2011 年度修士論文

バイオメトリック暗号における テンプレートの安全性対策に関する研究

− Fuzzy Commitment Scheme を用いた 共通補助データの作成 −

指導： 小松 尚久 教授
甲藤 二郎 教授

2012 年 2 月 6 日

早稲田大学 理工学術院 基幹理工学研究科 情報理工学専攻

5110B031-8　奥井 宣広

目次

第 1 章

序論

1.1　本研究の背景と目的

近年，インターネットの普及により通信技術は発達し，企業や行政のシステムのオンライン化が進みつつある．しかし，その反面，システムに対する脆弱性を狙った攻撃によるシステムの混乱，不正アクセスによる情報漏洩などが問題となり，漏洩した個人情報の悪用，すなわち偽造やなりすましなどの犯罪が増加してきている．このような，情報システムの安全性に対する要求の高まりから，本人確認手段としてバイオメトリック個人認証技術の適用が広まっている．

バイオメトリック個人認証は，個人の身体的，あるいは行動的特徴に基づいて認証を行うため，パスワードや IC カードのように，記憶，所持の煩わしさがないことなどの利便性がある．しかし，利用者，環境条件，生体情報といった様々な要素において脆弱性が存在しており，その対策が課題となっている．また，生体情報は，情報が漏洩した際に改変することができないため，個人の生体情報を登録したデータベース（以下，テンプレート）の漏洩には大きなリスクが伴う．このような背景から，強固なテンプレート保護技術を用いた安全性の高いシステムへの要求が高まっており，様々なテンプレート保護技術が研究されている [1]．

テンプレート保護手法の代表例として，キャンセラブルバイオメトリクス [3] とバイオメトリック暗号がある．それらの代表的手法である Fuzzy Vault Scheme[2] では，生体情報に偽の情報を付加し，補助データとして保管することで生体情報の推定を困難としている．しかし，Fuzzy Vault Scheme では，補助データを個人ごとに作成する必要があり，このため，補助データが攻撃者に漏洩した場合，オフライン攻撃等により個人の生体情報が推定される危険性があることから，生体情報の管理がシステム運用上の課題となる．

そこで，本研究では，共通補助データと Fuzzy Commitment Scheme を用いることにより，安全性の高いシステムを提案する．本研究で用いる共通補助データは個人の生体情報ではなく，指紋情報から同じ指であれば同一のビット列を出力し，個人データを生成するものである．このため，共通補助データが漏洩した場合でも，個人の生体情報が推定されることはなく，安全性の高いシステムを構築することが可能である．

1.2　本論文の構成

[第 1 章]　序論

研究を行うにあたっての背景，目的と，本論文の構成を述べる．

[第 2 章]　バイオメトリック個人認証の脆弱性と対策

バイオメトリック個人認証における脆弱性の定義および分類について述べる．また，その中でも情報漏洩の対策として用いられるテンプレート情報保護に関する研究事例を紹介する．

[第 3 章]　共通補助データを用いたバイオメトリック暗号

共通補助データの概要について述べ，Fuzzy Commitment Scheme を応用し，共通補助データを用いたバイオメトリック暗号の認証モデルを提案する．また，提案モデルに対してシステムに関する脅威と利用者の利便性の観点から考察を行う．

[第 4 章]　共通補助データを用いた指紋情報の量子化

センサから得られる指紋情報のずれや揺らぎを補正する手法として，指紋の中心点を用いた補正手法とリファレンスマニューシャを用いた補正手法の説明を行う．また，共通補助データを構成するエリアとして円形エリアを提案し，円形エリアの作成方法を述べる．さらに，共通補助データを用いて指紋情報の量子化する手法について説明する．

[第 5 章]　照合精度評価

提案手法による照合精度評価実験を行い，考察を行う．

[第 6 章]　結論

本論文のまとめを述べ，今後の課題を示す．

第 2 章

バイオメトリック個人認証の脆弱性と対策

バイオメトリック個人認証は，従来アクセス制御におけるパスワード代替利用の形態が主であった．現在は多くの情報がネットワークを介して共有化され，サービスが提供されている．また，バイオメトリック個人認証はなりすましやパスワードの盗み見などに対して非常に有効であり，作業の効率化，短縮化，ユーザビリティの面でも利便性がある．そのため，アクセス制御における認許可を確認するための手段から，非対面の状況でサービスに対する利用者課金などを行う際の本人を同定するための認証手段として位置づけられている．しかし，生体情報は個人性の高い身体的特徴であるため，パスワードや暗証番号とは異なった特徴の脆弱性が存在し，それらはプライバシー問題に起因する．

本章では，バイオメトリック個人認証の脆弱性に対する対策を明らかにするために，まず実際に対策を施す対象である脆弱性について説明し，情報システムへの適用における課題について述べる．そして，その中でもテンプレート情報保護に着目した研究事例について述べる．

2.1　バイオメトリック個人認証の脆弱性

バイオメトリック個人認証の脆弱性を明らかにするために，まず一般的な情報セキュリティにおける脆弱性について簡単に説明する．ここで，脆弱性，脅威，対策の定義を以下に示す [4]．

- 脆弱性：情報システム自身が持っている何らかの弱点，例えば情報システムの性質や設計，実装，運用のミス
- 脅威：情報セキュリティ上の要件を損ない，情報システムの持っている情報資産に対して不利益をもたらす攻撃や事故
- 対策：脆弱性を低減するために取られる何らかの措置

脆弱性は，ソフト製品やウェブアプリケーションなどのバグであり，情報システム内部の弱点を指す．脅威は，コンピュータ不正アクセスやコンピュータウィルスなどであり，情報システムの外部からの攻撃や事故である．対応する脅威と脆弱性が結びついて実際に不利益を生じさせる．つまり，脅威は情報システムの脆弱性を利用して不利益を引き起こすと言える．不利益を引き起

こさないためには，脅威，脆弱性に対して何らかの対策を立てる必要がある．しかし，脅威は情報システムの外部に存在するため排除するのは難しく，実際には情報システム自身が持っている脆弱性に対して対策を講じる．

バイオメトリック個人認証の脆弱性は，バイオメトリック個人認証自身の性質やバイオメトリック個人認証システムの設計，実装，運用のミスなどである．バイオメトリック個人認証には他のシステムとは異なる特有の脆弱性があり，バイオメトリック情報特有の性質に基づく脆弱性とパスワードや ID カードなどの他の個人認証方式にも共通する脆弱性でその程度がバイオメトリック情報特有の性質に依存する脆弱性の 2 種類に分類される [5]．バイオメトリック個人認証では，登録用バイオメトリック情報と照合用バイオメトリック情報が完全に一致することはないため，本人拒否が発生するが，パスワードや ID カードによる個人認証ではこのような脆弱性は存在しない．一方，パスワードや ID カードといった本人知識や所有による個人認証の場合，それらが第三者の手に渡った場合でも，登録者が解約や変更の手続きを行えば，成りすましを防ぐことができる．しかし，バイオメトリック個人認証の場合，登録者が指紋や顔などのバイオメトリック情報を任意に変更することができないため，成りすましなどの脅威に結びつく危険性があり，パスワードや ID カードによる個人認証に比べ，情報漏洩に対する脅威の程度が大きくなる．

バイオメトリック個人認証特有の脆弱性は，個人認証情報として用いているバイオメトリック情報の性質に起因する．ここで，バイオメトリック情報特有の脆弱性を図 2.1 に示すともに，以下に要約する [5]．

- バイオメトリック情報に存在する脆弱性
  - 複製：物理的にバイオメトリック情報を複製できる
  - 秘匿困難：バイオメトリック情報の秘匿が困難である
  - 変更不可：バイオメトリック情報を利用者が意図的に変更できない
  - 変化：バイオメトリック情報の状態が変化する
- バイオメトリクス装置に存在する脆弱性
  - 他人受入：他人受入が偶発的に発生する
  - 本人拒否：本人拒否が偶発的に発生する
  - 推定：テンプレート情報や照合結果からバイオメトリック情報が推定できる
  - センサ残留：バイオメトリック情報の痕跡がセンサ面に残留する
- 利用者に存在する脆弱性
  - 習熟：利用者がバイオメトリクス装置の使用方法を習熟しなければならない
  - 抵抗感：バイオメトリクス装置の使用に抵抗を感じる
- 運用条件，環境条件に存在する脆弱性
  - 入力条件：入力環境が精度に影響する
  - 認証パラメータ：認証パラメータの設定が精度に影響する

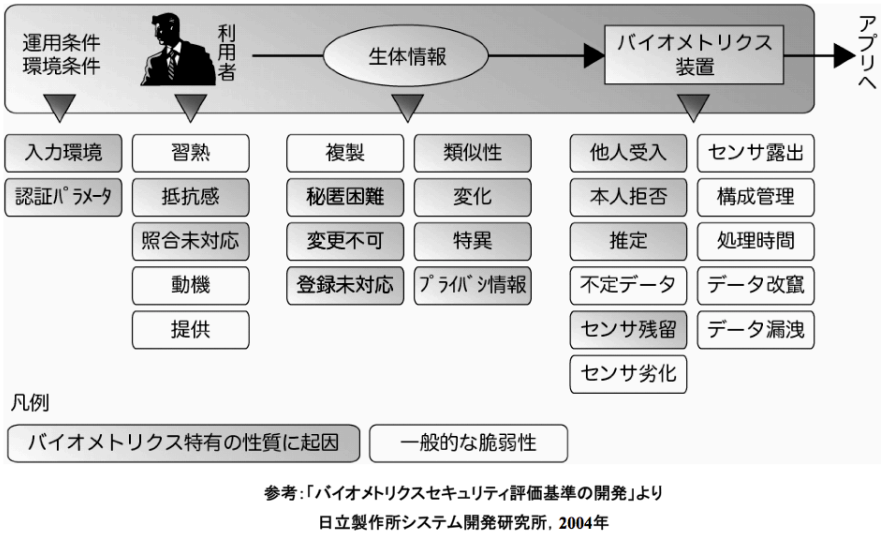


図 2.1　バイオメトリック個人認証の脆弱性

以上より，バイオメトリック個人認証を利用する際はこれらの脆弱性と結びつく脅威を考慮してシステムを運用していくことが重要となる．

2.2　テンプレート情報保護の研究事例

バイオメトリック個人認証には，前節で述べたように様々な脆弱性および脅威が存在し，その対策としてこれまでにいくつかの手法が提案されている [1]．その中でも，テンプレート情報は変更不可能であるため，情報漏洩に対するリスクが非常に大きく，高いテンプレート保護技術が求められている．テンプレート保護技術に関しては，これまで多くの方式が提案され，キャンセラブルバイオメトリクス [3]，Bioscrypt[6]，Anonymous Biometrics[7]，Fuzzy Vault Scheme[2]，統計的 AD 変換による鍵生成方式 [8]，Fuzzy Commitment Scheme[9] などが挙げられる．また，これらのテンプレート保護技術は大きく分け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の 2 つの方式に分類される．本節では，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の概要ついて説明し，本提案手法ではバイオメトリック暗号の安全性を高める手法のため，バイオメトリック暗号の代表的な研究事例について紹介する．

2.2.1　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 らによって提案されたテンプレート情報保護手法である [3]．これは，生体情報を多対一の対応を持つ一方向関数によって変形させ，元の情報を復元不可能な状態にし認証を行うという手法である．生体情報に予測不可能な変換を与え，元の情報を復元できないようにするという一方向性の概念を用いている．次に，キャ

ンセラブルバイオメトリクスの概要を，ネットワークを介したサーバ・クライアント型の認証システムを例にとり，図 2.2 を用いて説明する．

ユーザ登録時，クライアントはユーザの生体情報を取得して特徴量 X を抽出する．次に，X をパラメータ θ によって決まる関数 F_θ により変換し，変換特徴量 $F_\theta(X)$ をサーバに送信する．サーバはこれをテンプレートとして登録する．このとき，パラメータ θ はクライアントが保持し，サーバに対して秘匿しておく．

ユーザ認証時，クライアントはユーザの生体情報を取得して特徴量 X' を抽出し，これを F_θ により変換して，変換特徴量 $F_\theta(X')$ をサーバに送信する．サーバは，テンプレート $F_\theta(X)$ と変換特徴量 $F_\theta(X')$ を照合して，照合値を計算する．これによりサーバは元の特徴量 X，X' を知ることは出来ないが，X と X' の照合値を知ることが出来る．

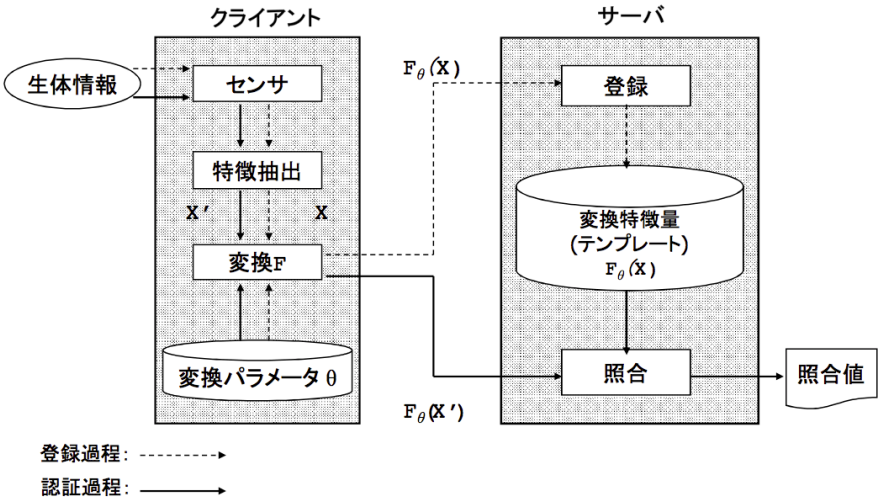


図 2.2　キャンセラブルバイオメトリクスの認証モデル

キャンセラブルバイオメトリクスの特徴

キャンセラブルバイオメトリクスを利用することで生じる特徴を以下に示す．

- 生体情報を一方向性関数を用い，変換した状態で登録，および照合を行うため，サーバからテンプレートが漏洩した場合，元の生体情報は秘匿されたままであり，偽造生体の作成に利用されるというリスクが低減できる．また，サーバ内に特徴量 X が存在しないため，内部犯の対策としても有効となっている．
- 変換パラメータ θ を変更することにより，テンプレートの更新が可能である．これによりテンプレート漏洩時に，変換関数を更新することができ，なりすましを防ぐことができる．
- 保護後のテンプレートの形式やデータの意味がテンプレート保護を行わない従来のテンプレートとの互換性を持っている．これにより，従来の特徴抽出やマッチングのアルゴリズム

がそのまま利用できるという運用上のメリットが存在する．

キャンセラブルバイオメトリクス特有の脆弱性

実際に，キャンセラブルバイオメトリクスを実現する上で安全性を確保するためには，キャンセラブルバイオメトリクスの脆弱性を把握し，それに対して対策を講じなければならない．具体的には次の脆弱性が挙げられる．図 2.3 は脆弱性の箇所を示している．

1. 変換パラメータの漏洩
   変換パラメータの漏洩により，変換関数が推測されてしまう．そのため，変換パラメータの漏洩時には，変換パラメータの変更により変換関数の更新が可能となることが要求される．
2. テンプレートから変換前の情報の推測
   変換関数の変換が小さいときには，変換後のテンプレートから変換前の情報が推測される．これにより，テンプレート漏洩時に特徴量の推測やなりすましの危険性が生じる．
3. 変換による照合精度の悪化
   一般的に，変換後の状態で特徴量を照合すると誤差が生じ，変換を適用しない場合と比較して精度が劣化する可能性がある．その劣化をできるだけ抑えることが要求される．
4. 照合値からテンプレートの推測
   照合値が類似度で求められる場合には，ヒルクライミング・アタックによりテンプレートの推測ができる場合がある．

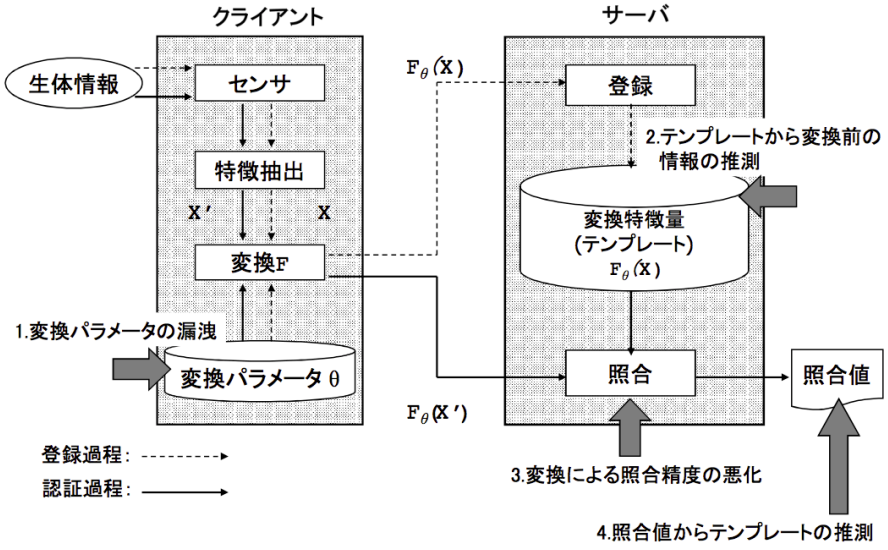


図 2.3　キャンセラブルバイオメトリクス特有の脆弱性

2.2.2　バイオメトリック暗号

バイオメトリック暗号は生体情報の歪みやノイズを補正して一意のデータを生成し，これを鍵として暗号技術に基づく認証を行う方式である．暗号技術としては，パスワード認証と同様にサーバに保管された生成鍵のハッシュ値を検証する認証手段や公開鍵をサーバに保管し，生成鍵を秘密鍵とする PKI に基づく認証手段がある．いずれの手段においても，サーバに元の生体情報と生成鍵を秘匿した状態で認証を可能とする．

バイオメトリック暗号の機能構造を図 2.4 に示す．登録時は，クライアントがユーザの生体情報 B_r を取得し，安定して一意の鍵 K を生成するための補助情報 W を生成する．補助情報 W はクライアントあるいはトークンが保持する．照合時は，登録時と同様にクライアントが生体情報 B_v を取得し，補助情報 W を用いて鍵 K を生成する．PKI に基づく認証手段の場合，公開鍵 K_V をサーバが保持し，生成鍵を秘密鍵 K_P として，CHAP 認証などにより秘密鍵を検証する．補助情報 W や鍵 K が漏洩した際は，鍵 K を変更し，補助情報 W の破棄および再登録により，生体情報を変更することなくセキュリティを維持できる．

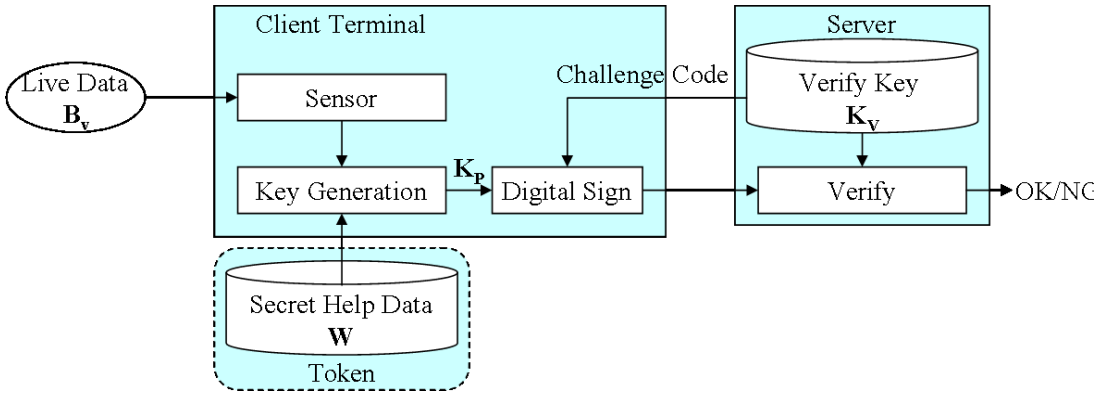


図 2.4　バイオメトリック暗号の機能構造

バイオメトリック暗号の研究事例

本節では，バイオメトリック暗号の研究事例として，Bioscrypt，Anonymous Biometrics，Fuzzy Vault Scheme，統計的 AD 変換による鍵生成方式，Fuzzy Commitment Scheme の説明を行う．

■ Bioscrypt

Bioscrypt[6] は暗号理論を用いてテンプレート情報を保護するとともに，入力画像の揺らぎを Helper Data を用いて訂正する機能を与えたテンプレート情報保護手法である．Soutar の

Bioscrypt では，次のような三つのステップによって元のバイオメトリック情報を隠蔽しつつテンプレート情報を登録し，テンプレート情報と新たなサンプルの照合を実現している．

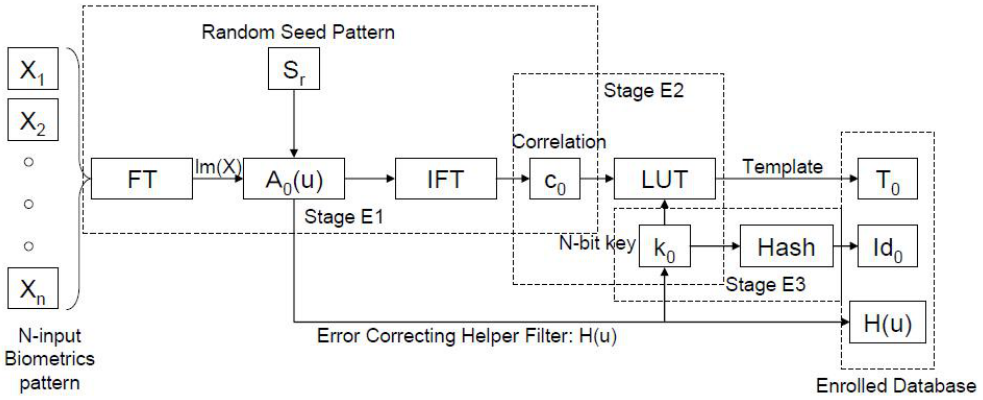


図 2.5　Bioscrypt の登録過程

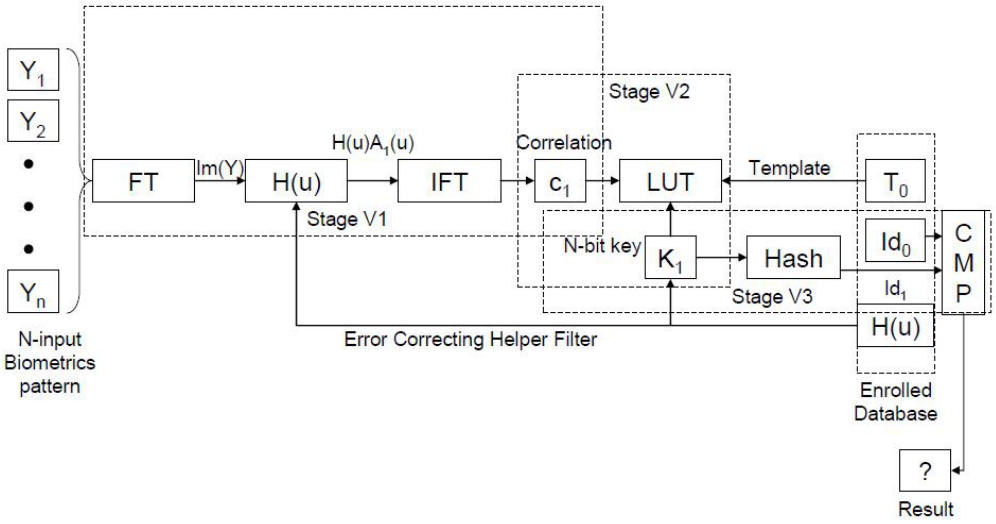


図 2.6　Bioscrypt の照合過程

図 2.5 に Bioscrypt の登録過程を示し，図 2.6 に照合過程を示す．図 2.5 において登録時の入力サンプルは，X_i $(i = 1, \cdots, n)$ である．それぞれの入力サンプルは，フーリエ変換によって周波数空間での表現に変換され，その虚数部 $im(X_i)$ の平均値 $A_0(u)$ に対して, 入力信号と全く無相関の信号 S_r を畳み込んで, それをフィルタ $H(u)$ とし, そのフーリエ逆変換を $c_0(X)$ とする．ここで全く夢相関の信号 S_r を畳み込むことによって，X を $H(u)$ や c_0 から推測することは不可能である．さらに，c_0 は二値化されて二次元ビットパターンになり，ランダムに設定されたキー k_0 の 0，1 に応じて 0，1 を示すビットパターンをルックアップテーブル（LUT）に記憶させ，その LUT がテンプレート情報 T としてデータベースに記憶される．

図 2.6 に示す照合時には同じ情報がノイズを受けて Y_i $(i = 1, \cdots, n)$ として観測されると考える．このようにして得られた Y_i に対して同じくフーリエ変換を行い，その虚数部 $im(Y_i)$ の平均値 $A_1(u)$ に対して，データベースから得た $H(u)$ を畳み込んで，フーリエ逆変換を行って $c_1(Y)$ を得る．$c_1(Y)$ を二値化した二次元ビットパターンにデータベースから読み出した LUT を適用して，LUT に記載された位置において 0，1 頻度を計算してキー k_1 を復元する．最後に，k_0 に適用したものと同じ hash 関数を適用し Id_1 を得て，Id_0 と一致すれば照合が成功する．

この方式でテンプレート情報のデータベースに保管される情報は，フーリエ変換した入力サンプルの虚数部の平均パターンにランダムなビットパターン S_r を畳み込んで得られたフィルタ $H(u)$，畳み込み結果をフーリエ変換して閾値処理した二次元二値ビットマップにランダムなキー k_0 を適用して得られるルックアップテーブル，k_0 の hash 値だけであり，これらの値から生のバイオメトリック情報 X_i や，その成分を復元することができないという復元困難性と，テンプレート情報のデータベースが漏洩した場合には，S_r あるいは k_0 を変更することで，新しいテンプレート情報を生成でき，漏洩したテンプレート情報を無効化することができる．無効化したテンプレート情報と新しいテンプレート情報は S_r と k_0 が無相関であるため一方から他方を推定することができないという安全性が保障されている．

■ Anonymous Biometrics

Tuyles らは複数のアーキテクチャを整理し，Helper Data を用いる Anonymous Biometrics[7] の一般形として図 2.7 を示した．図 2.7 において，登録時の入力サンプル X_i $(i = 1, \cdots, n)$ はエンコーダ E によって特徴ベクトル S と helper data W を生成する．特徴ベクトル S は hash 関数などの不可逆な一方向関数 F によって $F(S)$ に変形される．hash 関数を用いることで $F(S)$ から S を推定することを不可能にしている．単純な hash 関数は非常に接近した（距離 δ 以上離れた）4 点を互いに遠い位置に写像する．ところが，バイオメトリクスの入力データは常に揺らぎを含むため，照合時に同じ値を観測することはできない．ここでは，図 2.7 の様に登録時の入力 X_i が確率 $P(y|x)$ で表現される雑音を持つ通信路を通して照合時には Y_i として観測されるというモデルを用いる．小さな揺らぎがあって X_i の位置が動くと，hash 関数のために全く違う位置に写像されてしまい，X_i と Y_i はマッチングできない．そのため，揺らぎを含む入力から，常に一定の S を生成することが必要となる．

そこで，Helper Data W を別途生成し，W を用いて互いの距離が ε 以下の入力は同じ位置に写像されるようにする．また，互いの距離が ε 以上の入力は hash されるようにする．揺らぎがある照合入力サンプル Y_i $(i = 1, \cdots, N)$ に対して W を適用すると，そのデコード結果 V が登録時と同じ S を生成するためには，W は Y の誤り訂正を行うことと等価である．ただし，δ 以上の大きなエラーを持つ入力に対しても誤り訂正を行うことは，互いに離れた二つのサンプルに対して識別する能力がなくなることを意味しており，ε，δ の選定には定義が必要である．

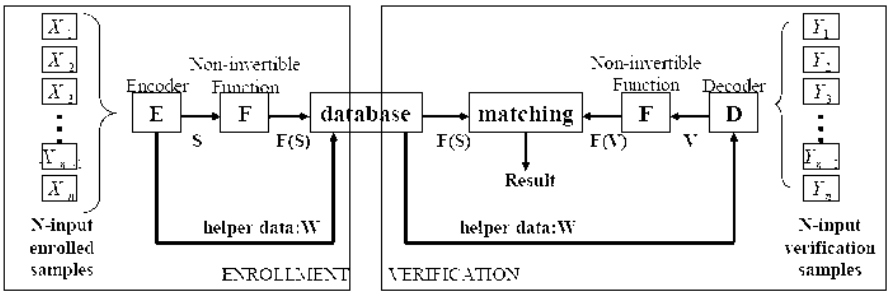


図 2.7　Helper data を使う Anonymous Biometrics の基本アーキテクチャ

Tuyles はこの考えが，Helper Data を画像のような連続値の特徴量に用いる場合と特徴点のような離散値に用いる場合のいずれにも適用できることを示した．

また，Bioscrypt や Anonymous Biometrics のように微小な変動に対する誤り訂正符号を導入した上で，一方向 hash 関数を適用する方式は，誤り訂正される範囲 ε と識別可能距離 δ のパラメータを指定して，識別性能を作り込むことが可能であり，広範囲に利用できることが予想されるが，現実の運用に当たっては以下のような課題が存在する．

Helper アーキテクチャは，登録情報に雑音がなく，照合情報に既知の確率密度分布を持つランダムなノイズが付加されるというモデルを用いて，十分多くのサンプルデータを用いることが前提である．しかし，登録，照合時に十分多くのサンプルを得ることは利便性の点で困難である．また，バイオメトリック情報の取得においては，ノイズは短期間には小さいが，時間が経つにつれて大きくなるという性質がある．

したがって，登録時に本人だけから複数回取得したサンプルを用いて，ノイズ推定を行った場合，長時間の運用においては誤り訂正の範囲を超えて，本人拒否が多発することが予測される．また，この方式は安全のために元のバイオメトリック情報を保持していないので，新しく取得したサンプルと登録時データベースを統合してテンプレート情報を更新することは難しい．

特徴点の場合には 2 種類のエラーが存在し，特徴点を見逃したり，擬似特徴点を検出したりする場合と，特徴点の検出には成功するがその座標や属性に誤差が含まれる場合がある．それぞれ発生原因が違い，発生頻度も違うため，誤り訂正はそれぞれのエラーモードに併せて設計しなければならない．Soutar や Tuyles が指摘するように，本アーキテクチャは離散特徴モデルにも理論的には適用可能であるが，最適な訂正方法はさらに検討を必要とする．

■ Fuzzy Vault Scheme

Fuzzy Vault Scheme[2] は 2002 年に A.Juels と MIT の M. Sudan によって提案された任意の情報の組を用いてある情報を隠す暗号方式である．まず，ロック過程において秘密情報 S を任意の情報の組 P を用いて解読不可能な状態に変換する．そして，アンロック過程において P と同じ

形式の情報の組 Q を与え，P と Q の大部分が一致すれば S を復元することができる．

Fuzzy Vault Scheme の概要を図 2.8 に示す．

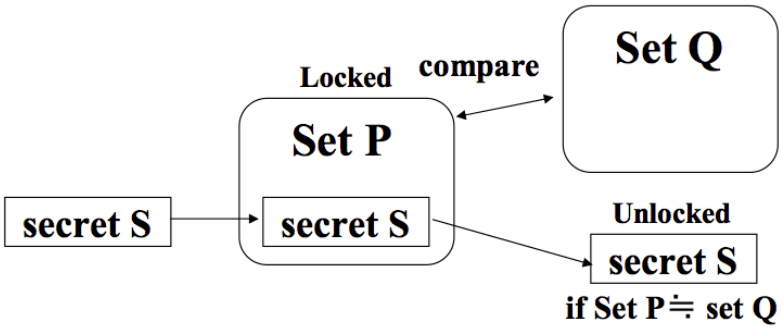


図 2.8　Fuzzy Vault Scheme の概要図

Fuzzy Vault Scheme のバイオメトリック個人認証への適用

Fuzzy Vault Scheme をバイオメトリック個人認証へ適用する場合は，秘密情報 S を秘密鍵とし，ロック情報 P とアンロック情報 Q に生体情報を適用する．認証システムにおいて登録者本人であればロック用生体情報とアンロック用生体情報，つまり P と Q は一致する可能性が高くなるために S を復元することができ，他人の場合は一致する可能性が低くなることが期待され S を復元することができない．

システムの概要図を図 2.9 に示し，ロック過程とアンロック過程の手順について述べる．

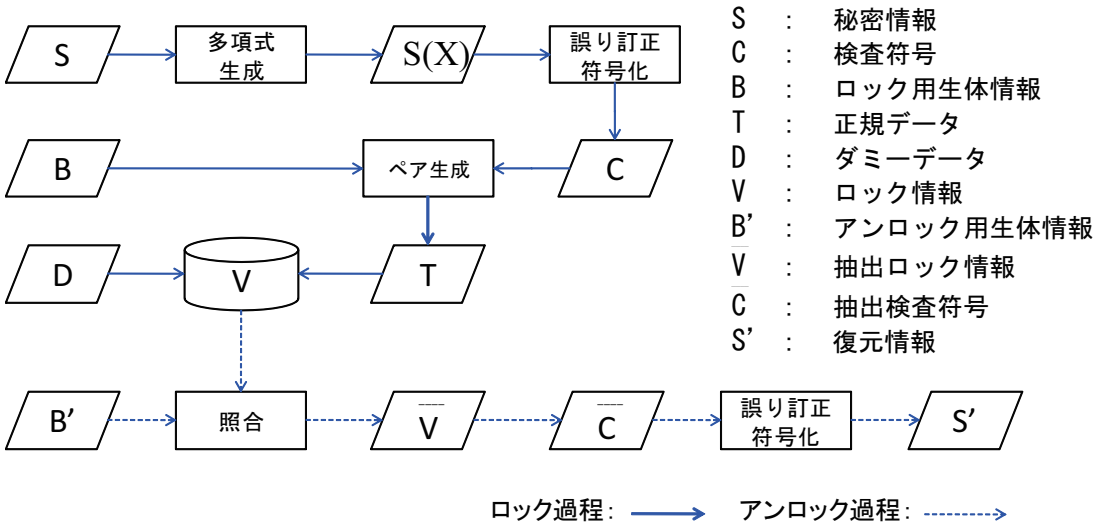


図 2.9　バイオメトリック個人認証への適用

- ロック過程
  1. 秘密鍵 S の要素を係数とする多項式 $S(X)$ を生成する．
  $$S(X) = S_1 + S_2X + \cdots + S_kX^{k-1}$$
  2. $S(X)$ を誤り訂正符号器に入力して符号語 F を作成する．得られた符号語のうち，検査符号 C の各要素とその参照番号 L とロック用生体情報 B の各要素をペアにしてテンプレート情報 T へ追加する．
  3. ダミーとして偽の生体情報と検査符号を B および C と重複しない範囲で作成し，作成されたダミーと参照番号をペアとしてダミーデータ D へ追加し，T へ加えてロック情報 V とする．
- アンロック過程
  1. アンロック用生体情報 B' を入力する．
  2. V の中の全てのペアと照合を行い，一致したペアを抽出する．
  3. 一致した全てのペア $\bar{V}$ から検査符号部 $\bar{C}$ を抽出し，誤り訂正用の多項式 $\bar{C}(X)$ を生成する．
  4. $\bar{C}(X)$ を誤り訂正符号器に入力することで多項式 $S'(X)$ が生成される．また，$S'(X)$ の係数から復元情報 S' が得られる．
  5. B と B' の類似性が高ければ $S = S'$ となり，秘密鍵 S が復元される．

このシステムの特徴としては以下のものがある．

- S や P，Q の値は任意に選択できる
- P や Q の並び順を考慮する必要はない
- アンロック時には完全一致ではなく大部分が一致すればよい
- 秘密情報 S はシステムに保管しなくていいため，セキュリティに有利である

そして，システムを実現するには，ダミーデータの数や具体的な多項式の作成法やパラメータ P，Q などの検討が必要となる．

■ 統計的 AD 変換による鍵生成方式

柴田らは統計的 AD 変換を用いた公開鍵の生成方式を提案している [8]．この方式は生体情報から常に一意なユニーク ID をリアルタイムに抽出する「統計的 AD 変換」を用い，得られる ID を認証鍵として利用し，生体情報によるネットワーク認証を実現している．そこでこの手法について説明する前に，用いられている統計的 AD 変換について説明する．

統計的 AD 変換の概要

統計的 AD 変換 [10] は，正規ユーザの生体情報の特徴量の平均や標準偏差が，不特定多数の生体情報の特徴量の平均や標準偏差と異なるという統計的な性質に基づき，ユーザ各々の生体情報をリアルタイムで常に一意なユニーク ID に変換することができる技術である．ここで，生体情報として指紋を用い，また指紋の特徴量としては，指紋を小さなブロックに分割し，各ブロック内の隆線の傾きを特徴量として，この方式の概要を説明する．

指紋の登録時，正規ユーザの指紋を複数回読み取り，それぞれの指紋データの特徴量を算出する．このとき，同一の生体情報であるが，読み取り誤差が混入するため，異なった生体情報のデータが得られる．その後，算出された特徴量の統計を測り，正規ユーザの指紋の特徴量の平均 μ と分散 σ を計算する．統計的な性質から (特徴量の誤差が正規分布に従っていると仮定して)，正規ユーザの指紋であれば，指紋の特徴量は約 99.7% の割合で $[\mu + 3\ \sigma,\ \mu - 3\ \sigma]$ の中に収まると期待できるため，この区間を正規ユーザの特徴量の許可範囲とする．(図 2.10) そして，分割されたすべての区間に対し，乱数を割り当てる．(図 2.11) 以下，各区間の境界と各区間の乱数を特徴量の「スケール」とする．指紋から ID を抽出するとき，同様に指紋を読み取り，そこから特徴量を算出する．その特徴量が含まれる区間に割り当てられた乱数を ID とする．

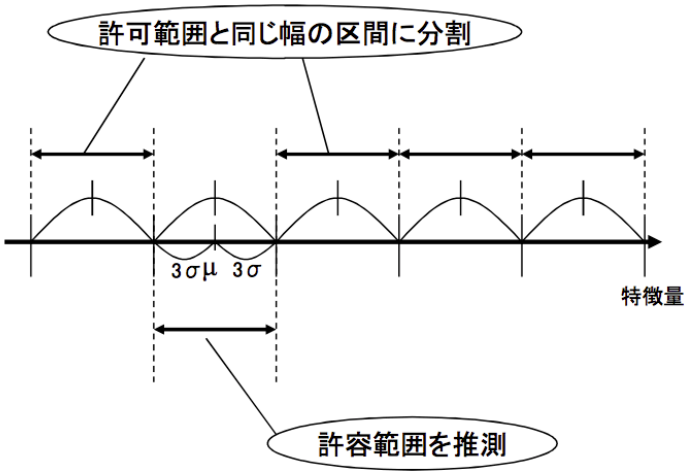


図 2.10　許可範囲の決定と他の区間の分割

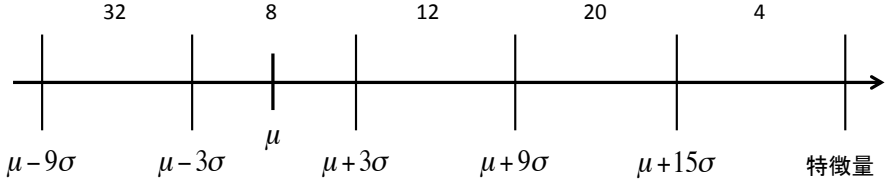


図 2.11　各区間への乱数の割り当て

統計的 AD 変換のバイオメトリック認証への適用

前述した統計的 AD 変換を通じて得られる，指紋 ID を用いたバイオメトリック個人認証について説明する．ただし，指紋は変更することができないため，他のなんらかの仕組みにより認証鍵の失効および更新に対処する必要がある．そこで，指紋 ID に乱数を結合したデータを認証鍵とする．ここで，指紋 ID に結合される乱数を，統計的 AD 変換の特徴量のスケールの中で各区間に割り当てられる乱数と区別するため，「パスナンバー」とする．

これを踏まえ，指紋 ID とパスナンバーを連結したデータをハッシュ化する方法を例にとって説明する．図 2.12 に登録過程を，図 2.13 に認証過程を示す．

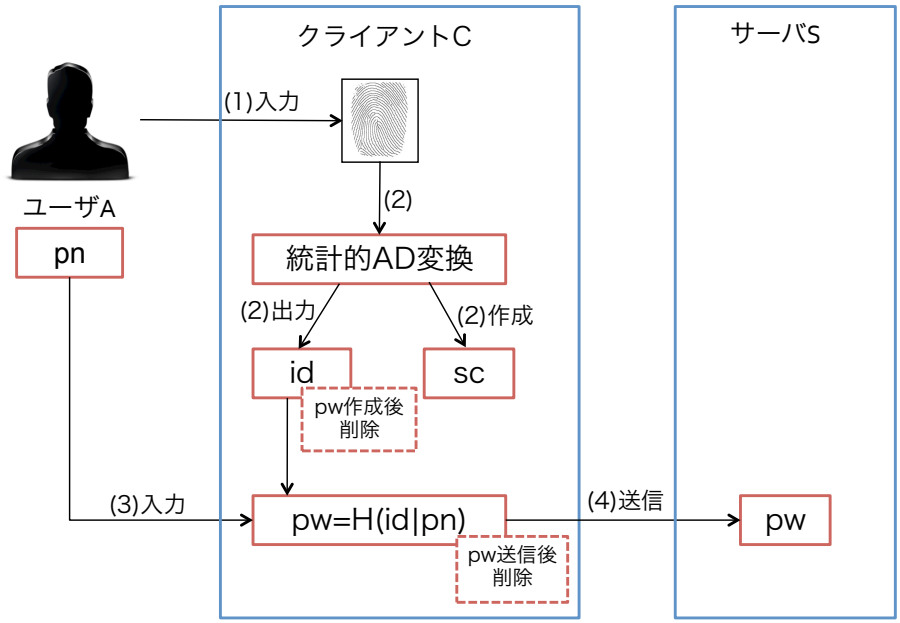


図 2.12　パスワードの登録

- パスワード登録手順
  1. ユーザ A はクライアント端末 C に指紋を複数回入力する．
  2. C は統計的 AD 変換の登録を行い，特徴量のスケール (図 2.10) を生成するとともに，指紋 ID を出力する．スケールを sc，指紋 ID を id とする．C は sc を記録する．
  3. A は C にパスナンバー pn を入力する．C は H(id|pn) を計算し，認証鍵 (パスワード)pw とする．C は即座に id を消去する．ここで H() は一方向性ハッシュ関数であり，記号'|' はデータの連結を意味する．
  4. C は pw をサーバ S に送る．この通信に限っては秘密チャネルを使用する．C は即座に pw を消去する．S は pw を保管する．

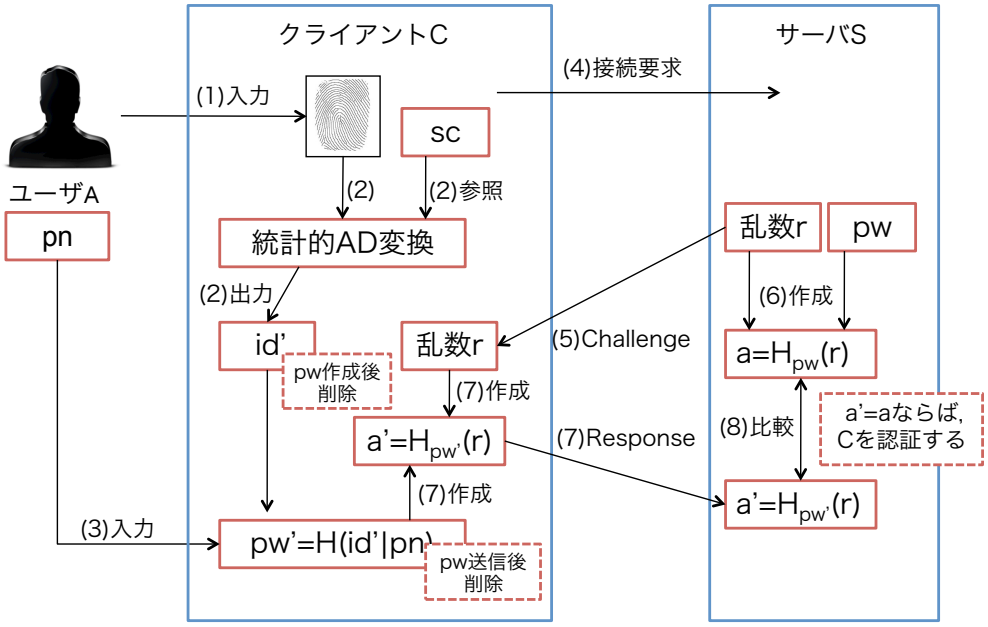


図 2.13　認証過程

- 認証手順
  1. ユーザ A はクライアント端末 C に指紋を 1 回入力する．
  2. C は指紋から特徴量を算出する．スケール sc を参照して，その特徴量が含まれる区間に割り当てられた乱数を指紋の ID として出力する．この指紋 ID を id' とする．統計的 AD 変換の性質上，正規ユーザの指紋であれば id'=id となる．
  3. A は C にパスナンバー pn を入力する．C は H(id'|pn) を計算し，認証鍵 pw' とする．C は即座に id' を消去する．正規ユーザの指紋であれば id'=id であるので，pw'=pw となる．
  4. A は C を通して，S に接続を要求する．
  5. S は乱数 r を生成し，チャレンジとして C に送る．
  6. S は，r と所持している pw から a=H_{pw}(r) を計算する．ここで H_{pw}() は pw を鍵とする鍵付き一方向性ハッシュ関数である．
  7. C は，受け取った r と 3. で生成した pw' を使って，a'=H_{pw}'(r) を計算する．C は即座に pw' を消去する．C は a' をレスポンスとして S に送る．
  8. S は，a'=a であれば C を認証する．

統計的 AD 変換による鍵生成方式によるバイオメトリック個人認証は，Challenge& Response 方式となっているため，通信路に認証鍵は流れない．そのため通信路からの情報漏洩に耐性を有するという特徴がある．しかし，この手法に対する脅威として生成されたハッシュ値には生成アルゴリズムに固有のゆがみが生じる可能性があり，ハッシュ空間上に一様に分布しないことを利

用し鍵解読の危険性が挙げられる．また，スケールの各区間から乱数を抽出し，ID を復元するため事前の位置合わせが必要となる．さらには，サーバに認証鍵を格納するため，サーバから認証鍵が漏洩した場合を考慮し，漏洩した認証鍵の安全性をより確保するために認証鍵の無効化を可能にしなくてはならない．このように，実現していく上でまだまだ検討しなくてはならない余地がある．

■ Fuzzy Commitment Scheme のバイオメトリック認証への適用

Fuzzy Commitment Scheme は 1999 年に A.Juels と M.Wattenberg によって提案された暗号化方式である [9]．Fuzzy Commitment Scheme は，登録情報から補助情報を作成し，補助情報を用いて登録情報とはわずかに異なる照合情報から登録情報を復元することができる．生体情報は，センサや環境条件による影響を受けやすく，本人であってもセンサから得られる結果には誤差が生じる．Fuzzy Commitment Scheme をバイオメトリック認証に適用することで，それらの誤差による影響を考慮した認証を行うことができる．

図 2.14 に Fuzzy Commitment Scheme のバイオメトリック認証への適用例を示し，以下に登録過程と照合過程の手順を述べる．

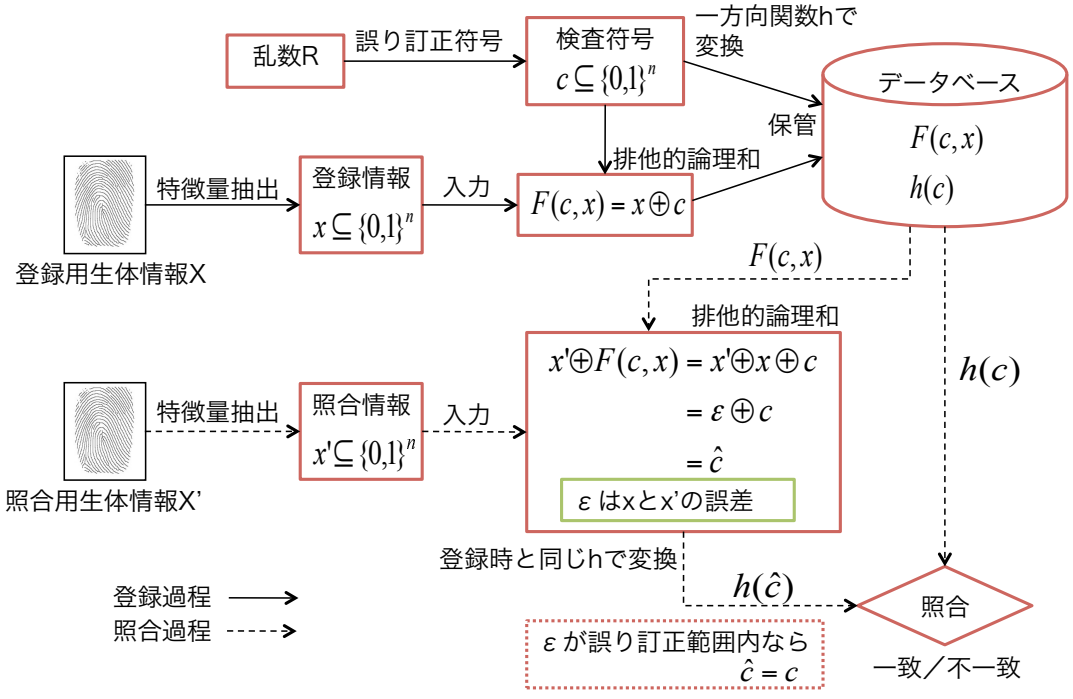


図 2.14　Fuzzy Commitment Scheme のバイオメトリック認証への適用例

- 登録過程
  1. 登録用生体情報 X から特徴量を抽出し，登録情報 $x \subseteq \{0,1\}^n$ に量子化を行いシステムに入力する．
  2. 乱数 R から m ビットの誤り訂正能力がある誤り訂正符号化によって検査符号 c を作成する．このとき登録情報 x と検査符号 c の符号長を一致させる．したがって，$c \subseteq \{0,1\}^n$ となる．
  3. 登録情報 x と検査符号 c の排他的論理和をとり補助情報 $F(c,x)$ を作成する．

$$F(c,x) = x \oplus c \tag{2.1}$$

  4. $F(c,x)$ をデータベースに保管する．また，検査符号 c が漏洩すると登録情報 x が特定されてしまうため，一方向関数 h を用いて c を変換した $h(c)$ をデータベースに保管する．

- 照合過程
  1. 照合用生体情報 X' から特徴量を抽出し，照合情報 $x' \subseteq \{0,1\}^n$ に量子化を行いシステムに入力する．
  2. データベースに保管されている $F(c,x)$ を使用して，x' と $F(c,x)$ の排他的論理和をとる．ただし ϵ は x と x' の誤差を示す．

$$x' \oplus F(c,x) = x' \oplus x \oplus c = \epsilon \oplus c = \hat{c} \tag{2.2}$$

  3. ϵ が誤り訂正範囲内であれば $\hat{c} = c$ となり，誤り訂正範囲外であれば $\hat{c} \neq c$ となる．登録過程と同じ一方向関数 h を用いて $\hat{c}$ を変換し，$h(\hat{c})$ とする．
  4. データベースに保管されている $h(c)$ を用いて $h(\hat{c})$ と比較を行う．このとき，ϵ が誤り訂正範囲内，すなわち x と x' のハミング距離 d が m ビット以内であるとき，$h(\hat{c}) = h(c)$ となり一致と判定され，ϵ が誤り訂正範囲外であるとき $h(\hat{c}) \neq h(c)$ となり不一致と判定される．

Fuzzy Commitment Scheme の特徴

- 誤り訂正を使用することで，生体情報のゆらぎを考慮した認証を行うことができるようになるため，本人受入率は上昇する．しかし，誤り訂正能力が高すぎると他人の特徴量でも本人認証を行われる可能性が上がり，他人受入率が上昇してしまう．したがって，最適な誤り訂正能力を設定する必要がある．
- c の情報が分からない場合 $F(c,x)$ から x を特定することはできないため，$F(c,x)$ は公開して利用可能である．しかし，c の符号長が短い場合，c を推測され $F(c,x)$ から x を特定されてしまう危険性があるため，c の符号長は十分に長くなくてはならない．

第 3 章

共通補助データを用いたバイオメトリック暗号

前章では，従来のテンプレート保護技術の研究事例について紹介した．Bioscrypt[6]，Anonymous Biometrics[7]，Fuzzy Vault Scheme[2]，統計的 AD 変換による鍵生成方式 [8]，キャンセラブルバイオメトリクス [3] らはすべて個人の生体情報に基づいてテンプレートを作成・保護する手法である．これらの手法は，保護されたテンプレートとその保護方式および保護に必要なパラメータが漏洩した場合，テンプレートから個人の生体情報が推測されてしまう危険性がある．そこで本研究では，共通補助データと Fuzzy Commitment Scheme を用いることで，テンプレートから個人の生体情報が推定できないバイオメトリック暗号方式を提案する．また，本研究での生体情報のモダリティは指紋とする．

本章では，共通補助データの概要について説明した後，共通補助データと Fuzzy Commitment Scheme を用いたバイオメトリック暗号の認証モデルについて説明し，その登録過程と照合過程について説明する．

3.1 共通補助データの概要

共通補助データの定義は，システムの利用者が共通して利用可能な補助データである．共通補助データの特徴は，個人の生体情報で構成されていない点と，個人ごとに作成しない点である．そのため，共通補助データが漏洩した場合でも，個人の生体情報を推定するのは困難であり，共通補助データは個人ごとに作成していないため公開して利用可能である．

本研究では生体情報のモダリティとして指紋を使用するが，指紋の特徴量に関しては付録 A に記述する．

3.2 共通補助データを用いたバイオメトリック暗号の認証モデル

生体情報はセンサや環境条件による影響を受けやすく，本人であってもセンサから得られる結果に誤差が生じる．それらの誤差による影響を考慮しつつ認証を可能とする方式として，Juels らにより Fuzzy Commitment Scheme が提案されている．Fuzzy Commitment Scheme は登録情

報から補助情報を作成し，その補助情報を用いて，登録情報とはわずかに異なる照合情報から秘密情報を誤り訂正符号により復元する方式である．本研究では，Fuzzy Commitment Scheme を応用し，共通補助データを用いたバイオメトリック暗号の認証モデルを提案する．

■本研究で使用する認証モデル

前章で紹介した研究事例では，個人の生体情報に基づいて個人ごとにテンプレートを作成しなければならない．したがって，テンプレートとその変換方式が漏洩した場合，個人の生体情報が推定されてしまう危険性がある．そこで本研究では，Fuzzy Commitment Scheme に着目する．Fuzzy Commitment Scheme は，誤り訂正を使用することで，生体情報のゆらぎを考慮した認証を行うことができ，同じ指であれば一意なビット列が生成でき，本人受入率を向上できる．本研究では，共通補助データを使用して本人特徴量から一意なビット列を生成し，Fuzzy Commitment Scheme を応用して，個人の生体情報が推定されないバイオメトリック暗号の認証モデルを提案する．図 3.1 に本提案システムの概要を示す．共通補助データを用いて指紋特徴量を量子化し，秘密情報から誤り訂正符号化によって得られた符号語と排他的論理和を用いてビット列 M を作成する．本研究では，このビット列 M をマスクデータと呼ぶことにし，マスクデータから元の生体情報は復元は困難である．

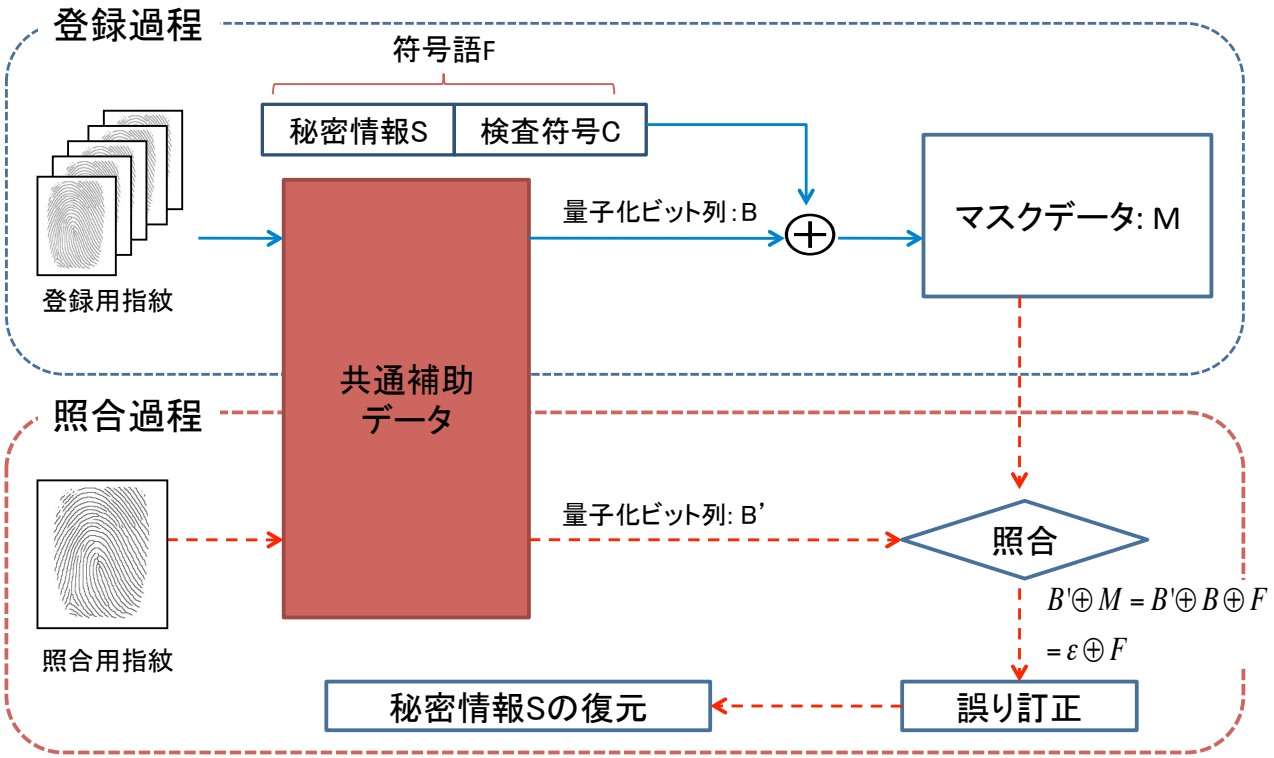


図 3.1　共通補助データを使用したシステムの概要

3.2 共通補助データを用いたバイオメトリック暗号の認証モデル

本提案システムは，共通補助データとマスクデータを，クライアントとサーバのどちらに保管するかで表 3.1 の 4 つのモデルが考えられる．

表 3.1 認証モデル

	クライアントに保管	サーバに保管
1	マスクデータ	共通補助データ
2	共通補助データ	マスクデータ
3	共通補助データ マスクデータ	
4		共通補助データ マスクデータ

表 3.1 の各モデルについて，システムの安全性とユーザの利便性，システム運用管理における利点と欠点について以下に述べ，表 3.2 にまとめる．また，マスクデータ漏洩によって元の生体情報を推定は困難であるが，本人認証を行われる危険性はあるものとする．

1. 共通補助データをサーバに，マスクデータをクライアントに保管する
   - システムの安全性
     マスクデータと量子化ビット列 B' の照合がクライアント上で行われ，クライアントーサーバ間では共通補助データと，照合後のビット列のみがやり取りされる．したがって，マスクデータが漏洩した場合，マスクデータに対するオフライン攻撃による秘密情報 S の復元の脅威が存在する．また，クライアントにマスクデータを保管することから，システム管理者がマスクデータの漏洩を検知することが難しく，マスクデータの更新が遅れる危険性がある．
   - ユーザの利便性
     ユーザが IC カード等でマスクデータを管理する必要があり，ユーザの利便性が低下する．
   - システム運用管理における利便性
     マスクデータが漏洩時に共通補助データの更新が容易に行える利点がある．しかし，マスクデータを保管する IC カード等をクライアントに配布しなければならず，運用上のコストがかかる．また，マスクデータが漏洩した場合，漏洩したクライアントのマスクデータを更新しなければならず，マスクデータの更新にコストがかかる．

2. 共通補助データをクライアントに，マスクデータをサーバに保管する
   - システムの安全性
     サーバ上に全てのマスクデータを保管しているため，マスクデータ漏洩時には，そのサー

バ上で認証を行なっている全ての人のマスクデータが漏洩してしまう危険性がある．さらに，マスクデータ漏洩時に行う共通補助データの更新においても，クライアントごとに行わなければならないため，共通補助データ更新が行えない可能性もあり，システムの安全性が低下する．

- ユーザの利便性
  共通補助データの更新によるマスクデータの再作成を行う場合，マスクデータをサーバに保管しているため 1 度で行える利便性がある．
- システム運用管理における利便性
  共通補助データの更新を全てのクライアントで行わなければならず，利便性が低下する．

3. 共通補助データとマスクデータを共にクライアントに保管する
   - システムの安全性
     1. の場合と同様の理由でシステム安全性の低下が考えられる．
   - ユーザの利便性
     1. の場合と同様の理由でユーザ利便性の低下が考えられる．
   - システム運用管理における利便性
     クライアント上に保管されているマスクデータの漏洩に対する検知や，マスクデータ漏洩時に行う共通補助データの更新をクライアントごとに行わなければならず，利便性が低下する．

4. 共通補助データとマスクデータを共にサーバに保管する
   - システムの安全性
     サーバ上に全てのマスクデータを保管しているため，マスクデータ漏洩時には，そのサーバ上で認証を行なっている全ての人のマスクデータが漏洩してしまう危険性がある．しかし，共通補助データをサーバ上で保管しているため，共通補助データの更新を容易に行うことができ，漏洩した全てのマスクデータによる攻撃を無効化することができる．
   - ユーザの利便性
     共通補助データの更新によるマスクデータの再作成を行う場合，マスクデータをサーバに保管しているため 1 度で行える利便性がある．
   - システム運用管理における利便性
     マスクデータが漏洩時に共通補助データの更新が容易に行える利点がある．

上記の理由により，本研究では，共通補助データとマスクデータをサーバ上に保管するモデルを提案し，以下の項で登録過程と照合過程について述べる．

表 3.2　各認証モデルの利点と欠点

	システムの安全性	ユーザの利便性	システム運用管理の利便性
1	×	×	△
2	×	○	×
3	×	×	×
4	○	○	○

3.2.1　登録過程

提案システムにおける登録過程の概要を図 3.2 に示し，登録過程の手順について述べる．

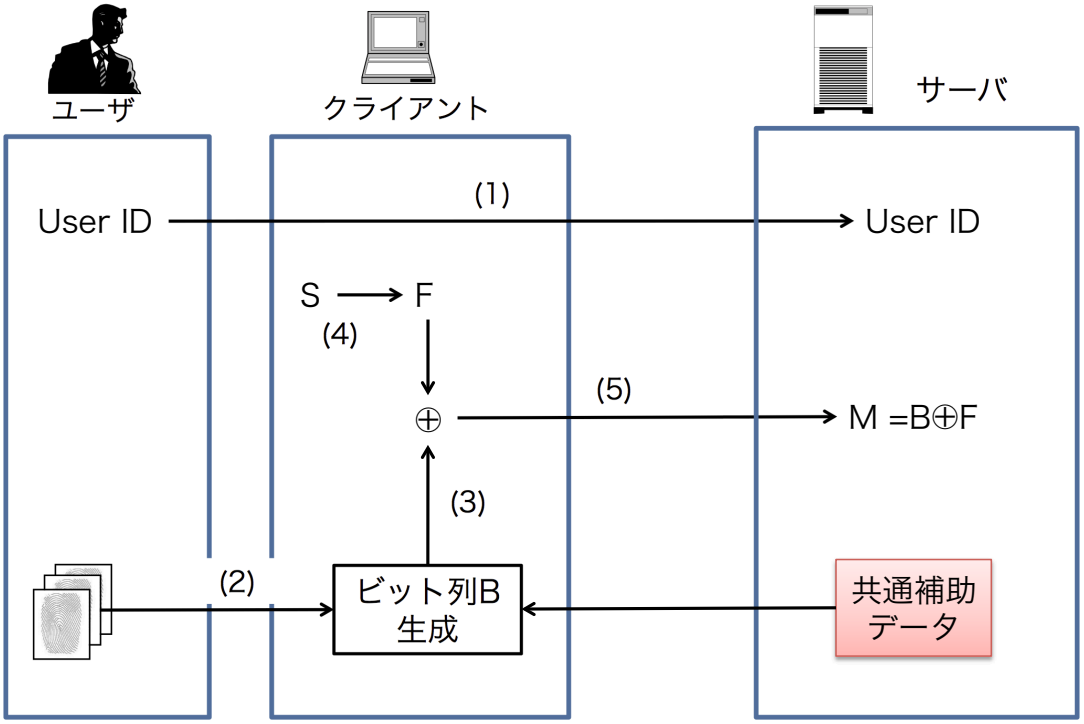


図 3.2　共通補助データを使用したシステムの登録過程

1. 秘密鍵 S と公開鍵 P のペアを算出する．S はクライアントが保持し，P はサーバに送信する．
2. ユーザはサーバに User ID を入力し，サーバはこれを保管する．
3. ユーザはセンサに生体情報を複数回入力し，特徴量を抽出する．
4. 共通補助データと特徴量からビット列 B を作成する．
5. 秘密情報 S から誤り訂正符号化により符号 F を作成する．なお，誤り訂正符号は組織符号とし，検査符号にあたる低次ビット部を符号 C として表す．このとき，ビット列 B と F の符

号長が等しくなるように符号 F を作成する．

6. ビット列 B と F の排他的論理和によりマスクデータ M を作成し，サーバに保管する．

$$B \oplus F = M \tag{3.1}$$

7. クライアントにある秘密鍵 S を破棄する．

サーバは User ID とマスクデータ M を関連付けて保管しておく．

3.2.2　照合過程

提案システムにおける照合過程の概要を図 3.3 に示し，照合過程の手順について述べる．

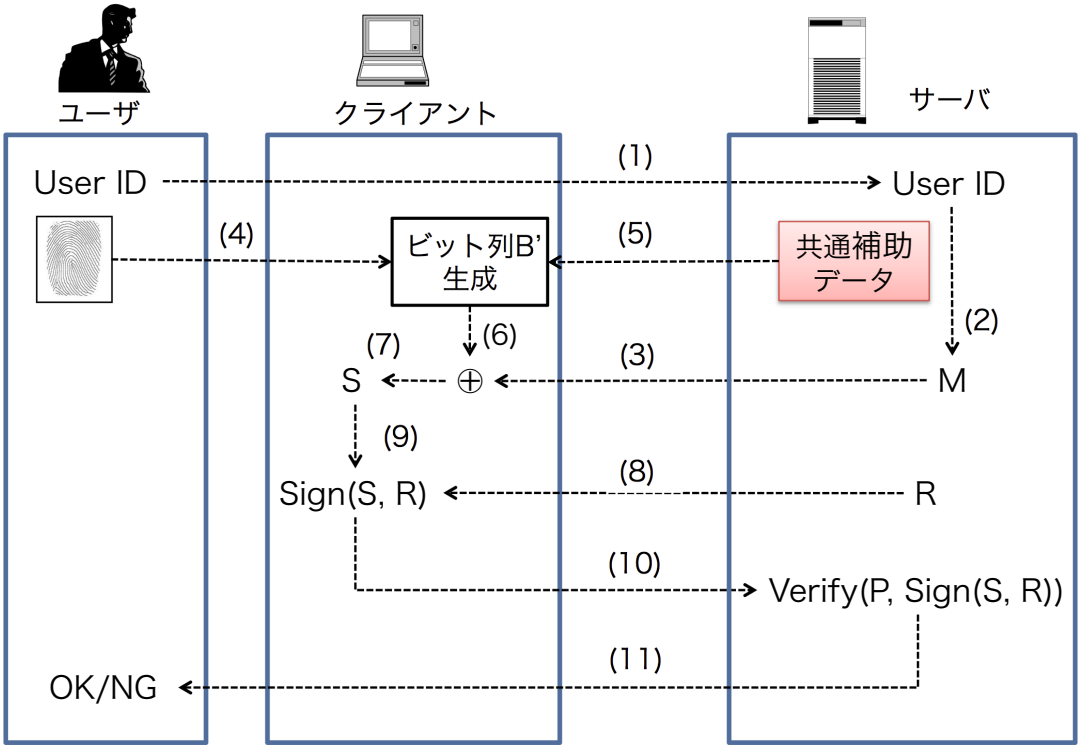


図 3.3　共通補助データを使用したシステムの照合過程

1. ユーザはサーバに User ID を入力する．
2. サーバは User ID からマスクデータ M を検索する．
3. サーバはマスクデータ M をクライアントに送信する．
4. ユーザはセンサに生体情報を入力し，特徴量を抽出する．
5. 共通補助データと特徴量からビット列 B' を作成する．このとき，生体情報のゆらぎから登録過程とは多少異なるビット列が作成される．

6. 登録過程で作成したマスクデータ M とビット列 B' の排他的論理和をとる．ϵ は B と B' の誤差を示す．

$$B' \oplus M = B' \oplus B \oplus F = \epsilon \oplus F \tag{3.2}$$

7. ϵ が誤り訂正能力以内であれば，誤り訂正を通じて秘密情報 S が復元される．
8. サーバは乱数 R を生成し，Challenge Code としてクライアントに送信する．
9. クライアントは秘密情報 S で乱数 R を署名し，これを $Sign(S, R)$ とする．
10. クライアントは Response として $Sign(S, R)$ をサーバに送信する．
11. サーバは $Sign(S, R)$ を公開鍵 P で復元し，乱数 R が復元できれば認証成功，そうでなければ認証失敗とする．

3.2.3　秘密情報の復元可能条件

式 3.2 において $\epsilon \oplus F$ から秘密情報 S が復元可能か求めるために，誤り訂正符号の復元条件を用いる．以下に誤り訂正符号の復元条件について述べる．

本研究では共通補助データを用いて指紋情報を量子化し，登録時にビット列 B，照合時にビット列 B' を出力する．量子化の手順は，4.3 節にて行う．秘密情報 S の要素数を k，検査符号の要素数を g とする．登録ビット列 B と照合ビット列 B' で一致したビット数を m_t，B と B' で不一致であるビット数を m_f とする．また，登録時もしくは照合時に，マニューシャの消失等が原因で消失誤りと判定されたビット数を e とする．本提案における消失誤りの判定方法は，4.3 節で述べる．図 3.4 に一致，誤一致の関係を示す．

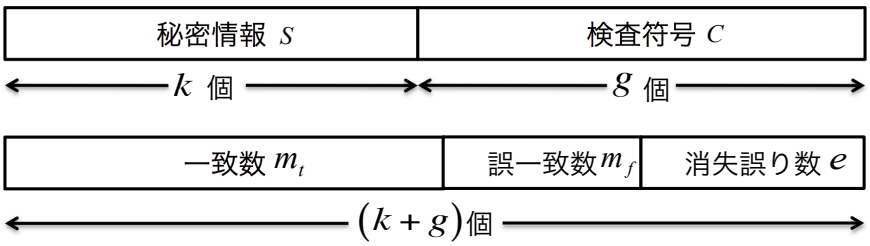


図 3.4　一致，誤一致の関係

図 3.4 より一致誤一致の関係から（3.3）式が成り立つ．次に誤り訂正可能条件式を（3.4) 式に示す．（3.3）式と（3.4）式から e を消去すると（3.5）式が導かれる．5 章の照合精度評価では，誤り訂正可能条件の（3.5）式を秘密情報 S の復元率の評価に用いる．

$$k + g = m_t + m_f + e \tag{3.3}$$

$$2m_f + e + 1 \leq g + 1 \tag{3.4}$$

$$k \leq m_t - m_f \tag{3.5}$$

第 4 章

共通補助データを用いた指紋情報の量子化

前章では，共通補助データの概要と，共通補助データを用いたバイオメトリック暗号の認証モデルについて説明した．本章では，指紋情報のずれや揺らぎを補正する手法で，指紋の中心点を用いた補正 [13] と，マニューシャ間の相対的な値を使用するリファレンスマニューシャを用いた補正 [14] について説明する．また，共通補助データを構成する円形エリアについて説明し，その作成方法について述べる．最後に，共通補助データを用いて指紋情報を量子化する手法について述べる．

4.1　指紋情報のずれや揺らぎ

センサから得られる指紋情報は，取得環境における気温や湿度の変化や，センサに入力する際の圧力や角度の違いなど様々な要因によって変化する．そのため，登録情報と照合情報に差異が生じ，認証精度に大きく影響する．したがって，指紋認証を行う場合，指紋情報の位置ずれや角度ずれなどの補正を行う必要がある．本節では，指紋の中心点を用いた補正 [13] とマニューシャ間の相対的な値を使用するリファレンスマニューシャを用いた補正 [14] について説明する．さらに，両者の補正精度について調査を行う．

4.1.1　指紋の中心点を用いた補正

図 4.1 は指紋の中心点を用いた補正の概要を示したものである．2 指とも同一指であるが，補正前ではマニューシャの位置が大きく異なり，正しく本人認証を行うことができない．中心点を用いた補正では，指紋の中心点を検出し，中心点が原点となるように他のマニューシャを平行移動させることによって位置ずれを補正することができる．

■指紋の中心点を用いた補正の長所

- マニューシャ以外の点を基準にすることで，登録時と照合時に取得できるマニューシャに差異がある場合でも，位置ずれの補正を行うことができる．

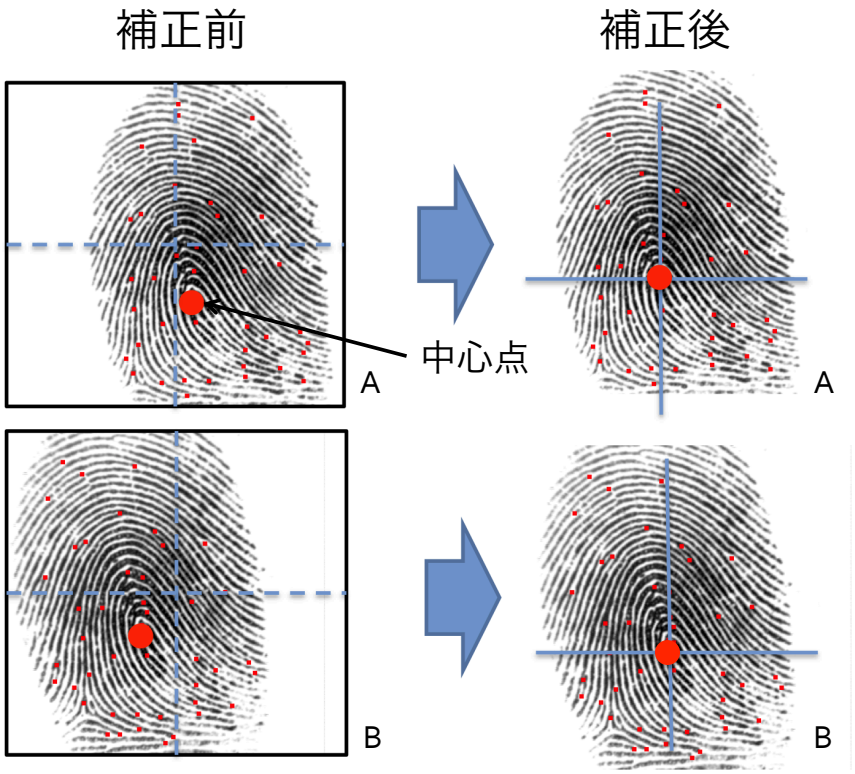


図 4.1　指紋の中心点を用いた補正

■指紋の中心点を用いた補正の短所

- 中心点の検出精度が，認証精度に大きく影響する．図 4.2 は 3 指とも同一の指であるが，中心点が正しく検出が出来なかった場合の一例である．このように，登録時と照合時で検出された中心点が異なる場合，本人認証を行うことができない．

図 4.2　中心点が正しく検出されない場合

4.1.2　リファレンスマニューシャを用いた補正

リファレンスマニューシャを用いた補正 [14] とは，特定のマニューシャを基準として，その他のマニューシャとの相対的な位置情報や角度情報を用いることで，位置ずれや角度ずれの補正を行う手法である．図 4.3 はリファレンスマニューシャを用いた補正の概要である．

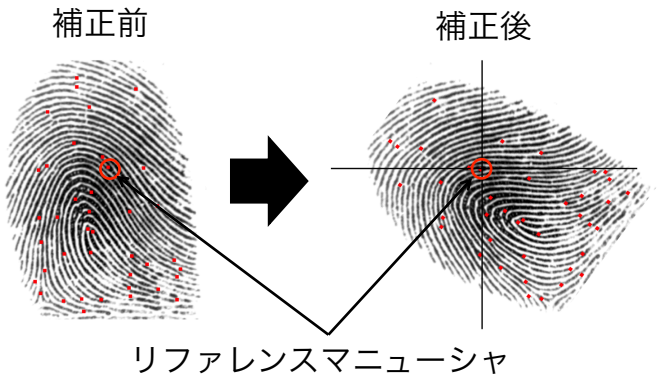


図 4.3　リファレンスマニューシャを用いた補正

■リファレンスマニューシャを用いた補正の手順

1. 1 枚の指紋画像から得られた m 個のマニューシャから，基準とするリファレンスマニューシャを 1 つ選定する．
2. リファレンスマニューシャが原点となるように，他のマニューシャを式 4.1 のようにアフィン変換し，新たな指紋情報を作成する．
3. 残りの $m-1$ 個のマニューシャから，基準とするリファレンスマニューシャを 1 つ選び，手順 2 と同様に変換する．この操作を m 個のマニューシャ全てがリファレンスマニューシャに選定されるまで繰り返す．すなわち，1 枚の指紋画像から，m 個の指紋情報が生成される．

$M_i = \left[\ x_i,\quad y_i,\quad \theta_i\ \right]$：マニューシャ i
$M_r = \left[\ x_r,\quad y_r,\quad \theta_r\ \right]$：リファレンスマニューシャ
$M_i^r = \left[\ x_i^r,\quad y_i^r,\quad \theta_i^r\ \right]$：変換後のマニューシャ i
W：指紋画像の横幅
H：指紋画像の縦幅

$$\begin{bmatrix} x_i^r \\ y_i^r \\ \theta_i^r \end{bmatrix} = \begin{bmatrix} cos\theta_r & -sin\theta_r & 0 \\ sin\theta_r & cos\theta_r & 0 \\ 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} x_i - x_r \\ -(y_i - y_r) \\ \theta_i - \theta_r \end{bmatrix} + \begin{bmatrix} \sqrt{W^2+H^2} \\ \sqrt{W^2+H^2} \\ 0 \end{bmatrix} \tag{4.1}$$

■テンプレート作成方法

リファレンスマニューシャを用いた補正によるテンプレート作成の概要を図 4.4 に示す．リファレンスマニューシャを用いた補正では，指紋情報として得られた全てのマニューシャに対して，上記の手順に従ってテンプレートの作成を行う．図 4.4 の場合では，マニューシャの総数が m 個であるため，リファレンスマニューシャの選定が m 通り存在し，ビット列 T_1〜ビット列 T_m が生成され，1 枚の指紋画像から m 個のテンプレートが作成される．

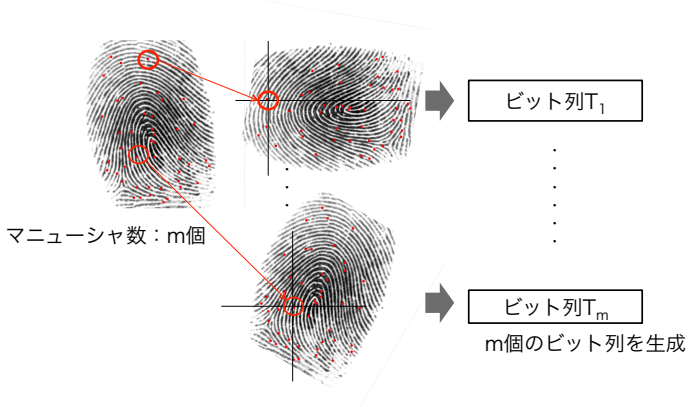


図 4.4　リファレンスマニューシャを用いた補正によるテンプレート作成の概要

■照合方法

照合方法の概要を図 4.5 に示す．登録時と照合時の両方共，図 4.4 のようにマニューシャの数だけテンプレートを作成する．照合では，照合テンプレートと登録テンプレートを総当りで行い，最も照合スコアが良いものを照合結果とする．図 4.5 を例にとると，登録時の指紋情報にマニューシャが m 個あるため，ビット列 T_1〜ビット列 T_m が生成され，合計 m 個の登録テンプレートが生成される．照合時の指紋情報にはマニューシャが n 個あるため，ビット列 Q_1〜ビット列 Q_n が生成され，合計 n 個の照合テンプレートが生成される．総当たりで照合を行うため，$m \times n$ 回の照合を行い，最も照合スコアが良いものを照合結果とする．

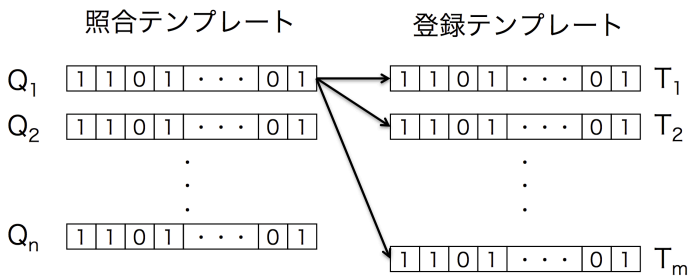


図 4.5　照合方法の概要

■照合スコア算出方法

リファレンスマニューシャを用いた補正による照合スコアの算出方法には，以下の Daugman らが提案した NHD(Normalized Hamming Distance)[11] を提案手法に応用して用いる．

登録ビット列 T_x と照合ビット列 Q_y で一致したビット数を m_t，T_x と Q_y で不一致であるビット数を m_f とする．登録時もしくは照合時に，エリアに一致するマニューシャが存在せず消失誤りと判定されたビット数を e とする．また，次式における $\overline{m_t + m_f}$ は，本人間照合における $m_t + m_f$ の平均値を示す．

$$HD_{raw} = \frac{m_f}{m_t + m_f}$$

$$NHD = 0.5 - (0.5 - HD_{raw})\sqrt{\frac{m_t + m_f}{\overline{m_t + m_f}}}$$

■リファレンスマニューシャを用いた補正の長所

- 中心点を検出する必要がないため，中心点を用いた補正のように，中心点の検出精度がそのまま認証精度に影響を与えることがない．また，中心点が検出できないような指紋画像に対しても認証を行うことができる．
- 登録時と照合時ですべてのテンプレートを総当りで照合することで，最も照合スコアが高いものを照合結果とすることができる．

■リファレンスマニューシャを用いた補正の短所

- マニューシャの数だけテンプレートが生成されるため，指紋の中心点を用いた補正と比較してテンプレートの容量が大きくなってしまう．
- 指紋の中心点を用いた補正が本人照合に必要な照合回数が 1 回であるのに対して，リファレンスマニューシャを用いた補正では，登録テンプレートと照合テンプレートの総当りを行った場合で，照合回数がマニューシャ数の 2 乗倍必要であり，照合に要する計算量が多い．

■中心点を用いた補正とリファレンスマニューシャを用いた補正の補正精度調査

マニューシャのもつ角度情報に着目し，中心点を用いた補正とリファレンスマニューシャを用いた補正の補正精度を調査する．図 4.6 に補正精度調査の概要を，表 4.1 に調査を行ったデータベースを示し，以下に調査手順を説明する．また，位置ずれ角度ずれの補正前において，マニューシャの位置情報，角度情報，属性情報を用いて，同一指の異なる指紋画像間で同一マニューシャを見つけ出すのは困難である．そのため，同一マニューシャの判定は指紋画像の目視によって行う．

- 中心点を用いた補正

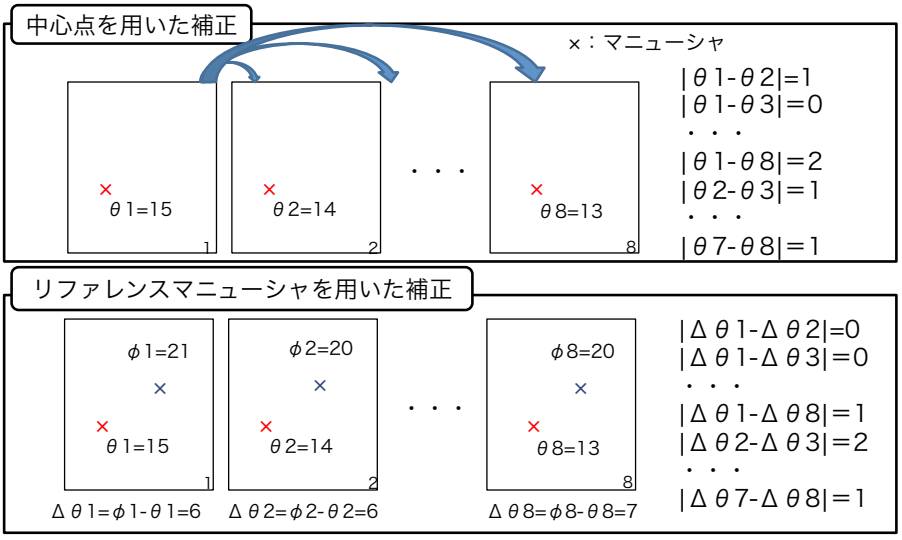


図 4.6　角度補正における精度調査の概要

表 4.1　補正精度調査に用いるデータベース

データベース	FVC2002
指の数	全 100 指中 30 指
1 指あたりの画像枚数	8
合計指紋画像枚数	240

1. 同一指における 8 枚の指紋画像全てに存在する同一のマニューシャを 1 つ選定する．
2. 同一指の指紋画像間で選定したマニューシャの角度差を求め，補正後の角度誤差とする．

- リファレンスマニューシャを用いた補正
  1. 同一指における 8 枚の指紋画像全てに存在する同一のマニューシャを 2 つ選定する．
  2. 選定した 2 つのマニューシャ間の角度差を求め，補正後のマニューシャの角度情報とする．
  3. 同一指の指紋画像間で 2. で算出した角度情報の差を求め，補正後の角度誤差とする．

図 4.7 に角度補正における精度調査の結果を示す．調査結果から，リファレンスマニューシャを用いた補正では，約 90%の割合で角度誤差が 1 レベル以下に収まっていることがわかる．また，中心点による補正では，角度誤差が最大で 5 レベルまであるのに対して，リファレンスマニューシャを用いた補正では，最大でも 3 レベルまでに留まっている．

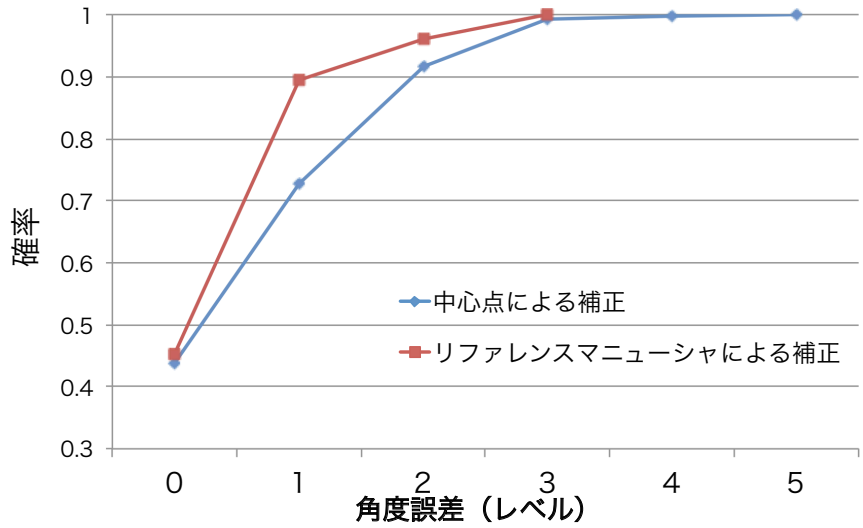


図 4.7　角度補正における精度調査の結果

4.2　共通補助データの作成方法

3.2 節で説明したシステムを用いる場合，マニューシャ情報から常に固定長のビット列を生成しなければならない．また，登録時には存在していたマニューシャが照合時には存在しない場合や，登録時には存在していないマニューシャが照合時には存在するといった消失マニューシャへの対策も行わなければならない．本研究では，指紋画像をエリアという予め定めた領域に分割して，エリアごとにマニューシャ情報を用いてビット列を生成する．このことにより，常に固定長のビット列を生成することができる．エリアの作成方法にはいくつかの既存研究があるが，本研究では円形エリアを使用し，補正後の指紋画像中心点から同心円状に配置する手法を提案する．

■既存手法の概要と問題点

指紋からユーザごとに固有のビット列を出力する手法として，Chulhan Lee らによる長方形を用いる手法 [15] や，Anil K. Jain らによる扇形を用いる手法 [16] などが提案されている． 図 4.8 に長方形エリアと扇形エリアの概要を示す．エリアを用いてマニューシャの位置情報を変換する場合，エリアの縁にあるマニューシャが，位置ずれによって登録時と照合時で異なるエリアに移動してしまう問題がある．長方形や扇形エリアの場合，エリアの角となる部分とそうでない部分で，位置ずれによる誤差の影響が異なる．また，マニューシャの位置分布には偏りがあると考えられるが，長方形や扇形エリアでは，マニューシャの位置分布を考慮したエリア設計がされていない．したがって，ビット列を生成するエリアに偏りが生じ，最終的に出力されるビット列にも偏りが生じてしまう可能性がある．

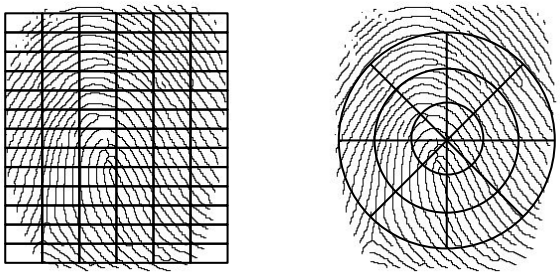


図 4.8　長方形エリアと扇形エリアの概要

■マニューシャ位置分布の調査

マニューシャの位置分布の偏りを調査するために，指紋データベースである FVC2002[12] を用いてマニューシャ位置分布の統計を求める．マニューシャ位置分布調査の諸元を表 4.2 に示す．位置分布の調査は，指紋の中心点を用いた補正後の指紋画像と，リファレンスマニューシャを用いた補正後の指紋画像で行う．指紋の中心点を用いた補正後のマニューシャの位置分布は，データベース内の各指紋画像に対して，指紋の中心点を座標 $(388, 374)$ となるように全マニューシャを平行移動した後のマニューシャ位置分布である．リファレンスマニューシャを用いた補正後のマニューシャ位置分布の調査方法を以下に述べる．データベース内の各指紋画像において，全マニューシャの中から 1 つをリファレンスマニューシャとして選定し，リファレンスマニューシャの座標が $\left(\sqrt{388^2+374^2}, \sqrt{388^2+374^2}\right) = (538.9, 538.9)$ となるように 4.1.2 節で説明した方法で他のマニューシャを変換する．この操作をデータベース内の全ての指紋画像に対して行い，変換後のマニューシャ位置分布をリファレンスマニューシャを用いた補正後のマニューシャ位置分布とする．

表 4.2　マニューシャ位置分布調査の諸元

データベース	FVC2002[12]
指の数	100 指
1 指あたりの画像枚数	8 枚
指紋画像の総数	800 枚
指紋画像の解像度	388 × 374 [pixel]
取得センサ	optical sensor ”TouchView II” by Identix
中心点及びマニューシャ抽出アルゴリズム	NFIS2[13]

指紋の中心点を用いた補正によるマニューシャの位置分布を図 4.9 に，リファレンスマニューシャを用いた補正によるマニューシャの位置分布を図 4.10 に示す．x 軸は指紋画像の横幅

(388[pixel])，y 軸は指紋画像の縦幅 (374[pixel])，z 軸はマニューシャの分布頻度を示す．図 4.9 と図 4.10 から補正後の指紋画像の中心部に近いほどマニューシャの分布は密になり，外縁部に行くほどマニューシャの分布が疎になっていることがわかる．

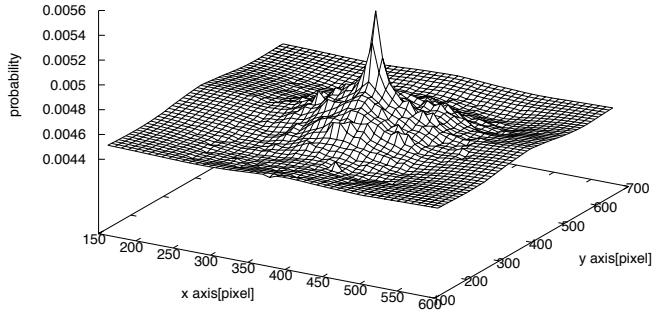


図 4.9　マニューシャ分布密度（中心点を用いた補正）

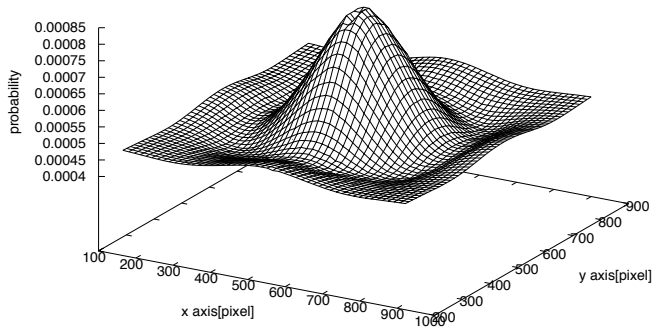


図 4.10　マニューシャ分布密度（リファレンスマニューシャを用いた補正）

■円形エリアの利点

上記の既存研究に対して，エリアの形状を円形にすることで，エリアの縁にあるマニューシャが位置ずれによって他のエリアに移動してしまう位置ずれによる誤差の影響を均一にすることができる．また，円形エリアを，補正後の指紋画像の中心部分では円形エリアの半径を小さくして密に分布させ，外縁部では半径を大きくして疎に分布させることで，マニューシャの位置分布を考慮したエリア設計が可能となる．このことにより，各エリアで均等な確率でビット列を生成することができるようになる．

4.2.1　円形エリアの作成方法

本節では，円形エリア作成の方針を述べた後に，円形エリア作成の手順を述べる．円形エリアの例を図 4.11 に示す．本研究では，図 4.11 に示すように円形エリアを補正後の指紋画像中心点から同心円状に配置する．

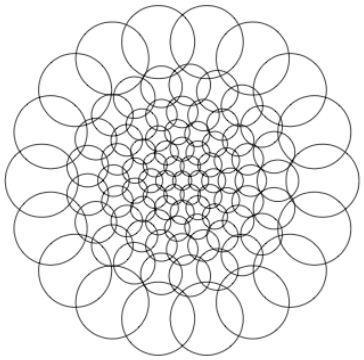


図 4.11　円形エリアの例

■円形エリア作成の基本方針

本研究では，マニューシャの位置分布を考慮した円形エリアを使用する．4.2 節で行ったマニューシャ位置分布の調査から，本研究で使用するリファレンスマニューシャを用いた補正後のマニューシャ位置分布に着目する．図 4.10 から補正後の指紋画像中心点（座標 (538.9, 538.9)）からの距離に応じたマニューシャの分布頻度を求めたものが図 4.12 である．本研究では，図 4.12 に着目し，補正後の指紋画像中心点からの距離を用いて各エリアに一致するマニューシャの数が均等になるように作成する．エリアとエリアに一致するマニューシャの関係を図 4.13 に示す．

図 4.10 から 2 次元のマニューシャ位置の度数分布に変換したものが図 4.14 である．マニューシャ位置分布の調査から，全体の 1%程度は指紋画像の両端に分布しているような特異なマニューシャが存在することが判明している．また指紋画像の形状から，マニューシャの分布は楕円状になっており，全てのマニューシャを考慮したエリアを設計した場合，図 4.15 に示すような一致するマニューシャが存在しないエリアが存在する恐れがある．そのため，図 4.16 のように，特異なマニューシャを除いた残り 99%のマニューシャ分布範囲に対してエリア設計を行う．

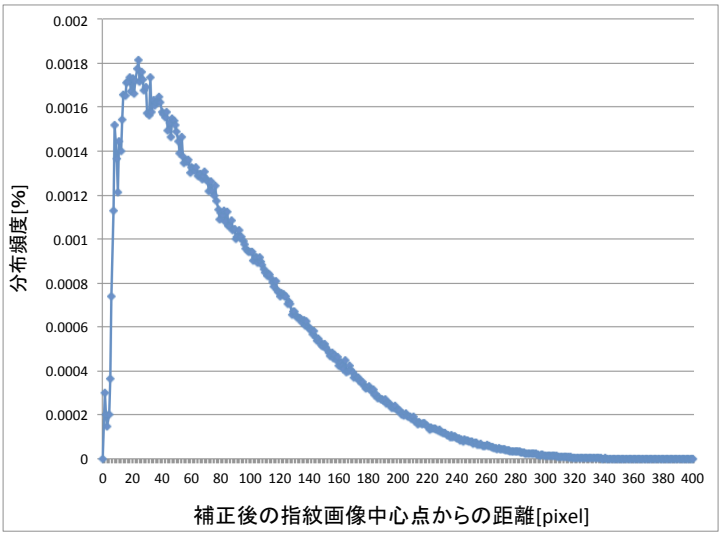


図 4.12　補正後の指紋画像中心点からの距離に応じたマニューシャの分布頻度

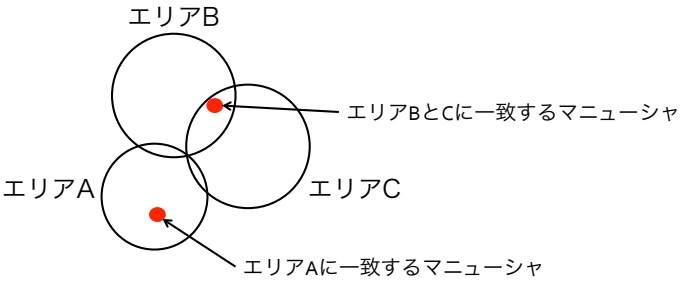


図 4.13　エリアとエリアに一致するマニューシャの関係

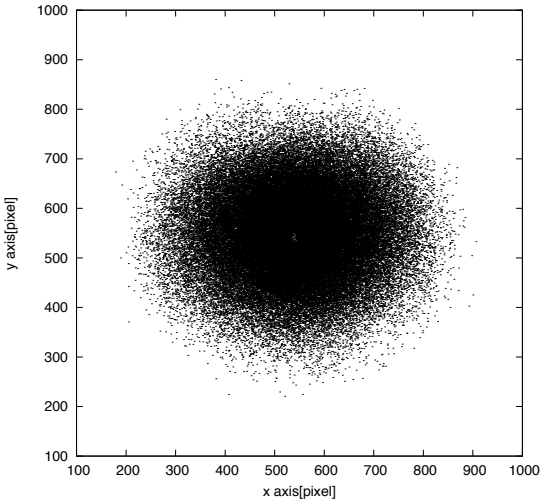


図 4.14　マニューシャの分布

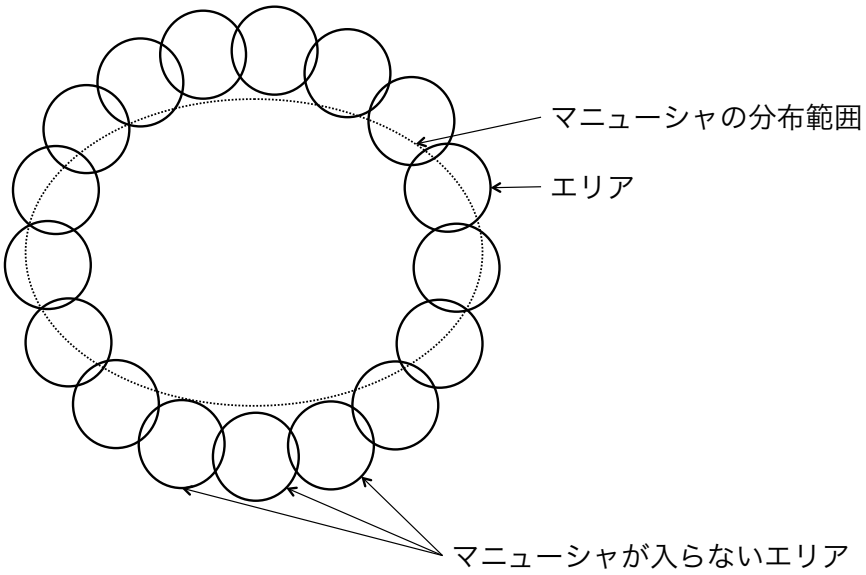


図 4.15　一致するマニューシャがないエリアの存在

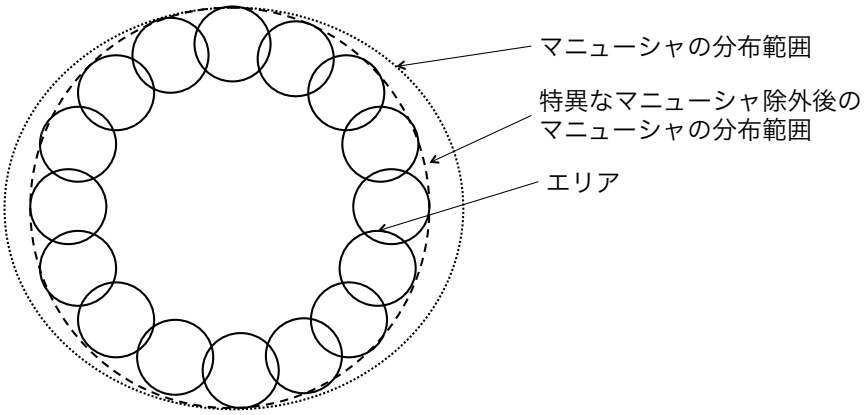


図 4.16　特異マニューシャ除外後のエリア構成

■円形エリアの作成手順

円形エリアの概要を図 4.17 に示す．円形エリア作成手順のフローチャートを図 4.18 に示し，図 4.18 に従って円形エリア作成手順を以下に述べる．

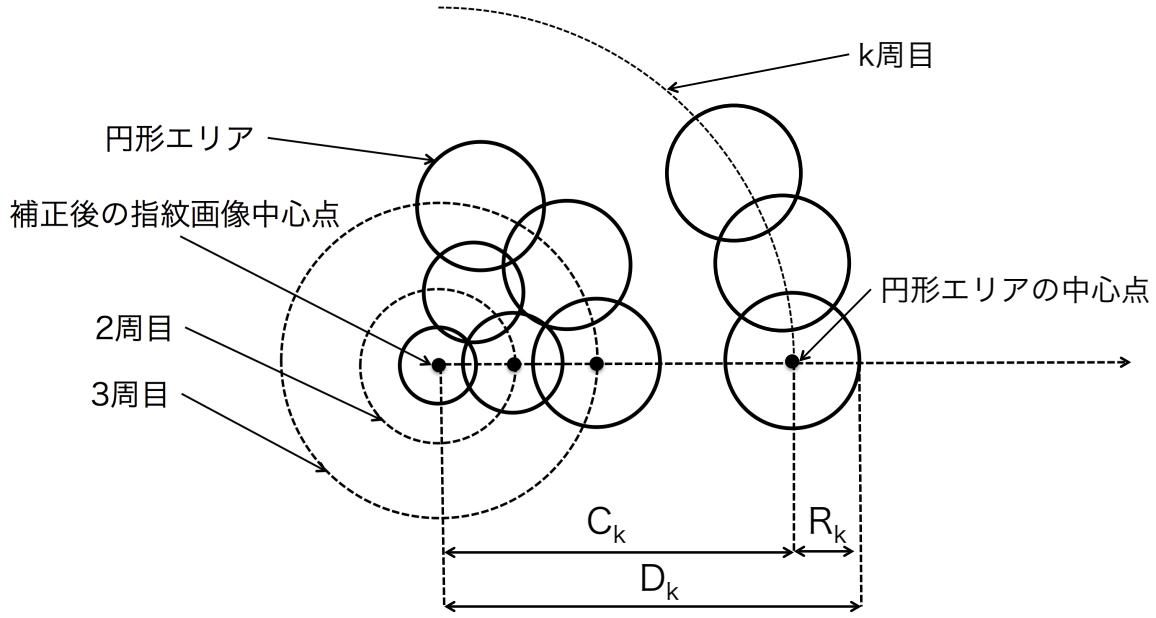


図 4.17　円形エリアの概要

1. 学習用の指紋データベースに含まれる全ての指紋画像に対して，4.2 節のマニューシャ位置分布の調査と同様に，リファレンスマニューシャを用いた補正後のマニューシャ位置分布の統計を求める．マニューシャ位置分布の統計から，補正後の指紋画像中心点から距離 d におけるマニューシャの集合（M_d）と，補正後の指紋画像中心点から距離 d におけるマニューシャの数（$|M_d|$）を算出する．また，補正後の指紋画像中心点から最も離れた位置にあるマニューシャまでの距離を d_{max} とする．ここで，以下のように記号を定義する．

N : 作成するエリア総数
M_d : 補正後の指紋画像中心点から距離 d におけるマニューシャの集合
$|M_d|$: 中心点から距離 d におけるマニューシャの数
A_k : k 周目のエリアの集合
$|A_k|$: k 周目のエリアの数
D_k : 補正後の指紋画像中心点から k 周目エリア外周までの距離の最大値
C_k : 補正後の指紋画像中心点から k 周目エリア中心点までの距離
R_k : k 周目のエリア半径

2. 作成するエリア総数 N を指定する．エリア作成の基本方針から各エリアに一致するマニューシャ数が等しため，各エリアに一致するマニューシャ数を B とすると，式 4.2 が成り立つ．

$$B = \frac{\sum_{d=0}^{d_{max}} |M_d|}{N} \tag{4.2}$$

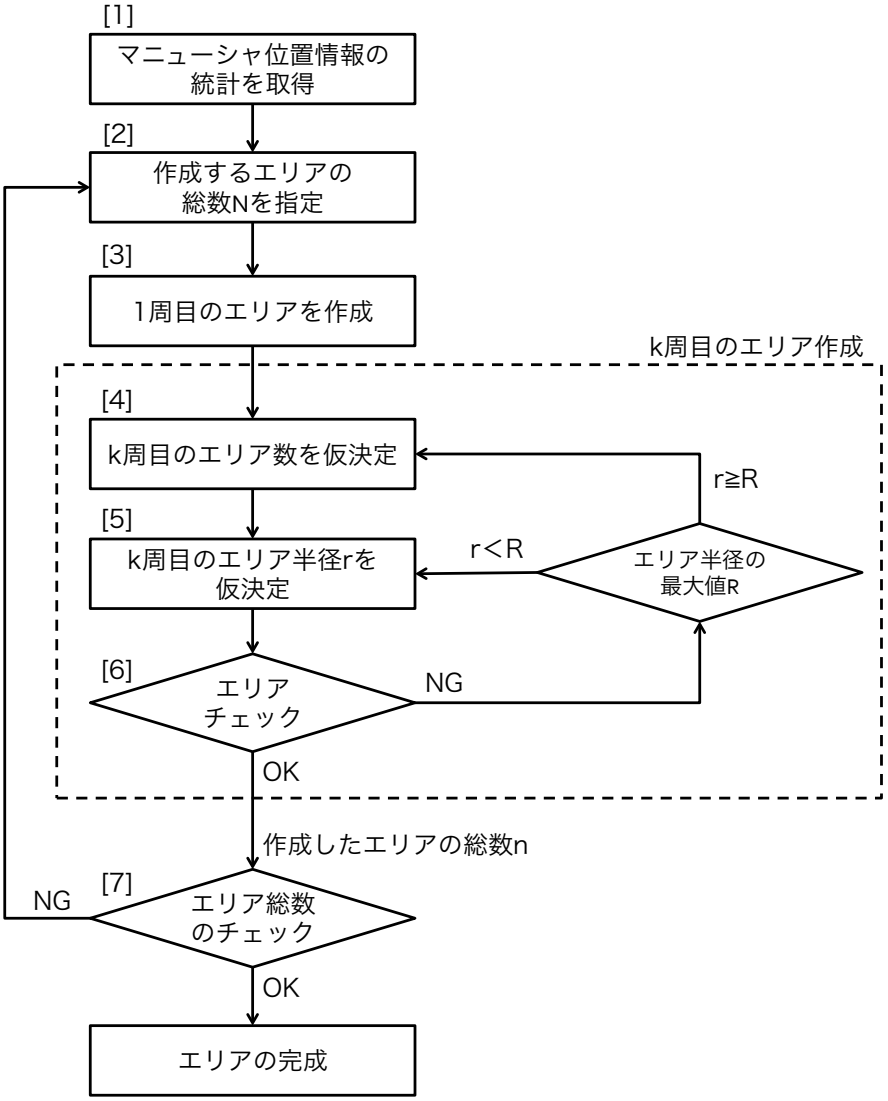


図 4.18　円形エリア作成のフローチャート

3. 1 周目のエリア作成方法の概要を図 4.19 に示す．1 周目のエリア数は 1 個（式 4.3）に固定する．このとき，1 周目のエリアに限り D_1 と R_1 は式 4.4 の関係にある．エリア作成の基本方針から各エリアに一致するマニューシャ数が等しく，$|M_d|$ と N から式 4.5 が成り立つ．式 4.4 と式 4.5 から，1 周目のエリア半径 R_1 を求める．

$$|A_1| = 1 \tag{4.3}$$

$$D_1 = R_1 \tag{4.4}$$

$$\sum_{d=0}^{D_1} |M_d| = B \times |A_1| \tag{4.5}$$

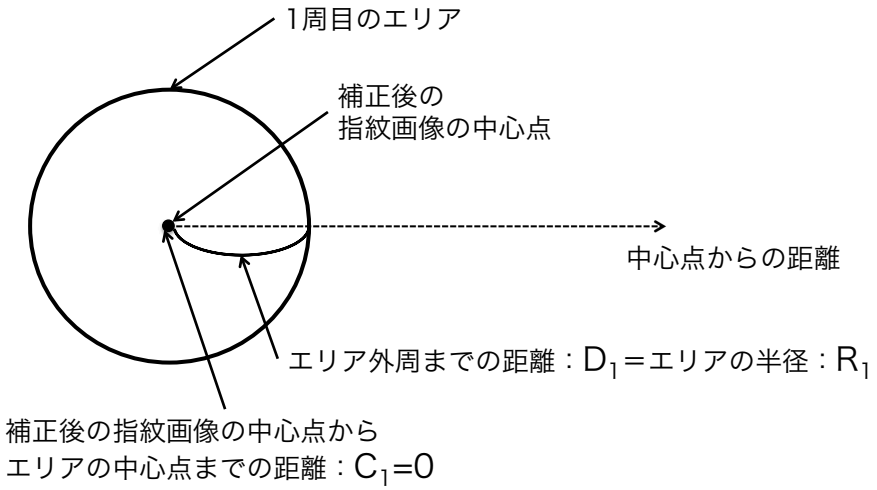


図 4.19　1 周目のエリア作成方法の概要

4. k 周目のエリア概要を図 4.20 に示す．k 周目のエリア数を 4 個（式 4.6）と仮決定する．この時，エリア作成の基本方針から各エリアに入るマニューシャ数が等しく，式 4.7 が成り立つ．式 4.6 と式 4.7 から D_k を求め，エリア中心点 C_k を式 4.8 のように定める．

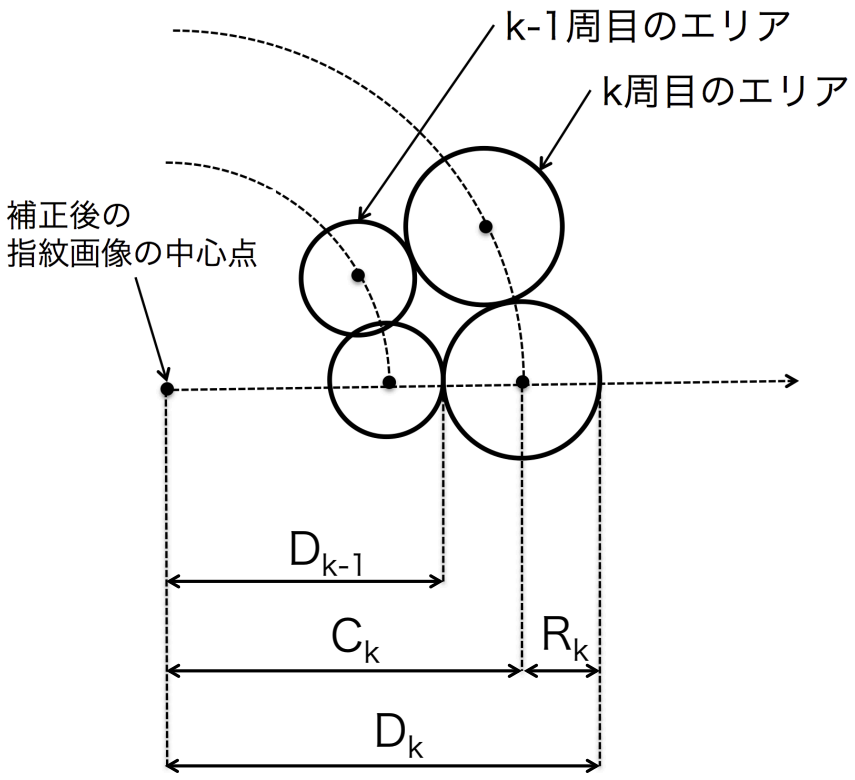


図 4.20　k 周目のエリア概要

$$|A_k| = 4 \tag{4.6}$$

$$\sum_{d=D_k+1}^{D_k} |M_d| = B \times |A_k| \tag{4.7}$$

$$C_k = \frac{D_k - D_{k-1}}{2} + D_{k-1} = \frac{D_{k-1} + D_k}{2} \tag{4.8}$$

5. k 周目のエリア半径 R_k の取りうる値の範囲（式 4.9）について定義する．R_k の最小値は，1 つ内側のエリアである $k-1$ 周目のエリアと接する場合とし，R_k の最大値は，1 つ内側のエリア半径 R_k の 1/3 を加えたものとする．また，エリア半径の最大値については，実験的に定めたものである．

$$D_k - C_k \leqq R_k \leqq D_k - C_k + \frac{R_{k-1}}{3} \tag{4.9}$$

6. R_k の最小値で作成されるエリアについて，半径 C_k 以下のいずれのエリアにも含まれない領域が存在しないかを式 4.10 にて調べる．式 4.10 を満たさない場合は，R_k の値を増やし，エリアの再作成を行い，再び円形エリア間の隙間を調べる．R_k の値が最大値に達しても式 4.10 を満たさない場合は，手順 4 に戻り，仮決定したエリア数 A_k の値を 1 増やす．式を満たす R_k が存在する場合，A_k, D_k, C_k, R_k を決定する．

$$\left\{ x \in \sum_{d=0}^{d=C_k} M_d : x \in \sum_{l=0}^{k} A_l \right\} = \phi \tag{4.10}$$

7. m 周目までに作成したエリアの総数 n が，手順 2 で指定した N の ± 3 以内であれば（式 4.12），エリア作成を完了する．式 4.12 を満たさない場合は，エリア作成失敗とし，手順 2 に戻り N の再指定を行う．

$$n = \sum_{k=1}^{m} |A_k| \tag{4.11}$$

$$N - 3 \leqq n \leqq N + 3 \tag{4.12}$$

4.3　共通補助データを用いた指紋情報の量子化手法

本節では，指紋のマニューシャと 4.2 節で作成した共通補助データの円形エリアとの照合に用いる照合閾値の説明をした後に，共通補助データを用いた指紋情報の量子化手法を説明する．

■照合閾値

指紋のマニューシャと共通補助データの円形エリアとの照合には，照合閾値を設けて判定を行う．本研究で用いる円形エリアは，補正後の指紋画像中心部では小さく密に，外縁部では大きく

疎に作成してあるため，中心部と外縁部では円形エリアの半径の長さが異なる．したがって，円形エリアの中心点からマニューシャまでの距離ではなく，円形エリアの半径に対する相対的な距離を閾値とする．照合閾値を用いることで，照合時に起きる位置ずれをある程度吸収することが期待できる．図 4.21 に照合閾値の概要を示す．円形エリアの中心点からの距離を d，円形エリアの半径を r とすると，照合閾値は d/r と定義する．

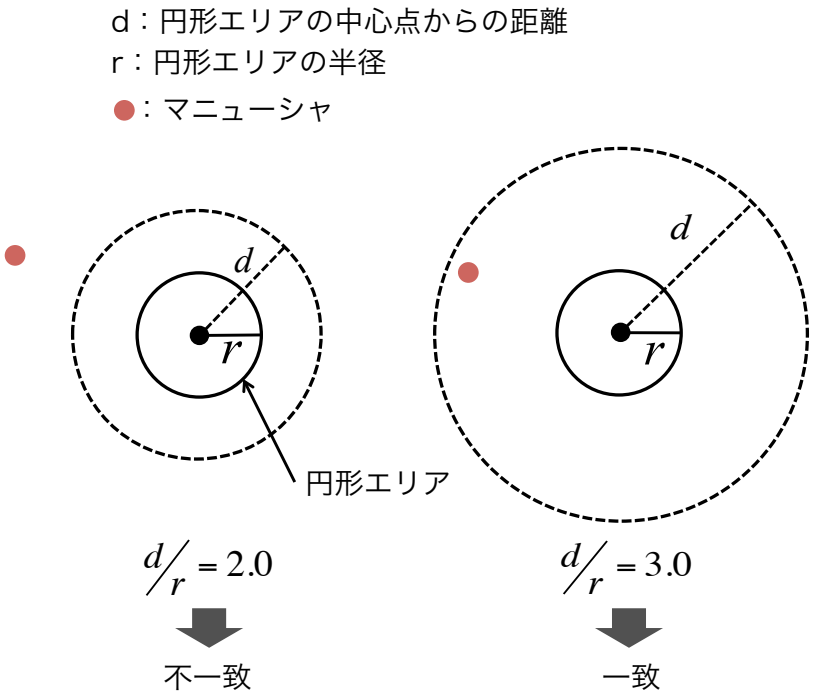


図 4.21　照合閾値の概要

図 4.21 の場合，照合閾値 $d/r = 2.0$ の時は，マニューシャは円形エリアと一致しないと判定される．照合閾値 $d/r = 3.0$ のときは，マニューシャは円形エリアと一致すると判定される．

■量子化方法

本研究では，共通補助データを用いて指紋のマニューシャ情報を量子化しビット列を生成する．最終的に出力されるビット列は，共通補助データの円形エリアごとにマニューシャ情報を量子化して得られるビット列をエリア番号順に組み合わせたものである．

本研究では，マニューシャの持つ角度情報に着目して量子化を行う．初めに，予め角度情報からビット列を出力する方法（以下，ビットスケール）を作成しておく．共通補助データの円形エリアとマニューシャの一致判定を照合閾値を用いて行い，エリアごとに一致したマニューシャの角度平均を算出し，ビットスケールを用いて量子化を行う．

ここで，ビットスケール作成方法としてマニューシャの角度情報 θ を n 分割する場合を一例として図 4.22 に示す．また，マニューシャの角度情報については付録 A で示す．本研究では角度情

報の 0 レベルから均等に分割しビットスケールを作成する．また，最終的に出力されるビット列の長さが一定となるよう各領域に割り当てるビット列の長さは一定にする必要がある．

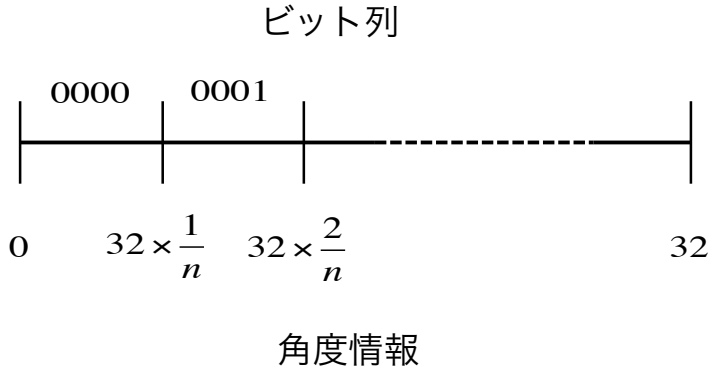


図 4.22　n 分割のビットスケールの一例

本研究では 5 章の精度評価実験にて，2 分割のビットスケールおよび 8 分割のビットスケールを用いるが，4 分割のビットスケールと同様に角度情報 0 レベルから均等に分割し，作成する．

■量子化手順

図 4.23 に量子化手順の概要を示し，以下にその手順を述べる．本節では簡単のため正方形エリアを使用している．また，センサから得られた指紋情報は位置ずれ角度ずれの補正を終えているものとする．

1. マニューシャと共通補助データにある円形エリアとの照合を行う．マニューシャの位置情報と照合閾値を用いて，マニューシャと円形エリアの一致判定を行う．
2. エリアごとに一致したマニューシャの角度情報の平均値 θ を算出する．
3. 算出した角度平均と予め作成したおいたビットスケールに従って，エリアごとにビットを出力する．この時，一致したマニューシャが存在しないエリアは消失誤りとする．図 4.23 は，角度レベルを 4 分割にした場合の例である．
4. エリアごとに出力したビットを，エリア番号順に組み合わせてビット列を作成する．

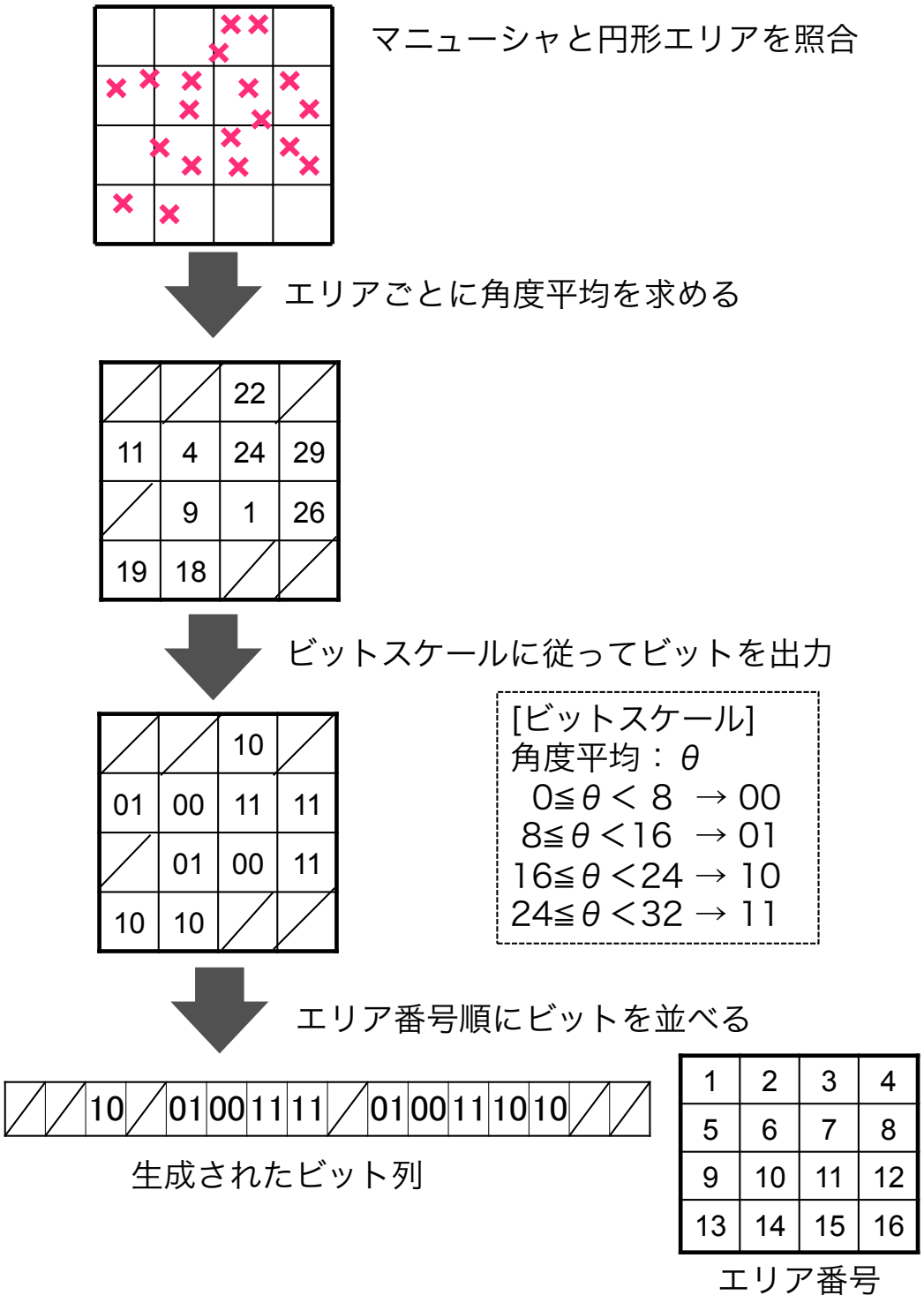


図 4.23　量子化手順の概要

第 5 章

照合精度評価

本研究では，センサから得られた指紋情報を 4.1.2 項で説明したリファレンスマニューシャを用いた補正を行い，4.2 節で作成した共通補助データを用いて，4.3 節の方法で指紋情報の量子化を行いビット列を生成する．

本章では，このビット列を用いて 3.2 節で述べたバイオメトリック暗号方式を構成する場合の照合精度を評価する．照合精度に影響を与えるパラメータとして，照合閾値，角度分割数，円形エリア数が考えられ，これらを推移し，登録用指紋画像と照合用指紋画像から作成されるビット列の各要素を比較し，秘密情報要素数と復元率の関係から照合精度評価を行う．照合精度評価に用いる式は，3.2.3 項に記述した誤り訂正符号の秘密情報復元条件式である式 3.5 を用いる．

照合精度評価実験結果は，登録用指紋画像と照合用指紋画像から作成されるビット列の各要素を比較し，秘密情報要素数と復元率の関係で示す．また，ビット列の誤合致率（FMR）と非誤合致率（FNMR）の関係を ROC カーブで示し，各パラメータの照合精度評価を行う．

5.1 各評価実験で共通する諸元

照合精度評価実験に用いる指紋データベース FVC2002[12] の諸元を表 5.1 に示す．また，FVC2002 の 100 指の中から 30 指を円形エリア作成用の学習データとして使用し，残りの 70 指を照合精度評価実験に用いる．

表 5.1 FVC2002 の諸元

指の数	100 指
1 指あたりの画像枚数	8 枚
指紋画像の総数	800 枚
指紋画像の解像度	388 × 374 [pixel]
取得センサ	optical sensor ”TouchView II” by Identix
中心点及びマニューシャの抽出アルゴリズム	NFIS2[13]

照合精度評価実験では，登録用指紋画像枚数は 3 枚とし，残りの 5 枚を照合用指紋画像とする．

照合精度評価実験に用いるデータの諸元を表 5.2 に示す．また，実験結果において，復元率の有効桁数は，Rule of 3[18] に基づき，本人復元率においては $3/350 = 0.00857\cdots$ より 1% 未満は切り捨て，他人復元率においては，$3/24150 = 0.000124\cdots$ により 0.1%未満は切り捨ててある．

表 5.2　照合精度評価実験に用いるデータの諸元

指の数	70 指
1 指あたりの画像枚数	8 枚
指紋画像の総数	560 枚
登録指紋画像枚数	3 枚
照合指紋画像枚数	5 枚
本人照合回数	350 回
他人照合回数	24150 回
リファレンスマニューシャの座標	(538.9, 538.9)
誤り訂正に用いる符号	Reed Solomon 符号

また，誤り訂正符号には Reed-Solomon 符号を用いる．角度分割数に応じて各円形エリアから出力されるビット数が異なるため，Reed-Solomon 符号の 1 シンボルを各円形エリアから出力されるビット列に対応づける．角度分割数とガロア拡大体の対応を表 5.3 に示す．また，秘密鍵復元可能条件は，式 3.5 となる．

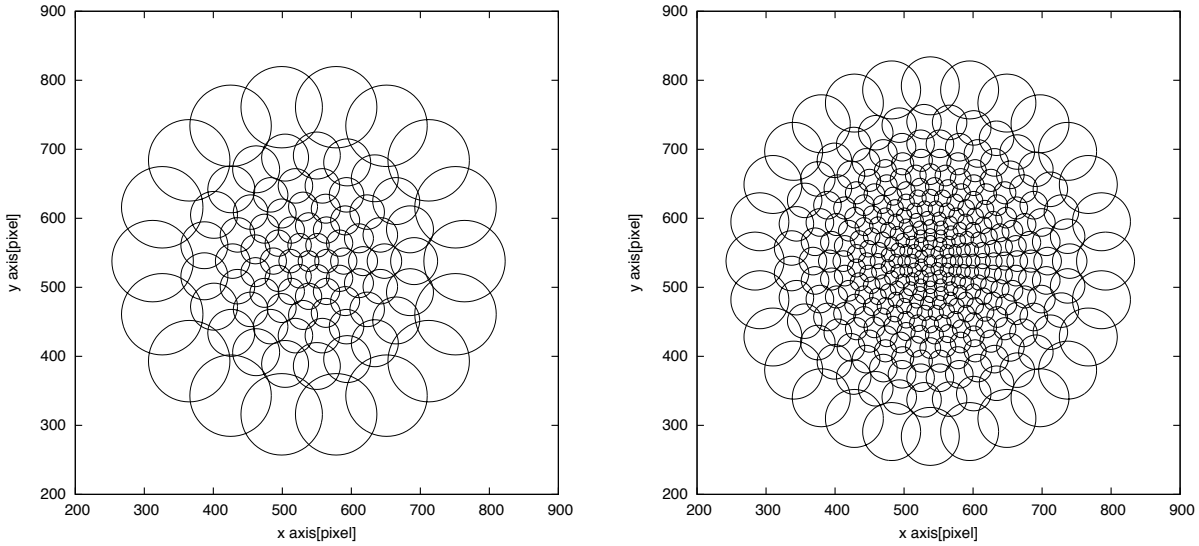
表 5.3　角度分割数とガロア拡大体の対応

角度分割数	ガロア拡大体
2 ∼ 3 分割	$GF(2^2)$
4 ∼ 7 分割	$GF(2^3)$
8 ∼ 15 分割	$GF(2^4)$
16 ∼ 31 分割	$GF(2^5)$

学習データを用いて 4.2.1 項の方法で作成したエリアから，円形エリア数が 91 個と 345 個のエリアを一例として図 5.1 に示す．

5.2　照合パラメータと照合精度の関係

本節では，照合精度に影響を与えると考えられる照合閾値，角度分割数，円形エリア数の値を推移させ，照合精度実験を行う．



円形エリア数 91 個　　円形エリア数 345 個

図 5.1　精度評価実験に用いるエリアの一例

5.2.1　照合閾値

本研究では，指紋のマニューシャと共通補助データの円形エリアとの照合に 4.3 節で説明した照合閾値を用いて行う．マニューシャの位置ずれによって，登録時に円形エリアの縁にあるマニューシャは，照合時に別の円形エリアへと移動してしまう可能性がある．照合閾値を大きくすることで，登録時よりも円形エリアの領域が大きくなり，照合時に起きるマニューシャの位置ずれをある程度許容できると考えられる．一方で，円形エリアの領域が大きくなることで，登録時に一致していなかったマニューシャを照合時に一致と判定してしまう可能性もある．

このように,照合閾値は照合精度に影響を与えると考えられる．本実験では照合閾値を 1.0 ～ 3.0 の間で 0.2 間隔で推移させ照合精度評価実験を行う．また，照合閾値による精度比較を行うため，円形エリア数は 345 個，角度分割数は 8 分割に固定する．本実験における諸元を表 5.4 に示す．

表 5.4　照合閾値による精度評価実験の諸元

円形エリア数	345 個
照合閾値	1.0 ～ 3.0 (0.2 刻み)
角度分割数	8 分割

■実験結果

照合閾値 1,0 ～ 3.0 の間で最も照合精度が高かった上位 4 つの秘密情報要素数と復元率の関係

を図 5.2 に示し，その ROC カーブを図 5.3 に示す．また秘密情報要素数 11 個（$4 \times 11 = 44$ ビット）における本人復元率と他人復元率を表 5.7 に示す．

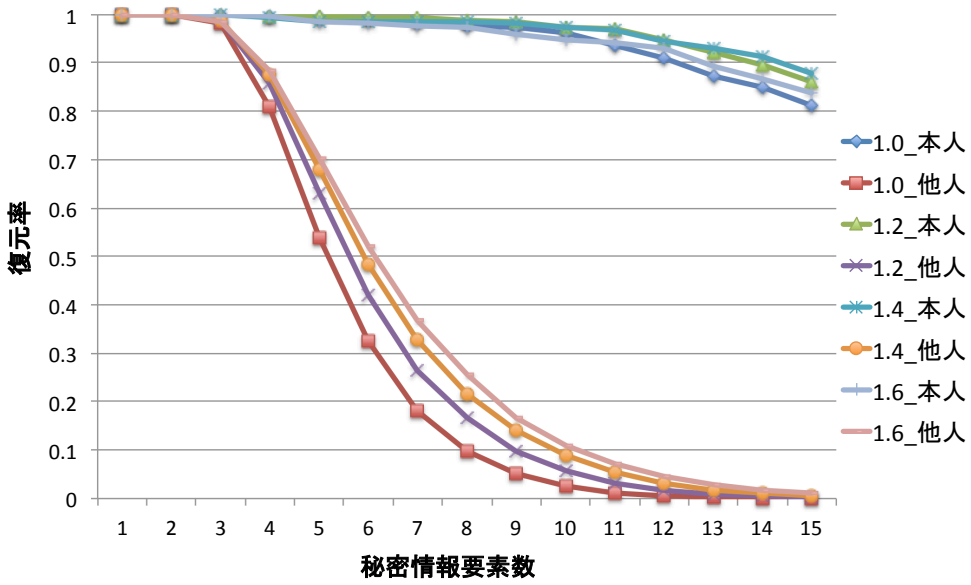


図 5.2　復元率結果（照合閾値による評価）

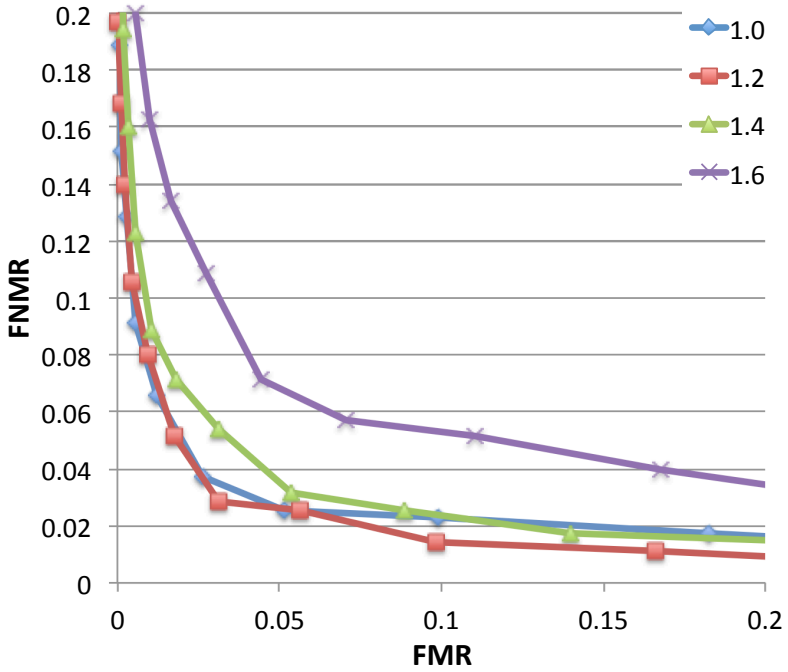


図 5.3　ROC カーブ（照合閾値による評価）

表 5.5　秘密情報要素数 11 個における復元率（照合閾値による評価）

照合閾値	本人復元率	他人復元率
1.0	0.93	0.065
1.2	0.97	0.031
1.4	0.96	0.053
1.6	0.94	0.070

■考察

実験結果の図 5.2 と図 5.3 から，照合閾値が 1.2 のとき最も照合精度が高く，照合閾値が 1.2 よりも大きくなるに従って照合精度が低下している．照合閾値を 1.2 よりも大きくすることにより，照合時の位置ずれをある程度許容できるようになることよりも，登録時に一致していないマニューシャが照合時に一致と判定される影響の方が大きいといえる．この結果より，リファレンスマニューシャを用いた補正により，マニューシャの位置ずれによる影響は小さいと考えられる．

5.2.2　角度分割数

本研究では，マニューシャの角度情報に着目し，共通補助データの円形エリアごとに一致したマニューシャの角度平均と，予め作成したおいたビットスケールからビット列を作成する．ビットスケールはマニューシャの角度分割数により構成する．角度分割数が少ない場合，同一指であれば同一ビット列を出力する可能性が高いが，同一ビット列を出力する角度範囲が広いため，他人の指であっても同一ビット列を出力してしまう可能性が高まる．一方で，角度分割数を増やすと，同一ビット列を出力する角度範囲が狭くなるため，他人の指が本人の指と同一のビット列を出力する可能性は低くなる．4.1.2 項で行った角度補正精度調査から，リファレンスマニューシャを用いた補正の場合であっても角度ずれの誤差を全て補正することはできていない．したがって，同一ビット列を出力する角度範囲が狭くなると，角度ずれの影響で同一指であっても異なるビット列を出力してしまう可能性が高くなる．

このように，角度分割数は照合精度に影響を与えると考えられる．本実験では角度分割数を 2 分割から 16 分割とした場合の照合精度比較を行う．また，円形エリア数は 345 個，照合閾値は 1.0 に固定する．本実験における諸元を表 5.6 に示す．

表 5.6　角度分割数による精度評価実験の諸元

円形エリア数	345 個
照合閾値	1.0
角度分割数	2 ～ 16 分割

■実験結果

角度分割数を 2 分割から 16 分割とした時の秘密情報要素数と本人復元率の関係を図 5.4 に，他人復元率との関係を図 5.5 示し，その ROC カーブを図 5.5 に示す．また秘密情報要素数 10 個（$4 \times 10 = 40$ ビット）における本人復元率と他人復元率を表 5.7 に示す．

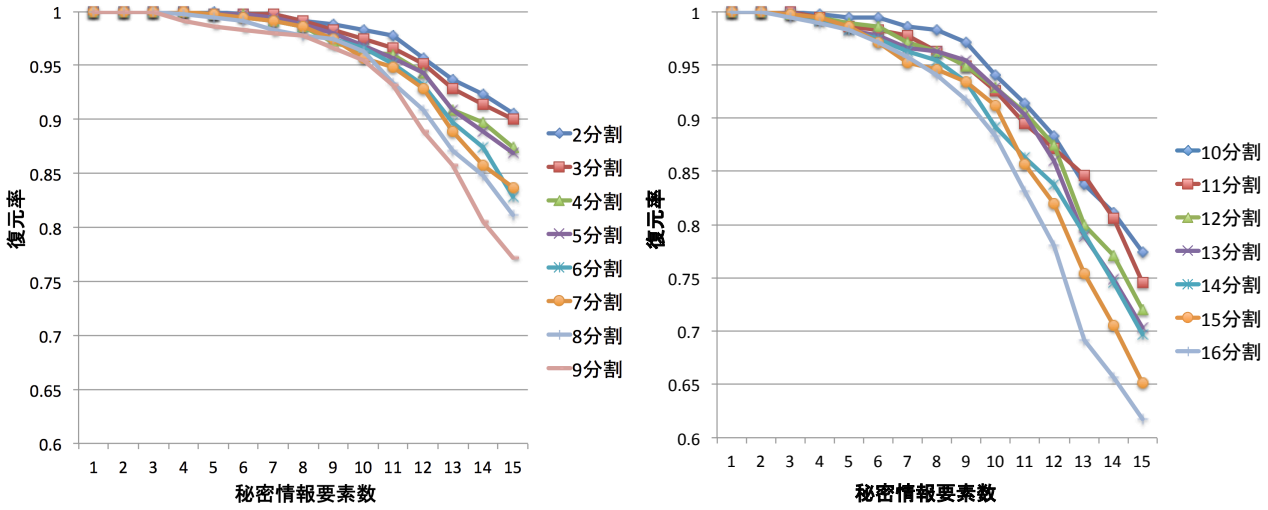


図 5.4　本人復元率結果（角度分割数による評価）

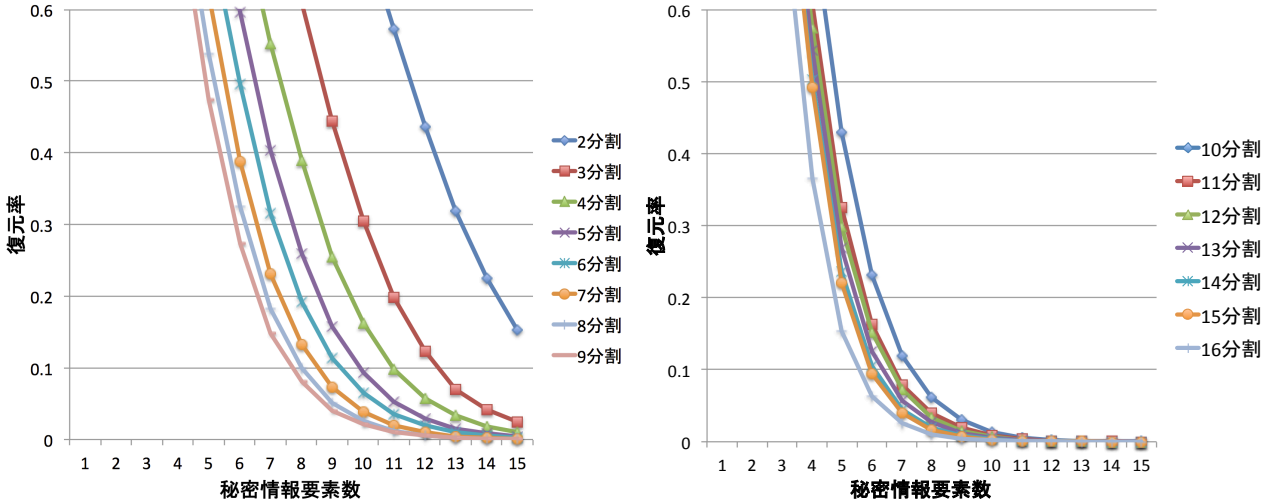


図 5.5　他人復元率結果（角度分割数による評価）

5.2　照合パラメータと照合精度の関係

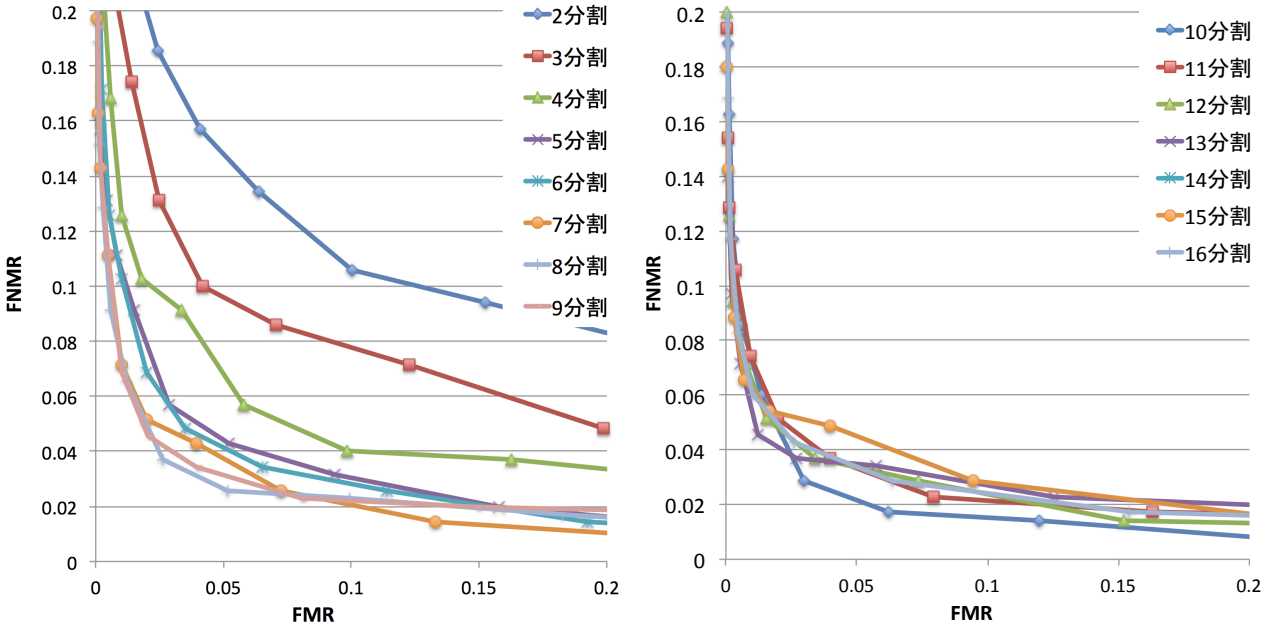


図 5.6　ROC カーブ（角度分割数による評価）

表 5.7　秘密情報要素数 10 個における復元率

角度分割数	本人復元率	他人復元率	角度分割数	本人復元率	他人復元率
2 分割	0.98	0.709	10 分割	0.94	0.013
3 分割	0.97	0.304	11 分割	0.92	0.009
4 分割	0.96	0.162	12 分割	0.92	0.007
5 分割	0.96	0.093	13 分割	0.92	0.005
6 分割	0.96	0.065	14 分割	0.89	0.004
7 分割	0.95	0.039	15 分割	0.91	0.002
8 分割	0.96	0.026	16 分割	0.88	0.001
9 分割	0.95	0.020			

■考察

実験結果の図 5.4～ 図 5.6，表 5.7 から角度分割数が 8 分割の時が僅かではあるが最も照合精度が高い．4.1.2 項で行った角度補正精度調査から，リファレンスマニューシャを用いた補正では，角度誤差が約 90%の確率で 1 レベル以内に収まっている．このことから，ビットスケールの角度分割数を，8 分割のように角度を細かい領域に分割しビット列を出力する場合でも，一致したマニューシャの存在する円形エリアにおいて，登録時と照合時で同一のビット列を出力する確率が高いと考えられる．図 5.4 や表 5.7 から，2 分割 ～9 分割において本人復元率は大きく低下してい

ない．

角度分割数を増やすことで，同一ビット列を出力する角度範囲が狭くなるため，他人の指が本人の指と同一のビット列を出力する可能性は低くなる．実験結果の図 5.5 や表 5.7 から，他人復元率は分割数を増やすことで低下していることがわかる．

5.2.3　円形エリア数

本研究では，4.2.1 項で説明した方法で円形エリアを作成し，照合閾値を用いて指紋のマニューシャと一致判定を行う．円形エリアの大きさは半径により定義されるが，円形エリア数の変化によって円形エリアの半径も変化する．円形エリア数が少ない場合，円形エリアの半径は大きくなり，各円形エリアの占める領域は大きくなる．このことにより，照合時にマニューシャが位置ずれによって他のエリアに移動してしまう位置ずれによる誤差の影響を低くすることができる．しかし，一つの円形エリアに複数のマニューシャが一致する可能性が高くなり，ビット列を出力する円形エリアが少なくなってしまう．円形エリア数を多くした場合，エリアの半径は小さくなり，各円形エリアの占める領域は小さくなる．このことにより，一つの円形エリアに複数のマニューシャが一致する可能性は低くなり，ビット列を出力する円形エリアが得られた指紋情報に含まれるマニューシャの数に近づくと考えられる．一方で，照合時の位置ずれの影響は大きくなると考えられる．

このように，エリア数は照合精度に影響を与えると考えられる．本実験では，学習データから作成した円形エリア数の異なるエリアを用いて照合精度の比較を行う．また，照合閾値は 1.0，角度分割数は 8 分割に固定する．本実験における諸元を表 5.8 に示す．

表 5.8　円形エリア数による精度評価実験の諸元

円形エリア数	68 個，91 個，121 個，148 個 ，188 個 269 個，299 個，345 個，360 個
照合閾値	1.0
角度分割数	8 分割

■実験結果

各円形エリア数の時の秘密情報要素数と本人復元率の関係を図 5.7 に，他人復元率の関係を図 5.8 に示し，その ROC カーブを図 5.9 に示す．また秘密情報要素数 10 個（$4 \times 10 = 40$ ビット）における本人復元率と他人復元率を表 5.9 に示す．

5.2　照合パラメータと照合精度の関係

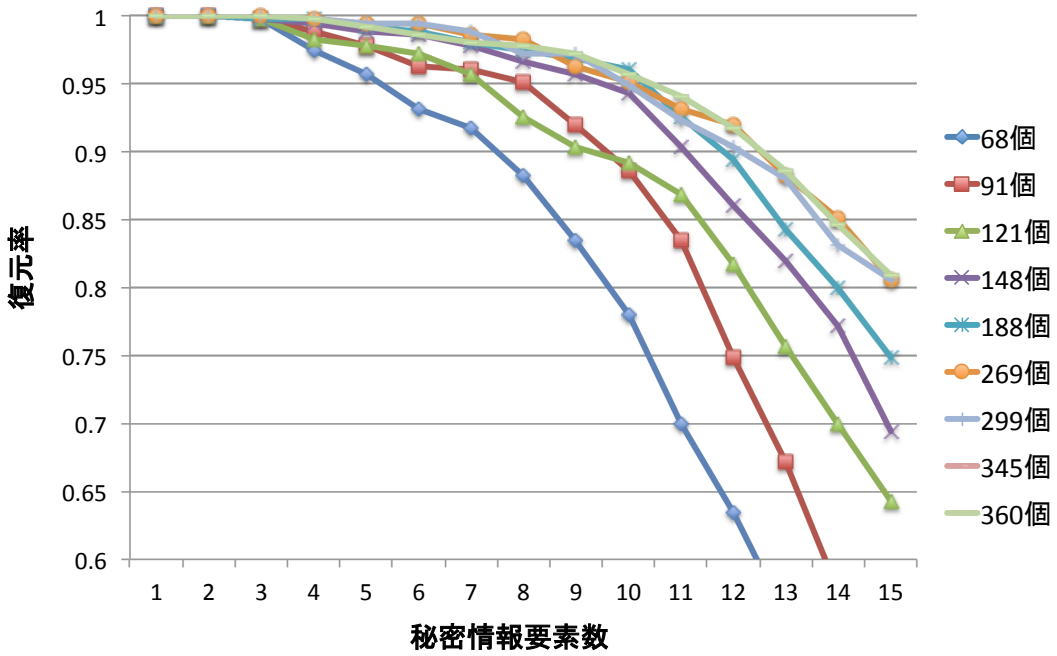


図 5.7　本人復元率（円形エリア数による評価）

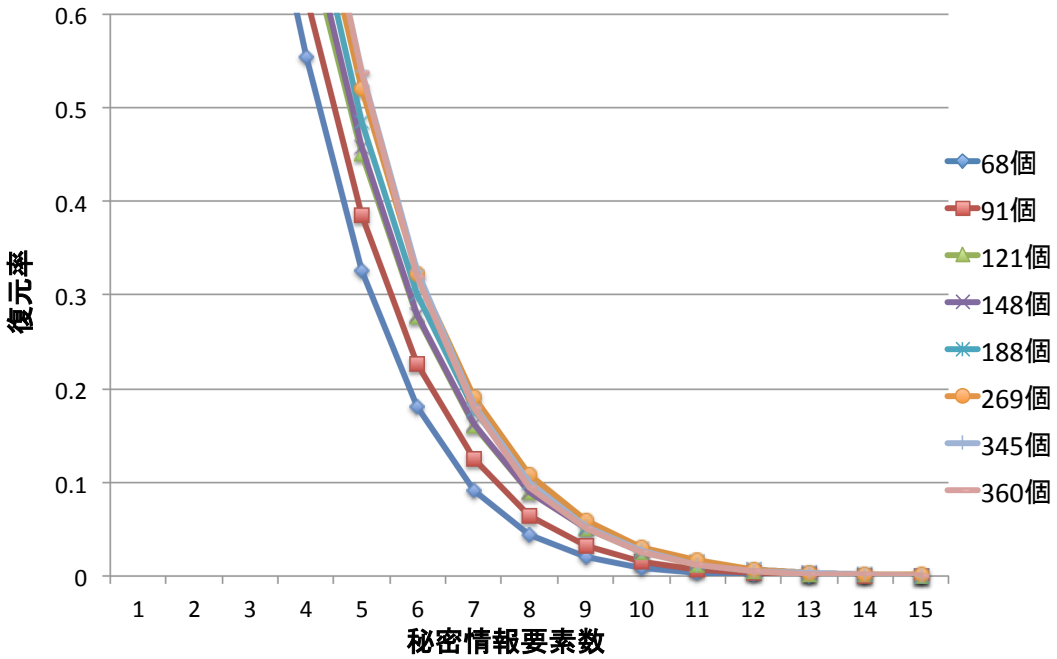


図 5.8　他人復元率（円形エリア数による評価）

■考察

実験結果の図 5.9 から円形エリア数が 345 個の時が最も照合精度が高い．図 5.8 から円形エリ

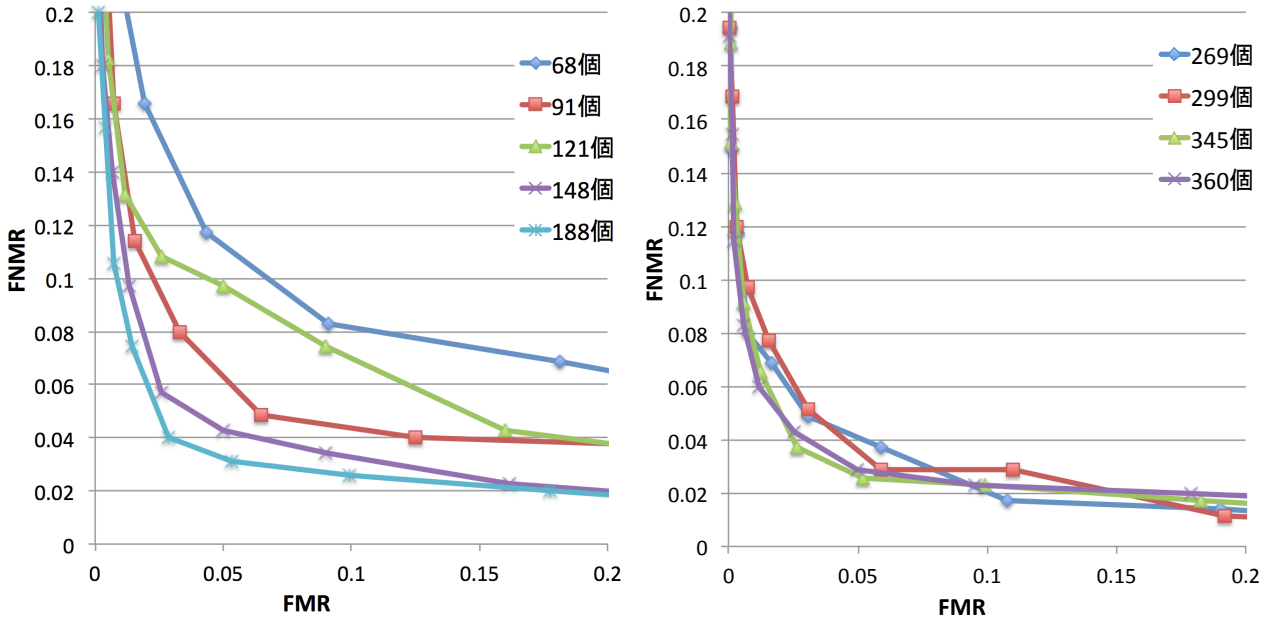


図 5.9　ROC カーブ（円形エリア数による評価）

ア数が 68 個から 188 個に増えるに従って照合精度が高くなっていることがわかる．一方で，円形エリア数を 188 個から増やした場合，照合精度の向上はほとんどは見られない．円形エリア数を増やすことは，本人と他人の識別能力は向上するが，マニューシャの位置ずれによる本人間の照合精度は低下するトレードオフの関係にあると考えられる．

表 5.9　秘密情報要素数 10 個における復元率（円形エリア数による評価）

エリア数	本人復元率	他人復元率
68 個	0.78	0.008
91 個	0.88	0.015
121 個	0.89	0.025
148 個	0.94	0.025
188 個	0.96	0.028
269 個	0.95	0.030
299 個	0.94	0.030
345 個	0.96	0.026
360 個	0.95	0.025

5.3　リファレンスマニューシャを用いた補正の照合精度への影響

センサから得られる指紋情報の位置ずれ角度ずれを補正する手法として，4.1.1 項と 4.1.2 項で指紋の中心点を用いる補正手法とリファレンスマニューシャを用いる補正手法の説明を行った．

本実験では，宿沢らが提案している共通テンプレートを用いた手法 [17] と提案手法の精度比較を行う．共通テンプレートを用いた手法では，本研究と同様に円形エリアを使用しているが，円形エリアの作成方法は手動によるものである．また，精度評価に使用している指紋データベースは研究室内のものであり，品質の悪い指紋に対しては取り直しを行うなどデータベース全体として品質の高い指紋により構成されている．

本実験においては，宿沢らの実験結果のうち，最も照合精度が高い円形エリア数 85 個，照合閾値 2.0，角度分割数 4 分割の結果を用いる．また，リファレンスマニューシャを用いた補正では，宿沢らの手法に最も近い円形エリア数 91 個，角度分割数を 4 分割とし，これらの条件のもとで 5.2 節で行った実験において最も照合精度が高かった照合閾値 1.2 を用いる．また，円形エリア数においてはリファレンスマニューシャを用いた補正において最も照合精度が高い 345 個のものについても比較を行った．また，円形エリア数 345 個については，角度分割数が 4 分割と 8 分割で実験を行った．本実験における諸元を表 5.10 に示す．

表 5.10　位置ずれ角度ずれ補正による評価に用いるデータの諸元

	指紋の中心点	リファレンスマニューシャ
指紋データベース	研究室内データベース	FVC2002
指の数	140 指	70 指
1 指あたりの画像枚数	5 枚	8 枚
登録指紋画像枚数	3 枚	
照合指紋画像枚数	2 枚	5 枚
本人照合回数	280 回	350 回
他人照合回数	38920 回	24150 回
円形エリア数	85 個	91 個，345 個
照合閾値	2.0	1.2
角度分割数	4 分割	4 分割，8 分割
中心点及びマニューシャの抽出アルゴリズム	NFIS2[13]	

■実験結果

照合精度実験を行った各パラメータの組み合わせを表 5.11 示す．秘密情報要素数と復元率の関係を図 5.10 に示し，その ROC カーブを図 5.11 に示す．また秘密情報要素数 11 個（$4 \times 11 = 44$

ビット）における本人復元率と他人復元率を表 5.12 に示す.

表 5.11　実験結果一覧（位置ずれ角度ずれ補正による評価）

	位置ずれ角度ずれ補正	円形エリア数	照合閾値	角度分割数
1	指紋の中心点	85 個	2.0	4 分割
2	リファレンスマニューシャ	91 個	1.2	4 分割
3	リファレンスマニューシャ	345 個	1.2	4 分割
4	リファレンスマニューシャ	345 個	1.2	8 分割

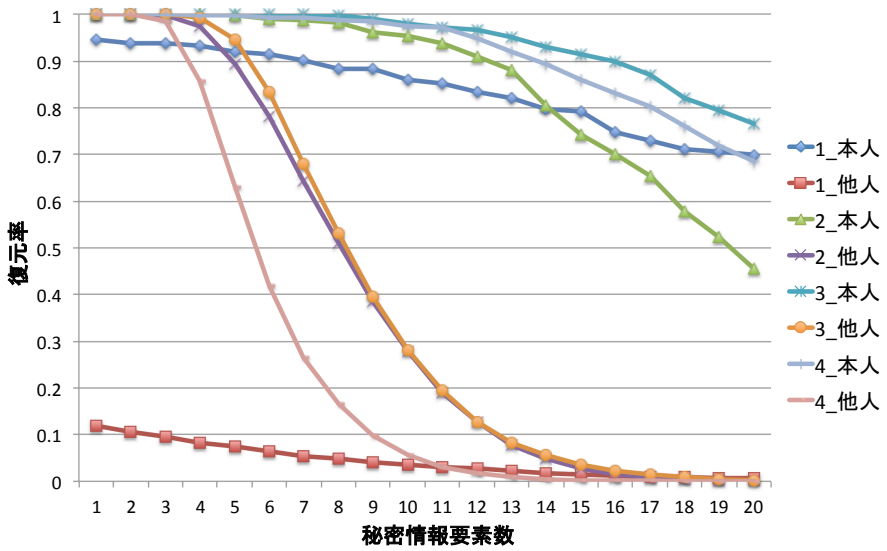


図 5.10　復元率結果（位置ずれ角度ずれ補正による評価）

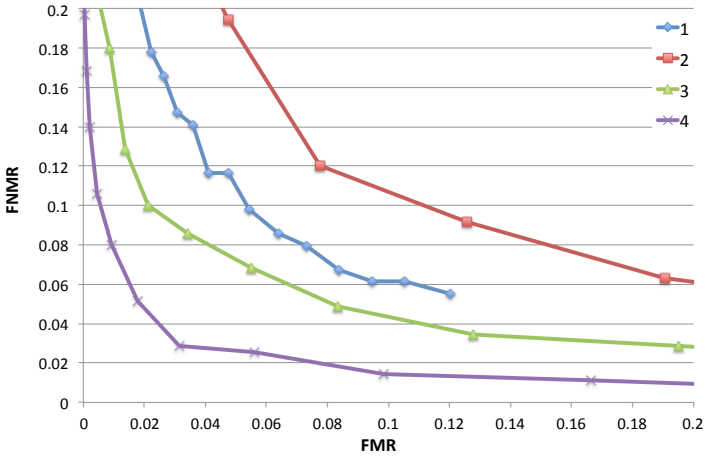


図 5.11　ROC カーブ（位置ずれ角度ずれ補正による評価）

表 5.12　秘密情報要素数 11 個における復元率（位置ずれ角度ずれ補正による評価）

	本人復元率	他人復元率
1	0.85	0.030
2	0.97	0.190
3	0.97	0.195
4	0.97	0.031

■考察

実験結果の図 5.11 から，リファレンスマニューシャを用いた補正で円形エリア数が 91 個の場合，指紋の中心点を用いた補正で円形エリア数が 85 個と比較して照合精度が低下した．これは，4.1.2 項で説明したリファレンスマニューシャを用いた補正では，指紋画像の面積を 4 倍にしているため，円形エリア数が同一の場合，各円形エリアの領域が大きくなり，一つの円形エリアに複数のマニューシャが一致する可能性が高くなり，ビット列を出力する円形エリアが少なくなってしまうため，照合精度が低下すると考えられる．図 5.11 から，リファレンスマニューシャを用いた補正においては，円形エリア数が 85 個の約 4 倍である 345 個の時に照合精度が向上していることがわかる．

指紋の中心点を用いた補正においては，角度分割数が 4 分割の時に最も高い照合精度を示している [17] が，リファレンスマニューシャを用いた補正では，角度分割数を 4 分割から 8 分割に増やすことで，さらに照合精度が向上している．これは，4.1.2 項で行った角度補正精度調査から，指紋の中心点を用いた補正よりもリファレンスマニューシャを用いた補正のほうが角度補正精度が高いことが要因として考えられる．

また，5.2.1 項の照合閾値による評価において，リファレンスマニューシャを用いた補正では照合閾値 1.2 の時に最も高い照合精度を示したが，中心点を用いた補正では，照合閾値 2.0 の時が最も照合精度が高い [17]．この結果から，リファレンスマニューシャを用いた補正の方が指紋の中心点を用いた補正よりもマニューシャの位置ずれ補正精度が高いと考えられる．

この実験結果から，マニューシャの位置ずれ角度ずれの補正精度が照合精度に大きく影響を与えていると考えられる．

本章で行った全ての照合精度評価実験から，最も照合精度が高い円形エリア数，照合閾値，角度分割数の組み合わせを表 5.13 に示す．

表 5.13　最も照合精度が高い組み合わせ

円形エリア数	345 個
照合閾値	1.2
角度分割数	8 分割

第 6 章

結論

6.1　まとめ

本研究では，Fuzzy Commitment Scheme を応用して，共通補助データを用いることにより個人の生体情報が推定されないバイオメトリック暗号の認証モデルを提案した．そして，生体情報として指紋を用いた場合の交通補助データの作成方法と，共通補助データと指紋情報から一意なビット列を作成する方法を検討した．検討内容は以下の通りである．

- 3 章ではバイオメトリック暗号の認証モデルを 4 つ提案し，それぞれのモデルについて，マスクデータの安全性に関する脅威と利用者の利便性に対する影響について述べた．さらに，本提案モデルに適する認証モデルに関して考察を行った．
- マニューシャの位置ずれ角度ずれを補正する手法として，指紋の中心点を用いる補正手法とリファレンスマニューシャを用いる補正手法の説明を行った．
- 共通補助データを構成するエリアとして円形エリアを提案し，円形エリアの作成方法を述べた．
- 共通補助データを用いて指紋情報を量子化する方法として，円形エリアと一致したマニューシャの角度平均に着目し，ビットスケールを用いてビット列を出力する方法を述べた．また，ビットスケールを構成する角度分割について説明を行った．

6.2　今後の検討課題

今後の検討課題を以下に示す．

- エリア作成手法の再検討
  4.2.1 項で説明したエリア作成手法では，同心円状にある円形エリアの重なりに対してほとんど考慮がされていない．したがって，同心円上にある円形エリア同士の重複する領域が非常に大きいエリアが作成される場合がある．したがって，同心円状にある円形エリアの重複も考慮したエリア作成手法を検討する必要がある．

- システムの利用シーンを想定した上での課題を検討

本提案手法は，照合精度評価実験から位置ずれや角度ずれに対して照合精度が落ちにくいという利点があり，ドアノブをセンサとして用いるなど位置ずれや角度ずれの影響が大きい環境に適用できる可能性がある．そこで，そのような環境における利用シーンを想定した上で課題を抽出し，検討する．

- システムに対する脅威と対策の検討
  本論文では，3 章においてマスクデータに対する脅威について考察を行い，安全性と利便性の観点から有効なモデルとして共通補助データとマスクデータをサーバに保管するモデルを提案したが，マスクデータへの攻撃手法やその対策手法に関して検討を行なっていない．Fuzzy Commitment に対する攻撃として Kelkboom, E.J.C.[19] や Scheirer, W.J.[20] らの攻撃手法が知られているが，これらを調査すると共に，未知の攻撃手法による脅威がないか検討する必要がある．

謝辞

本研究を進めるにあたり，終始懇切丁寧な御指導，御助言を賜りました小松尚久教授，甲藤二郎教授に心から深く感謝の意を表します．また，適切な助言を頂きました研究員大木哲史氏，博士 3 年披田野清良氏，修士 2 年伊藤恭英氏，修士 1 年林祥平氏を始め，小松研究室の皆様に深く感謝いたします．

2012 年 2 月 6 日

奥井　宣広

参考文献

[1] 鷲見和彦, 松山隆司, 中嶋晴久. “バイオメトリクス認証テンプレート保護に関する研究,” *Proceedings of the 2005 Symposium on Cryptography and Information Security*, Vol. 2, pp. 535–540, 2005.

[2] A. Juels and M. Sudan. “A Fuzzy Vault Scheme,” *IEEE International Symposium on Information Theory*, No. 408, 2002.

[3] Ratha N., Connell J., and Bolle R. “Enhancing security and privacy in biometrics based authentication systems,” *IBM Systems Journal*.

[4] 瀬戸洋一. “ユビキタス時代のバイオメトリクスセキュリティ,” 日本工業出版株式会社, 2003.

[5] 瀬戸洋一. “バイオメトリクスセキュリティ入門,” ソフト・リサーチ・センター, 2004.

[6] Soutar C., Roberge D., Stoianov A., Gilroy R., and Kumar V. “Biometric Encryption,” *http://www.bioscrypt.com/asset/BiometricEncryption.pdf*

[7] Tuyls P. and Goseling J. “Capacity and examples of template-protecting biometric authentication systems,” *EV Workshop BioAW*, No. 77, 2004.

[8] 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 and Response 型ネットワーク認証の提案,” 情報処理学会研究報告, pp. 179–186, 2004.

[9] A. Juels and M. Wattenberg. “A Fuzzy Commitment Scheme,” *Sixth ACM Conference on Computer and Communications Security*, pp. 28–36, 1999.

[10] 柴田陽一, 三村昌弘, 高橋健太, 中村逸一, 曽我正和, 西垣正勝. “メカニズムベース PKI-指紋からの秘密鍵動的生成,” 情報処理学会研究報告, Vol. 45, No. 8, pp. 1833–1844, 2004.

[11] Daugman J.. “Probing the Uniqueness and Randomness of IrisCodes: Results From 200 Billion Iris Pair Comparisons, ” *Proceedings of the IEEE*, Vol.96, pp.1927–1935, 2006.

[12] FVC2002. Second fingerprint verification competition. *http://bias.csr.unibo.it/fvc2002/*

[13] National Institute of standards and Technology. Nist fingerprint image software2. *http://fingerprint.nist.gov/nifs/*

[14] Zhe Jin, Andrew Beng Jin Teoh, Thian Song Ong and Connie Tee. “Secure Minutiae-Based Fingerprint Templates Using Random Triangle Hashing,” *Lecture Notes in Computer Science*, pp. 521–531, Springer Berlin, 2009.

[15] Chulhan Lee and Jaihie Kim. “Cancelable fingerprint template using minutiae-based bit-strings,” *Journal of Network and Computer Applications*, pp. 236–246, Elsevier, 2010.

[16] Anil K. Jain, Salil Prabhakar, Lin Hong and Sharath Pankanti. “Filterbank-Based Fin-

gerprint Matching," *IEEE Transactions on Image Processing*, Vol.9, pp. 846–859, 2000.

[17] 宿沢晃平, 大木哲史, 山崎恭, 小松尚久. "共通テンプレートを用いたバイオメトリック暗号の構成に関する一検討," 映像情報メディア学会技術報告, pp. 49–52, 2009.

[18] ISO 19795 Part 1 Annex B, pp. 39, 2006.

[19] Kelkboom, E.J.C., Breebaart, J., Kevenaar, T.A.M., Buhan, I. and Veldhuis, R.N.J.. "Preventing the Decodability Attack Based Cross-Matching in a Fuzzy Commitment Scheme," *IEEE Transactions on Information Forensics and Security*, Vol.6, pp. 107–121, 2011 .

[20] Scheirer, W.J. and Boult, T.E.. "Cracking Fuzzy Vaults and Biometric Encryption," *Biometrics Symposium*, pp. 1–6, 2007.

付録 A

指紋の特徴量

指紋の特徴量としてマニューシャを用いる．マニューシャは以下の 3 つのパラメータで構成する．

1. エリア番号（f）
2. 端点，分岐点の属性（a）
3. 端点，分岐点の角度（θ）

以上の 3 つのパラメータ（f_i,a_i,θ_i）を 1 つの組にしてマニューシャとして扱う．

A.1　エリア

エリアとは，マニューシャの位置情報を変換したものである．マニューシャはセンサに指を置いたときの位置，角度，圧力などによって，同一の指であっても毎回異なる結果が得られる．そのため，指紋画像を分割してエリアを作成しマニューシャの位置情報として用いることで，生体情報のゆらぎによるマニューシャの位置ずれをある程度吸収できる．ただし，エリアの形状を正方形とすると，各エリアにおいて中心点からエリアの境界線までの距離が一定とならず，水平方向に対して斜めの方向への位置ずれの許容範囲が大きくなる．そこで，本研究では，各エリアにおいて位置ずれの許容範囲が均一になるように円形のエリア（以下，円形エリア）を用いる．マニューシャの分布は指紋画像の中心部により多く存在し，外縁に近づくほど少なくなる傾向にあるので，図 A.1 のように，円形エリアの大きさを指紋画像中心部では小さく密に，外縁部では大きく疎に設計する．

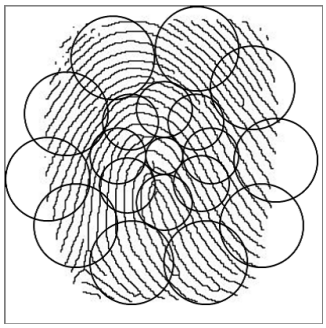


図 A.1　円形エリアの概要

A.2　端点，分岐点の属性，角度

端点，分岐点の概要を図 A.2 に示す．端点は隆線ベクトルの開始もしくは終了位置，分岐点は 1 本の隆線から分岐して複数の隆線に分かれる位置を表す．

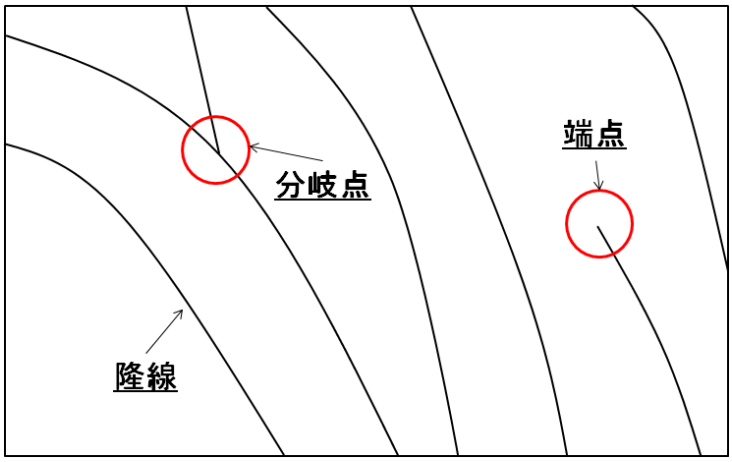


図 A.2　端点，分岐点の概要

端点，分岐点の角度の取り方を図 A.3 に示し，以下に述べる．

- 端点
  y 軸方向と隆線の延長線上の角度
- 分岐点
  2 本に隆線が 1 本の隆線になる方向と y 軸方向の角度

角度は 360 度を 32 分割し，角度レベル 0 から 31 までで表現する．1 レベルは 11.25 度に相当する．

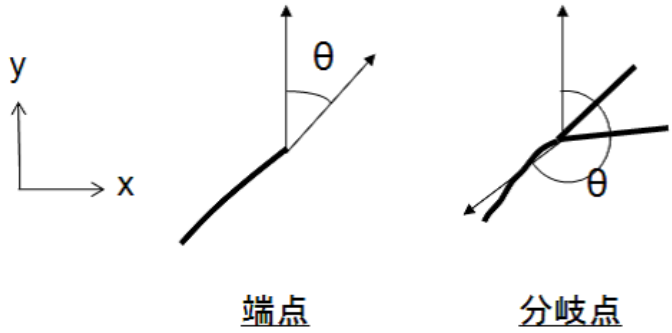


図 A.3　端点，分岐点の角度

関連業績

【 学会発表 】

マニューシャの位置情報を考慮した指紋情報からの生体鍵生成手法に関する一検討

2012 年 1 月 暗号と情報セキュリティシンポジウム

奥井 宣広，大木 哲史，小松 尚久

SCIS 2012 The 29th Symposium on
Cryptography and Information Security
Kanazawa, Japan, Jan. 30 - Feb. 2, 2012
The Institute of Electronics,
Information and Communication Engineers

マニューシャの位置分布を考慮した 指紋情報からの生体鍵生成手法に関する一検討

Cryptographic Key Generation from Fingerprint based on Minutiae Distribution

奥井 宣広 * 大木 哲史 † 小松 尚久 *
Norihiro Okui Tetsushi Ohki Naohisa Komatsu

あらまし 情報システムを利用するユーザの利便性と安全性を両立する認証手法として，生体認証が注目されている．しかし，生体情報は変更不可能な情報であり，生体情報の漏洩には大きなリスクを伴う．したがって，これらを安全に保管・更新する手法を実現することにより，生体認証の更なる普及が促進されることが期待できる．生体情報の安全性を保ちつつ認証を行う手法は，一般にテンプレート保護型生体認証と呼ばれる．本稿ではその中でも生体情報から生成される一意な鍵 (以下，生体鍵) を暗号用の鍵として使用することでネットワーク認証を行い，ユーザ認証とクライアント認証を同時に実現する手法であるバイオメトリック暗号とその代表的手法である Fuzzy Commitment Scheme に着目する．Fuzzy Commitment Scheme を用いた生体鍵生成では，本人の指紋から出力されるビット列を誤り訂正符号により訂正することで生体鍵を生成する．このため，前処理として入力された指紋から固定長のビット列を出力する必要があり，ビット列変換の精度が鍵生成精度に大きく影響する．マニューシャから固定長のビット列を出力する手法としては，マニューシャをエリアと呼ばれる領域に分割し，エリアに対応したビットを出力する手法が多く提案されている．本稿では，従来手法である長方形や扇形のエリアに対して，よりマニューシャの位置分布や位置ずれの影響を考慮したエリア設計を行うことで，鍵生成精度の向上を目指す．

キーワード 生体認証，生体鍵生成，バイオメトリック暗号，指紋情報，マニューシャ

1 まえがき

近年，情報システムの安全性に対する要求の高まりから，本人確認手段としてバイオメトリック個人認証が普及しつつある．また，ブロードバンドの普及により，クラウド上で提供するサービスが増加し，ネットワーク認証の重要性が増している．このような背景から，バイオメトリック認証を用いてユーザ認証とクライアント認証を同時に実現することで，ユーザの利便性とシステムの安全性を両立できることが期待される．

バイオメトリック認証は，個人の身体的，あるいは行動的特徴に基づいて認証を行うため，パスワードや IC カードのように，記憶，所持の煩わしさがないことなどの利便性と，第三者によるなりすましが容易ではないという安全性を兼ね備えている．一方で，利用者，環境条件，運用条件，バイオメトリック装置といった様々な要素において脆弱性が存在しており，これらの脆弱性に対して適切な対策を講じることが重要な課題となっている．

バイオメトリック認証では，個人の身体的特徴や行動的特徴から抽出した個人の固有の情報を，認証システム内のデータベースにテンプレートとして登録する．また，生体情報には数に限りがあり，変更不可能な情報であることから，従来のパスワードを用いた認証のように容易にパラメータを変更することができない．したがって，テンプレートが漏洩した場合，生体情報を取り替えることは非常に困難であり，テンプレートの漏洩には大きなリスクを伴う．このような背景から，より安全性の高いバイオメトリック認証を実現するために，テンプレートから元の生体情報の復元を困難にし，テンプレート漏洩時には再登録により元のテンプレートを無効化することを可能にする様々な手法が提案されており，これらは一般にテンプレート保護技術と言われている．

テンプレート保護技術を用いたバイオメトリック認証は，一般にテンプレート保護型バイオメトリック認証と

* 早稲田大学理工学術院, 169-8555 東京都新宿区大久保 3-4-1, Faculty of Science and Engineering, Waseda University, 3-4-1 Okubo, Shinjuku-ku, Tokyo, Japan
† 早稲田大学理工学研究所, 169-8555 東京都新宿区大久保 3-4-1, Research Institute for Science and Engineering, Waseda University, 3-4-1 Okubo, Shinjuku-ku, Tokyo, Japan

呼ばれ，その代表的な手法として，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 [2] が挙げられる．本稿ではその中でも生体情報から生成される一意な鍵 (以下，生体鍵) を暗号用の鍵として使用することでネットワーク認証を行い，ユーザ認証とクライアント認証を同時に実現する手法であるバイオメトリック暗号に着目する．

バイオメトリック暗号の代表的な手法として，Fuzzy Vault Scheme[3] や Fuzzy Commitment Scheme[4] が提案されている．本稿では，Fuzzy Commitment Scheme に着目し，生体情報のモダリティとして指紋を用いた場合の一適用例を提案する．Fuzzy Commitment Scheme を用いた生体鍵生成では，本人の指紋から出力されるビット列を誤り訂正符号により訂正することで，生体鍵を生成する．したがって，前処理として入力された指紋から固定長のビット列を出力する必要があり，ビット列変換の精度が鍵生成精度に大きく影響する．

指紋の特徴量であるマニューシャを用いて固定長のビット列を生成する手法として，指紋画像をエリアという領域に分割し，エリア内に含まれるマニューシャ情報を用いてビット列を出力する手法が多く提案されている．本稿では，従来手法である長方形や扇形のエリアに対して，よりマニューシャの位置分布や位置ずれの影響を考慮したエリア設計を行うことで，鍵生成精度の向上を目指す．

2　従来研究

2.1　従来のエリア設計手法

指紋からユーザごとに固有のビット列を出力する手法として，Lee らによる長方形を用いる手法 [7] や，Jain らによる扇形を用いる手法 [9] などが提案されている．図 1 に長方形エリアと扇形エリアの概要を示す．

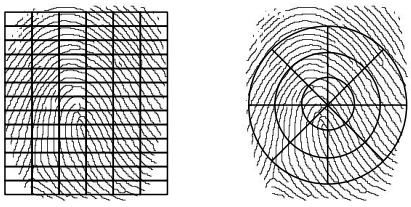


図 1: 長方形エリアと扇形エリアの概要

Sutcu らによる直方体を用いた手法 [7] では，x,y,z の 3 軸からなる直交座標系を設定し，x 軸と y 軸をそれぞれマニューシャの位置情報である x 座標と y 座標に，z 軸をマニューシャの角度情報に対応させて，マニューシャを座標空間上にプロットする．座標空間上に複数の直方体のエリアを生成し，エリアごとのエリアに含まれているマニューシャ数を用いてビット列を生成する．また，事前準備として学習データを用いて，各エリアに含まれるマニューシャ数をパラメータとした閾値を決定しておく．直方体の構造は非公開とし，独自の指紋データベースを用いた照合精度評価では，ユーザ特有の直方体構造を用いた場合，EER は 2.7 %であるが，全ユーザで共通の直方体構造を用いた場合では EER は 5 %となっている．

Lee らによる長方形を用いる手法 [8] では，マニューシャを座標平面上にプロットし．座標平面を長方形のエリアで分割する．長方形エリア内に含まれるマニューシャの角度情報を用いてビット列をエリアごとに出力する．また，長方形の一辺の長さは実験的に決める．出力されたビット列は，個人ごとに乱数である PIN を用いてビット列の順序を変更する．照合精度評価では FVC2004 を用いており，EER はほぼ 0 %を達成している．しかし，PIN が流出した場合，照合精度は大きく低下すると考えられる．実際に PIN を固定した照合精度評価では EER は 10%程度まで低下している．

Jain らによる扇形を用いる手法 [9] では，マニューシャを座標平面上にプロットし，座標平面上に扇形のエリアを作成し，扇形のエリアに含まれるマニューシャの角度情報を用いてビット列を出力する．出力されたビット列は PIN を用いてビット列の順序を変更する．長方形の手法と同様に，PIN が流出した場合は照合精度は低下し，FVC2002 を用いた照合精度評価において EER は 5 %強となっている．

2.2　従来手法の課題

エリアを用いてマニューシャの位置情報を変換する場合，エリアの縁にあるマニューシャが，位置ずれによって登録時と照合時で異なるエリアに移動してしまう問題がある． 図 2 に示すように長方形や扇形エリアの場合，エリアの角となる部分とそうでない部分で，位置ずれによる誤差の影響が異なる．また，マニューシャの位置分布には偏りがあると考えられるが，長方形や扇形のエリアでは，マニューシャの位置分布を考慮したエリア設計がされていない．したがって，ビット列を生成するエリアに偏りが生じることが考えられる．

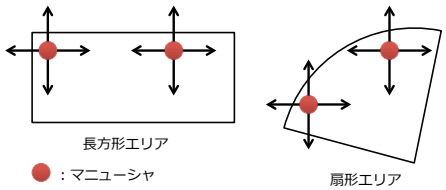


図 2: マニューシャの位置ずれの影響

本稿では，従来のエリア設計手法に対して，よりマニューシャの位置分布や位置ずれの影響を考慮したエリア設計を行うことで，照合精度を向上させることを目的とする．

3　提案手法

マニューシャの位置ずれ角度ずれの補正を行う手法について 3.1 節で説明した後，本稿で用いる円形エリアの設計手法を 3.2.2 節で述べる．そして，円形エリアを用いた指紋情報からのビット列出力方法を 3.3 節で説明する．

3.1　マニューシャの位置ずれ角度ずれ補正

センサから得られる指紋情報は，取得環境における気温や湿度の変化や，センサに入力する際の圧力や角度の違いなど様々な要因によって変化する．そのため，登録情報と照合情報に差異が生じ，認証精度に大きく影響する．したがって，指紋認証を行う場合，マニューシャの位置ずれや角度ずれなどの補正を行う必要がある．

マニューシャの位置ずれや角度ずれを補正する手法として，指紋の中心点を用いる補正手法 [5] とリファレンスマニューシャを用いた補正手法 [6] が多く用いられている．

指紋の中心点を用いる補正手法は，隆線情報などから指紋の中心点を検出し，中心点を原点とし全てのマニューシャを平行移動させることで位置ずれの補正を行う．この手法では，角度ずれの補正を行うことができない問題に加え，指紋の中心点の検出精度が本人認証精度に大きく影響を与え，中心点が正しく検出できなければ本人認証を行うことができない．

リファレンスマニューシャを用いた補正手法は，基準とするマニューシャとの他のマニューシャの相対的な値を用いることで，マニューシャの位置ずれと角度ずれの補正を行う．リファレンスマニューシャを用いた手法は，中心点を検出する必要がないため，中心点が検出できない低品質な指紋画像も認証に用いることができる．また，マニューシャ間の相対的な値を用いることで角度ずれの補正を行うことができ，指紋の中心点を用いた補正よりも，同一マニューシャであれば同一の情報がより正確に得られることが期待できる．

本稿では，マニューシャの位置ずれ角度ずれ補正手法として，リファレンスマニューシャを用いた補正に着目する．

3.1.1　照合方法

リファレンスマニューシャを用いた補正における照合方法の概要を図 3 に示す．

登録時の指紋画像に含まれるマニューシャ総数が m 個であるとした場合，リファレンスマニューシャを用いた補正を行うと，リファレンスマニューシャの選定が m 通り存在するため，m 個の指紋情報が得られる．各指紋情報と共通補助データからビット列を作成する．

したがって，1 枚の指紋画像からビット列 T_1〜ビット列 T_m が生成され，m 個の登録ビット列が作成される．照合時も登録時と同様に補正を行いビット列の作成を行う．照合時の指紋画像に含まれるマニューシャ総数が n 個であるとした場合，ビット列 Q_1〜ビット列 Q_n が生成され，合計 n 個の照合ビット列が生成される．

登録ビット列と照合ビット列の照合は総当たりで行い，最も照合スコアが良いものを照合結果とする．図 3 においては，$m \times n$ 回の照合を行う．

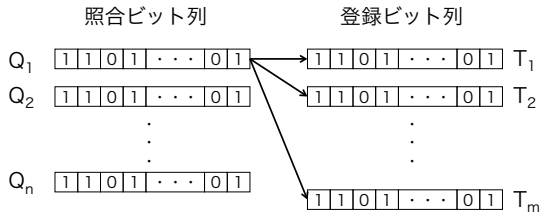


図 3: 照合方法の概要

3.2　円形エリア

3.2.1　エリア設計方針

本稿では，マニューシャの位置分布と位置ずれの影響を考慮したエリアの設計を行う．マニューシャの位置分布には偏りがあると考えられ，指紋の中心部分に多く分布していると考えられる．しかし，本稿ではリファレンスマニューシャを用いた補正により，リファレンスマニューシャと原点とし他の全マニューシャを変換するため，指紋の中心部分にマニューシャが多く分布しているとは限らない．したがって，リファレンスマニューシャを用いた補正後の指紋情報によるマニューシャの位置分布について調査を行う．

マニューシャ位置分布調査の諸元を表 1 に示す．

表 1: マニューシャ位置分布調査の諸元

データベース	FVC2002 DB1 SetA[10]
指の数	100 指
1 指あたりの画像枚数	8 枚
指紋画像の総数	800 枚
指紋画像の解像度	388 × 374 [pixel]
取得センサ	optical sensor ”TouchView II” by Identix
マニューシャ抽出 アルゴリズム	NFIS2[5]

リファレンスマニューシャを用いた補正後のマニューシャ位置分布の調査方法は，データベース内の各指紋画像において，全マニューシャの中から 1 つをリファレンスマニューシャとして選定し，リファレンスマニューシャの座標が $\left(\sqrt{388^2+374^2}, \sqrt{388^2+374^2}\right) = (538.9, 538.9)$ となるように 3.1 節で説明した方法で他のマニューシャを変換する．この操作をデータベース内の全ての指紋画像に対して行い，変換後のマニューシャの位置分布をリ

ファレンスマニューシャを用いた補正後のマニューシャの位置分布とする．

リファレンスマニューシャを用いた補正によるマニューシャの位置分布を図 4 に示す．x 軸は補正後の指紋画像の横幅 (388 × 2[pixel])，y 軸は指紋画像の縦幅 (374 × 2[pixel])，z 軸はマニューシャの分布頻度を示す．図 4 から補正後の指紋画像の中心部に近いほどマニューシャの分布は密になり，外縁部に行くほどマニューシャの分布が疎になっていることがわかる．また，研究室の学生から採取した指紋データベースを用いて同様の調査を行ったが，図 4 と同様に，リファレンスマニューシャを用いた補正後の指紋画像中心部に近いほどマニューシャの分布が密になるという結果が得られた．したがって，リファレンスマニューシャを用いた補正後のマニューシャ位置分布は，一般的に図 4 のような分布であると考えられる．

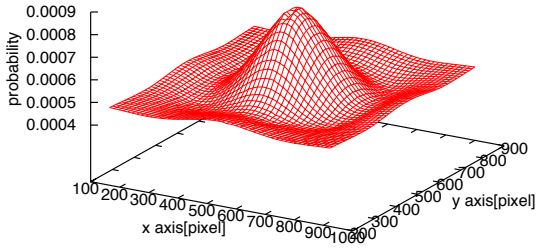


図 4: マニューシャ分布密度（リファレンスマニューシャを用いた補正）

図 4 から補正後の指紋画像中心点（座標 (538.9, 538.9)）からの距離に応じたマニューシャの分布頻度を求めたものが図 5 である．本稿では，図 5 に着目し，リファレンスマニューシャを用いた補正後の指紋画像中心点からの距離を用いて，各エリアに含まれるマニューシャの数が均等になるように作成する．

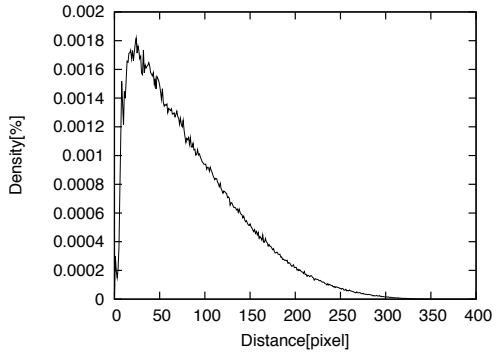


図 5: 補正後の指紋画像中心点からの距離に応じたマニューシャの分布頻度

2.2 項で述べたように，従来のエリア設計手法では，マニューシャの位置ずれによる影響が考慮されていない．そこで本稿では，円形のエリアを用いる．エリアの形状を円形にすることで，エリアの縁にあるマニューシャの位置ずれの誤差を均等にすることが期待できる．また，円形のエリア同士を少し重ねて配置し，エリアの縁にあるマニューシャは両方のエリアに一致ささえることで，位置ずれの誤差を許容することができると考えられる．

これらのエリア設計方針から，本稿では，図 6 に示すように円形エリアを，リファレンスマニューシャを用いた補正後の指紋画像中心点から同心円状に配置する．

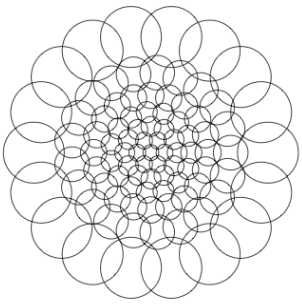


図 6: 円形エリアの例

3.2.2 円形エリア作成方法

円形エリア作成手順のフローチャートを図 7 に示し，エリア作成手順を以下に述べる．

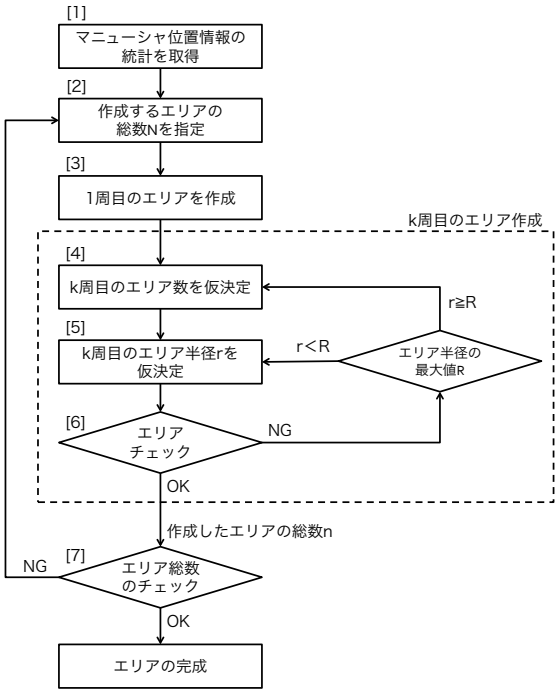


図 7: 円形エリア作成のフローチャート

1. 学習用の指紋データベースに含まれる全ての指紋画像に対して，リファレンスマニューシャを用いた補正後のマニューシャ位置分布の統計を求める．マニューシャ位置分布の統計から，補正後の指紋画像中心点から距離 d におけるマニューシャの集

合（M_d）と，補正後の指紋画像中心点から距離 d におけるマニューシャの数（$|M_d|$）を算出する．また，補正後の指紋画像中心点から最も離れた位置にあるマニューシャまでの距離を d_{max} とする．ここで，以下のように記号を定義する．

N ： 作成するエリア総数

M_d ： 補正後の指紋画像中心点から距離 d におけるマニューシャの集合

$|M_d|$ ： 中心点から距離 d における マニューシャの数

A_k ： k 周目のエリアの集合

$|A_k|$ ： k 周目のエリアの数

D_k ： 補正後の指紋画像中心点から k 周目エリア外周までの距離の最大値

C_k ： 補正後の指紋画像中心点から k 周目エリア中心点までの距離

R_k ： k 周目のエリア半径

2. 作成するエリア総数 N を指定する．エリア作成の基本方針から各エリアに一致するマニューシャ数が等しいため，各エリアに一致するマニューシャ数を B とすると，次式が成り立つ．

$$B = \left(\sum_{d=0}^{d_{max}} |M_d| \right) \Big/ N \tag{1}$$

3. 1 周目のエリア作成方法の概要を図 8 に示す．1 周目のエリア数は 1 個（$|A_1| = 1$ ）に固定する．このとき，1 周目のエリアに限り D_1 と R_1 は $D_1 = R_1$ の関係にある．エリア作成の方針から，$|M_d|$ と N から次式が成り立つ．$D_1 = R_1$ と (2) 式から，1 周目のエリア半径 R_1 を求める．

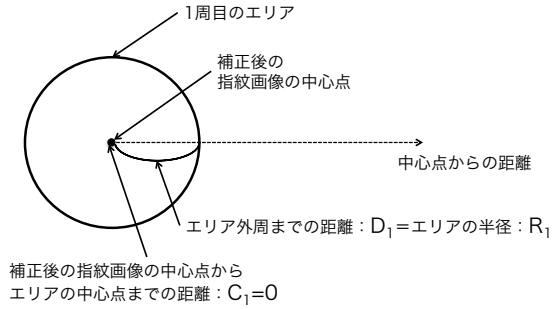


図 8: 1 周目のエリア概要

$$\sum_{d=0}^{D_1} |M_d| \quad = \quad B \times |A_1| \tag{2}$$

4. k 周目のエリア概要を図 9 に示す．k 周目のエリア数を 4 個（$|A_k| = 4$）と仮決定する．この時，(2) 式と同様に (3) 式の関係が成り立つ．$|A_k| = 4$ と (3) 式から D_k を求め，エリア中心点 C_k を (4) 式のように定める．

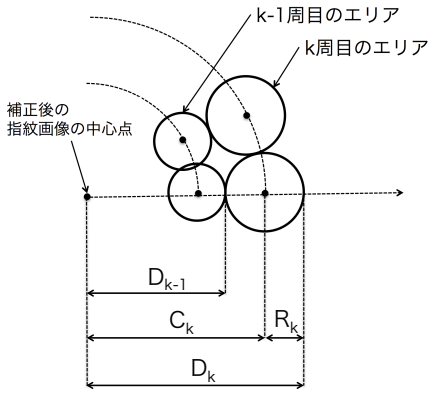


図 9: k 周目のエリア概要

$$\sum_{d=D_k+1}^{D_k} |M_d| \quad = \quad B \times |A_k| \tag{3}$$

$$C_k \quad = \quad \frac{D_{k-1} + D_k}{2} \tag{4}$$

5. k 周目のエリア半径 R_k の取りうる値の範囲（次式）について定義する．R_k の最小値は，1 つ内側のエリアである $k-1$ 周目のエリアと接する場合とし，R_k の最大値は，1 つ内側のエリア半径 R_k の 1/3 を加えたものとする．また，エリア半径の最大値については，実験的に定めたものである．

$$D_k - C_k \leq R_k \leq D_k - C_k + \frac{R_{k-1}}{3} \tag{5}$$

6. R_k の最小値で作成されるエリアについて，半径 C_k 以下のいずれのエリアにも含まれない領域が存在しないかを次式にて調べる．(6) 式を満たさない場合は，R_k の値を 1 増やし，エリアの再作成を行い，再び円形エリア間の隙間を調べる．R_k の値が最大値に達しても (6) 式を満たさない場合は，手順 4 に戻り，仮決定したエリア数 A_k の値を 1 増やす．(6) 式を満たす R_k が存在する場合，A_k, D_k, C_k, R_k を決定する．

$$\left\{ x \in \sum_{d=0}^{d=C_k} M_d : x \in \sum_{l=0}^{k} A_l \right\} = \phi \tag{6}$$

7. m 周目までに作成したエリアの総数 $n = \sum_{k=1}^{m} |A_k|$ が，手順 2 で指定した N の ± 3 以内であれば（次式），各円形エリアにエリア番号を割り振り，エリア作成を完了する．(7) 式を満たさない場合は，

エリア作成失敗とし，手順 2 に戻り N の再指定を行う．

$$N-3 \leq n \leq N+3 \tag{7}$$

3.3 指紋情報の量子化

本稿では，センサから得られたマニューシャ情報の位置ずれ角度ずれを補正するためにリファレンスマニューシャを用いた補正を行い，補正後のマニューシャ位置情報を円形エリアに変換する．次に，円形エリアごとにマニューシャの角度情報を用いてビット列を出力する．最終的に出力されるビット列は，円形エリアごとに出力したビット列をエリア番号順に組み合わせたものである．

本稿では，マニューシャの持つ角度情報に着目して量子化を行う．初めに，角度情報と出力するビット列の対応（以下，ビットスケール）を作成しておく．円形エリアとマニューシャの一致判定を行い，エリアごとに一致したマニューシャの角度平均 $\overline{\theta}$ を算出し，ビットスケールを用いて量子化を行う．

ここで，ビットスケール作成方法を説明する．マニューシャの角度情報は 32 レベルに量子化されており，1 レベルあたり 11.25 度である．ビットスケールは 32 レベルある角度情報を分割することで作成する．図 10 にマニューシャ角度情報を n 分割した場合の例を示す．本稿では角度情報を 0 レベルから均等に分割しビットスケールを作成する．分割後の各領域にビット列を割り当て，エリアごとにマニューシャの角度平均 $\overline{\theta}$ とビットスケールを照合し，対応するビット列を出力する．また，固定長のビット列を出力するよう各領域に割り当てるビット列の長さは一定にする必要がある．

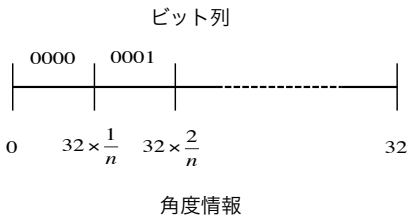


図 10: n 分割のビットスケールの例

図 11 に量子化手順の概要を示し，以下にその手順を述べる．図 11 では簡単のため正方形エリアを使用している．また，センサから得られた指紋情報は位置ずれ角度ずれの補正を終えているものとする．

1. マニューシャ円形エリアの照合を行う．マニューシャの位置情報を用いて，マニューシャと円形エリアの一致判定を行う．

2. エリアごとに一致したマニューシャの角度情報の平均値 $\overline{\theta}$ を算出する．

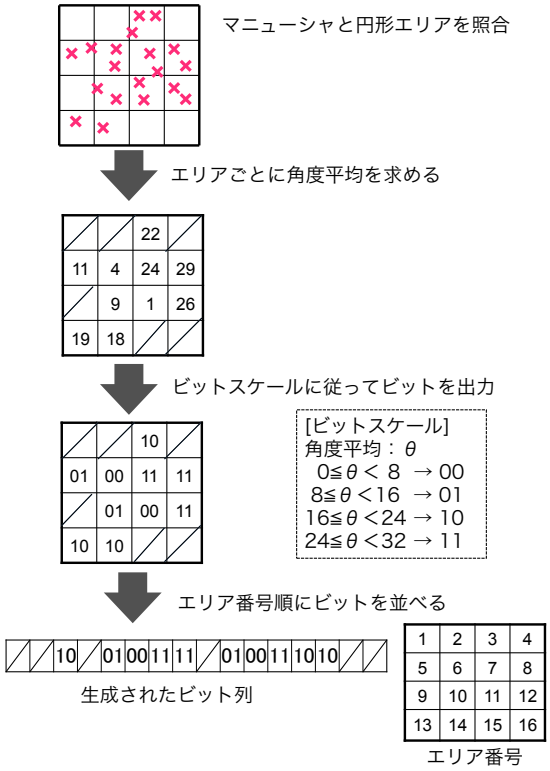


図 11: 量子化手順の概要

3. 算出した角度平均と予め作成したビットスケールに従って，エリアごとにビットを出力する．この時，一致したマニューシャが存在しないエリアは消失誤りとする．図 11 は，角度レベルを 4 分割にした場合の例である．

4. エリアごとに出力したビットを，エリア番号順に組み合わせてビット列を作成する．

4 照合精度評価

4.1 出力ビット列による評価

本提案手法により出力されたビット列を，FNMR(False Non-Match Rate) と FMR(False Match Rate) の観点から照合精度評価を行い，既存のエリア作成手法との比較を行う．

4.1.1 評価方法

リファレンスマニューシャを用いた補正を使用する場合，3.1.1 項で説明した照合方法を用い，最も照合スコアが良いものを照合結果とする．リファレンスマニューシャを用いた補正による照合スコアの算出方法には，以下の Daugman らが提案した NHD(Normalized Hamming Distance)[11] を提案手法に応用して用いる．

登録ビット列 T_x と照合ビット列 Q_y で一致したビット数を m_t，T_x と Q_y で不一致であるビット数を m_f とする．登録時もしくは照合時に，エリアに一致するマニュー

シャが存在せず消失誤りと判定されたビット数を e とする．また，次式における $\overline{m_t + m_f}$ は，本人間照合における $m_t + m_f$ の平均値を示す．

$$HD_{raw} = \frac{m_f}{m_t + m_f}$$

$$NHD = 0.5 - (0.5 - HD_{raw})\sqrt{\frac{m_t + m_f}{\overline{m_t + m_f}}}$$

4.1.2 照合精度実験

照合精度実験にはデータベースは FVC2002[10] を使用し，全 100 指のうち 30 指を 3.2.2 項で説明した円形エリア作成用の学習データとして使用し，照合精度実験は残りの 70 指を使用する．また，本提案手法において，照合精度に影響を与えるパラメータは，円形エリア数，ビットスケール作成における角度分割数であり，これらのパラメータを推移させて実験を行う．

これらの実験諸元を表 2 に示す．

表 2: 照合精度実験の諸元

データベース	FVC2002 DB1 SetA[10]
学習データ	30 指
照合データ	70 指
登録用指紋枚数	3 枚
照合用指紋枚数	5 枚
本人照合回数	350 回
他人照合回数	24150 回
円形エリア数	68, 91, 121, 148, 188 227, 269, 299, 345
角度分割数	4〜12 分割

円形エリア数と角度分割数を推移させて実験を行った結果，円形エリア数が 345 で角度分割数が 8 分割の時に最も良い照合精度を示した．その時の照合精度実験結果を，FMR を横軸に，FNMR を縦軸にとった ROC カーブを用いて図 12 に示す．また，表 3 に実験結果をまとめる．

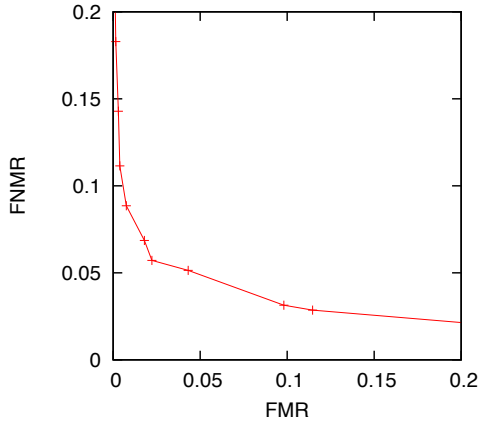


図 12: 実験結果（ROC カーブ）

2.1 節で紹介した従来のエリア作成手法とは実験に使用しているデータベースが異なるため，直接に比較を行うことはできないが，いずれの手法も EER は 5 %以上となっている．図 12 の実験結果より，FMR と FNMR の和が最小となる組み合わせは，(FMR, FNMR) = (0.02, 0.057) であることから，従来手法と比較して同等かそれ以上の照合精度であると考えられる．

表 3: 照合精度実験の実験結果

円形エリア数	345
角度分割数	8 分割
(FMR, FNMR)	(0.02, 0.057)
FMR100[10]	FNMR = 8.8[%]

4.2 生体鍵復元による評価

前節では，指紋情報から提案手法により出力したビット列間の照合精度の評価を行った．しかし，Fuzzy Commitment Scheme を用いた生体鍵生成では，本人の指紋から出力されるビット列を誤り訂正符号により訂正することで，生体鍵を生成する．そこで，4.1.1 項で説明した照合スコアにより決定した登録ビット列と照合ビット列を用いて，秘密鍵復元の照合精度評価を行う．

4.2.1 秘密鍵復元可能条件

登録ビット列と照合スコアが最も高い照合ビット列の一致，誤一致の関係を図 13 に示す．

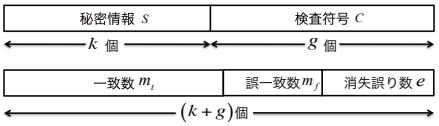


図 13: 一致，誤一致の関係

誤り訂正符号には Reed-Solomon 符号を用いる．また，角度分割数が 8 分割の場合は，1 つの円形エリアから 4 ビットを出力するため $GF(2^4)$ ガロア拡大体を用い，1 シンボルを各円形エリアから出力されるビット列に対応づける．秘密鍵復元可能条件は，大木らの秘密鍵復元のための条件 [12] と等しく，次式となる．

$$k \leq m_t - m_f$$

4.2.2 照合精度実験

実験諸元は表 2 と同じである．4.1.2 項と同様に FMR を横軸に，FNMR を縦軸にとった ROC カーブを用いて図 14 に示す．また，表 4 に実験結果をまとめる．

表 4: 誤り訂正による照合精度実験結果

円形エリア数	345
角度分割数	8 分割
(FMR, FNMR)	(0.02, 0.037)
FMR100[10]	FNMR = 6.5[%]

図 14 の実験結果から，(FMR, FNMR)=(0.02, 0.037) の時 FMR と FNMR の和が最小となった．この時，$m_t -$

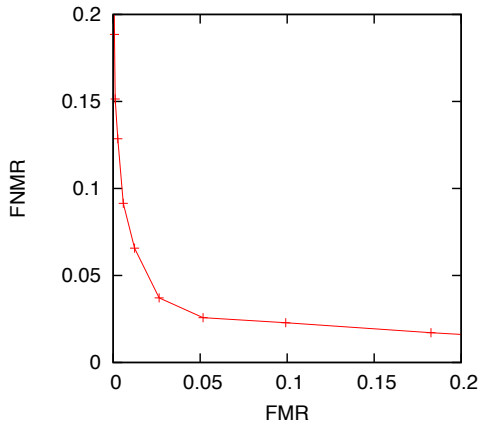


図 14: 実験結果（ROC カーブ）

m_f の値は 10 であり，生体鍵のビット長は $10 \times 4 = 40$ ビットである．また，FMR が 1% 以下となるときの FNMR は 6.5% であり，この時，$m_t - m_f$ の値は 11 であり，生体鍵のビット長は $11 \times 4 = 44$ ビットである．誤り訂正を用いることで FMR は上昇し，FNMR は減少すると考えられるが，全体として FNMR の減少による影響が大きく，誤り訂正を通じた照合精度は向上した．

5 まとめ

本稿では，リファレンスマニューシャを用いた補正後のマニューシャ位置分布や位置ずれの影響を考慮したエリア設計手法として，円形エリアを補正後の指紋画像中心点から同心円上に配置する手法を提案した．また，提案手法によって出力されたビット列における照合精度評価を行った．

本稿ではビットスケールの作成を角度レベル 0 から均等に分割することで作成したが，エリアによってマニューシャの角度情報に偏りが生じている可能性がある．したがって，エリアごとの角度情報の偏りを考慮したビットスケール作成を行うことで，照合精度の向上と安全性の高いビット列を生成できる可能性がある．

また，各エリアから出力されるビット列がランダムであると仮定した場合に，生体鍵のビット長が 40 ビットの時最も良い照合精度となったが，安全性の面において，生体鍵の情報量がやや少ないと考えられる．したがって，より情報量の多い生体鍵においても十分な照合精度が達成できるよう円形エリアの設計方法などを見直す必要がある．

参考文献

[1] 鷲見和彦, 松山隆司, 中嶋晴久, “バイオメトリクス認証テンプレート保護に関する研究,” Proceedings of the 2005 Symposium on Cryptography and Information Security, Vol.2, pp.535-540, 2005.

[2] Ratha N., Connell J., Bolle R., “Enhancing security and privacy in biometrics based authentication systems,” IBM Systems Journal, Vol.40, pp.614-634, 2001.

[3] A. Juels, M. Sudan, “A Fuzzy Vault Scheme,” IEEE International Symposium on Information Theory, No.408, 2002.

[4] A. Juels, M. Wattenberg, “A Fuzzy Commitment Scheme,” Sixth ACM Conference on Computer and Communications Security, pp.28-36, 1999.

[5] National Institute of Standards and Technology. NIST fingerprint image software 2. http://fingerprint.nist.gov/nfis/

[6] Zhe Jin, Andrew Beng Jin Teoh, Thian Song Ong and Connie Tee. “Secure Minutiae-Based Fingerprint Templates Using Random Triangle Hashing,” Lecture Notes in Computer Science, pp.521-531, Springer Berlin, 2009.

[7] Sutcu Y., Rane S., Yedidia J., Draper S. and Vetro A.. “Feature Transformation of Biometric Templates for Secure Biometric Systems Based on Error Correctiong Codes,” Computer Vision and Pattern Recognition Workshops 2008, pp.1-6, 2008

[8] Chulhan Lee and Jaihie Kim. “Cancelable fingerprint template using minutiae-based bit-strings,” Journal of Network and Computer Applications, pp.236-246, Elsevier, 2010.

[9] Zhe Jin, Thian Song Ong, Tee C., Teoh A.B.J., “Generating Revocable Fingerprint Template Using Polar Grid based 3-Tuple Quantization Technique,” Circuits and Systems (MWSCAS) 2011 IEEE 54th International Midwest Symposium, pp.1-4, 2011.

[10] FVC2002. Second fingerprint verification competition. http://bias.csr.unibo.it/fvc2002/

[11] Daugman J.. “Probing the Uniqueness and Randomness of IrisCodes: Results From 200 Billion Iris Pair Comparisons, ” Proceedings of the IEEE, Vol.96, pp.1927-1935, 2006

[12] 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, pp.2077-2087, 2009