SCIS 2005 The 2005 Symposium on Cryptography and Information Security
Maiko Kobe, Japan, Jan.25-28, 2005
The Institute of Electronics, Information and Communication Engineers

バイオメトリクス認証テンプレート保護に関する検討

Study on Template Protection for Biometric Authentication

鷲見和彦* 松山隆司 * 中嶋晴久†
Kazuhiko Sumi Takashi Matsuyama Haruhisa Nakajima

あらまし バイオメトリクス個人認証は通常の暗証番号や暗号と違い、バイオメトリクスデータは漏洩してしまった際に取り替えることができないという問題点を持っている．そのため、いったん登録したテンプレートを再登録によって無効化する技術と、テンプレートから元のバイオメトリクスデータを復元したり、他の装置用のテンプレートに作り変えたりするなどの操作を不可能にする技術が必要である．本発表では、このようなテンプレート保護技術をサーベイし、従来技術の問題点を指摘し解決策を示す．これまでの技術には，照合率のスコアを用いてテンプレートが推定できたり，データのモデルがイメージマッチングには適合しているが特徴点マッチングに適合していないなどの課題があり，特徴点抽出におけるエラーモデルを含めて研究すべきことを指摘した．

キーワード Biometrics Authentication, Template Protection, Distance Metrics

1 はじめに

バイオメトリクス個人認証は，唯一の物体の保有や，秘密の情報の保有などのの代わりに本人の生物学的な独自性を用いて本人を認証するものである．バイオメトリクス個人認証は，なりすましにくいという安全性と本人に常に備わっているという利便性が特徴であり，安全な社会の実現には不可欠な認証方法である．

一般的に，バイオメトリクスでは，顔や手の形状などの外見的な特徴，指紋・掌紋・虹彩・網膜や手の静脈などの発生学的にランダムな特徴を持つ身体部位から得られる特徴, あるいは, 署名, 音声, 歩行パターンなどのように安定して現れる行動的特徴などの生体特徴を抽出し，あらかじめ登録された特徴のデータベース (テンプレートと呼ぶ) との間でパターン間の類似性を評価して，十分類似性が高ければ本人と認証する．これらの生体特徴は，特殊な装置を使わなければ可視化することが難しく，かつ，それを模倣したサンプルの製造や使用が困難であるため，容易に人に教えたり貸し借りができる秘密情報や物証より安全であるとされてきた．

ところが，近年の研究によれば，バイオメトリクス個人認証に対して多くの潜在的危険性が指摘されるようになってきた．たとえば，本人の協力や不注意により生のバイオメトリクス情報を得ることができれば，ある条件においては簡単にバイオメトリクス認証装置を詐称する人工サンプルを製作したり，データを詐称される可能性が指摘されはじめた．また，これまで民間におけるバイオメトリクスの利用は，テンプレートを相互に流通させない小規模の閉じたシステムに限られてきたが，バイオメトリクス個人認証の普及によって，様々な場面でバイオメトリクスが使用されるのに伴い，認証機関自身が不正を働き，テンプレートや個人情報を悪用する可能性を考慮しなければならない．生のバイオメトリクスサンプルが得られなくても，テンプレートから認証を可能にするバイオメトリクスサンプルを復元する可能性も指摘されている．このような危険性に対して，バイオメトリクス情報は一旦第三者に知られてしまった場合に，パスワードと違って新しいものと置き換えられないという点が致命的である．

この問題を解決するために，テンプレートを暗号化して保存したり，テンプレートあるいはテンプレートと認証処理を読み出し保護された可搬性メディア内部で行うなどの解決策が示されているが，これらの方式は小さな閉じたシステムでしか成り立たない．たとえば，電子パスポートのように，ある組織 (国) で登録したテンプレートを第三者に示して所有者を認証するようなアプリケーションにおいては，テンプレートを読み出して第三者が取得した生のバイオメトリクスデータとの間で認証をマルチベンダ環境でサポートしなければならない．バイオメトリクスを取得するセンサを含めて認証アルゴリズムを含めての隠蔽は不可能でありテンプレート自身を暴露されてた場合にも安全性を確保するテンプレート保護技

* 京都大学〒 606-8501 京都市左京区吉田本町, Kyoto University, Yoshida Honmachi, Sakyo, 606-8501, Japan
† 社団法人日本自動認識システム協会, 〒 106-0032 東京都港区六本木 3-1-28, 3-1-28 Roppongi, Minato, Tokyo 106-0032, Japan

- **Given**
  Target ID in FR database: TID
- **Preprocessing**
  Normalize, center, equalize local image database: Img[i]
  Calculate eigenface representation: EF[k], $1 \le k \le 400$
- **Determine starting image, Img[0]**
  for i = 1 to number_images
    match_score[i] = req_match_score(Img[i], TID)
    Img[0] = Img[match_score == min(match_score)];
- **Optimize image estimate, Img[j]**
  for j = 0 to optimization_tries
    EF_j= EF[j % number_eigenfaces]
  for k = −3 to 3
    score[k]= req_match_score(Img[j] + $c\,k\,EF_j$, TID)
    set k_{max} to value which maximizes score[k]
  Img[j+1] = Img[j] + $ck_{max}\,EF_j$
  crop Img[j+1] if values outside image bounds

図 1: テンプレートから元のバイオメトリクスデータを復元するアルゴリズム [9]

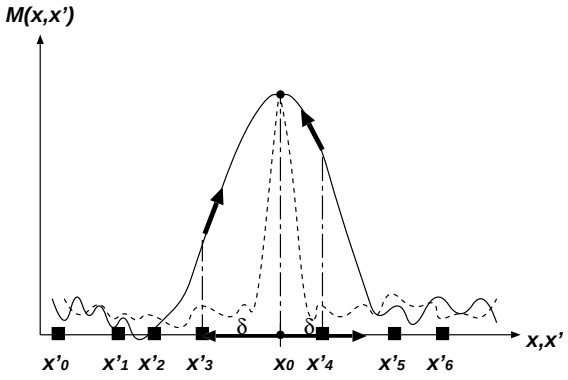

図 2: テンプレート x_0 とデータベース x'_i から元のバイオメトリクスデータを復元可能な条件

術が求められている．

本論文では，このようなテンプレート保護技術についてこれまでの研究開発事例をサーベイし，現状での課題と解決すべき方策を明らかにする．以下，第 2 章ではテンプレートが漏洩した場合の危険性に関する指摘をまとめ, 3 ではテンプレート保護に関するこれまでの主要な研究開発事例をまとめる．

2　テンプレートが漏洩した場合の危険性

生のバイオメトリクスデータを何らかの方法で入手して人工的に模擬したサンプルをつくること [8] は可能であることは指摘されていたが，テンプレートが特徴ベクトルなどの生のバイオメトリクス情報ではなかったり，テンプレートから生のバイオメトリクス情報が直接復元不可能な形式であれば，テンプレートから生のバイオメトリクス情報は復元されないと考えられてきた．それに対して，Hill[5] は元の画像を含まないマニューシャだけの指紋のテンプレートから認証可能な人工指パターンが生成可能なことを示し，Adler[9] は，主成分分析の固有画像への係数しか示されていない顔画像テンプレートから，同じテンプレートを生成でき認証に成功する顔画像を復元できることを示した．

従来，テンプレートは生のバイオメトリクス情報から特徴抽出処理を通して生成され，かつ，特徴抽出処理は画像情報から一部の有用な情報のみを抽出する変換であり，その逆変換は一意に決定できないことから，テンプレートから元のバイオメトリクス情報を復元することは不可能であるとされてきた [6]．しかし Adler は，顔画像を例題にして，十分な大きさの顔画像データベースとアタックすべき目標のテンプレート，および，そのテンプレートと任意のバイオメトリクスサンプルとの間の照合率を得るアルゴリズムがあれば，図 1 に示すアルゴリズムによって元の顔画像を復元できることを示した．

このようなアルゴリズムが成立する条件について考察すると，十分大きなデータベースにはある確率密度 P_X に従った分布のサンプル X が含まれており，初期画像の探索は十分大きなデータベースから目標テンプレート x_0 に一番近いサンプル x' が，テンプレートの照合率を与える関数 $M(x, y)$ において x_0 に向かって単調増加する範囲内に見つかることが十分条件である．この様子を図 2 に示す．図において，照合率の関数 M が実線のように x_0 を中心として $(-\delta, +\delta)$ の範囲で単峰性を持っていれば，データベースに含まれるサンプル $x'_i (i = 1, N)$ からもっとも類似するサンプルを初期値として山登り探索が可能であるが，破線のように δ が小さければ，山登り探索ができず，結果的に元のバイオメトリクスデータを復元することはできない．

3　テンプレート保護に関する研究開発事例

前章で述べたようなテンプレートの漏洩に対する安全性を強化するために，これまでいくつかの手法が提案されてきている．テンプレートを暗号化して保管することもその一例ではあるが，認証機関の内部にも悪意ある管理者が存在する可能性を考えると，テンプレートの復号を前提としたシステムは安全とはいえない．そこで，本章ではオリジナルのテンプレートを必要としないバイオメトリクス認証システムについて研究開発の事例をサーベイする．このような事例としては，Private biometrics[1], Bioscript[3]，Cancelable biometrics[4]，Fuzzy commitment[7]，Quantizing secret extraction[10]，Significant component secret extraction[11] などがある．これらの手法に共通的な概念として，情報の拡散による元データの隠蔽や，Helper data を用いた生のバイオメトリクスデータの揺らぎの吸収などのアイディアが挙げられる．以下，具体的な事例として Cancerable biometrics, Bioscript, Anonymous biometrics[12] についてサーベイする．

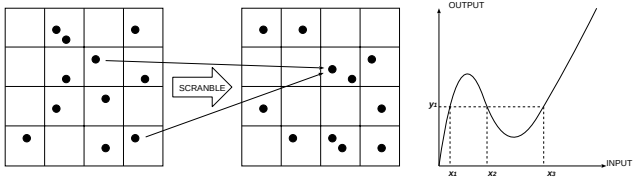

図 3: 一方向の不可逆変換によるテンプレート保護の概念

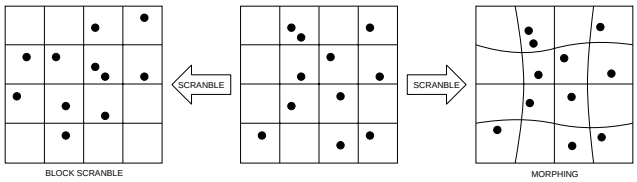

図 4: ブロックスクランブルとモーフィングによるテンプレート保護の概念

3.1 Cancelable Biometics

Cancerable biometrics[4] は IBM の Ratha らによって提案されているテンプレート保護方法である．この手法は, バイオメトリクスデータを多対 1 の対応を持つ一方向関数 (図 3) によって変形させ，元のデータが復元できないようにすること．予測不可能な幾何学的変換 (図 4) を与えて，元のデータが復元できないようにするという概念を用いている．図では，たとえば二次元のデータをブロックごとスクランブルして，複数のブロックから同じブロックへ特徴点を写像させると，元の特徴点配置は一意には復元不可能となる．あるいは，連続値関数の場合には，同図右のような関数を用いて変形させると，変換後の値 y から変換前の値 x を一意に復元不可能である．Ratha はこの概念の具体的な実現方法として予測不可能な幾何学的変換 (図 4) を与えて，元のデータが復元できないようにすることを提案した．図 4 右に示す変換では，ブロック単位で位置を入れ替えることにより元のテンプレートを予測することが困難になっている．この手法は離散的に存在する特徴点のテンプレートを保護するのに適している．また, 同図右の変換では，ブロックの形状に幾何的歪みが加えられ，それに合わせて元の図形を歪ませている．この手法は，ブロック境界での連続性が保存されるので画像のテンプレートを保護するのに適している．

この方式の優れた点は保護後のテンプレートの形式やデータの意味がテンプレート保護を行わない従来のテンプレートとの互換性である．そのため, 特徴抽出やマッチングのアルゴリズムがそのまま利用でき，プライバシー保護されたテンプレートへの移行がスムーズに行えるという運用上のメリットが大きい．

一方，ブロックスクランブルの場合には, ブロックを小さく取ると特徴点の微少な位置ずれに対してミスマッチが生じるため，位置ずれの許容力よりもブロックを大きく取らねばならない．そのためスクランブルのパターンが限られるという問題がある．また，モーフィングの場合にも小さな変形はスクランブルの効果がなく，大きな変形のパターンは限られるという問題がある．

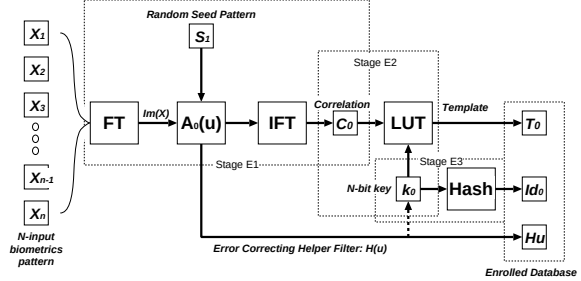

図 5: Bioscript の登録過程

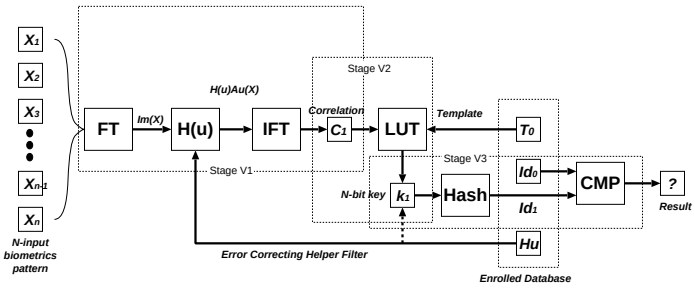

図 6: Bioscript の照合過程

さらに，第 2 に示したように，従来型のマッチングにおいては，類似度が連続値で得られる場合が多く，その場合，たとえ直接元のテンプレートが復元できなくても，ほどほどに良いテンプレートを初期値として探索し，そこから山登り探索を行えば，他人になり済ますことのできるテンプレートを生成可能であるという危険性は残ったままである．

3.2 Bioscript

前節の Cancerable biometrics のような一方向関数は使うが特徴抽出やマッチングのアルゴリズムに互換性を持たせた方式とは異なり，暗号理論を用いてテンプレートを保護するとともに，入力画像の揺らぎを helper data を用いて訂正する機能を与えたものが考案された．Soutar の Bioscript[3] では，次のような三つのステップによって元のバイオメトリクスデータを隠蔽しつつテンプレートを登録し，テンプレートと新たなサンプルとの照合を実現している．

図 5 に Bioscript の登録過程を示し，図 6 に照合過程を示す．図 5 において登録時の入力サンプルデータは $X_i(i = 1, ..., N)$ である．それぞれの入力サンプルは，フーリエ変換によって周波数空間での表現に変換され，その虚数部 $\mathrm{im}(X_i)$ の平均値 $A_0(u)$ に対して，入力信号

と全く無相関の信号 S_r を畳み込んで，それをフィルタ $H(u)$ とし，そのフーリエ逆変換を $c_0(X)$ とする．ここで全く無相関の信号 S_r を畳み込むことによって，X を $H(u)$ や C_0 から推測することは不可能である．さらに，C_0 は二値化されて二次元ビットパターンになり，ランダムに設定されたキー k_0 の $0,1$ に応じて $0,1$ を示すビットパターンをルックアップテーブル (LUT) に記憶させ，その LUT がテンプレート T としてデータベースに記憶される．データベースには，キー k_0 にハッシュ関数を適用して得られるハッシュ値 Id_0 とフィルタ $H(u)$ も併せて記憶される．

図 6 に示す照合時には同じデータがノイズを受けて $Y_i(i = 1, ..., N)$ として観測されると考える．このようにして得られた Y_i に対して，同じくフーリエ変換を行い，その虚数部 $\mathrm{im}(Y_i)$ の平均値 $A_1(u)$ に対して，データベースから得た $H(u)$ を畳み込んで，フーリエ逆変換を行って $c_1(Y)$ を得る．$c_1(Y)$ を二値化した二次元ビットパターンにデータベースから読み出したテンプレート (LUT) を適用して，LUT に記載された位置において $0,1$ 頻度を計数してキー k_1 を復元する．最後に，k_0 に適用したものと同じハッシュ関数を適用して Id_1 を得て，Id_0 と一致すれば照合が成功する．

この方式でテンプレートデータベースに保存されるデータは，フーリエ変換した入力サンプルの虚数部の平均パターンにランダムなビットパターン S_r を畳み込んで得られたフィルタ $H(u)$, 畳み込み結果をフーリエ逆変換して閾値処理した二次元二値ビットマップにランダムなキー k_0 を適用して得られるルックアップテーブル, k_0 のハッシュ値だけであり，これらの値から生のバイオメトリクスデータ X_i や，その成分を復元することができないという復元困難性と，テンプレートデータベースが漏洩した場合には，S_r あるいは k_0 を変更することで，新しいテンプレートを生成でき，漏洩したテンプレートを無効擦ることができる．無効化したテンプレートと新しいテンプレートとは S_r と k_0 が無相関であるため一方から他方を推定することができないという安全性が保証されている．

3.3 Anonymous Biometrics

Tuyles らは文献 [1] [2] [7] [10] [11] に示された複数のアーキテクチャを整理し，Helper Data を用いる Anonymous Biometrics の一般形として図 9 を示した [12].

図 9 において，登録時の入力サンプル $X_i(i = 1...N)$ はエンコーダ E によって特徴ベクトル S と helper data W とを生成する．特徴ベクトル S はハッシュ関数などの不可逆な一方向関数 F によって $\mathrm{F}(S)$ に変形される．ハッシュ関数を用いることで $\mathrm{F}(S)$ から S を推定することを不可能にしている．単純なハッシュ関数は図 7 の様に非常に接近した (距離 δ 以上離れた) 点 ABCD を互

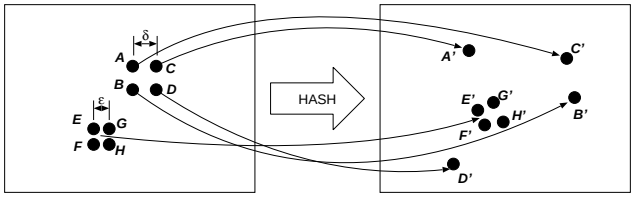

図 7: ハッシュ関数の働きとデータに含まれるノイズ

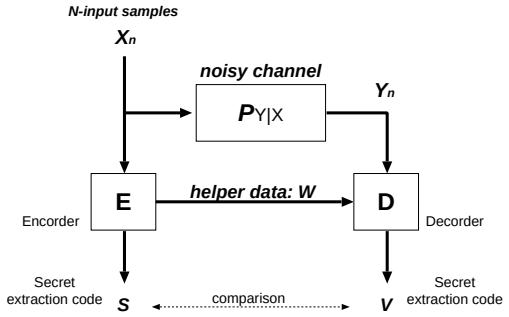

図 8: Helper data と登録サンプル X, 照合サンプル Y との関係

いに遠い位置に写像する．ところが，バイオメトリクスの入力データは常に揺らぎを含んでいるため，照合時には同じ値を観測することはできない．ここでは, 図 8 の様に登録時の入力 X_i が確率 $P_(y|x)$ で表現される雑音を持つ通信路を通して照合時には Y_i として観測されるというモデルを用いる．小さな揺らぎがあって X_i の位置が動くと，ハッシュ関数のために全く違う位置に写像されてしまい X_i と Y_i とはマッチングできない．そのため，揺らぎを含んだ入力から，常に一定の S を生成することが必要となる．

そこで，Helper Data W を別途生成し，W を用いて，互いの距離が ϵ 以下の入力は同じ位置に写像されるようにする．また，互いの距離が δ 以上の入力はハッシュされるようにする．図 8 において，揺らぎがある照合入力サンプル $Y_i(i = 1...N)$ に対して W を適用すると，そのデーコード結果 V が登録時と同じ S が生成できるようになるためには，W は Y のエラー訂正を行うことと等価である．ただし，δ 以上の大きなエラーを持つ入力に対してもエラー訂正を行うことは，互いに離れた二つのサンプルに対して識別する能力がなくなることを意味しており，ϵ, δ の選定には注意が必要である．

Tuyles はこの考えが，Helper Data を画像のような連続値の特徴量に用いる場合 [11] と, 特徴点のような離散値に用いる場合 [10] のいずれにも適用できることを示した．

また，第 3.2 に示した方式は，anonymous biometrics

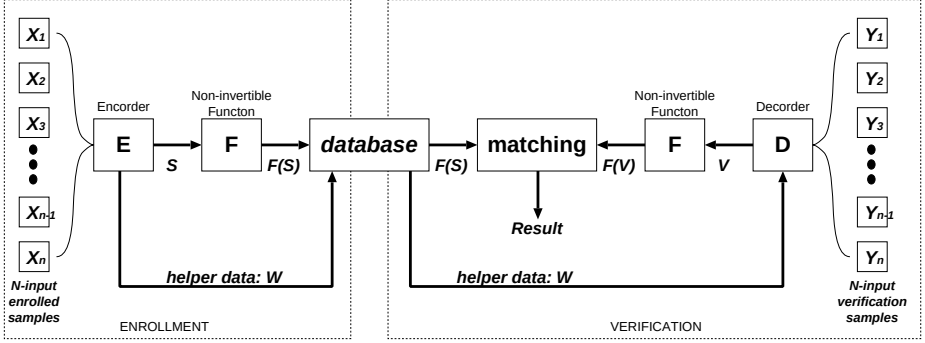

図 9: Helper data を使う Anomymous Biometrics の基本的アーキテクチャ

よりも複雑そうに見えるが，無相関信号 S_r との畳み込みや，ランダムビット列 k_0 をキーとした 0,1 パターンの計数 (LUT 生成) がハッシンングに相当し，S_t との畳み込み結果を保存して，それを再度読み出して入力信号に畳み込んで c_1 を得る部分と，LUT を参照して k_1 を復元する部分が Helper data になっており, Helper アーキテクチャを二重に適用したことに相当すると解釈できる．

4　従来研究の課題と対策

第 3 章に紹介したテンプレートを保護方式には，

1. Distortion transform: 近傍での距離が保存され，遠方での距離が大きく変化する幾何的な変形を与える手法

2. Hashing with helper data: 微少な変動に対するエラー訂正コードを導入した上で，一方向ハッシュ関数を適用する．

という二つの方向がある．

前者は，従来の特徴抽出や照合処理との互換性が高く，システムの移行の障壁が低いので，既存の中・小規模バイオメトリクス個人認証システムをアップグレードするために利用するには適しているが，テンプレートの秘匿の性能の点では十分ではなく，照合関数の仕様が公開されていたり，不特定多数の認証機関へ配布するような用途では安全とは言えない．

後者は，エラー訂正される範囲 ϵ と，識別可能距離 δ とのパラメータを指定して，識別性能を作り込むことが可能であり，広範囲に利用できることが予想されるが，現実の運用に当たっては以下のような課題が残っている．

4.1　入力雑音モデルの推定

Helper アーキテクチャでは，登録データには雑音がなく, 照合データに既知の確率密度分布を持つランダムなノイズが付加されるというモデルを用い，十分の多くのサンプルデータを用いることが前提であった．しかし，登録・照合時に十分多くのサンプルを得ることは利便性の点で困難であり，また，バイオメトリクスサンプルの取得においては，ノイズは短期間には小さいが，時間が経つにつれて大きくなるという性質がある．

したがって，登録時に，本人だけから複数回取得したサンプルを用いて，ノイズ推定を行った場合，長期間の運用においてはエラー訂正の範囲を越えて，本人拒否が多発することが予測される．また，この方式では安全のために元のバイオメトリクスデータを保持していないため，新しく取得したサンプルと登録済のデータベースを統合してテンプレートを更新することは難しい．

また，特徴点の場合には二種類のエラーが存在し，特徴点を見逃し (false negative) たり，議事特徴点を検出 (false positive) したりする場合と，特徴点の検出には成功するがその座標や属性に誤差が含まれる (position error, attribute error) 場合がある．それぞれ，発生原因が違い，発生頻度も違うために，なエラー訂正はそれぞれのエラーモードに併せて設計されるべきである．Sautar や Tuyls が指摘するように，本アーキテクチャは離散特徴モデルにも理論的には適用可能であるが，最適な訂正方法はさらに検討を要するであろう．

4.2　雑音モデルと識別性能要求の矛盾

雑音が大きな場合でも識別性能の限界からある程度以上にはエラー訂正範囲を広げられない．(無理に広げると，false match が常に発生するようになる) また, 山登り探索による攻撃を予防するためには，類似度を連続値として提示することは危険である．そのため，最近傍類似サンプルとの距離以上の雑音が発生する確率の高い状況では，false non-match rate が高まり，利便性が大きく損なわれることが予測される．これは，前述の特徴点のエラーモードに対するモデルの単純さにも起因することが予測される．

4.3　複合バイオメトリクスへの拡張困難性

山登り探索による攻撃を予防するためには，類似度を連続値として提示することは危険である．したがって，個別モードのバイオメトリクス認証結果を統合する複合

バイオメトリクスは設計しにくい．(論理的的な乗算または加算による統合しか設計できない.) 複合バイオメトリクスを実現するには，特徴抽出の段階で統合された特徴を与えるべきであるが，このような統合を，モードごとにマルチベンダーで設計することは非常に難しい．

4.4 課題の解決に向けて

これまでの技術を検討して以上のような課題が判明したので，現在次のような改善を行うことを検討している．

1. 過去のデータベースから入力雑音モデルをオフラインで推定し，登録時の個人サンプルから得られる雑音モデルの不完全さを補う．
2. 雑音モデルの要因別ヘルパーデータの設計と実装．特に，特徴点の座標や特徴点の属性を用いたマッチングに対して，適切な雑音モデルを立てて，それに応じたヘルパーデータ/エラー訂正をインプリメントすることで，識別性能とノイズ耐性との両立が見込める．

5 まとめ

バイオメトリクスの国際間相互運用や大規模な個人認証システムが始まろうとしている中で，テンプレートの保護を考慮した認証技術に関しては，わが国ではほとんど取り組まれてこなかった．今回，海外のテンプレート保護・認証技術を調査し，いくつかの研究・製品化事例をまとめたが，まだまだ問題点が散見される．今後, 特に特徴点方式のテンプレート保護技術を中心に，バイオメトリクスデータの取得と特徴抽出に関するモデルの進化による識別性能の向上への取り組みが進むと思われる．また，複合バイオメトリクスへの適用に関しても，今後の課題としてたいへん興味深い．

謝辞

本研究は，社団法人日本自動認識システム協会との共同研究「バイオメトリクス技術の評価環境・標準化」によるものである．本研究のの遂行にあたり文部科学省 21 世紀 COE プログラム「知的社会基盤構築のための情報学拠点形成」および科学研究費補助金特定領域研究 13224051 の支援を受けた．

参考文献

[1] Davida, G., Frankel, Y., Matt, B., “On enabling secure applications through offline biometric identification”, proc. IEEE Symp. on Security and Privacy, pp.148-157, 1998

[2] Juels A., Wattenberg M., “A fuzzy commitment scheme”, 6th ACM Conf. Comp. and Comm. Security, pp.28-36, 1999

[3] Soutar C., Roberge D., Stoianov A., Gilroy R., Kumar V., “Biometric Encryption”, http://www.bioscrypt.com/assets/Biometric_Encryption.pdf

[4] Ratha N., Connell J., Bolle R., “Enhancing security and privacy in biometircs based authentication systems”, IBM Systems Journal 40, pp.61-634, 2001

[5] Hill C.J., “Risk of masquerade arising from the storage of biometrics”, Bachelor thesis, Dept. of CS, Australian National University, 2002

[6] International Biometric Group, “Generating Images from Templates”, I.B.G. White Paper, 2002, (http://www.ibgweb.com/reports/public/reports/templates_images.html)

[7] Juels A., Sudan, M., “A fuzzy vault scheme”, proc. IEEE Int. Symp. Inf. Theory, p.408, 2002

[8] Matsumoto T., Matsumoto H., Yamada K., Hoshino S., “Impact of artificial g̈ummy f̈ingers on fingerprint systems”, Optical Sec. and Counterfeit Deterrence Techn. IV. Vol. 4677, SPIE, 2002

[9] Adler A., “Sample images can be independently restored from face recognition template”, Can. Conf. Electrical Computer Eng., pp.1163-1166, 2003

[10] Linnartz J.P., Tuyls P. “New shielding functions to enhance privacy and prevent misuse of biometric templates”, proc. 4th Int. Conf. on Audio and Video Based Biometric Person Authentication, pp.393-402, 2003

[11] Verbitskiy E., Tuyls P., Denteneer D., Linnartz J.P., “Reliable biometric authentication with privacy protection”, proc. 24th Symp. Inf. Theory in the Benelux, pp.125-132, 2003

[12] Tuyls P., Goseling J., “Capacity and examples of template-protecting biometric authentication systems”, ECCV Workshop BioAW, no.77, 2004, (//http://eprint.iacr.org/2004/106.pdf)

[13] Maltatu M., D’Alessandro R., D’Amico R., “Toward ubiquitous acceptance of biometric authentcation: template trotection techniques”, ECCV Workshop BioAW, no.97, 2004

原 稿 整 理 票

送付先:

〒 674-8555
明石市大久保町西脇 64
富士通研究所 セキュアコンピューティング研究部 気付
SCIS2005 明石事務局 宛

講演番号	336
講演題目 (和文)	バイオメトリクス認証テンプレート保護に関する検討
講演題目 (英文)	Study on Template Protection for Biometric Authentication
第１著者名	鷲見 和彦
事務局使用欄	