3L3-OS-06b-2

生体情報のプライバシーを守るテンプレート保護型生体認証技術

Biometric Template Protection: A Privacy Preserving Method for Biometric Authentication

大木 哲史[*1]　甲藤 二郎[*2]
Tetsushi OHKI　Jiro KATTO

[*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

Biometrics technologies are considered as one of the methods of authentication technology. However, once a biometric feature is compromised, it is unable to permanently utilize a secure authentication against the replay attack because of its unique and permanent characteristics. For these reasons, attention is focused on the biometric template protection techniques. This paper presents the trend of standardization and technical issues on biometric template protection techniques, and describes our standardizing proposal which is evaluating guideline of the biometric template protection technologies.

1. はじめに

バイオメトリック認証は，記憶，所持の煩わしさから解放されるといった利便性があり，入退室管理や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，サーベランスシステムなどのトラッキングなどへの展開が期待されている．生体認証について，現在一般への普及を阻害している要因として，生体認証特有の脆弱性や生体情報がプライバシー情報の一種である特性が考えられる．このような状況の対策として，様々なテンプレート保護型生体認証技術の研究が進んでいる．さらに，ISO/IEC JTC 1/SC 27 や SC37，ITU-T/SG17 WP2/Q.9 において，この技術を利用した標準化が行われている．本稿では，テンプレート保護型生体認証の概要，および保護性能の評価の必要性とその評価項目について紹介する．

2. テンプレート保護型生体認証

従来，生体認証においてはシステム運用による管理や，テンプレートの暗号化によりテンプレートの保護が行われてきた．しかし，これらの保護技術にはソーシャルエンジニアリングや管理者による不正，暗号鍵の漏えいといった脅威に対し安全性を担保できないといった問題が存在した．そこで近年では，(1) 生体情報を秘匿したまま照合が可能 (2) 登録されたテンプレートの再作成が可能，といった特性を備えたテンプレート保護型生体認証技術が提案されている．ここではテンプレート保護型生体認証技術をバイオメトリック暗号とキャンセラブルバイオメトリクスに大別してそれぞれの技術について詳述する．

2.1 バイオメトリック暗号

バイオメトリック暗号技術は，生体情報からユーザ固有の鍵を動的に生成し，暗号技術に基づく認証を行なうことで，生体情報そのものをサーバに提示せずに，生体情報に基づく認証を実現する技術である．認証システムの機能は図 1 に示すように，クライアント内で生体情報から動的に鍵 K_P を生成するバイオメトリック鍵生成部分と，生成された鍵 K_P を用いて暗号技術に基づく認証を行なう部分に大別される．代表的手法として Juels らによる Fuzzy Commitment Scheme[Juels 99] や

連絡先: 大木哲史，早稲田大学理工学研究所，東京都新宿区大久保 3-4-1 55S505，03-5286-2916，ohki@suou.waseda.jp

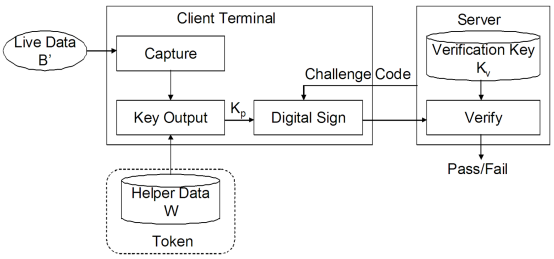

図 1: バイオメリック暗号

Fuzzy Vault Scheme[Juels 02] を基礎としてこれらを指紋照合や虹彩照合へと適用する手法が多く提案されている [大木 09].

2.1.1 バイオメトリック暗号の特徴と課題

一般に生体情報は，位置ずれ，歪み，経年変化，環境ノイズなど様々な要因で変化し，デジタルデータとして一定でない．しかし暗号技術に基づく認証と連携するためには，不定なデータからユーザ毎に一定の鍵データを生成する必要がある．このため，個人内での誤差を許容する目的で，鍵 K_P の生成には，生体情報 B に依存した補助情報 W を用いる．W はまた，鍵が漏洩した場合にこれを破棄・更新する役割も果たす．補助情報 W としては誤り訂正符号を用いるのが一般的である．本手法は，鍵 K_P の生成後の処理を既存の暗号プロトコルに委譲することができるため，既存の暗号プロトコルとの親和性が高いと言える．一方，現在提案されている多くの手法においては，W による誤り訂正を目的として生体情報を固定長のバイナリへ変換する際に個人識別性能が低下することが大きな課題となっている．

2.2 キャンセラブルバイオメトリクス

キャンセラブルバイオメトリクスは 2001 年に IBM の Ratha らによって提唱されたテンプレート保護型生体認証方式 [Ratha 01] であり，クライアントは認証時に取得した生体情報 B' を，パラメータ U に依存した変換関数 F_U を用いて $F_U(B')$ に変換し，予めユーザの生体情報 B を同じ F_U で変換した $F_U(B)$ と照合することでスコア (B と B' の類似度) を

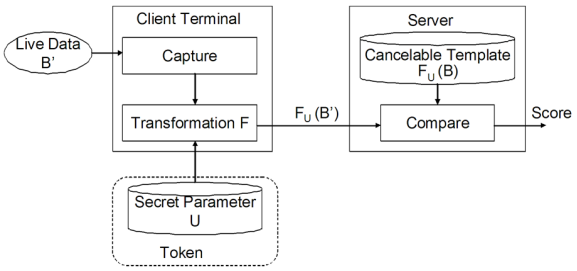

図 2: キャンセラブルバイオメトリクス

計算方式である．キャンセラブルバイオメトリクスシステムの一般的な機能構成を図 2 に示す．

2.2.1 キャンセラブルバイオメトリクスの特徴と課題

本方式は，仮に $F_U(B)$ あるいは U が漏洩しても，U を U' に更新し，$F_U(B)$ を破棄して $F_{U'}(B)$ を登録しなおすことで，生体情報そのものを変更することなくセキュリティを保つことができる．また，$F_U(B)$ をサーバへ送信するモデルであるため，提案されている多くの手法では，バイオメトリック暗号で問題となっているような鍵生成に伴う精度劣化は抑えられている．一方，$F_U(B')$ の盗聴によるリプレイ攻撃や，$F_U(B')$ からの生体情報の復元等の危険性，パラメータ U の漏洩により $F_U(B)$ から容易に B が復元可能となる可能性も存在する．これらの問題に対しては，高橋らによる手法 [高橋 08] のようにセキュアな通信路や Trusted Third Party によるパラメータ U の管理を行う手法が提案されている．このような手法は既存のテンプレート保護技術とのハイブリッドな手法とも言える．

3. テンプレート保護型生体認証の評価方法

従来の生体認証は，認証精度によって各技術の比較評価を行うことが一般的であった．一方，テンプレート保護型生体認証技術はテンプレートの安全性を保ちつつ，高い認証精度を達成することを目的としており，このため認証精度と安全性の両側面から，各技術の比較評価を行う必要がある．生体認証の評価に関しては ISO/IEC JTC 1/SC 27 においてセキュリティ評価ガイドラインである ISO 19792 が，また ISO/IEC JTC 1/SC 37 において精度評価に関する標準である ISO 19795 が標準化されているが，テンプレートの安全性を考慮した評価に関する標準化は存在しなかった．この状況をふまえ，筆者らは 2009 年より ITU-T SG17 においてテンプレート保護型生体認証の安全性評価ガイドラインを推進してきた．なお，本提案は 2012 年 4 月に ITU-T X.1091:'A guideline for evaluating telebiometric template protection techniques'[ITU-T SG17 12](以下，X.1091) として正式に標準化された．

3.1 X.1091

X.1091 内では，ISO 19792 に沿った評価手順に加え，テンプレート保護型生体認証特有の評価項目，および評価要件と評価手順が提案されている．ここでは X.1091 内で定義したテンプレート保護型生体認証特有の主な評価項目について紹介する．

Difficulty of restoring biometric information

保護されたテンプレート $F_U(B)$ もしくは補助情報 W から元の生体情報 B を復元する困難性に関する評価項目．情報理論的，もしくは計算量的安全性に関する根拠となる記述，また生体情報の復元に関連するパラメータの明確化が求められる．

Difficulty of restoring key information

保護されたテンプレート $F_U(B)$ もしくは補助情報 W から鍵情報 K_P やパラメータ情報 U を復元する困難性に関する評価項目．生体情報の復元を評価する際と同様に，情報理論的，もしくは計算量的安全性に関する根拠となる記述，また生体情報の復元に関連するパラメータの明確化が求められる．

Authentication accuracy

認証精度に関する評価項目．テンプレート保護を行った際の認証精度，および保護を行わない場合と比較した精度劣化の度合を評価する．

Diversity

テンプレートの再作成に関する評価項目．単一の生体情報から U や W を変化させて複数の保護テンプレートを作成する際，どれだけ多くのテンプレートが作成可能かを評価する．また作成した複数のテンプレートから，それらが同一の生体情報から作成されたかを推定することの困難性を評価する．

Interdependency

上記 4 つの評価項目について，トレードオフの関係がある場合明確に示す．一般に認証精度の劣化を少なくするほど，生体情報や鍵の復元が容易になると言われており，特にこれらのトレードオフを示すことが重要となる．

4. おわりに

本稿では，生体情報のプライバシーを守りつつ認証を行う技術であるテンプレート保護型生体認証について概説し，さらに各技術を比較評価するために必要となる評価項目について，ITU-T X.1091 に基づき報告した．X.1091 はテンプレート保護型生体認証を評価する際の評価項目および評価手順の共通化・明確化を目的とした文書であり，評価項目の評価方法については概説するに留められいる．それぞれの評価項目に対するより具体的な評価方法を検討することで，評価者および第三者にとってより使いやすい基準としていくことを今後の課題としたい．

参考文献

[ITU-T SG17 12] ITU-T SG17, : X.1091: A guideline for evaluating telebiometric template protection techniques (2012)

[Juels 99] Juels, A. and Sudan, M.: A Fuzzy Commitment Scheme, *ACM CCS* (1999)

[Juels 02] Juels, A. and Sudan, M.: A fuzzy vault scheme, *proc IEEE Int. Symp. Inf. Theory*, p. 408 (2002)

[Ratha 01] Ratha, N. K., Connell, J. H., and Bolle, R. M.: Enhancing security and privacy in biometrics based authentication systems, *IBM Systems Journal 40*, pp. 614–634 (2001)

[高橋 08] 高橋 健太, 比良田 真史, 三村 昌弘, 手塚 悟：セキュアなリモート生体認証プロトコルの提案, 情報処理学会論文誌, Vol. 49, No. 9, pp. 3016–3027 (2008)

[大木 09] 大木 哲史, 披田野 清良, 小松 尚久, 笠原 正雄：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, 情報処理学会論文誌, Vol. 50, No. 9 (2009)