別紙 1

論文の内容の要旨

論文題目	Fundamental Limits of Biometric Identification Systems with Noisy Enrollment （登録過程の雑音を考慮した生体識別システムの情報理論的性能解析）
学位申請者	VAMOUA YACHONGKA

生体識別システムは，データベースに予め登録されている情報とユーザが有する物理的な生体データを照合し，ユーザを識別する技術である．ここで，言及している生体データは，例えば，指紋，顔，静脈などといった個体特有の生体情報を指している．生体データを利用した識別方法は，パスワードやICカードに基づく識別方法に比べ，高い利便性と安全性をもたらすことが期待されており，注目を集めている． 現在，その技術はオンラインモバイル決済や空港における入出国管理などの幅広い分野で応用されている．本論文では，生体識別システムを数理モデル化し，情報理論的手法を用いてシステムにおける最適性能を解析する．本論文では，システムの符号器が情報源から生成された生体データの系列を直接観測できない遠隔情報源モデルを仮定して結果を導出する．

論文は六章から構成されており，第一章では研究背景，関連する従来研究と本研究の目的を述べる．第二章は解析する上で必要となる記号の定義や重要な技術用語について説明する．第三章では，遠隔情報源に対するシステムの性能を評価する．そして，第四章では秘密鍵が二つあるモデルを導入し，さらに第五章ではこのシステムモデルをガウシアン情報源と通信路に拡張した場合について議論する．最後に，本研究のまとめと今後の展望を第六章で記述する．この概要ではこの研究における主な成果である第三章から第五章までの内容を中心に説明する．

まず，本研究の一つ目の結果（第三章の内容）について説明する．従来の研究では，解析のプロセスを簡単にするため，データベースの制約及び登録過程における雑音を考慮していないモデルの理論限界を明らかにした．この種のモデルは符号器がそのまま情報源系列を観測することができる，近傍情報源モデルとしても知られている．しかし，現実的に，生体データをデータベースに登録する際は，必ずスキャナーを通し特徴を抽出しなければならず，当然雑音が発生する．そのため，符号器が生体データを直接観測できない遠隔情報源のシステムを仮定することが自然といえる．また，現代はビッグデータの時代にあり，ハードウェアコ

ストの観点から考えると，システムデータベースの制約（圧縮）を課すことが重要である．そこで本研究では，現実のシステムに近づけるために，登録過程における雑音とデータベースの圧縮を考慮し，生体識別システムにおける信頼性（システムの誤り確率），利便性（登録可能なユーザ数と使用可能な秘密鍵のレート），効率性（データベースに保存されるテンプレートのレート），及び安全性（生体データの情報漏洩レート）の理論限界を評価する．具体的には，鍵共有で良く知られている①秘密鍵が生体データから生成されるシステムと②外部から独立に与えられるシステムを解析する．両方のシステムモデルにおいて，生体データの系列は離散無記憶情報源から生成され，登録過程及び識別過程における通信路は無記憶と仮定する．得られた結果として，①のシステムでは，システムの誤りをゼロに収束させる条件の下で，ユーザ数と秘密鍵のレートがトレードオフの関係にあり，テンプレートと情報漏洩のレートにおける必要最小限の値（下限）はユーザ数のレートに依存することが分かる．すなわち，ユーザ数のレートが大きくなるにつれ，取りえる秘密鍵の個数が少なくなる．そして，テンプレートと情報漏洩のレートの下限もユーザ数のレートに応じ，変動する．②のシステムではテンプレートのレートの下限はユーザ数のレートに依存せず一定であり，他のレートの関係は①のシステムと同様であることが示せる．

次に，第四章で議論する二つの秘密鍵が存在するシステムの解析結果について説明する．これまでの研究の流れでは生成される秘密鍵（生成鍵）と交付される秘密鍵（交付鍵）は別々のシステムとして扱われていた．しかし，本論文では二段階認証のシステムにおける理論限界を導出することを目指し，その一例として生成と交付鍵が同時に存在するモデルを仮定する．さらに，このモデルにおいて，秘密鍵同士に一定の相関がある一般的なケースを想定する．結果として，ユーザ数，交付鍵，生成鍵のレートはトレードオフの関係にあるが，鍵同士の相関を許すことで，それらのレートの和が相関している分だけ大きくとれることが判明した．また，プライバシーのレートの下限はユーザ数のレートのみに依存するが，テンプレートのレートの下限はユーザ数及び交付鍵のレートに影響されることも明らかとなる．

最後に，第五章の内容について説明する．一般に，生体データ（信号）の特徴ベクトルは連続値で表現される．そこでこの章では，第四章で検討しているモデルをガウシアン情報源と通信路に拡張し，システムの性能をより計算可能な形式で特徴づける．得られる結果として，高い秘密鍵のレートと小さな情報漏洩のレートを同時に達成することが困難であることが分かった．その主な理由は，秘密鍵の利得と情報漏洩の量にトレードオフの関係があることから，以下のように説明できる．秘密鍵の利得を大きくするには，登録過程と識別過程において，生体データの系列に加わる雑音をなるべく少なくすることが好ましい（高性能な量子化器を使用する）が，情報漏洩も大きくなる傾向にある．一方で，情報漏洩を小さく抑えるためには，登録過程において，生体データの系列に加わる雑音をある程度保ちながら，識別過程において生体データの系列に加わる雑音の除去する必要があるが，この操作によって秘密鍵の利得が落ちてしまう．この結論から，高い秘密鍵のレートを実現するか少ない情報漏洩を重視するかによって，異なるアプローチで生体識別システムを設計する必要があることが示唆される．

別紙２

論文審査の結果の要旨

学位申請者氏名　VAMOUA YACHONGKA

審査委員主査　八木　秀樹

委員　川端　勉

委員　大濱　靖匡

委員　小川　朋宏

委員　岩本　貢

（*自筆署名の場合に限り、押印省略可）

生体識別システムは，システムデータベースに予め登録されている情報とユーザが有する物理的な生体データを照合し，ユーザを識別する技術である．本論文では，生体識別システムを数理モデル化し，情報理論的手法を用いてシステムにおける最適性能を解析している．論文の内容を以下にまとめる．

第１章では生体識別システムに関する背景と関連研究を紹介し，本論文の目的と論文の構成を記している．

第２章では生体識別システムの数理モデルと，第３章以降で必要になる記号や概念を定義している．

第３章では，生体データをデータベースに登録する際に雑音が発生する通信路を仮定した上で，符号化の圧縮レートの制約を課した問題を提案し，その性能を解析している．特に，生体識別システムにおける信頼性（システムの誤り確率），利便性（登録可能なユーザ数と使用可能な秘密鍵のレート），効率性（データベースに保存されるテンプレートの符号化レート），及び安全性（生体データの情報漏洩レート）の理論限界を評価している．扱っているシステムモデルは，秘密鍵が生体データから生成されるモデル（モデルG）と②外部から独立に与えられるモデル（モデルC）である．得られた結果として，モデルGでは，識別の誤り確率をゼロに収束させる条件の下で，ユーザ数と秘密鍵のレートがトレードオフの関係にあり，テンプレートと情報漏洩のレートにおける必要最小限の値（下限）はユーザ数のレートに依存することを示している．そして，テンプレートと情報漏洩のレートの下限もユーザ数のレートに応じて変動することも明らかにしている．モデルCに対しては，テンプレートの符号化レートの下限はユーザ数のレートに依存せず一定であり，他のレートの関係性はモデルGと同様であることを示している．

第４章では生体識別システムの二段階認への応用を念頭において，二つの秘密鍵が存在するシステムモデルを提案し，性能を評価している．従来の研究では生

成される秘密鍵（生成鍵）を扱うシステムと交付される秘密鍵（交付鍵）を扱うシステムは別のモデルとして扱われていたが，ここでは生成と交付鍵が同時に存在するモデルを仮定している．さらに，このシステムにおいて，秘密鍵同士に一定の相関がある一般的なケースまで含めて議論している．結果として，ユーザ数，交付鍵，生成鍵のレートはトレードオフの関係にあるが，鍵同士の相関を許すことで，相関を零に制限した場合に比べて，それらのレート和の相関が許容される分だけ大きくとれることを示した．また，プライバシーのレートの下限はユーザ数のレートのみに依存するが，テンプレートのレートの下限はユーザ数及び交付鍵のレートに影響されることも明らかにした．これらの結果は，システムの設計に重要な指針を与えている．

第５章では，ガウス分布に従う情報源と通信路を仮定して，第４章で提案したシステムの性能を解析している．確率変数のガウス性を利用することにより，各レートの関係を計算可能な形式で特徴づけている．秘密鍵の利得と情報漏洩の量にトレードオフの関係があることに加え，高い秘密鍵のレートと小さな情報漏洩のレートを同時に達成することが困難であることを明らかにした．この結果から，高い秘密鍵のレートを実現するか少ない情報漏洩を重視するかによって，異なるアプローチで生体識別システムを設計する必要があることが示唆される．

第６章では，まとめと今後の研究の発展性について詳しく述べている．

以上の結果から，本論文は博士(工学)の学位論文として十分に価値があるものと認める．