

指紋がキーとなる金庫 "Indexed Fuzzy Vault" の開発

大貫 泰紀 高橋 佑介

1. はじめに

近年、キャッシュカードの偽造や暗証番号の盗撮などに対応するため、パスワードに代わる生体認証の導入が進んできた。生体情報は、パスワード認証に比べ本人が所持する情報がなく、利便性が高い。しかしネットワークを介して認証を行う場合、ネットワーク上で生体情報の盗聴や検証者であるサーバ側の不正という危険性がある。この問題を解決する手法として、Juels らによって不完全な情報から秘密情報を抽出することができる Fuzzy Vault Scheme が提案されている。そこで、指紋に対するインデックス付マニユーシャと最小距離マニユーシャマッチングによる Indexed Fuzzy Vault を提案する。

2. 提案方式

2.1 Fuzzy Vault Scheme

Fuzzy Vault Scheme とは、完全には一致していない情報の組を用いてある情報を隠す暗号方式である。Fuzzy Vault Schemeはロックとアンロックの2つのステップからなる。まず秘密情報 s を、情報 A を用いて符号化する。このとき A の特定を困難にするためにチャフを追加する。これを Vault R (ロック情報)とする。図1に Vault作成の流れを示す。Vault R から s を復元する(アンロック)には、 A と同様な形式を取る情報 B を用い、この A と B の大部分が一致していた場合のみ、RS符号により s を復元できる。

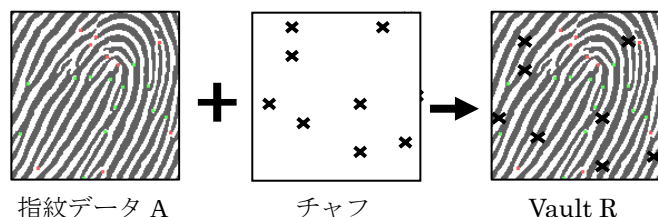


図1. Vault作成の流れ

2.2 提案方式 Indexed Fuzzy Vault

Fuzzy Vault Scheme はアンロックの過程で RS 符号を用いる。Reed-Solomon(RS)符号は巡回符号の一つで、情報ビットをブロックに分割し、検査符号を付加することで、ブロック単位の誤り訂正が可能な符号である。

Fuzzy Vault Scheme を指紋認証に適用する場合、認証時に抽出される情報 B は不安定であり、登録情報 A と同じ順番で得られるとは限らないため、誤り訂正符号を適用できない。この問題を解決するために、登録情報のマニユーシャに対してインデックスを付加する。この時、チャフにも同

様にインデックスを付加することで本人以外の認証を困難にする。マッチングの際には、Vault R と特徴量 B でユークリッド距離が最小のデータの組を選ぶ。選んだデータの組をインデックスの順に並び替えることで、元の符号語と同じ並び順になり s を復元できる。

3. 実装, 評価

3.1 実験

本方式による認証精度を明らかにするため、RS符号の誤り訂正能力 t を変化した場合について、他人受入率 (FAR), 本人拒否率(FRR) の変化を求める。FRRについては、本人の指紋50枚を使って求める。FARについては各インデックスの候補の中からランダムに選択した場合の認証率で算出する。

3.2 実験結果

図2に t についての認証精度を示す。本実験で最も誤りが小さかったのは $t = 6$ のときであり、 $FAR = 0$, $FRR = 0.02$ であった。

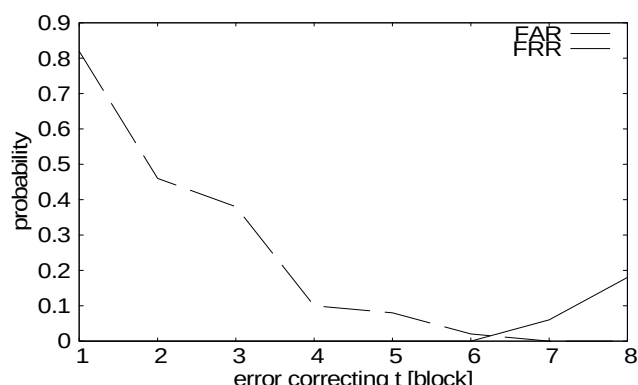


図2. 誤り訂正能力 t についての認証精度

4. おわりに

特徴点にインデックスを付加することで、FuzzyVault Scheme を指紋認証に適用した。今後の課題として、安全性を保証するために十分なチャフの数と認証率の関係を明らかにすることが考えられる。

参考文献

- [1] A. Juels and M. Sudan, "A Fuzzy Vault Scheme", IEEE Intl'. Symp. Inf. Theory, pp. 408-413, 2002.
- [2] 大貫, 高橋, 永井, 菊池, "インデックス付マニユーシャによる Fuzzy Vault の実装と評価", 暗号と情報セキュリティシンポジウム, SCIS2007, 2007. (発表予定)