View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by DSpace at Waseda University

早稲田大学大学院　基幹理工学研究科

博　士　論　文　概　要

論　文　題　目

Security Evaluation of Protected Template in Biometric Cryptosystems

バイオメトリック暗号における保護テンプレートの安全性評価に関する研究

申　請　者

Seira	HIDANO
披田野	清良

情報理工学専攻　計算知能研究

2011 年 12 月

通信技術の発達によるクラウドサービスの普及やスマートフォンを中心とする小型情報端末の進化に伴い，ユビキタス社会のさらなる進展が期待される一方，システムの欠陥を狙った不正アクセスや,情報漏洩に伴う個人情報の悪用,偽造，なりすましの危険性が増加している．このため，情報の機密性と完全性を確保するとともに，ネットワークを介した通信における利用者本人の確認が重要な課題となっている．ここで，本人固有の特徴を用いた生体認証は，忘却や紛失などの危険性が少なく，また認証精度が個人の管理状態に依存する要因が少ないことから，研究開発とともに標準化検討が活発に進められている．

一方，生体認証においてシステムに保管されている生体情報（以下，テンプレート）は，個人性を多く含む機微情報であり，変更することができないため，情報漏洩に対するリスクが非常に大きい．また，ネットワーク利用により生体認証が広く普及した場合，エンドユーザが必ずしも十分にテンプレートを安全に管理するための専門知識を持ち合わせているとは限らない．このため，近年，生体情報を暗号技術などにより解読不可能な状態に変換し，生体情報の秘匿性を保ちつつ認証を可能とするテンプレート保護型生体認証が注目されている．しかしながら，それらの安全性に関する議論では，理想的な条件を仮定した理論評価のみが先行しており，生体情報間の相関性など，実世界における生体認証に特有な制約を考慮したうえで定量的に評価可能かつ標準的な評価手法は存在しない．このような安全性評価では，テンプレート保護型生体認証が実用化された際に，ネットワークサービスにおいて要求される安全性のレベルを十分に達成できず，なりすましなどの予期せぬ危険性が生じる可能性がある．

以上の背景のもとで，本研究では，テンプレート保護型生体認証の一方式であるバイオメトリック暗号に注目し，実験的に評価可能かつ情報量に基づく安全性の定量的評価手法に着目する．バイオメトリック暗号は，生体情報の安全性だけでなく，秘密鍵の秘匿生にも優れており，CHAP（Challenge Handshake Authentication Protocol）などの既存の認証プロトコルとの親和性が高く実用性の面から有望な手法といえる．しかしながら，バイオメトリック暗号において秘匿化された秘密鍵には統計的な偏りが生じる可能性があり，また生体情報間には強い相関性があるため，安全性を理論的にモデル化することはきわめて困難と考えられる．そこで，実験的に評価可能な安全性評価手法により，それらの統計的な偏りや相関性を考慮した評価が可能になると期待できる．また，情報量に基づく評価により，テンプレート保護手法間の比較だけでなく，一般的に，情報量に基づき安全性を評価するパスワードや暗証番号などのその他の認証手段との相互の比較が可能になると期待できる．

本論文では，バイオメトリック暗号の安全性評価項目である保護テンプレートから秘密鍵および生体情報を推定する困難さに着目し，情報量に基づく安全性の定量的評価手法を提案する．

第 1 章は序論であり，本研究の背景と目的について述べた．

第 2 章「テンプレート保護型生体認証の安全性評価」では，まず，テンプレート保護型生体認証の従来手法について概観し，安全性評価および情報量評価の問題点について述べた．次いで，申請者が ITU-T SG17 課題 9 へ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に関する標準化寄書として提案した，安全性評価尺度を策定するうえで基本となるテンプレート保護型生体認証の安全性評価モデルについて述べた．なお，本標準化寄書は，2009 年 9 月に勧告案プロジェクト X.gep として承認され，現在は勧告化へ向けた議論が進んでいる．

第 3 章「推定エントロピーを用いた Fuzzy Fingerprint Vault の安全性評価手法」では，Fuzzy Vault Scheme を用いたバイオメトリック暗号において，安全性評価項目の 1 つである秘密鍵の推定困難性について着目し，推定エントロピーを用いた安全性の定量的評価手法を提案した．Fuzzy Vault Scheme では，秘密鍵を誤り訂正符号化した際に得られる検査符号と生体情報の組に偽の検査符号と生体情報の組（以下，ダミーデータ）を加え，これを保護テンプレート（以下，ロック情報）とすることにより安全性を担保している．しかしながら，漏洩したロック情報から秘密鍵の復元を試みた場合，復元情報のパターンやその出現頻度には統計的な偏りが生じる．そこで，本研究では，まず，それらの統計的な偏りを利用した秘密鍵推定に関する脅威を明らかにし，次いで，当該脅威を試行した際に得られる復元情報のサンプルを用いて実験的に評価可能な推定エントロピーの減少率を評価尺度として採用することを提案した．また，バイオメトリック暗号において秘密鍵の推定困難性と秘密鍵の復元精度は同時に考慮すべき評価項目であるため，Fuzzy Vault Scheme を指紋認証に適用し，秘密鍵の復元精度と推定エントロピーの減少率を定量的に評価した結果を示した．その結果，ダミーデータの作成方法によりダミーデータ数の増加に伴う精度劣化を抑えつつ，秘密鍵推定に関する脅威に対しての安全性も同時に高められることを示した．

第 4 章「Renyi エントロピーを用いた虹彩情報の情報量評価手法」では，生体情報の情報量評価尺度として，生体情報間の距離に着目した 2 次の Renyi エントロピー（以下，Renyi エントロピー）を採用し，Renyi エントロピーを用いた生体情報の情報量評価手法を提案した．バイオメトリック暗号の安全性評価項目の 1 つである生体情報の推定困難性に関する議論では，保護テンプレートの安全性を生体情報の情報量に基づき証明する試みがある．しかしながら，生体情報間の複雑な相関性を考慮して生体情報の確率分布を推定することはきわめて難しく，その確率分布から導出される Shannon エントロピーなどは生体情報の情報量評価尺度として適さない．そこで，本研究では，まず，生体情報間の距離分布のみから導出可能な Renyi エントロピーを生体情報の情報量評価尺度として採用することを提案した．生体情報間の距離分布は，生体情報のサンプルを用いた他人間照合実験を通して得られる距離のサンプルを学習データとして推定できる．また，

Renyiエントロピーを評価することにより,生体情報のShannonエントロピーの上界と下界を定めることできる．次いで，提案手法をDaugmanの虹彩コードを用いた虹彩認証に適用し，虹彩情報の情報量を定量的に評価した結果を示した．Daugmanの虹彩認証モデルでは，虹彩情報間の距離分布は二項分布でモデル化される．そこで，この二項分布の性質に基づき，虹彩情報のRenyiエントロピーをパラメトリックに評価する方法を明らかにした．そして，評価結果より，虹彩認証の安全性は環境要因の影響を受けて大きく変化することを示した．

第5章「指紋情報の情報量評価」では，第4章で提案した生体情報の情報量評価手法が多様なモダリティへ適用できることを示すために，指紋認証への適用方法を明らかにするとともに，指紋情報の情報量を定量的に評価した結果について述べた．Renyiエントロピー評価では，生体認証の標準的な精度評価方法に従い生体情報サンプルの収集および照合を行うことにより生体情報間の距離分布の推定精度を高めることができ，任意のモダリティへの適用が期待できる．また，指紋認証では，指紋の隆線の端点や分岐点における位置や角度に関する情報をマニューシャ情報とし,指紋情報は複数のマニューシャ情報の集合として記述される．そこで，本研究では，指紋認証への適用に際して，まず，指紋情報間の距離分布が理想的に超幾何分布でモデル化できることを示した．次いで，この超幾何分布の性質に基づき，指紋情報のRenyiエントロピーをパラメトリックに評価する方法を明らかにした．そして，評価結果より，指紋認証の安全性は，指紋情報の記述形式と距離に関する諸パラメータに依存して大きく変化することを示した．

第6章「Fuzzy Commitment Schemeにおける保護テンプレートの安全性評価」では，Fuzzy Commitment Schemeを用いたバイオメトリック暗号において，生体情報推定に関する脅威を明らかにするとともに，当該脅威に対する安全性を定量的に評価した結果について述べた．Fuzzy Commitment Schemeを用いたバイオメトリック暗号では，秘密鍵を誤り訂正符号化した際に得られる符号語とビット列で記述された生体情報との排他的論理和を計算し，これを保護テンプレート（以下，コミットメント）とすることにより安全性を担保している．しかしながら，従来のコミットメントの安全性に関する議論では，生体情報の情報量が十分に大きいことを前提としており，生体情報間の相関性により，当該情報量が減少し，生体情報の推定が容易となる可能性については言及されていない．そこで，本研究では，まず，Fuzzy Commitment Schemeを指紋認証に適用し，第4章で提案した生体情報の情報量評価手法に基づき指紋情報の情報量を定量的に評価することにより，指紋情報間に強い相関性があることを明らかにした．次いで，それらの相関性を利用したなりすましに関する脅威を示し，生体情報間の相関性により安全性が著しく減少することと，コミットメント漏洩時の安全性が通常運用時に比べて大きく減少することを理論的および実験的に示した．

第7章は結論であり，本論文のまとめと今後の課題について述べた．

早稲田大学　博士（工学）　学位申請　研究業績書

氏 名　　披田野 清良　　印

（２０１１年１１月　現在）

種 類 別	題名、　発表・発行掲載誌名、　発表・発行年月、　連名者（申請者含む）
○論文	Renyi エントロピーを用いた虹彩情報の情報量評価手法 情報処理学会論文誌, Vol.52, No.9, pp.2631-2649, 2011 年 9 月 披田野清良, 赤尾直彦, 小松尚久, 高橋健太
論文	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, pp.2077-2087, 2009 年 9 月 大木哲史, 披田野清良, 小松尚久, 笠原正雄
○国際 会議	A Metric of Identification Performance of Biometrics based on Information Content Proceedings of the 11th International Conference on Control, Automation, Robotics and Vision (ICARCV2010), pp.1274-1279, December 2010 Seira HIDANO, Tetsushi OHKI, Naohisa KOMATSU and Kenta TAKAHASHI
○国際 会議	On Biometric Encryption using Fingerprint and It’s Security Evaluation Proceedings of the 10th International Conference on Control, Automation, Robotics and Vision (ICARCV2008), pp.950-956, December 2008 Seira HIDANO, Tetsushi OHKI, Naohisa KOMATSU and Masao KASAHARA
講演 （研究会）	指紋情報の Renyi エントロピー推定に関する一考察 情報処理学会研究報告, Vol.2011-CSEC-55, 2011 年 12 月（発表決定） 披田野清良, 市野将嗣, 高橋健太, 小松尚久
講演 （研究会）	Fuzzy Commitment Scheme を用いたバイオメトリック暗号におけるテンプレートの安全性に関する一考察 コンピュータセキュリティシンポジウム 2011（CSS2011）論文集, pp.89-94, 2011 年 10 月 披田野清良, 市野将嗣, 大木哲史, 高橋健太, 小松尚久
講演 （研究会）	An Security Evaluation Method of Fingerprint Authentication Using Renyi Entropy 8th Ambient GCOE International Symposium, Poster Session, Waseda University, July 2011 Seira HIDANO and Naohisa KOMATSU
講演 （研究会）	最小距離エントロピーを用いた虹彩情報の情報量推定に関する一考察 2011 年暗号と情報セキュリティシンポジウム（SCIS2011）予稿集, 3E1-4 , 2011 年 1 月 赤尾直彦, 披田野清良, 小松尚久
講演 （研究会）	最小距離エントロピーを用いた虹彩情報の情報量評価に関する一考察 コンピュータセキュリティシンポジウム 2010（CSS2010）論文集, pp.633-638, 2010 年 10 月 赤尾直彦, 披田野清良, 大木哲史, 小松尚久

早稲田大学　博士（工学）　学位申請　研究業績書

種 類 別	題名、　発表・発行掲載誌名、　発表・発行年月、　連名者（申請者含む）
講演 （研究会）	A Method to Evaluate Security Levels of Biometric Cryptosystems using Estimated Entropy 8th Ambient GCOE International Symposium, Poster Session, Waseda University, September 2009 Seira HIDANO, Tetsushi OHKI and Naohisa KOMATSU
講演 （研究会）	Biometric Encryption を用いた話者照合用のテンプレート作成手法に関する一考察 コンピュータセキュリティシンポジウム 2008（CSS2008）論文集，pp.803-808，2008 年 10 月 柏木希美，披田野清良，大木哲史，小松尚久
講演 （研究会）	Fuzzy Vault Scheme を用いた Biometric Encryption の安全性評価に関する一考察 バイオメトリックシステムセキュリティ研究会，第 13 回研究発表会予稿集，pp.65-70，2008 年 6 月 披田野清良，大木哲史，小松尚久，笠原正雄
講演 （学会 大会）	Fuzzy Commitment Scheme における生体情報の推定困難性に関する一考察 第 10 回情報科学技術フォーラム（FIT2011）講演論文集，第 4 分冊，pp.229-230，2011 年 9 月 披田野清良，市野将嗣，小松尚久，高橋健太
講演 （学会 大会）	虹彩情報の Renyi エントロピー推定に関する一考察 第 10 回情報科学技術フォーラム（FIT2011）講演論文集，第 4 分冊，pp.231-232，2011 年 9 月 披田野清良，赤尾直彦，市野将嗣，小松尚久，高橋健太
その他 （標準化 寄書）	Revision proposals and comments for TD178: A guideline for evaluating biometric protection techniques ITU-T Study Group 17, Working Party 2, Question 9 (Telebiometrics), September 2009 Naohisa KOMATSU, Tetsushi OHKI, Seira HIDANO and Yoshiaki ISOBE
その他 （標準化 寄書）	Proposal of the New Discussion item for Telebiometrics - Evaluation framework for protection techniques of biometric template ITU-T Study Group 17, Working Party 2, Question 9 (Telebiometrics), February 2009 Naohisa KOMATSU, Tetsushi OHKI, Seira HIDANO and Yoshiaki ISOBE