

R3 基準指紋との参照ベクトルに基づく生体認証方式

河野 瞬

畔上 洋平

1. はじめに

現在の指紋認証技術には、リモートサーバ上で認証することから生じる生体情報のリスクが指摘されている。これに対して、生体情報を直接使わないゼロ知識証明を用いた認証の試みがあるが、特徴量がスキャンの度に変動するという生体情報特有の問題点が大きな課題になっていた。そこで、本研究では、指紋の隆線ベクトルと n 個の基準ベクトルとの類似度から成る n 次元の参照ベクトルを基に認証を行う方式を提案する。提案方式は生体情報の次元が安定し、ゼロ知識証明に適している。

2. 提案方式

2.1 参照ベクトル

[1]を用いて、入力指紋の中心部を抽出し、 21×21 のメッシュに細分化された各々の領域から隆線の向きを16方向に量子化した値を441次元の特徴ベクトル \mathbf{b} とする(図1参照)。

入力された指紋の特徴ベクトル \mathbf{b} と、 n 人から得られる基準データ $\mathbf{a}_1, \dots, \mathbf{a}_n$ とのコサイン尺度 $x_i = F(\mathbf{b}, \mathbf{a}_i) / \|\mathbf{b}\| \cdot \|\mathbf{a}_i\|$ を $i=1, \dots, n$ について求める。これらの類似度を n 次元のベクトル $\mathbf{x} = (x_1, \dots, x_n)^T$ とし、これを入力 \mathbf{b} の参照ベクトルと呼ぶ。



$$\mathbf{b} = \begin{bmatrix} 3 & 4 & 10 & 12 & 12 \\ 2 & 1 & 14 & 13 & 13 \\ 1 & 0 & 15 & 14 & 13 \\ 0 & 0 & 15 & 14 & 13 \\ 0 & 15 & 15 & 14 & 13 \end{bmatrix}$$

図1: 指紋画像と特徴ベクトル \mathbf{b} の例

2.2 基準データ相関ベクトル方式

参照ベクトル \mathbf{x} から公開鍵アルゴリズムによるコミットメントを求め登録する。認証時は入力されたベクトル \mathbf{y} と参照ベクトル \mathbf{x} との距離が閾値 τ よりも近いこと、すなわち $F(\mathbf{x}, \mathbf{y}) \geq \tau$ となるような \mathbf{y} を入力したということをゼロ知識証明する。これにより、生体情報を秘匿したまま認証することを可能にする。ただし登録時に用いた乱数を耐性のあるデバイスに格納しておく必要がある。

3. 評価実験

3.1 隆線ベクトルを用いた認証精度

被験者4人の指紋を各々100個取得し、最初の1個をテンプレートとし、残りの99個について、コサイン尺度での比較を行い4人分の平均FRR(本人拒否率)を求めた。また、他人36人の指紋からFAR(他人受入率)を求めた。認証精度を図2のRidgeで示す。

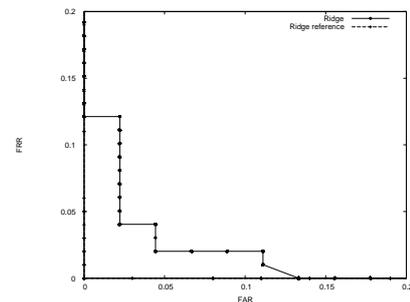


図2: 隆線ベクトルとその参照ベクトルの認証精度

3.2 参照ベクトルを用いた認証精度

本人以外の45個の基準データと3.1のスコアから、 $n=45$ 次元の参照ベクトルを求め、参照ベクトル同士の類似度を用いたFARとFRRを図1 Ridge referenceに示す。これらの認証方式から Equal Error Rate(EER)を求め表1に整理する。

表1: 各認証方式と参照ベクトルのEER

認証方式	基本 EER[%]	参照 EER[%]
隆線ベクトル	4.4	0
マニューシャ	0	30.0

4. おわりに

本認証方式を実装した。実験により、隆線ベクトル方式は参照ベクトルにすることにより向上することがわかった。今後の課題として、十分な精度が得られる最適な基準データを人工的に作り上げることがある。

参考文献

- [1] "NIST Fingerprint Image Software 2 (NFIS2)", 2004.
- [2] 菊池, 河野, 畔上, 西垣, 尾形: "直交基底指紋への参照度の特徴量とした安全な生体認証プロトコル", 暗号と情報セキュリティシンポジウム SCIS2009 (発表予定), 2009
- [3] 永井, 菊池, 尾形, 西垣, 秘密計算に適する距離の使用によるリモート生体認証, 暗号と情報セキュリティシンポジウム SCIS 2008, 2008.