審 査 の 結 果 の 要 旨

氏　　名　　高橋 健太

古典的な個人識別手法であるパスワードやICカードは，いずれも盗難ならびに忘失・紛失の可能性があるのに対して，生体認証はそのような危険性が低く，安全で便利に個人を識別できる．しかし広く実用化されている生体認証では，登録時に生体情報から抽出したテンプレートと呼ばれる情報をICカード等に記録しておき，認証時には観測された生体情報とICカード等内のテンプレートを比較することで個人を識別している．しかしこれではICカード等の携帯が必要となり，課題が残っている．

これに対し，テンプレートをサーバに保管し，ネットワーク経由で認証を行う技術が研究されてきた．キャンセラブルバイオメトリクスは，生体情報を暗号化したまま照合する技術で，万一テンプレート情報が漏洩してもテンプレートを破棄・更新することができる．またバイオメトリック暗号では，誤り訂正符号理論を利用することで公開鍵暗号技術を活用することができる．しかし，これらの従来手法ではリプレイ攻撃への脆弱性や，生体情報の秘匿性と認証精度の両立が困難であるなど，課題も残されており実用化には届いていなかった．

本論文では，認証精度を劣化させることなく，サーバ上の生体情報を完全に秘匿できる手法を提案している．また，安全性を確保しつつICカード等の携帯を不要とするプロトコルの提案に加え，生体テンプレートが持つプライバシー情報量を定義し，実用と理論の両面で生体認証の研究分野に大きな貢献をしている．

本論文は，全体で8章からなる．第１章では，生体認証に関する背景の説明と，本論文で目指す生体認証技術の要件が明示されている．第２章では，既存の手法として，キャンセラブルバイオメトリクスと，バイオメトリック暗号について，その技術概要ならびに課題点について明快に説明されている．

第３章は，correlation-invariant random filtering（CIRF）という手法を提案している．これはガロア体上の数論的変換（NTT）をほどこしランダムな画像Kを掛けてキャ

ンセラブルバイオメトリクスを実現するもので,実験により認証精度の劣化がほとんどないことを示している．また全画素値が非零なら，生体情報が完全に秘匿されることを証明している．続く第４章では，ガロア体 Fq 上の多項式環 Fq[x,y] を考え，イデアル I’=（x^m − α，y^n − β）に対する剰余環 Fq[x,y]/I’ 上に CIRF を拡張した CIRPM（correlation-invariant random polynomial multiplication）を定義している．I’が極大イデアルになるよう α，β，m，n を選択することで，Fq[x,y]/I’が体になり，常に生体情報が完全に秘匿される．しかもこれによる認証精度の低下はまったくない．これにより，認証精度の劣化なしに生体情報の完全秘匿を達成した．

第５章では,まず既存のキャンセラブルバイオメトリクスは健全性に問題があることを指摘している.すなわち端末が登録時生体情報に近い情報を持っていない場合でもサーバが認証してしまう場合がありうる．この問題に対し，本論文が提案する手法では，生体情報の照合と同時に，端末が鍵となるランダムな画像Kを知っていることをゼロ知識証明により証明する．これにより，端末が変換される前の生体情報を持っていることが確認できるようになり，プロトコルの健全性を達成した．

第６章では，従来ICカード等に記録されていた鍵となるランダムな画像Kをサーバに格納する方式である Store on Server（SOS）モデルを提案している．提案手法では画像パラメータKとテンプレートTを別々のサーバに格納し,端末がワンタイムパラメータLを生成する．これにより，パラメータサーバ，認証サーバ，端末のいずれかが悪意を持っていても安全なシステムが構築できる.これによりICカード等の携帯が不要となり,利便性の格段な向上を達成した．

第７章では，生体テンプレートに含まれるプライバシー情報の情報量 Biometric System Entropy（BSE）を定義している．これにより，任意の生体認証システムにおける生体テンプレートが有するプライバシー情報量を評価する指標を得た．また，BSEが生体情報の類似度分布のダイバージェンス D(f||g) で近似されることを証明した．さらにこれを用いて指紋，顔，マルチモーダルのプライバシー情報量を評価した．

第８章では上記の成果を総括している．すなわち，高い認証精度を維持しつつ，テンプレート漏洩やリプレイ攻撃などに耐性を有する完全な安全性を達成し,さらにICカード等の携帯を不要とする格段の利便性の向上を実現した.これにより世界で初めて安全なリモート生体認証を実現しており，これは生体認証の分野で画期的な研究と言える．

よって本論文は博士（情報理工学）の学位請求論文として合格と認められる。