1** に n^V，n^U のみを変動させた結果を示す．表 1 には代表的なものとして誤り訂正強度をそれぞれ $m^V = 7$，$m^U = 6$ に固定したものを記載した．同様に，m^V，m^U の影響を分析するため，**表 2** に m^V，m^U のみを変動させた結果を示す．セキュリティパラメータはそれぞれ $n^V = 5$，$n^U = 5$ に固定したものである．なお，今回の実験における FTAR は，本人の指紋に対する FTAR が平均約 0.075（7.5%），他人の指紋に対する FTAR が平均約 0.33（33%）であった．

表 1 より，n^V，n^U のそれぞれが大きくなるに従って本人拒否率が小さくなり，他人受入率が大きくなっていることが分かる．表 2 より，m^V，m^U についても同じ傾向であった．

5.2 アンサンブルモデルの適用と誤り訂正の導入の効果

本論文の主旨は，a) アンサンブルモデルの適用，および，b) 誤り訂正の導入による統計的 AD 変換の精度向上である．そこで，a および b の導入効果を評価するために，以下の各方式との比較検討を行った．

方式 1：従来の統計的 AD 変換[3)]
　方式 1-a：特徴量 $\boldsymbol{V}$ のみからの ID 抽出
　方式 1-b：特徴量 $\boldsymbol{U}$ のみからの ID 抽出
方式 2：アンサンブルモデルのみを適用した統計的 AD 変換
方式 3：誤り訂正のみを導入した統計的 AD 変換
　方式 3-a：特徴量 $\boldsymbol{V}$ のみからの ID 抽出
　方式 3-b：特徴量 $\boldsymbol{U}$ のみからの ID 抽出
方式 4：提案方式
　方式 4-a：アプローチ 1 による ID 抽出
　方式 4-b：アプローチ 2 による ID 抽出
　　方式 4-b-1：特徴量 $\boldsymbol{V}$ をベースとした ID 抽出
　　方式 4-b-2：特徴量 $\boldsymbol{U}$ をベースとした ID 抽出

上記のそれぞれの方式に対して，各種パラメータ（n^V，m^V，n^U，m^U）の組合せによる統計的 AD 変換を実行し，FRR＋FAR が最小となった場合のデータを**表 3** にまとめた．また，方式 3-a と方式 3-b に対しては，FRR が最小となった場合（FRR を最小とするパラメータの組合せが複数あった場合には，その中で FRR＋FAR が一番小さくなるもの）のデータも併記してある（両者を区別するために，FRR を最小にするデータを方式 3-a’，方式 3-b’ と呼び分けることにする）．

まず，方式 1-a（従来の統計的 AD 変換：$\boldsymbol{V}$ のみ使用），方式 1-b（従来の統計的 AD 変換：$\boldsymbol{U}$ のみ使用）と方式 2（アンサンブルモデルのみ適用）を比較すると，方式 1-a の FRR＋FAR が一番小さいことが分かる．3.1 節で複数の特徴量を組み合わせるにあたっては各特徴量ごとの本人拒否率 FRR をゼロに近づけることが肝要であることを述べたが，誤り訂正を導入していない方式 2 においてはそれぞれの特徴量における FRR を十分低減させることができず，複数の特徴量を組み合わせることによって逆に精度の劣化が起こっている．

次に，方式 1-a（従来の統計的 AD 変換：$\boldsymbol{V}$ のみ使用）と方式 3-a（誤り訂正のみ導入：$\boldsymbol{V}$ のみ使用），あるいは，方式 1-b（従来の統計的 AD 変換：$\boldsymbol{U}$ のみ使用）と方式 3-b（誤り訂正のみ導入：$\boldsymbol{U}$ のみ使用）を比較すると，両者の FRR＋FAR に大差はないことが分かる．3.2 節で述べたとおり，誤り訂正は本人拒否率 FRR を低減させる一方で他人受入率 FAR を増加させてしまうため，単に誤り訂正を導入しただけでは FRR＋FAR を下げることができていない．

これらに対し，方式 4-b-1（提案方式：アプローチ 2：$\boldsymbol{V}$ ベース）は，方式 1-a（従来の統計的 AD 変換：$\boldsymbol{V}$ のみ使用），方式 1-b（従来の統計的 AD 変換：$\boldsymbol{U}$ のみ使用）に対して，FRR+FAR の低減を達成している．ただし，方式 4-a（提案方式：アプローチ 1）および方式 4-b-2（提案方式：アプローチ 2：$\boldsymbol{U}$ ベース）においては精度の改善がみられない．方式 3-a（誤り訂正のみ導入：$\boldsymbol{V}$ のみ使用：FRR+FAR 最小）と方式 3-b（誤り訂正のみ導入：$\boldsymbol{U}$ のみ使用：FRR＋FAR 最小）

表 2 様々な m を用いた ID 抽出結果
Table 2 Experimental results of ID extraction using various values of m.

m^V \ m^U		4	5	6	7	8
5	FRR［%］	1.35	0.79	0.56	0.45	0.34
	FAR［%］	1.17	1.35	1.54	1.72	1.84
	FRR+FAR［%］	2.52	2.14	2.10	2.17	2.18
6	FRR［%］	1.35	0.79	0.56	0.45	0.34
	FAR［%］	1.42	1.63	1.85	2.06	2.21
	FRR+FAR［%］	2.77	2.42	2.41	2.51	2.54
7	FRR［%］	1.35	0.79	0.56	0.45	0.34
	FAR［%］	1.67	1.92	2.16	2.41	2.59
	FRR+FAR［%］	3.02	2.71	2.73	2.86	2.92
8	FRR［%］	1.35	0.79	0.56	0.45	0.34
	FAR［%］	1.98	2.26	2.54	2.80	3.02
	FRR+FAR［%］	3.33	3.05	3.10	3.26	3.36
9	FRR［%］	1.24	0.68	0.34	0.23	0.11
	FAR［%］	39.99	46.52	52.56	58.53	63.99
	FRR+FAR［%］	41.23	47.20	52.90	58.76	64.10

表 3 各方式による ID 抽出の結果
Table 3 Experimental results of ID extraction by comparative schemes.

	従来の統計的 AD 変換		アンサンブルモデルの適用	誤り訂正の導入				提案方式		
	Vのみ	Uのみ	複数の特徴量	Vのみ		Uのみ		アプローチ 1	アプローチ 2	
									Vベース	Uベース
	方式 1-a	方式 1-b	方式 2	方式 3-a (FRR+FAR 最小)	方式 3-a' (FRR 最小)	方式 3-b (FRR+FAR 最小)	方式 3-b' (FRR 最小)	方式 4-a	方式 4-b-1	方式 4-b-2
n^V	6	−	6	4	5	−	−	5	4	5
m^V	−	−	0	8	5	−	−	5	8	5
n^U	−	6	7	−	−	4	6	6	6	4
m^U	−	−	0	−	−	4	5	5	5	4
FRR［%］	0.90	10.47	5.74	0.45	0.34	6.53	0.11	0.34	0.45	6.64
FAR［%］	0.79	19.67	0.23	1.02	2.56	22.21	60.43	1.74	0.73	0.69
FRR+FAR［%］	1.69	30.15	5.97	1.47	2.90	28.75	60.54	2.08	1.18	7.33

の結果から分かるように，特徴量 $\boldsymbol{U}$ を用いた際の精度は特徴量 $\boldsymbol{V}$ に対して 1 桁以上悪い．このため，特徴量 $\boldsymbol{U}$ を特徴量 $\boldsymbol{V}$ と対等に扱う方式 4-a や特徴量 $\boldsymbol{U}$ をベースにする方式 4-b-2 については，FRR + FAR の低減が得られなかったのだと考えられる．

なお，方式 3-a（誤り訂正のみ導入：$\boldsymbol{V}$ のみ使用：FRR + FAR 最小）におけるパラメータ（$n^V = 4$, $m^V = 8$）と方式 3-b'（誤り訂正のみ導入：$\boldsymbol{U}$ のみ

使用：FRR 最小）におけるパラメータ（$n^U = 6$, $m^U = 5$）の組合せによって方式 4-b-1（提案方式：アプローチ 2：特徴量 $\boldsymbol{V}$ ベース）が得られている．この事実から，特徴量 $\boldsymbol{V}$ の FRR＋FAR が最小となる $n^V = 4$, $m^V = 8$ のパラメータに対して特徴量 $\boldsymbol{U}$ の FRR が最小となる $n^U = 6$, $m^U = 5$ のパラメータを組み合わせるという提案方式のアプローチ 2 によって，本人拒否率 FRR を保ったまま，他人受入率 FAR の改善が達成されていることが確認できる．これは，今回用意したすべての n^V, m^V, n^U, m^U の組合せを総当たりで試した中でも，FRR＋FAR が最小となるパラメータの組合せであった．

以上より，統計的 AD 変換の精度改善に対しては，適切な特徴量をベースとしたアプローチ 2 によって，アンサンブルモデルの適用と誤り訂正の導入をあわせて実施することが有効であるという結果が示された．ただし，アプローチ 1 に対するアプローチ 2 の優位性については，今回の実験でそれが認められただけであり，これが一般的に成立するかどうかについては今後，理論的・実験的に検証していく必要がある．

6. ま と め

本論文では，生体鍵生成の精度向上を目指し，統計的 AD 変換にアンサンブルモデルの適用と誤り訂正の導入を行った．指紋を例にとり，「隆線の傾き」と「周波数成分」という 2 種類の特徴量を用いて，実際に評価実験を行い，提案方式の有効性を示した．本方式はより多くの特徴量から ID 抽出を行うことでさらに精度を向上させることができると考えられる．今後，より多くの特徴量を用いて実験を行い，本方式を検証していきたい．

また，本方式は指紋への適用に限ったものではなく，複数の特徴量を得ることができるすべての生体情報に適用可能であると考えられる．すでに生体認証として用いられている生体情報を中心に本方式の適用性を議論していきたい．特に，指紋においては，人工物による指紋の偽造および偽造指紋の誤受入という現象が知られており[11]，自身の生体情報の管理が問題になると考えられる．すなわち，本論文で提案している「生体情報から秘密鍵を生成する方式」の採用によって，ユーザは確かに秘密鍵の管理からは開放されるものの，自分の生体情報を秘匿しなければならないという新たな管理を強いられることにもなりうる．そういう意味でも，より管理のしやすい（漏洩しにくい）生体情報を用いての生体鍵生成を考えていくことは重要だと認識している．

謝辞 本研究を行うにあたり，多大なるご助力をいただいた株式会社日立製作所三村昌弘様，高橋健太様に深く感謝の意を表する．また，本研究は一部，(財) セコム科学技術振興財団の研究助成を受けた．ここに謝意を表する．

参 考 文 献

1) Stinson, D.R.: *Cryptography: Theory and Practice*, CRC Press, Inc. (1995).
2) 瀬戸洋一：サイバーセキュリティにおける生体認証技術，共立出版 (2002).
3) 柴田陽一，三村昌弘，高橋健太，中村逸一，曽我正和，西垣正勝：メカニズムベース PKI—指紋からの秘密鍵動的生成，情報処理学会論文誌，Vol.45, No.8, pp.1833–1844 (2004).
4) Feng, H. and Wah, C.C.: Private key generation from on-line handwritten signatures, *Information Management & Computer Security*, pp.159–164 (2002).
5) Chang, Y.-J., Zhang, W. and Chen, T.: Biometric-based cryptographic key generation, *IEEE Conference on Multimedia and Expo 2004* (2004).
6) 特許庁：調査対象技術の技術概要「バイオメトリック照合の入力･認識」. http://www.jpo.go.jp/shiryou/s_sonota/hyoujun_gijutsu/biometric/gaiyou.pdf
7) Marcialis, G.L., Roli, F. and Loddo, P.: Fusion of multiple matchers for fingerprint verification, *Proc. Workshop on Machine Vision and Perception* (2002).
8) Juels, A. and Wattenberg, M.: A Fuzzy Commitment Scheme, *ACM CCS 1999* (1999).
9) 大木哲史，小松尚久，笠原正雄，山崎 恭：バイオメトリクス個人認証における誤り訂正符号の適用に関する一考察，暗号と情報セキュリティシンポジウム 2003（SCIS2003），pp.293–298 (2003).
10) Hong, L., Wan, Y. and Jain, A.: Fingerprint Image Enhancement: Algorithm and Performance Evaluation, *IEEE Trans. pattern analysis and machine intelligence*, Vol.20, No.8, pp.777–789 (1998).
11) 松本 勉：セキュリティ技術の弱点を発見したらどうしますか?，電子情報通信学会誌，pp.202–204 (2001).

(平成 18 年 11 月 29 日受付)
(平成 19 年 6 月 5 日採録)

柴田　陽一（学生会員）

平成 15 年静岡大学情報学部情報科学科卒業．平成 16 年同大学大学院情報学研究科修士課程修了．現在，同大学院理工学研究科博士後期課程．情報セキュリティに関する研究に従事．

宮木　　孝

平成 17 年静岡大学情報学部情報科学科卒業．平成 19 年同大学大学院情報学研究科修士課程修了．同年三菱電機エンジニアリング入社．在学中，情報セキュリティに関する研究に従事．

水野　忠則（フェロー）

昭和 20 年生．昭和 44 年名古屋工業大学経営工学科卒業．同年三菱電機（株）入社．平成 5 年静岡大学工学部情報知識工学科教授．平成 8 年情報学部情報科学科教授．平成 18 年より創造科学技術大学院長．工学博士．情報ネットワーク，モバイルコンピューティング，ユビキタスコンピューティングに関する研究に従事．著訳書としては『コンピュータネットワーク』（日経 BP），『モダンオペレーティングシステム』（ピアソン・エデュケーション）等がある．電子情報通信学会，IEEE，ACM 各会員．情報処理学会フェロー．

西垣　正勝（正会員）

平成 2 年静岡大学工学部光電機械工学科卒業．平成 4 年同大学大学院修士課程修了．平成 7 年同博士課程修了．日本学術振興会特別研究員（PD）を経て，平成 8 年静岡大学情報学部助手．平成 11 年同講師，平成 13 年同助教授．平成 18 年より同大創造科学技術大学院助教授．平成 19 年より准教授．博士（工学）．情報セキュリティ，ニューラルネットワーク，回路シミュレーション等に関する研究に従事．