生体認証テンプレート保護技術の動向

鷲見和彦
三菱電機株式会社先端技術総合研究所

アウトライン

- 背景
- テンプレート漏洩に伴う脅威
- テンプレート保護の方式と分析
- テンプレート保護の実装事例と分析
- テンプレート保護の課題と展望
- まとめ

背景

- バイオメトリクス個人認証の普及
  - システムの大規模化・オープン化
    - パスポートなど公的個人認証
    - 登録システムと認証システムが分かれる
  - 類似した応用システムが多数存在する
    - 物理セキュリティ(住宅、企業、会員専用…)
    - 情報セキュリティ(業務系認証、商取引…)
    - 利便目的のカジュアルな応用が現れる(入場券、閲覧権、個人サービス…)

テンプレート共通化・流通とは

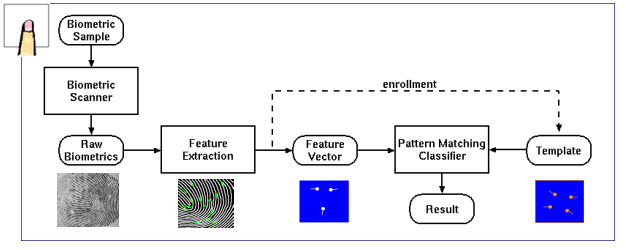
- 利点:
  - 複数アプリケーションが同じテンプレートを使う
  - 組織間での信用継承が可能(パスポートなど)
  - システム開発・登録/運用の安定性とコスト
  - 国際標準化が進行中 (ISO19794)
- 欠点:
  - テンプレート漏洩・悪用の可能性
  - 標準化によりリバースエンジニアが容易
  - 一旦漏洩すると回復不能

アウトライン

- 背景
- テンプレート漏洩に伴う脅威
- テンプレート保護の方式と分析
- テンプレート保護の実装事例と分析
- テンプレート保護の課題と展望
- まとめ

バイオメトリクス認証のモデル

- 登録されたテンプレートと入力されたバイオメトリクスデータから抽出された特徴ベクトルとのパターンマッチングを行う

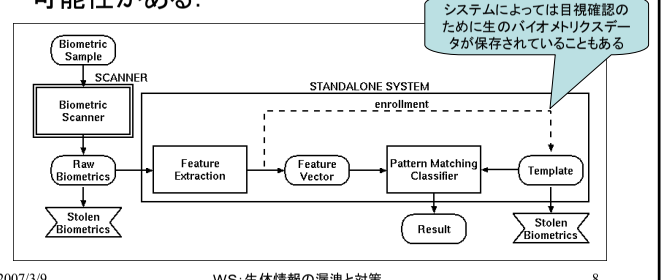


テンプレート脆弱性分析

- 漏洩個所
  - センサの生データを盗み見る
    - センサ信号を傍受、(トロイの木馬による略取も)
    - 生データが保管されたデータベースから盗む
  - テンプレートを盗み出す
    - センターデータベースから盗む
    - センターと装置間の通信を傍受
    - 照合装置に保管されたテンプレートを盗む
    - 個人が携帯するテンプレートを盗む
  - 放置・廃棄されたデータ・機械から取り出す

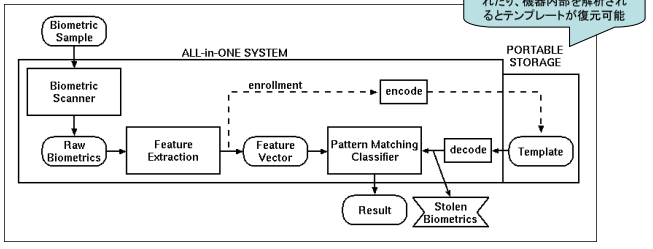
テンプレート漏洩シナリオ(1)

- スキャナと認証システムの間に生のバイオメトリクスデータが存在したり、テンプレートが認証システム内部に保存されたりすると、傍受・盗難の可能性がある.



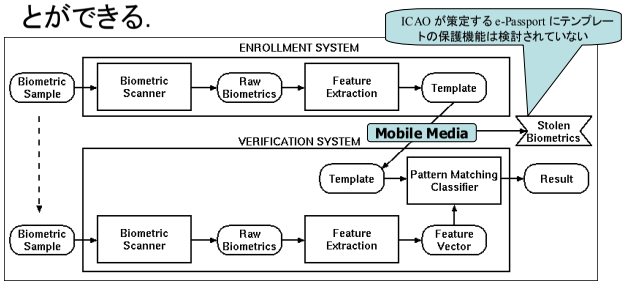
テンプレート漏洩シナリオ（2）

- スキャナー体のスタンドアロンシステムやICカードに暗号化したテンプレートを保存することで、安全性が高まるが、システムが復号していると復号されたテンプレートを入手できる.



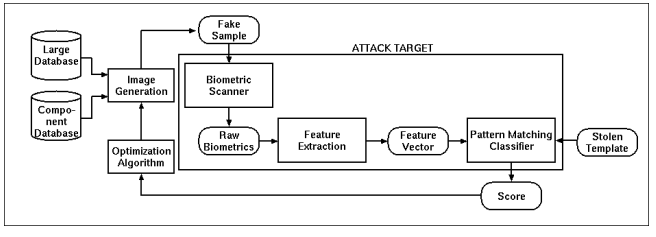
テンプレート漏洩シナリオ（3）

- テンプレートの相互運用可能なオープンシステムでは、テンプレートのフォーマットが公開されており、運用次第で容易にテンプレートを読み取ることができる.



テンプレートが漏洩すると？

- 攻撃ターゲットのシステム内部が隠蔽されていても、テンプレートと十分なデータがあれば、詐称可能なバイオメトリクスサンプルは生成可能である.（Adler,2003）



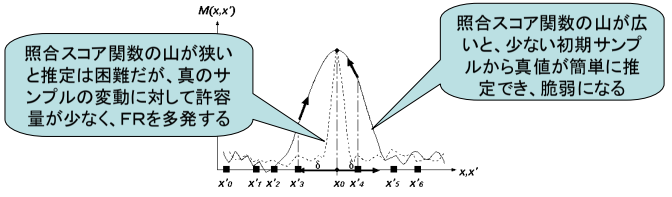
推定の例

- 他人の顔を初期値として登録者を詐称する顔画像を生成した（Adler,2003）

一番類似度の高い実在サンプルを初期値にして、特徴を構成する成分ごとに類似度スコアの山登り探索を行った
人が見ると合成されたことがわかるが、照合関数が返す距離は小さいので認証システムを詐称できる

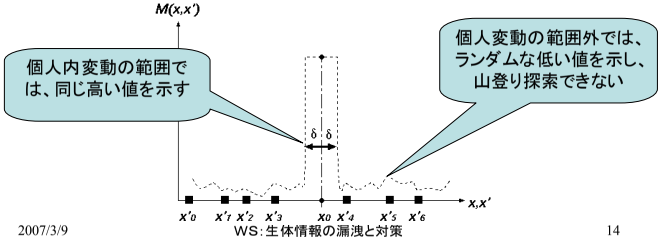
推定可能性

- ほとんどのバイオメトリクス認証方式は、認証結果としてテンプレートとサンプルとの類似度（または距離）を出力することができるので、局所最適解につかまらないように十分な初期値を与えると最適化で認証可能サンプルを生成できる.



理想的な照合関数

- 合致するパターン x から個人内変動 σ の範囲でだけ一定の高い値を示し、それ以外では低いランダムな値をとる関数であれば、互いに σ だけ離れた全ての可能性を調べなければ合致する x を見つけられない



アウトライン

- 背景
- テンプレート漏洩に伴う脅威
- テンプレート保護の方式と分析
- テンプレート保護の実装事例と分析
- テンプレート保護の課題と展望
- まとめ

テンプレートプロテクションの要件

- 復元不可能
  - テンプレートから元のバイオメトリクスデータを復元出来ない
- 改竄検知
  - テンプレートが登録後に改変されたことを検出できる
- 推定不可能
  - テンプレートから認証可能なバイオメトリクスデータを生成できない
- 無効化可能
  - 万一推定された場合にも、そのバイオメトリクスデータを認証しない別のテンプレートを生成できる

テンプレートプロテクションの分類

- 暗号化-復号化
  - テンプレートを暗号化して保存
  - 照合時に装置内部で復号化て利用する
    - ほどよい安全性(秘匿性、改竄検知性)
    - バイオメトリクスと暗号技術は独立
    - 装置内部に侵入されると脆弱・山登り探索可能
- 暗号化と暗号化空間における照合
  - 暗号化されたテンプレートを復号せずに照合
    - 完全な安全性(復元不能、推定不能、破棄可能)
    - バイオメトリクスと暗号技術の複合
    - 非暗号化方式に比べ性能低下が生じる

Matching in Encrypted Space (暗号化照合)

- 複数のアイディアの組み合わせで実現
  - A. 秘密パラメータによるデータ変換
  - B. 部分的な信号除去
  - C. ランダムパターンとの畳み込み
  - D. 個人内揺らぎの許容/補償
  - E. 揺らぎ許容照合
  - F. 秘密鍵の隠蔽
  - G. 秘密鍵の生成

A. 秘密パラメータによる変換

- テンプレートデータの座標を、秘密のパラメータにより幾何変換し、変形させる
  - テンプレートは保護しないが、アプリケーションごとに異なる変換パラメータを用いると、アプリケーション間でのテンプレート交換が出来ない
  - 変換パラメータが推定できなければ、変換前のテンプレートに戻すことも困難(推定困難)
  - パラメータを変更するとテンプレートを無効化可能
  - 照合には、未変換のテンプレートと同じアルゴリズムが利用でき、従来方式との互換性が高いが、互換性を保てるパラメータ空間はそれほど広くない

B. 部分的信号除去

- 生のバイオメトリクスデータから存在しなくても同一性を確認できる情報を選択的に消去し、原信号の復元を困難にする
  - たとえば
    - 二次元指紋画像をフーリエ変換して、パワー項を削除すると元の信号は復元できないが、位相項に隆線の位置情報が残されていることを利用する
    - 特徴ベクトルから一部の情報を削除する
  - 原信号を完全には復元できないが、選択方法によってはキャンセラブルには出来ない

C. ランダムパターンとの畳込み

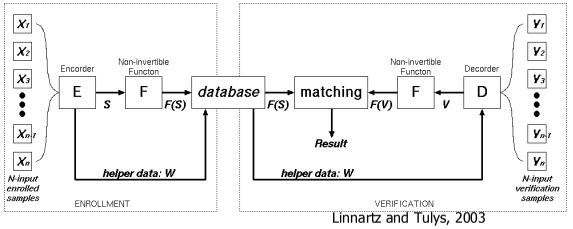
- 生のバイオメトリクスデータや特徴量に対して、ランダムなパターンを畳み込む
  - 元の信号を復元出来ない（復元不可能）
  - ランダムパターンを再発生させて畳み込めば、違うパターンを生成できる（無効化可能）
  - 信号が一部失われるので精度が低下する

D. 個人内揺らぎの許容と補償

- 暗号化空間では1bitの誤りも許容されないが、本人内のバイオメトリクスデータは変動するので、ある一定範囲の変動を許容する
  - たとえば
    - 幅をもった粗い量子化を行う
    - 揺らぎのない共通項だけをフィルタリングする相関フィルタ
    - 主成分分析による主要成分の抽出
  - Anonymous Biometrics では Helper data として紹介
  - 許容範囲をきめるのが難しい
    - 許容範囲が大きいと他人を受け入れやすくなる
    - 許容範囲が少ないと本人が拒否されやすくなる

D. Anonymous Biometrics

- エンコードと一方向 hash によって復元不可能なテンプレートと、データの揺らぎを補正する働きをもつ helper data とをテンプレートに持ち、認証成功時に毎回同じ鍵を生成する



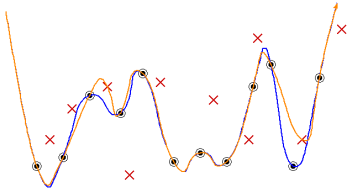
Linnartz and Tulys, 2003

E. 揺らぎ許容照合

- 二つの符号列がある程度似ているときにだけ照合が成功するような照合関数や、ある程度似た鍵を与えると解ける暗号
  - たとえば
  - Fuzzy Vault
    - N個の正解符号とN'個の偽符号のうち、m個の符号が一致すれば解ける暗号
    - 範囲N-m以内の揺らぎは許容できる
    - m/N' のパラメータ設定が難しい
  - 相関照合
    - 複数の参照点との距離を二次特徴ベクトルとするパターンマッチング
    - 精度と安全性のチューニング方法が課題

E. Fuzzy Vault

- ある秘密情報$a_m a_{m-1},...,a_1$に基づいて多項式 $f(x) = a_m x^m + a_{m-1} x^{m-1} + ... + a_1$（青色）を生成する
- 本人から得られるN個の特徴点 x_i と多項式の値 $f(x_i)$ の組（◎）をテンプレートに記録し、多項式に乗らないN'個の偽点（×）を加える
- 本人のデータから得られたN個の特徴点（◎）のうち、最低 m 個が得られれば、正しい多項式（青色）が復元できるが、偽の特徴点（×）が含まれると、異なった多項式（橙色）が得られる



F. 鍵の隠蔽と取り出し

- ハッシュされた秘密鍵がテンプレートに含まれる
  - 照合が成功したとき、ハッシュされた鍵の値が一致し、照合成功が通知される
  - テンプレートをオフラインで解析して、鍵を推定可能

G. 鍵の生成

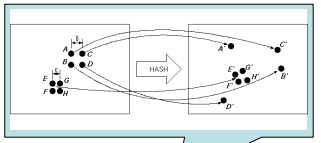
- 鍵は照合が成功したときにのみ同じ値が生成される
  - 鍵の安全性は高い
  - ハッシュされた鍵はアプリケーションが管理しなければならない

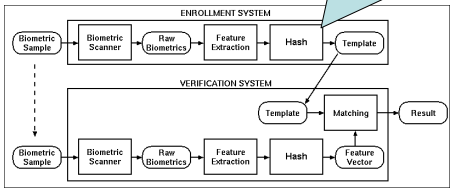
アウトライン

- 背景
- テンプレート漏洩に伴う脅威
- テンプレート保護の方式と分析
- テンプレート保護の実装事例と分析
- テンプレート保護の課題と展望
- まとめ

Private Template Cancelable Biometrics

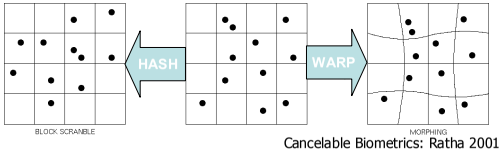
- 秘密パラメータによる幾何変換(A)を、画像や特徴点座標に適用した





Private Template Cancelable Biometrics

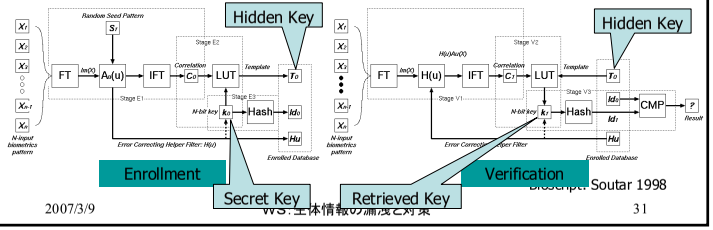
- インプリメント制約:変動するバイオメトリクスデータに対しても、同じ hash 値が得られること
  - 特徴点の場合:ブロック単位での入れ替え
  - 画像の場合:モーフィング
- 利点:従来の認証アルゴリズムが利用できる
- 欠点:照合スコアからテンプレートは推定可能



Cancelable Biometrics: Ratha 2001

Bioscript

- 入力画像のフーリエ変換した位相項(B)に、相関フィルタで揺らぎを吸収(D)、ランダムパターンを畳み込んで(B)得られたパターンを変換テーブルとして、秘密鍵をエンコードして保存(F)
- 利点:微小位置ずれ許容、無効化可能
- 欠点:秘密鍵推定可能、変形・歪みがあると本人拒否

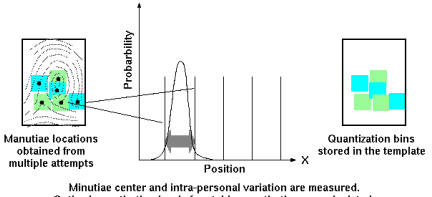


Bioscript: Soutar 1998

統計的量子化

Nishigaki 2004

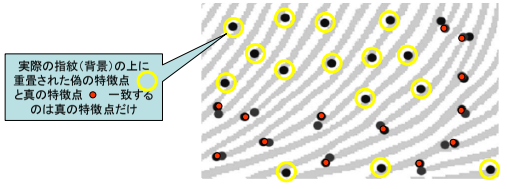
- 指紋の隆線方向を本人の揺らぎを考慮して量子化する(D)
  - 事前に揺らぎが正確に予測できれば理想的な量子化が実現できる
  - 大局的アライメントは別途必要
  - 揺らぎの予測が正確か?大量の特徴点が生成消滅する低品質の指紋に対してどのように適用できるか?



Minutiae center and intra-personal variation are measured.
Optimal quantization levels for stable quantization are calculated.

Fingerprint Vault

- 真の特徴点と偽の特徴点（chaff）および秘密多項式の値をテンプレートに登録、入力サンプルの特徴点（赤）と一致した点を用いて、多項式の係数を求める(E)
- 利点：微小位置変動は従来の特徴点照合と同じアルゴリズムで吸収可能
- 欠点：事前の概略位置合わせ必要



Clancy et al., 2003

Fingerprint Vault の改良 (Uludag 2003)

- 特徴点の代わりに、特徴点間の相対情報（距離、方位）を用いる
- 平行移動に対して不変な特徴なので、位置あわせ不要
- 相対情報なので情報量が落ちている

Uludag et al., MSU, 2003-2005

Fingerprint Vault の改良 (Yang 2004)

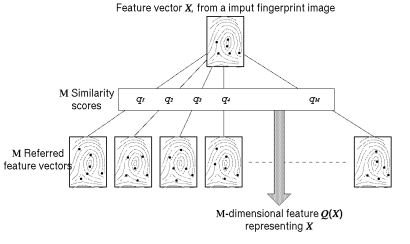
- 特徴点の代わりに、3つの特徴転換の相対情報（距離、方位角の差）を特徴量とする
- 平行・回転移動に不変であるのでアライメントが不要
- 相対情報なので、情報量が落ちている

Yang, UCLA, 2004

相関照合

Sakata, Maeda, and Sasakawa: ICB2006

- 特徴ベクトル X を M 個の任意の参照点からの距離 $Q(X)$ で置き換える(E)
  - 基準データを入れ替えることで無効化可能
  - 基準データが少なければ推定がより困難
  - 基準データ数が多いと推定成功の可能性がある



アウトライン

- 背景
- テンプレート漏洩に伴う脅威
- テンプレート保護の方式と分析
- テンプレート保護の実装事例と分析
- テンプレート保護の課題と展望
- まとめ

これまでの研究の問題

- 雑音に頑健な方式は、安全性が不完全
  - Private template, Cancelable biometrics
- ほどほど頑健だが、究極の攻撃に不完全
  - Bioscript,
- 大局的アライメント(回転・平行移動)が事前に必要
  - Bioscript, Fuzzy Vault の応用,
- 本人拒否率と他人受け入れ率を制御するパラメータが決めにくい
  - Fuzzy Vault, 相関照合, etc.

課題:認識対認証のジレンマ

- パターン認識=ほどほどの類似の許容
- 認証=完全な一致を要求
- 雑音耐性と安全性は背反する
  - 姿勢(並進・回転最大6自由度)、変形(非剛体弾性ひずみ)の補正には探索が必要
  - 探索を可能にすると、適当な初期値から真値の推定を可能にする
  - 信号の欠落、部分隠蔽、装飾などの誤りを訂正する能力は、本来拒否すべき入力を受け入れやすくする

開発すべき技術

- テンプレート保護に適した認証アルゴリズム
  - 位置合わせと照合との分離・独立
  - 個人内変動と個人間変動の分離・独立
  - 位置合わせ、個人内変動のモデル化と補償
  - 類似度(距離)カーブがシャープな照合関数
- 個人性の少ない情報による位置合わせ+個人変動補償を行い、あいまい照合行う アルゴリズムが有効
- 個別バイオメトリクスごとの実装方式開発

まとめ

- テンプレートの脆弱性解析
  - テンプレート保護はバイオメトリクス普及に重要
  - 脆弱なシステムの氾濫は社会の混乱を招く恐れ
- テンプレート保護技術の調査・分析
  - 7種の要素技術に分類し、従来研究を整理
- 問題点の指摘と今後の方策
  - 保護に適したアルゴリズムの必要性

参考文献

- 鷲見 和彦, 松山 隆司, 中嶋 晴久, "バイオメトリクス個人認証テンプレート保護技術の考察", 暗号と情報セキュリティシンポジウム予稿集 SCIS 2005, pp.535-540, (2005)
- U. Uludag, S. Pankanti, S. Prabhakar, and A. Jain: Biometric Cryptosystems: Issues and Challenges, Proc. of the IEEE, Vol.92, No.6, (2004)
- 宇根正志, 松本勉: "生体認証システムにおける脆弱性について—身体的特徴の偽造に関する脆弱性を中心に—", 日本銀行金融研究所 Discussion Paper No. 2005-J-2, http://www.imes.boj.or.jp/ (2005)
- 宇根正志, 田村裕子: "生体認証における生体検知機能について", 日本銀行金融研究所 Discussion Paper No. 2005-J-15, http://www.imes.boj.or.jp/ (2005)
- Ishida S., Mimura M., Seto Y., "Development of Personal Authentication Techniques Using Fingerprint Matching Emebeded in Smart Cards", IEICE Trans. Inf. & Sys., Vol.84-D, No.8, pp.802-818, 2001
- 磯部義明, 瀬戸洋一, 小松尚久:ディジタル署名により完全性を保証した生体認証モデルの提案とプロトシステムの開発, 画像電子学会誌, Vol.33, No.2, pp.161-170 (2004)
- 瀬戸洋一(編著):ユビキュタス時代のバイオメトリクスセキュリティ, 2002
- Jules A., Sudan, M., "A fuzzy vault scheme", proc. IEEE International Symposium on Information Theory, p.408, 2002
- 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
- Tuyls P., Goseling J., "Capacity and examples of template-protecting biometric authentication systems", ECCV Workshop BioAW, no.77, 2004
- T. Charles Clancy, Negar Kiyavash, and Dennis J. Lin, "Secure smart-card based fingerprint authentication", Proc. ACM SIGMM workshop on Biometrics methods and applications, pp.45-52, 2003
- S. Yang and I. Verbauwhede, "Automatic Secure Fingerprint Verification System Based on Fuzzy Vault Scheme," IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2005), pp. 609-612, March 2005.
- U. Uludag, S. Pankanti and A. Jain, "Fuzzy Vault for Fingerprints", Proc. of Audio- and Video-based Biometric Person Authentication (AVBPA) 2005, pp. 310-319, Rye Brook, NY, July 2005.
- 柴田陽一, 中村逸一, 三村昌弘, 高橋健太, 西垣正勝, 統計的AD変換による生体情報を用いたChallenge&Response型ネットワーク認証の提案, 情報処理学会研究報告, 2004-CSEC-26-27, pp179-186(2004.7)
- Koji Sakata, Takuji Maeda, Masahito Matsushita, Koichi Sasakawa and Hisashi Tamaki, "Fingerprint Authentication Based on Matching Scores with Other Data", LNCS: Advances in Biometrics: International Conference, ICB 2006, vol.3832, pp.280-286, 2006, Springer
- G. Davida, Y. Frankel, B. J. Matt, and R. Peralta, "On the relation of error correction and cryptography to an offline biometric based identification scheme", Proc. Workshop Coding and Cryptography (WCC'99), pp. 129–138.
- F. Monrose, M. K. Reiter, and S. Wetzel, "Password hardening based on keystroke dynamics", in Proc. 6th ACM Conf. Computer and Communications Security, 1999, pp. 73–82.
- 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 SCIS2003, 5A-3