Nish!gaki Laboratory

07/03/09
ZeroBIO研究プロジェクトワークショップ
「生体情報のプライバシー」

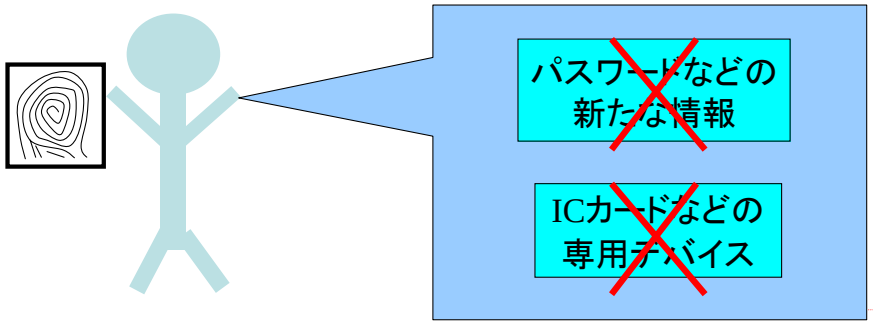
指紋からの生体鍵生成

静岡大学 創造科学技術大学院
西垣　正勝
nisigaki@inf.shizuoka.ac.jp

生体情報の利便性

Nish!gaki Laboratory

- 生体情報は本人があらかじめ所持している情報であり、本人認証を行うために新たな情報の記憶や専用デバイスを所持する必要がなく、ユーザの利便性が高い。



生体情報はあいまい

Nish!gaki Laboratory

- 指紋、虹彩・・・・身体的特徴
- 署名、声紋・・・・行動的特徴

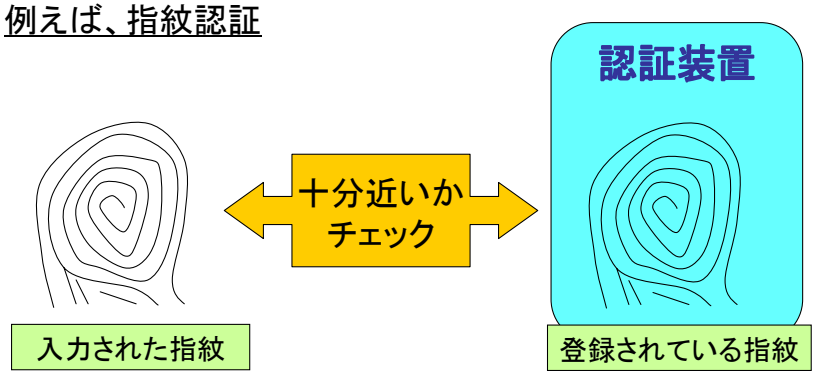
DNAを除いて、ほとんどの生体情報は
アナログデータである

読み取り時に人的、外的要因に
よって何らかの誤差が混入するため、
一意なディジタルデータへの変換が難しい

従来の生体認証

Nish!gaki Laboratory

例えば、指紋認証



同一のディジタルデータが得られないため
生体情報の類似性を見るという方法を採らざるをえない

生体認証から生体鍵へ

Nish!gaki Laboratory

生体情報はあいまい **常に同一のディジタルデータを得られない！**

このままでは、多方面への応用に不便である

特に・・・

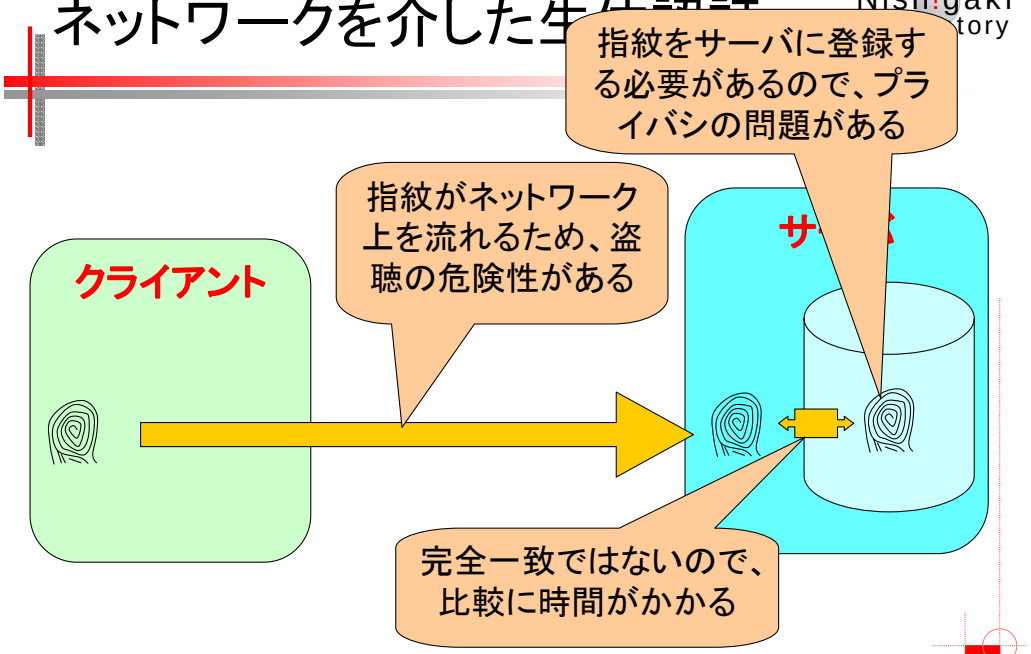
暗号方式を基盤とする技術

- PKIを用いた公開鍵暗号・署名
- Challenge & Response認証

etc.

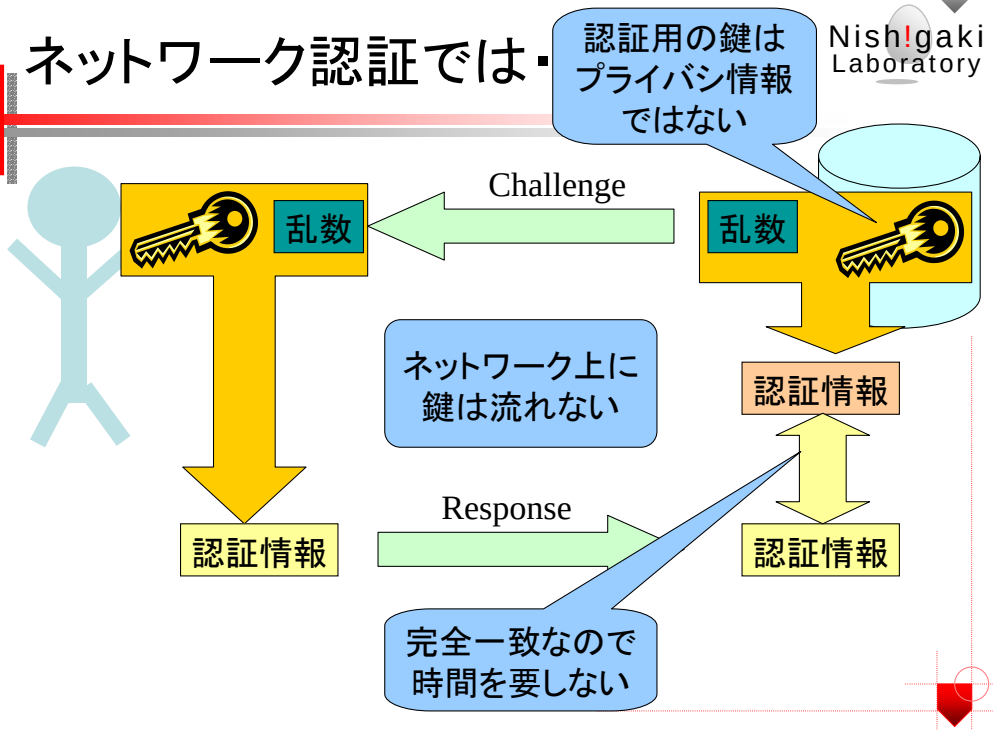
ネットワークを介した生体認証

Nish!gaki Laboratory



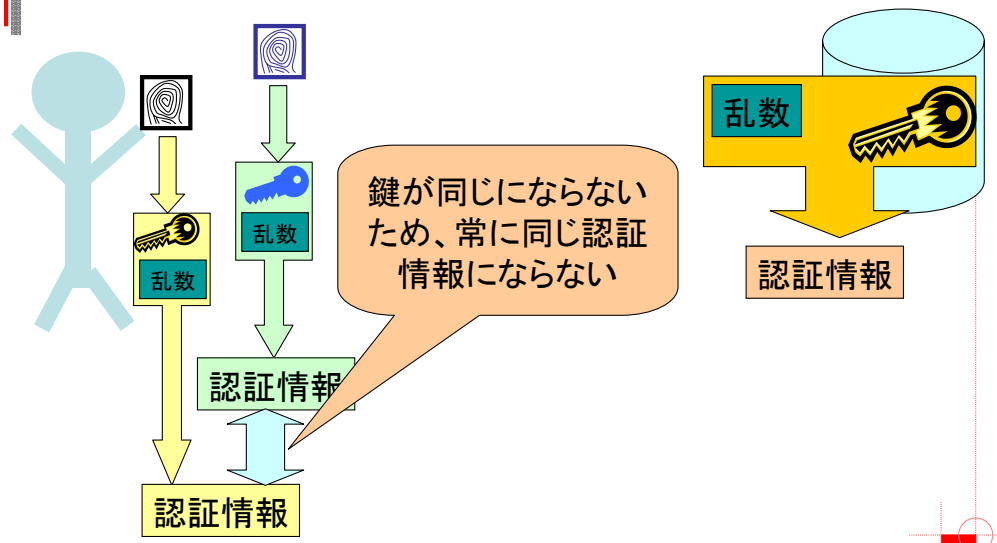
ネットワーク認証では・

Nish!gaki Laboratory



生体情報を用いてネットワーク認証を行うには

Nish!gaki Laboratory



生体認証から生体鍵へ

Nish!gaki Laboratory

生体情報はあいまい **常に同一のディジタルデータを得られない！**

このままでは、多方面への応用に不便である

特に・・・

暗号方式を基盤とする技術

- PKIを用いた公開鍵暗号・署名
- Challenge & Response認証

etc.

生体情報から一意な鍵を生成する技術が必要

Key Generation Biometrics

Nish!gaki Laboratory

- 生体情報から鍵生成を行うアプローチ
  - – 誤り訂正符号を利用する方式
    - 生体情報から得られた値を誤り訂正符号として扱い、誤り訂正によって、本人の生体情報に含まれる誤差を許容する方式
  - – 統計解析を利用する方式
    - 統計解析により本人の生体情報の変動範囲を予測し、予測した範囲内の値には一意な鍵を割り当てる方式

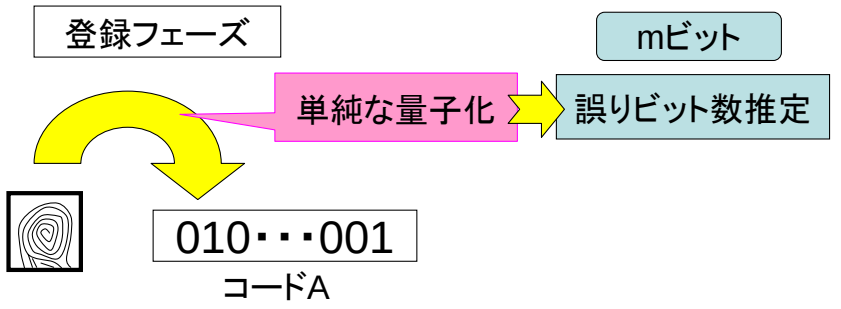
誤り訂正符号を利用する方式

Nish!gaki Laboratory

- 誤り訂正符号を利用する方式
  - – Fuzzy Commitment
    - A. Juels and M. Wattenberg. “a fuzzy commitment scheme”, In G. Tsudik, editor, sixth ACM Conference on Computer and Communications Security, pp.28-36. ACM Press, 1999.
  - – Fuzzy Vault
    - A. Juels and M. Sudan. “a fuzzy vault scheme”. proc IEEE Int. Symp. Inf. Theory, p.408, 2002.

Fuzzy Commitment

Nish!gaki Laboratory



Fuzzy Commitment

Nish!gaki Laboratory

登録フェーズ

mビット誤り
符号生成器

010・・・001
コードA

100・・・101
誤り訂正符号R

コミットメントC = A⊕R

データベース

Fuzzy Commitment

Nish!gaki Laboratory

認証フェーズ

011・・・011
コードA＋誤差 = A’

登録時のコードAと
わずかに異なる

010・・・001
コミットメントC

データベース

Fuzzy Commitment

Nish!gaki Laboratory

認証フェーズ

101・・・111
R’ = R＋誤差

A-A’ 間で異なるビット
＝
R-R’ 間で異なるビット

mビット以下

A’⊕C = A’⊕(A⊕R) = R’

011・・・011
コードA＋誤差 = A’

010・・・001
コミットメントC

登録時のコードAと
わずかに異なる

mビット以下

データベース

Fuzzy Commitment

Nish!gaki Laboratory

誤り訂正

誤差がmビット
以下なので
Rが復元可能

101・・・111
R’ = R＋誤差

A-A’ 間で異なるビット
＝
R-R’ 間で異なるビット

mビット以下

100・・・101
誤り訂正符号R

010・・・001
コミットメントC

R⊕C = R⊕(A⊕R)

010・・・001
コードA

データベース

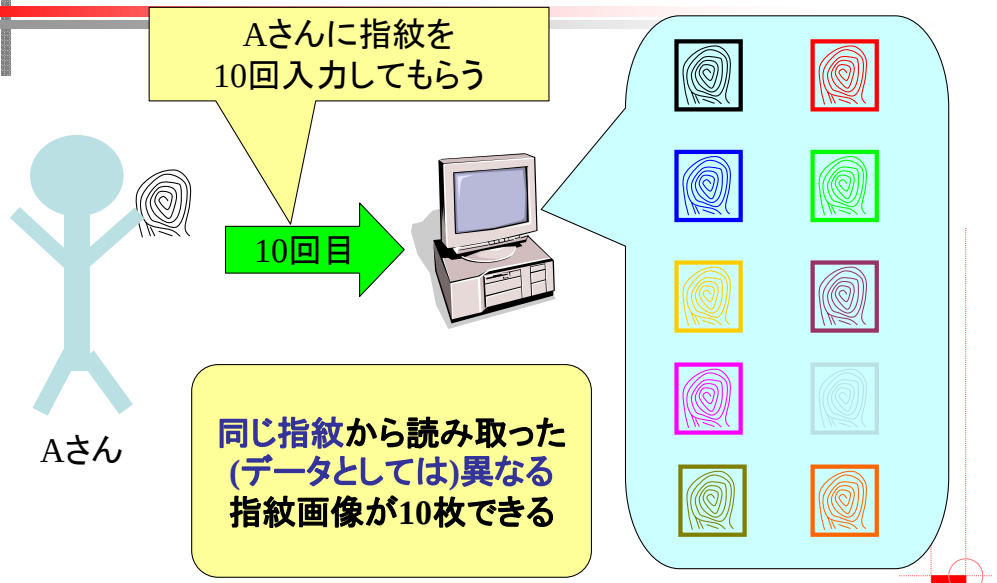
統計解析を利用する方式

Nish!gaki Laboratory

- 統計解析を利用する方式には
  - あいまいな特徴量を利用しない方式（事後学習型）
    - F. Monrose, M.K. Reiter, Q.Li, and S. Wetzel
      “Cryptographic key generation from voice”
  - 本人の許可区間を定める方式（事前解析型）
    - Bioscript社（C.Soutar, et.al）
      “Biometric encryption”
    - Y.Chang, W. Zhang and T. Chen
      “Biometric-based cryptographic key generation”
    - Hao Feng and Chan Choong Wah
      “Private key generation from on-line handwritten signatures”
    - **柴田,三村,高橋,西垣**
      “統計的AD変換”

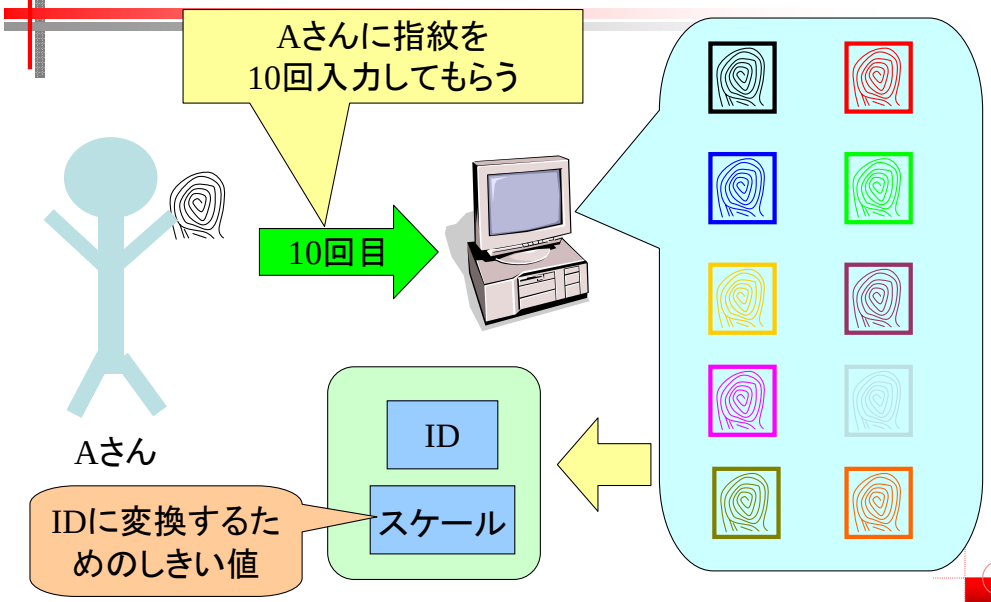
指紋読み取り×10

Nish!gaki Laboratory



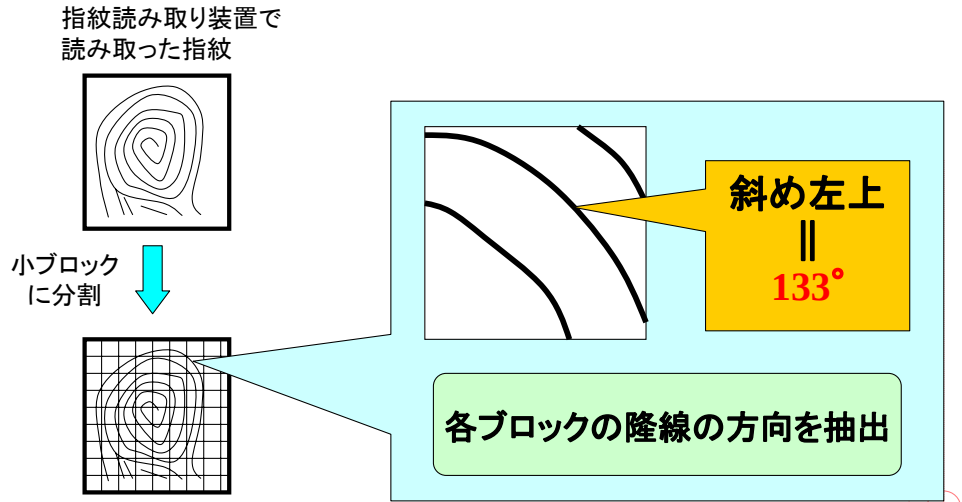
指紋読み取り×10

Nish!gaki Laboratory



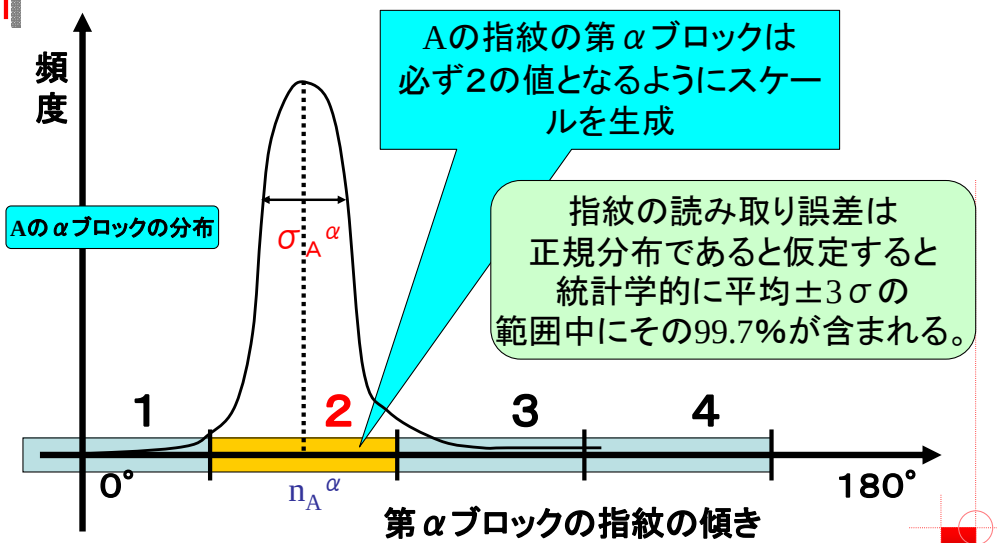
一例として指紋をAD変換してみよう

Nish!gaki Laboratory



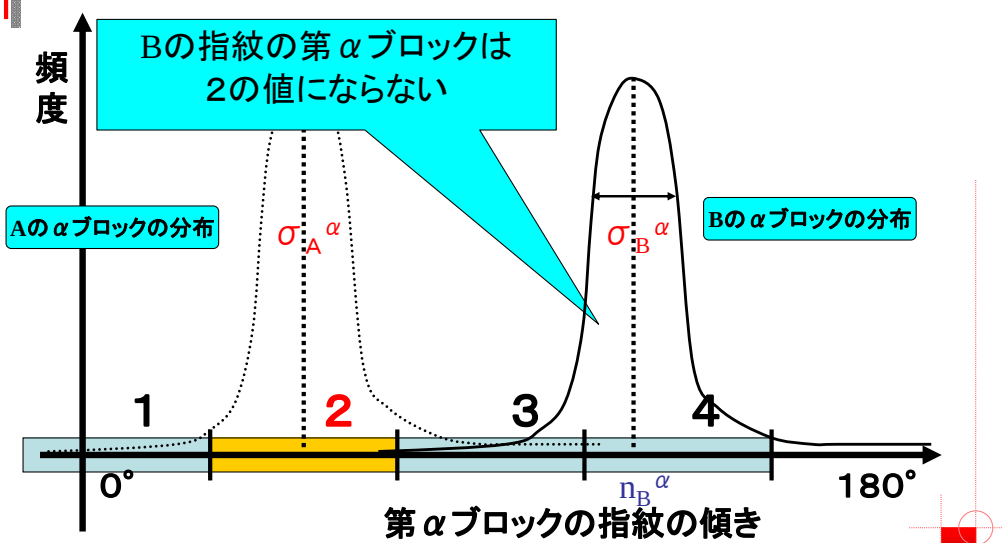
統計解析処理による スケール（特徴分布データ）の作成

Nish!gaki Laboratory



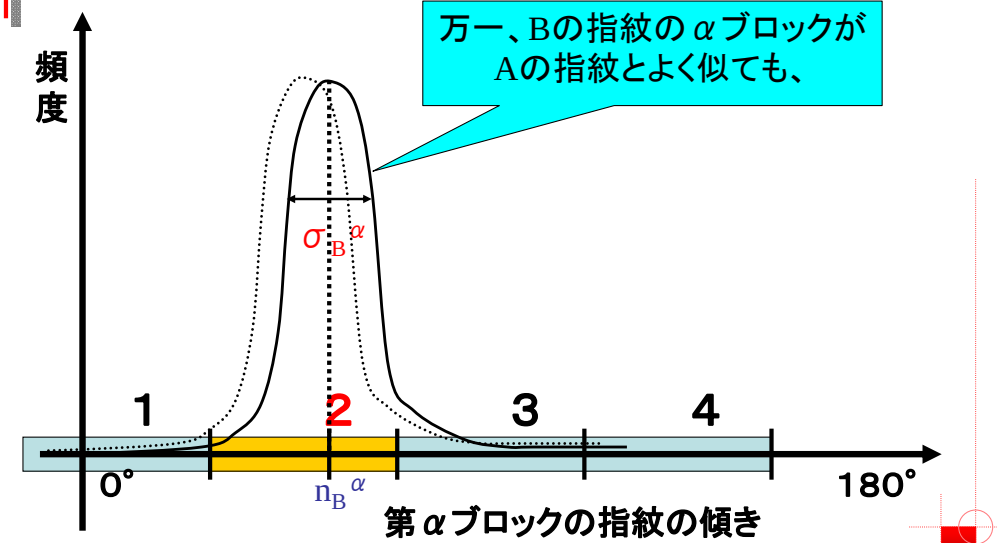
統計解析処理による スケール（特徴分布データ）の作成

Nish!gaki Laboratory



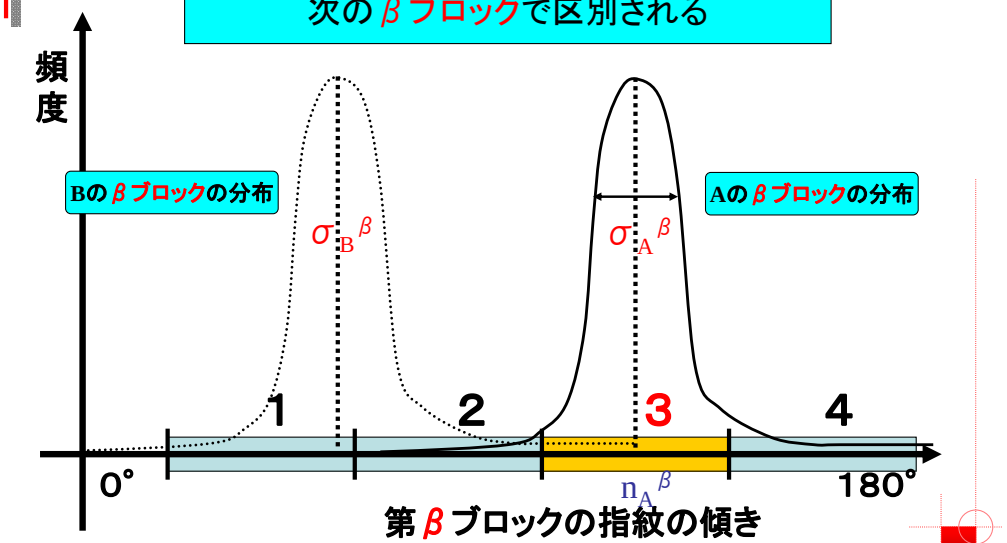
統計解析処理による スケール（特徴分布データ）の作成

Nish!gaki Laboratory

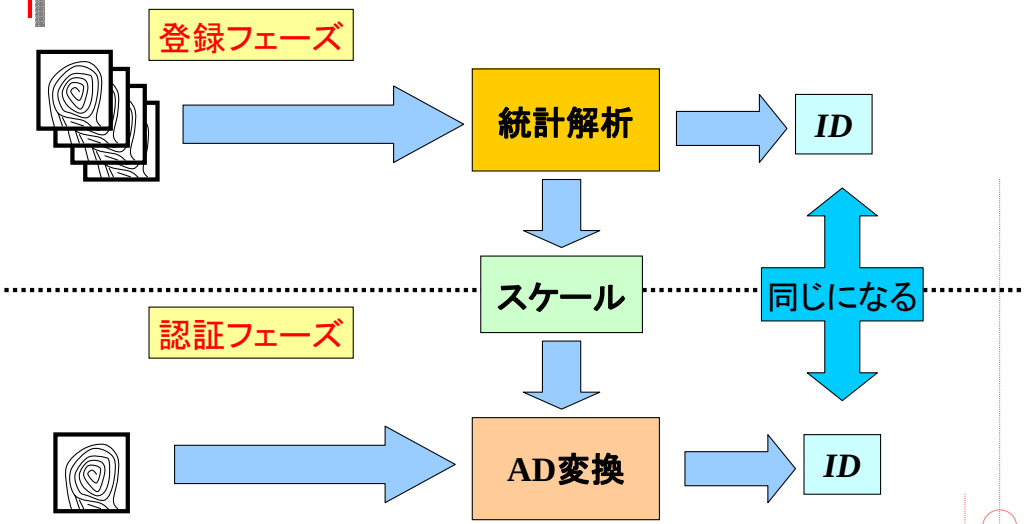


統計解析処理による スケール（特徴分布データ）の作成

Nish!gaki Laboratory



統計的AD変換の流れ



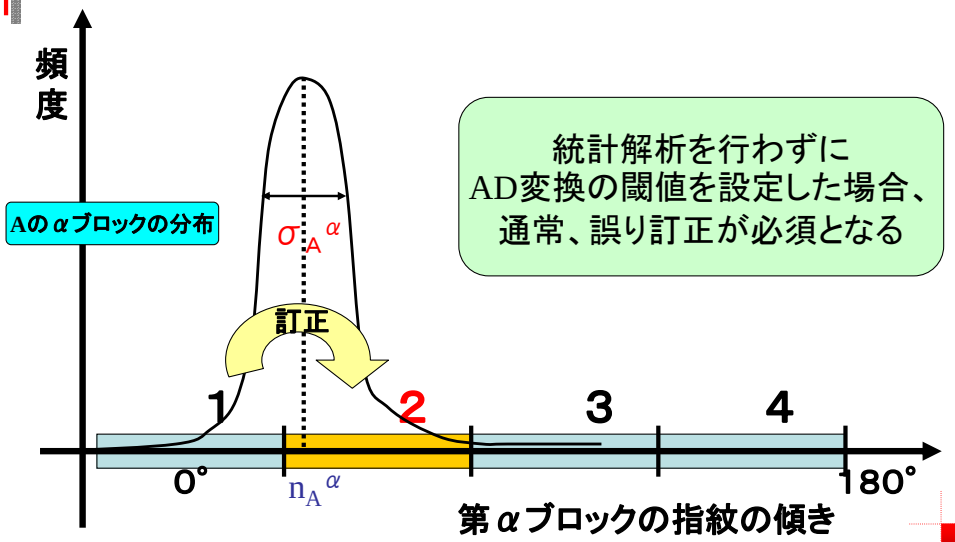
それぞれの問題点

- 生体情報から鍵生成を行うアプローチ
  - 誤り訂正符号を利用する方式
    - 本人の誤りを訂正できる代わりに**他人の誤りも訂正してしまう**ため、全体の精度を向上させる効果があまり期待できない
      誤り訂正＝FARを犠牲にしてFRRを減少させる
  - 統計解析を利用する方式
    - 登録時に取得できる**生体情報の数には限りがある**ため、統計解析を正確に行うことは実質不可能であり、正確な鍵生成を行えない可能性が残る

誤り訂正の影響

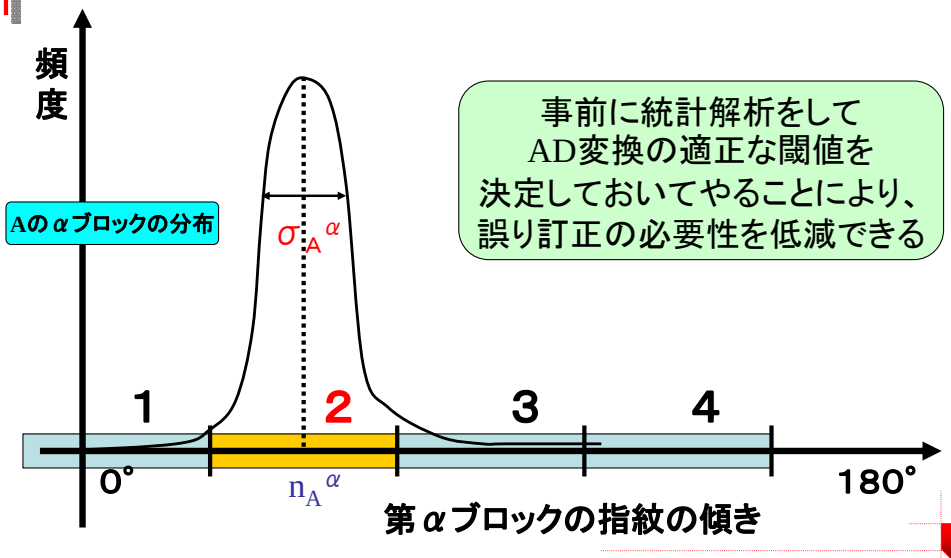
- ID抽出の精度向上へのアプローチ
  - 本人拒否率(FRR)
    - 誤り訂正によって、本人の特徴量から必ず一意なIDが生成されるようにする
  - 他人受入率(FAR) ⇕ トレードオフ
    - 誤り訂正によって、他人の特徴量から本人と同じIDが生成されやすくなってしまう

通常のAD変換



統計解析処理を利用したAD変換

Nish!gaki Laboratory



事前に統計解析をして
AD変換の適正な閾値を
決定しておいてやることにより、
誤り訂正の必要性を低減できる

誤り訂正と統計処理の併用

Nish!gaki Laboratory

- ID抽出の精度向上へのアプローチ
  - 本人拒否率(FRR)
    - 誤り訂正によって、本人の特徴量から必ず一意なIDが生成されるようにする
  - 他人受入率(FAR)

トレードオフ

    - 誤り訂正によって、他人の特徴量から本人と同じIDが生成されやすくなってしまう

統計解析の併用により
誤り訂正を控えつつFRRの悪化も防ぐ

統計的AD変換における スケール幅の影響

Nish!gaki Laboratory

- ID抽出の精度向上へのアプローチ
  - 本人拒否率(FRR)
    - スケールの幅を大きく設定することで本人の特徴量から必ず一意なIDが生成されるようにする
  - 他人受入率(FAR)

トレードオフ

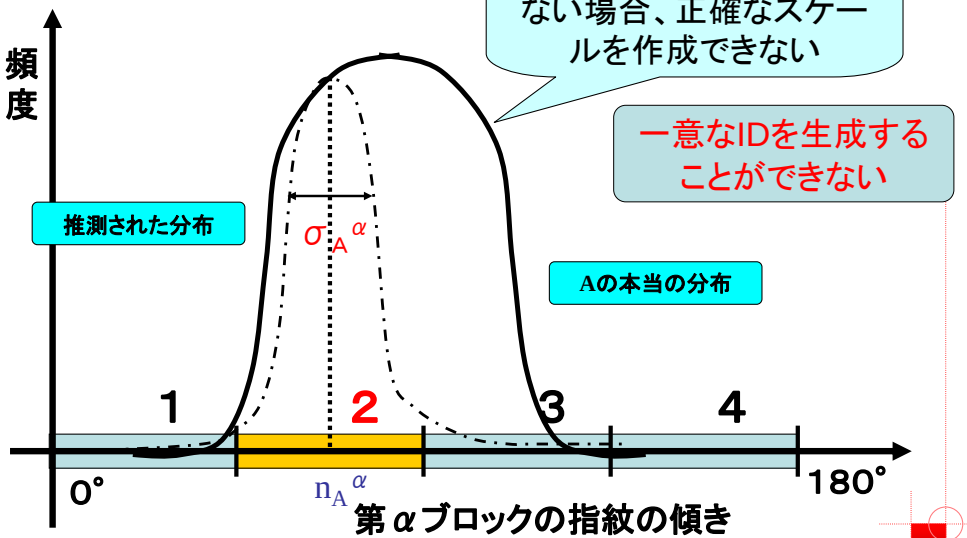
    - スケールの幅をできるだけ狭く設定することで他人の特徴量から本人と同じIDが生成されにくくする

統計解析処理の限界

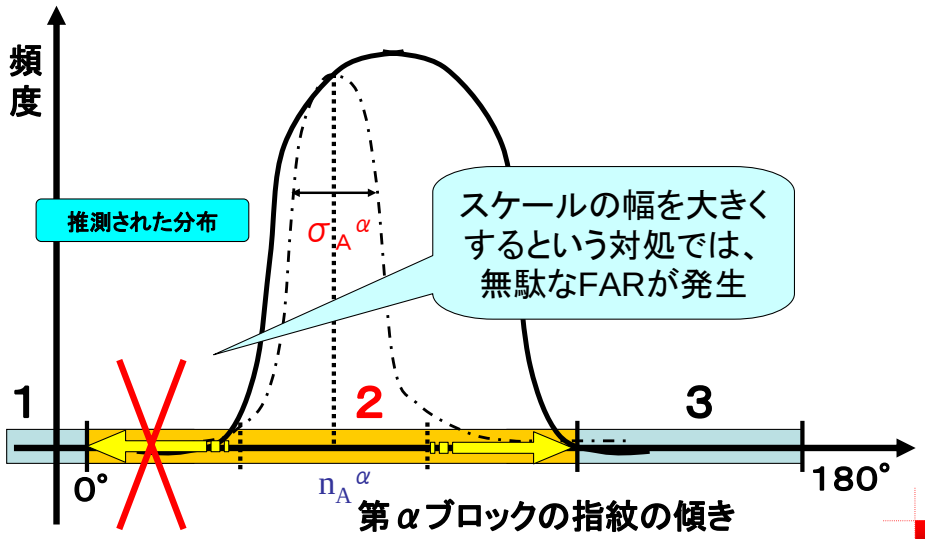
Nish!gaki Laboratory

本当の分布を推測しきれない場合、正確なスケールを作成できない

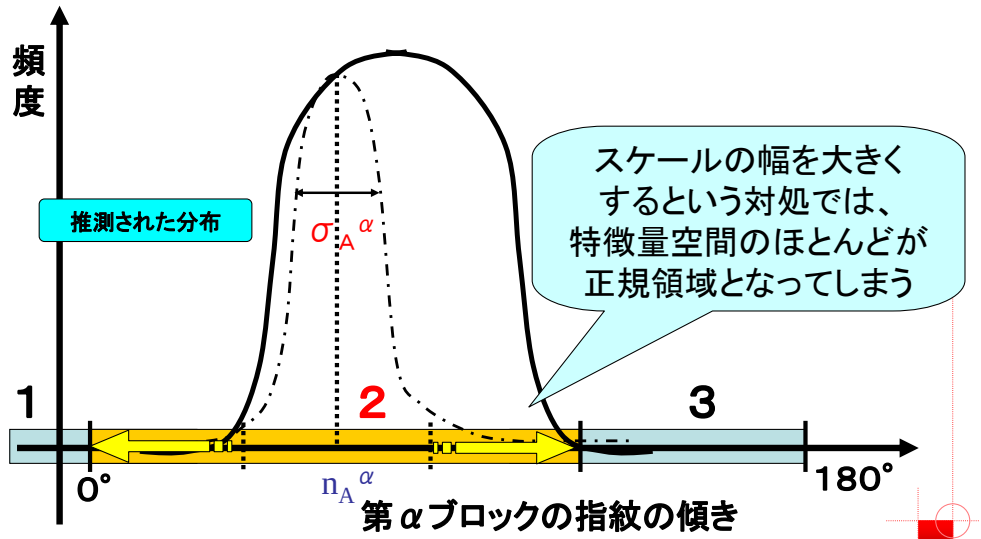
一意なIDを生成することができない



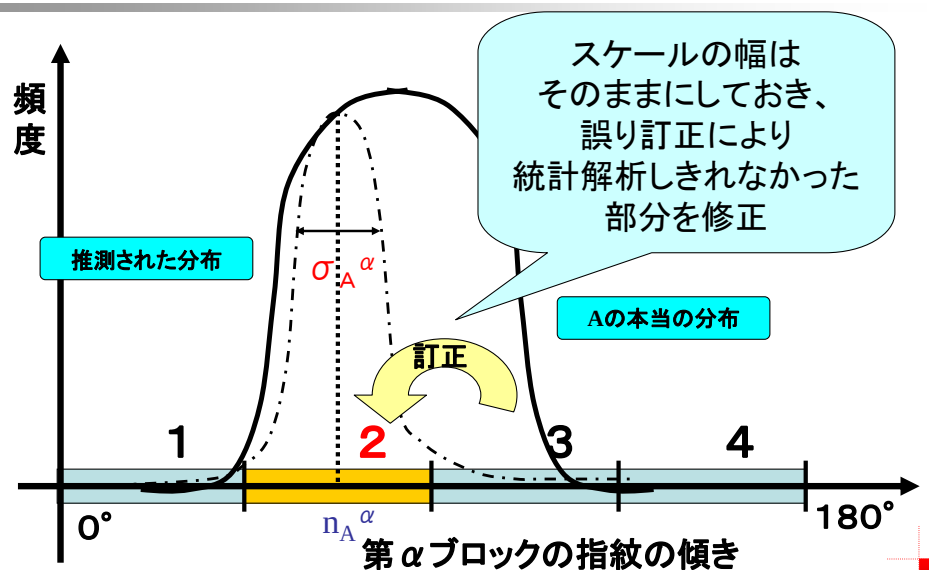
統計解析処理の限界



統計解析処理の限界



統計解析処理の限界を誤り訂正



統計的AD変換と誤り訂正の併用

- ID抽出の精度向上へのアプローチ
  - 本人拒否率(FRR)
    - スケールの幅を大きく設定することで本人の特徴量から必ず一意なIDが生成されるようにする
  - 他人受入率(FAR)
    - スケールの幅をできるだけ狭く設定することで他人の特徴量から本人と同じIDが生成されにくくする

トレードオフ

誤り訂正の併用により
統計解析の不完全性を修正

複数の生体情報からのID抽出

- 個々のFRR（本人拒否率）はゼロに近づける
  - スケールの幅を大きく設定する
    - 統計解析により得た標準偏差のn倍に設定
  - 誤り訂正の誤り許容数を大きく設定する
- FAR（他人受入率）は生体情報の数で向上
  - 多くの生体情報（特徴量）からID抽出を行う

我々のアプローチ

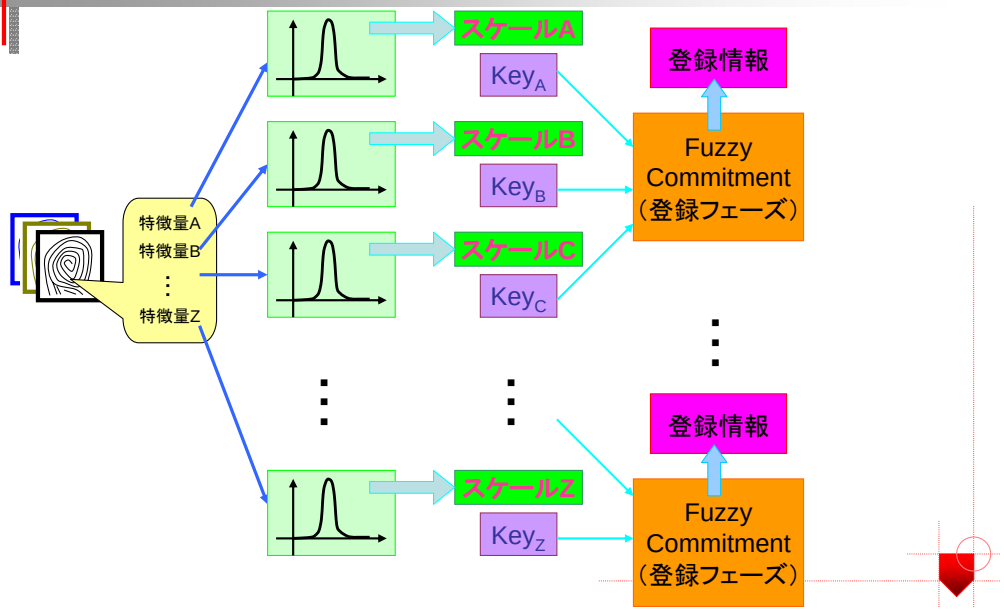
- 統計解析と誤り訂正の併用により、
  それぞれの問題点を補うことができないか
  - 誤り訂正符号を利用する方式
  - 統計解析を利用する方式

} の併用

統計的AD変換＋Fuzzy Commitment

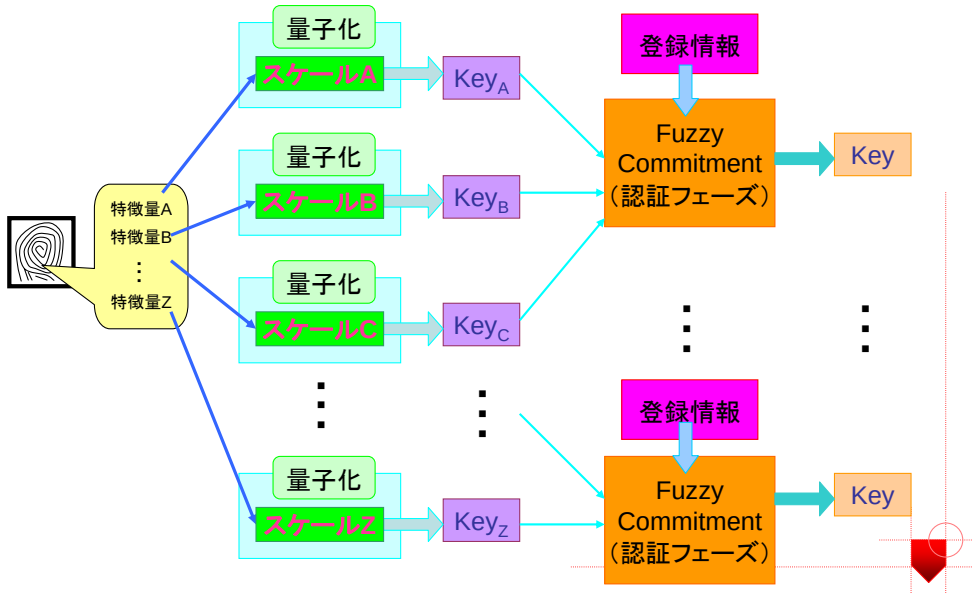
登録フェーズ

統計解析による方式 ＋ 誤り訂正符号による方式



鍵生成フェーズ

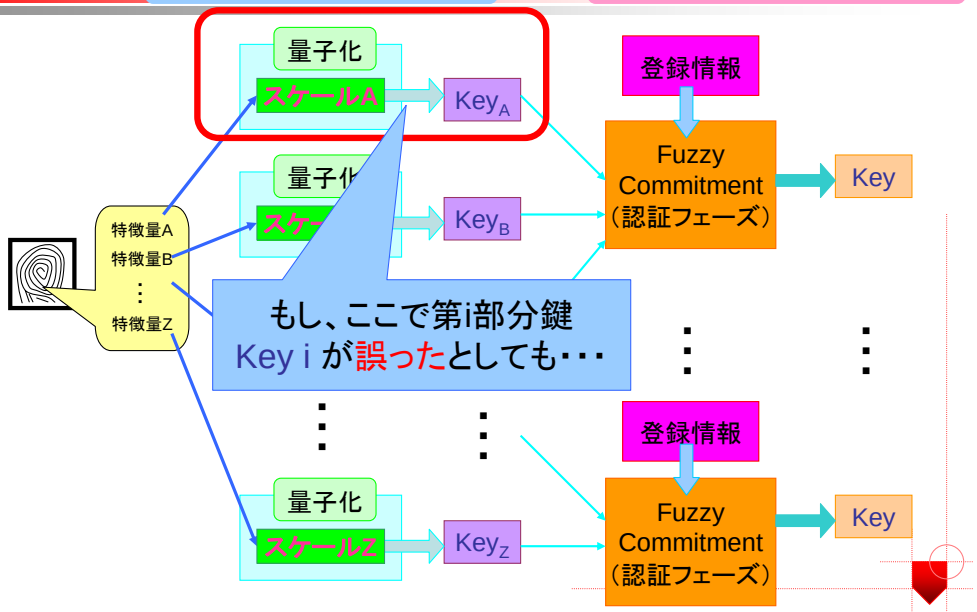
統計解析による方式 ＋ 誤り訂正符号による方式



鍵生成フェーズ

Nish!gaki Laboratory

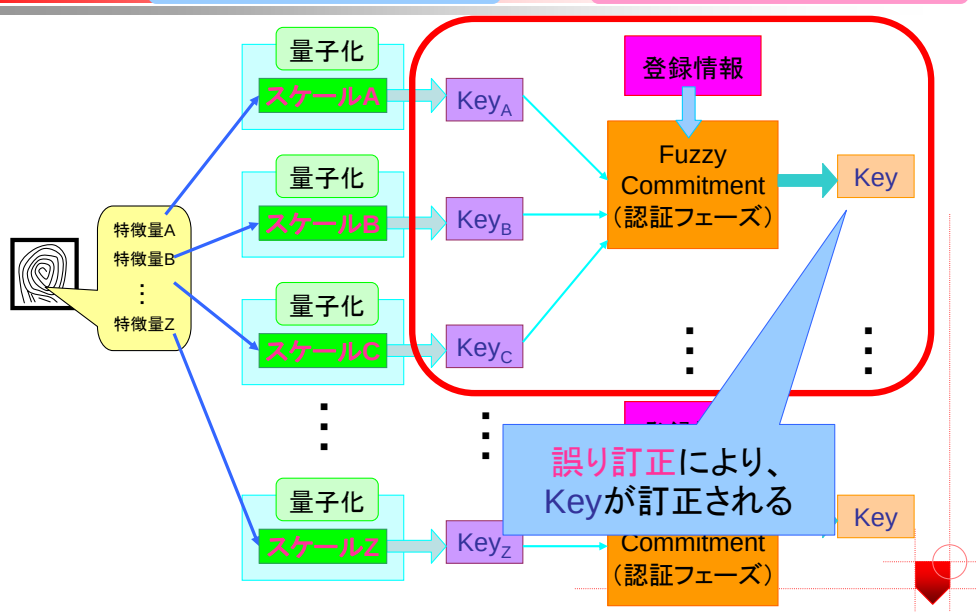
統計解析による方式 ＋ 誤り訂正符号による方式



鍵生成フェーズ

Nish!gaki Laboratory

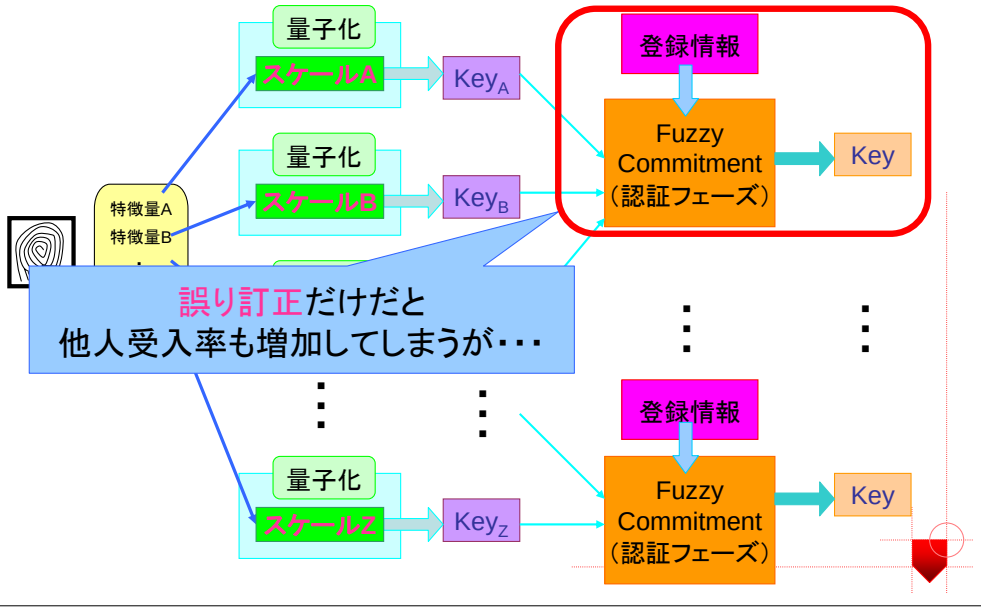
統計解析による方式 ＋ 誤り訂正符号による方式



鍵生成フェーズ

Nish!gaki Laboratory

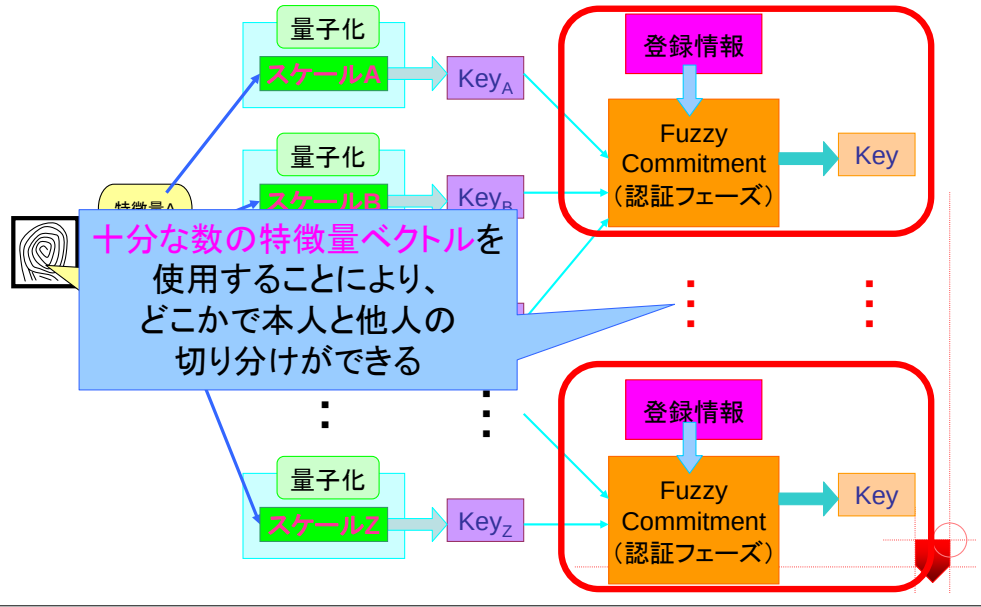
統計解析による方式 ＋ 誤り訂正符号による方式



鍵生成フェーズ

Nish!gaki Laboratory

統計解析による方式 ＋ 誤り訂正符号による方式



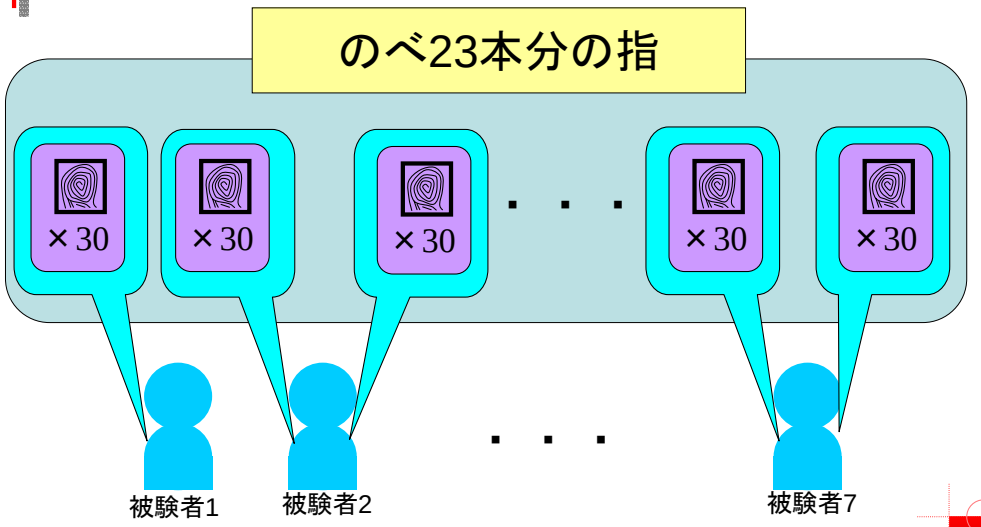
検証実験

Nish!gaki Laboratory

- 被験者は本学の男子学生7人
  - のべ23本の指紋から各30枚の指紋画像を採取
  - 各指30枚の画像を、登録用の10枚とFRR検証用の20枚に分ける
  - 他のすべての指の指紋画像(22指×30枚)をFAR検証に用いる
- 特徴量の数は64個
  - 指紋画像(300×300画素)を18×18画素のサブ画像に分割し、その中心8×8個のサブ画像のそれぞれから隆線角度を算出
- 各種セキュリティパラメータを変化させながら実験を行う
  - n : 許容区間の幅の広さ
  - p : 誤り訂正をするにあたって連結する特徴量の数
  - r : 誤り訂正強度mを決める係数
- FARとFRRの和で評価を行う

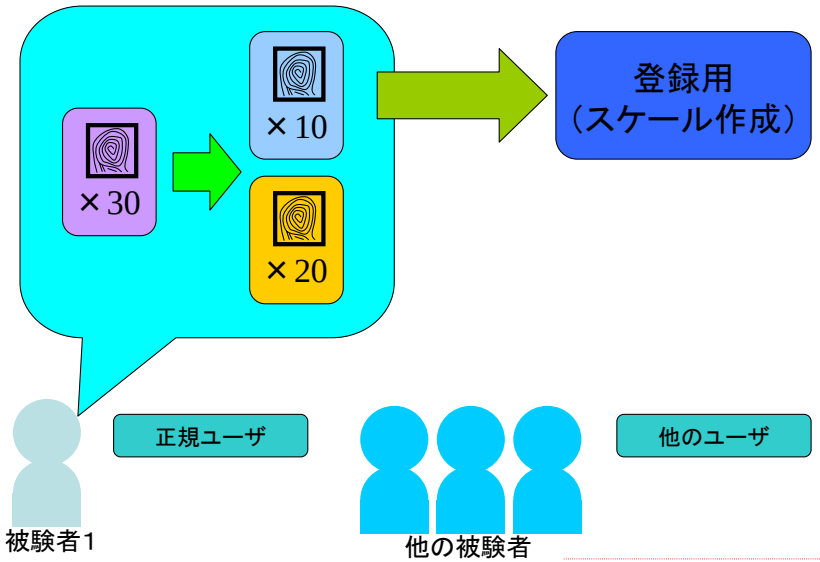
Nish!gaki Laboratory

検証実験



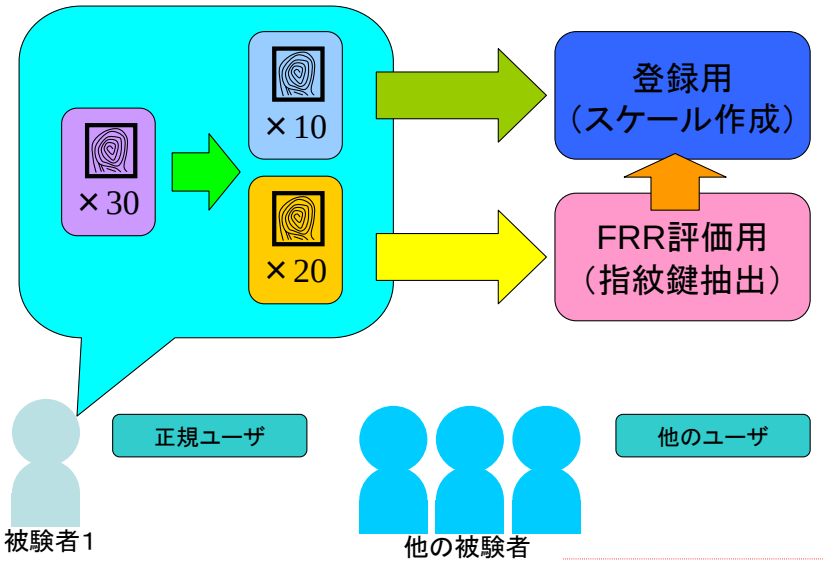
Nish!gaki Laboratory

検証実験

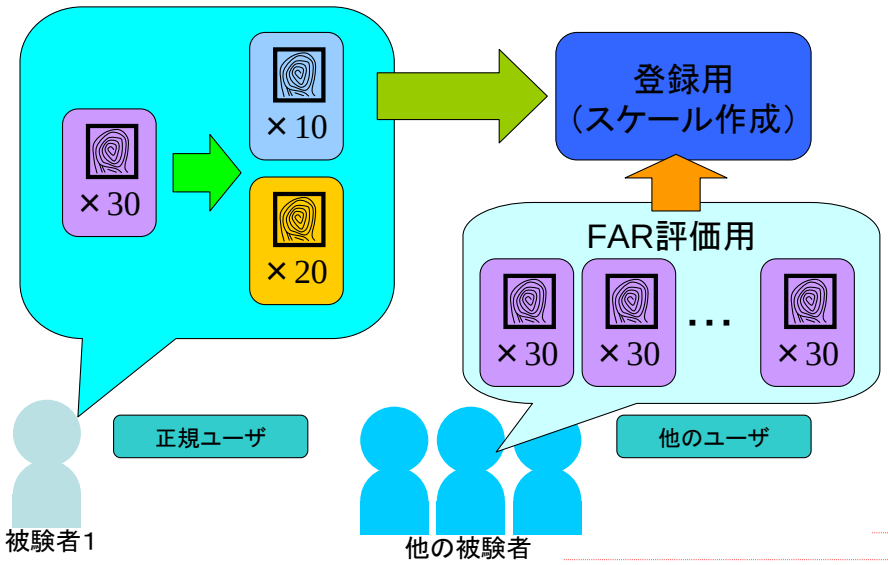


Nish!gaki Laboratory

検証実験



検証実験



実験結果：rの値を固定し、nとpの認証精度への影響をチェック

- r=0.15の場合

		スケールの幅の倍率n							
		2.0	3.0	4.0	5.0	6.0	7.0	8.0	9.0
連結数pの特徴量の	64	0.123	0.097	0.082	0.092	0.090	0.100	0.096	0.116
	32	0.128	0.096	0.082	0.094	0.088	0.097	0.094	0.210
	16	0.146	0.095	0.079	0.093	0.086	0.103	0.100	0.194
	8	0.144	0.096	0.092	0.085	0.075	0.097	0.096	0.111
	4	0.181	0.136	0.103	0.090	0.084	0.092	0.090	0.119
従来方式		0.546	0.292	0.191	0.132	0.116	0.115	0.106	0.117

– 連結する特徴量の数 p によって精度が最もよくなる n にばらつきがあるが、すべての特徴量を連結するよりも、ある程度(今回の実験では8個程度)の数の連結を行うほうが精度が改善されるようである

実験結果：pの値を固定し、nとrの認証精度への影響をチェック

- p=8の場合

		スケールの幅の倍率n							
		2.0	3.0	4.0	5.0	6.0	7.0	8.0	9.0
誤り強度を決める係数r	0.2	0.119	0.092	0.084	0.097	0.085	0.099	0.094	0.111
	0.175	0.138	0.097	0.096	0.090	0.079	0.098	0.094	0.111
	0.15	0.144	0.096	0.092	0.085	0.075	0.097	0.096	0.111
	0.125	0.167	0.103	0.090	0.085	0.084	0.105	0.099	0.111
	0.1	0.174	0.100	0.090	0.098	0.102	0.101	0.098	0.111
従来方式		0.546	0.292	0.191	0.132	0.116	0.115	0.106	0.117

– 誤り強度 m を決定する係数 r によって精度が最もよくなる n にばらつきがあるが、r=0.15のときに約0.075(7.5%)となっており、精度が向上していることが確認された

まとめ：生体鍵生成

- 誤り訂正符号を利用する方式
- 統計解析を利用する方式　　の併用

- 統計的AD変換＋Fuzzy Commitment
  - 統計解析と誤り訂正符号を組み合わせ、互いの方式を補った方式
  - 研究室レベルでの実証実験の結果、
    - n：許容区間の幅の広さ n=6.0
    - p：誤り訂正をするにあたって連結する特徴量の数 p=8
    - r：誤り訂正強度mを決める係数 r=0.15

    を採用した場合が最も精度がよく、FAR+FRR＝約0.075（7.5%）
    ＃統計解析のみ：最高でFAR+FRR＝約0.106(10.6%)
  - 今後の課題
    - 他の特徴量の追加
    - 各パラメータの決定方式の構築
    - 実用レベルの実証実験
    - 少ないサンプルからの完璧な特徴量の統計的バラツキ分布の推定