# Fuzzy Commitment Scheme を指紋マニューシャマッチングに適用した実験と評価

武藤 祐貴† 姜 玄浩* 井沼 学‡ 今井 秀樹†‡

†中央大学理工学研究科, *中央大学研究開発機構
112-8551 東京都文京区春日 1-13-27

{yuuki-mutoh,kang}@imailab.jp
‡産業技術総合研究所情報セキュリティ研究センター
101-0021 東京都千代田区外神田 1-18-13 秋葉原ダイビル 10 階 1003 号室

{inuma.manabu,h-imai}@aist.go.jp

**あらまし** 生体認証システムにおける暗号理論的なテンプレート保護技術として Juels らによって提案された Fuzzy commitment scheme や Fuzzy vault scheme は多くの研究者によって研究されている．なかでもマニューシャマッチング方式を用いた指紋認証技術に対する既存研究では，マニューシャの個数が照合のたびに異なるため 2 つの集合の類似度を用いる Fuzzy vault scheme の応用例のみが研究されていた．そこで，我々は SCIS2009 の研究において Fuzzy commitment scheme の応用手法を提案し，理論的な安全性を検証した．本稿では，この理論研究をもとに，実際の指紋データベースを用いた実装，実験を行い提案手法の認証精度と安全性を再検証する．

# An Experiment and Evaluation of Fuzzy Commitment Scheme for Fingerprint Minutiae Matching Algorithm

Yuki Muto† Hyunho Kang* Manabu Inuma‡ Hideki Imai†‡

†Graduate School of Science and Engineering, Chuo University
*Research and Development Initiative, Chuo University
1-13-27 Kasuga Bunkyo-ku Tokyo 112-8551 Japan

{yuuki-mutoh,kang}@imailab.jp
‡Research Center for Information Security (RCIS),
National Institute of Advanced Industrial Science and Technology (AIST)
Akihabara-Daibiru Room 1003 1-18-13 Sotokanda Chiyoda-ku Tokyo 101-0021 Japan

{inuma.manabu,h-imai}@aist.go.jp

**Abstract** In the recent years, numerous theoretical researches were achieved concerning a Fuzzy commitment scheme and a Fuzzy vault scheme to solve the problems of biometric template protection. In particular, a Fuzzy vault scheme is highly suitable for unordered data with arbitrary dimensionality, such as fingerprint minutiae. Therefore, there has been very little research on a Fuzzy commitment approach to implement fingerprint template protection. In our previous work, we have proposed the application of a Fuzzy commitment algorithm and have proved the security of the scheme. In this paper, the experimental work, including accuracy and security, will be presented followed by our previous work.

## 1　はじめに

近年，指紋や静脈，虹彩などの個人の生体的な特徴を本人認証に応用した生体認証が普及してきている．生体情報は本人特有のものであり，忘却や失効の心配がいらない．しかし従来のパスワードやＩＣカードによる認証と比べると，生体情報は変更が利かない点で不便である．また，生体情報はそれ自体が大切なプライバシーとなるので，漏洩に対する安全性はパスワードやＩＣカード以上に重要な問題となる．さらに生体情報の漏洩が起きた場合，ユーザの個人情報漏洩という問題にとどまらず，ユーザの財産を狙い，本人と偽り認証システムにアクセスするなりすましなどの被害も起こると考えられる．現行システムの生体情報漏洩に対する対策は，登録した生体情報や照合時に読み取られた生体情報を暗号化することである．しかし，たとえ本人の正しい生体情報であっても，登録時と照合時で必ずしも一致するわけではないため，これら 2 つの生体情報を比較するときには暗号化したデータを復号して類似度を計算している．よって，例えばサーバで照合を行うような現行システムでは，サーバによる管理ミスや不正によって復号時に元の生体情報が漏洩してしまう危険性がある．このような問題の解決策として，生体情報を変換したまま類似度を計算する手法や，本人の生体情報に近いものがシステムに提示されない限り元の生体情報が現れないようにする手法が提案されている．これらの手法のひとつとして Juels らは Fuzzy commitment scheme[1] や Fuzzy vault scheme[2] と呼ばれる誤り訂正符号を用いた暗号理論的な手法を提案した．このアプローチは，認証に用いられる生体情報が量子化されていることが条件となるものの，誤り訂正符号の選択やパラメータ設定を適切に行うことで安全な手法となることが知られている．

本稿では，マニューシャマッチング方式を用いる指紋認証に対する Fuzzy commitment scheme の応用について研究する．著者らの知る限り，既存研究においてマニューシャマッチング方式に Fuzzy vault scheme を応用した研究は存在するものの，Fuzzy commitment scheme を応用したものは存在しない．この主な理由として，集合の差異によって誤り訂正できる Fuzzy vault scheme がマニューシャ集合のマッチングに自然に応用できること，また，順序固定の記号列を扱う Fuzzy commitment scheme は読み取りのたびに個数や順序が異なるマニューシャ情報との相性が良くないと考えられていることなどがあげられる．しかしながら，我々は位置情報で順序を定め，登録時と認証時にマニューシャが現れなかった場所を消失記号として扱うことで自然に Fuzzy commitment scheme が適用できることを発見し，提案した手法の安全性を従来の Fuzzy vault scheme の応用手法 [4][5] と比較した [3]．より具体的には，計算量に制限のない攻撃者がオフライン攻撃によって元の生体情報を復元する攻撃の成功確率を Juels [1][2] に従って計算した．その結果，我々の提案手法は [4]，[5] よりも安全であることが示された．しかしながら，これはあくまでも安全性のみを考慮した理論値であり，実際のシステムでは認証精度とのトレードオフが考えられる．よって本稿では，実際のデータベース (15 人分の右手人差し指の指紋画像 1 人につき 5 画像) を用いて [3] の提案手法を実装し，実験を行った．

## 2　マニューシャマッチング方式

指紋認証の手法のひとつであるマニューシャマッチング方式を述べる．マニューシャマッチング方式は指紋の隆線から端点・分岐点などのマニューシャ(特徴点) を抽出し，その位置や隆線方向などをテンプレートと照合することで個人を認証する方式である．取得した指紋画像からマニューシャを抽出し，各マニューシャの位置関係などを利用してテンプレートと一致しているかを調べる．その際，対応している各マニューシャが一致しやすいように照合画像の平行移動や回転を行い，対応した各マニューシャがそれぞれ一致しているかを判定する．マニューシャ同士が一致しているかどうかの判定は，基本的には位置と方向の情報を用いて行う．一致と判断されたマニューシャの数を類似度として，照合の指紋の類似度があらかじめ決められた閾値以上ならば一致と判定し，閾値未満なら不一致

と判定する．また，上記のものも含めマニューシャ情報としては以下のものがある．

1. 位置情報 (座標点・エリア)
2. 角度情報 (隆線ベクトル)
3. 属性情報 (端点・分岐点)
4. 隆線数情報 (マニューシャ間)

# 3 Fuzzy scheme

## 3.1 Fuzzy commitment scheme

Fuzzy commitment scheme は，Juels らによって提案された暗号方式のひとつである．登録情報と誤り訂正符号により補助情報 (commitment) を作成し，登録情報と近い認証情報を用いて誤り訂正により秘密情報が復元される．誤り訂正符号として $GF(q)$ 上の $(q,k)-$RS 符号を用いる．以下にロック過程とアンロック過程を示す.

### 3.1.1 ロック過程

**Step 1** 秘密情報 $s$ と登録に必要な情報 $A$ を決定する．

$$A = (a_1, a_2, \cdots, a_{q-1}, a_q) \quad (a_i \in GF(q))$$

$$s = (s_1, s_2, \cdots, s_{k-1}, s_k) \quad (s_i \in GF(q))$$

**Step 2** $s$ を符号語 $g$ に符号化し，$C = g - A$ よりコミットメント $C$ を得る．

$$g = (g_1, g_2, \cdots, g_{q-1}, g_q) \quad (g_i \in GF(q))$$

$$C = (g_1 - a_1, g_2 - a_2, \cdots, g_{q-1} - a_{q-1}, g_q - a_q)$$

**Step 3** $C$ をデータベースに登録する．

### 3.1.2 アンロック過程

**Step 1** 認証に必要な情報 $A'$ を決定する．

$$A' = (a'_1, a'_2, \cdots, a'_{q-1}, a'_q) \quad (a'_i \in GF(q))$$

**Step 2** 登録されている $C$ から $g' = C + A'$ を計算し，$g'$ を得る．

**Step 3** $g'$ を最小距離復号法 (Berlekamp-Massey 法など) を用いて復号し，$s'$ を得る．

ここで $A$ と $A'$ の $a_i - a'_i$ 間で一致しなかった個数を $e$，消失した個数を $h$ とすると，以下の復号条件を満たせば $s' = s$ となる．

**復号条件**

$$2e + h \leq q - k$$

## 3.2 Fuzzy vault scheme

Fuzzy vault scheme は，Juels らによって提案された任意の情報の組により秘密情報を秘匿する暗号方式のひとつである．任意の秘密情報をロック情報でロックし，ロック情報に十分近いアンロック情報を用いて誤り訂正により秘密情報を復元する．誤り訂正符号として $GF(q)$ 上の $(t,k)-$RS 符号を用いる．以下にロック過程とアンロック過程を示す.

### 3.2.1 ロック過程

**Step 1** 任意の秘密情報 $s$ を決め，多項式 $f(X)$ を作る．

$$s = (s_1, s_2, \cdots, s_{k-1}, s_k) \quad (s_i \in GF(q))$$

$$f(X) = s_1 + s_2 X + \cdots + s_{k-1} X^{k-2} + s_k X^{k-1}$$

**Step 2** ロック情報 $A = (a_1, a_2, \cdots, a_{t-1}, a_t)$ を用いて $\{(a_i, f(a_i))\}_{i=1}^{t} = \{(x_i, y_i)\}_{i=1}^{t}$ を作る．

**Step 3** 次を満たす $\{(x_i, y_i)\}_{i=t+1}^{r} (x_i, y_i \in GF(q))$ をランダムに選び，Step 2 で生成した $\{(x_i, y_i)\}_{i=1}^{t}$ に付加して vault $V = \{(x_i, y_i)\}_{i=1}^{r}$ とする．

$$\{x_i\}_{i=t+1}^{r} \cap \{a_i\}_{i=1}^{t} = \phi$$

$$y_i \neq f(x_i) \ (t+1 \leq i \leq r)$$

### 3.2.2 アンロック過程

**Step 1** $A$ と同じデータ形式の $A' = (a'_1, a'_2, \cdots, a'_{t-1}, a'_t)$ を用意する．$(a'_i \in GF(q))$

**Step 2** vault$V = \{(x_j, y_j)\}_{j=1}^{r}$ と $A'$ から訂正に用いる受信語を次のようにして作る．
各 $a_i (1 \leq i \leq t)$ に対して $a_i = x_{j_i}$ となる $x_{j_i}$ が存在する．これらを用いて $c' = \{(x_{j_i}, y_{j_i})\}_{i=1}^{t}$ を受信語とする．

**Step 3** Step 2 の $c'$ を受信語として最小距離復号法で復号する．
ダミー情報とマッチした組の数を $m_f$ とすると，$m_f \leq \frac{t-k}{2}$ のとき正しい多項式 $f(X)$ を復元することができる．

## 4 Fuzzy scheme を用いた認証モデル

Fuzzy scheme を用いたバイオメトリクス認証のモデルを図 1 に示す．

登録時に，バイオメトリクス情報 $A$ と任意に選んだ秘密情報 $s$ から作られるデータ ( commitment や vault ) を $E(A, s)$ で表す．

**登録** クライアントは任意の生体情報 $A$ と秘密情報 $s$ から $H(s), E(A, s)$ を作り，$H(s)$ をテンプレートとしてサーバに登録し，$E(A, s)$ をユーザの IC カードなどの端末に保存する．

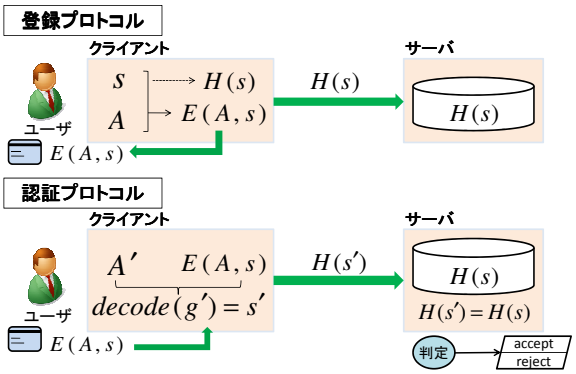


図 1: Fuzzy Scheme 認証モデル

**認証** クライアントは IC カードに保存されている $E(A, s)$ と任意の生体情報 $A'$ を用いて $g'$ を取り出し，誤り訂正により $g''$ に復号し，それにより得られた $s'$ から $H(s')$ を生成しサーバに送る．
サーバは以下を確かめ，承認・拒否を決定する．
$H(s') = H(s) \rightarrow accept$
$H(s') \neq H(s) \rightarrow reject$

## 5 安全性の定義

本稿では，計算量に制限がなく $E(A, s)$ を知っている攻撃者のオフライン攻撃に対する安全性を考える．

Fuzzy vault scheme の場合，$E(A, s) = V = \{(x_i, y_i)\}_{i=1}^{r}$ である (3.2.1 を参照)．攻撃者は知ってる $V$ を用いて次のような多項式 $f$ をすべて計算する．

$$\#\{(x, y) \in V | f(x) = y\} = t$$

これらの $f$ から任意に 1 つ選び，対応する $s$ と $V$ を用いて生体情報 $A$ を復元する (攻撃①)．登録時の $f$ と同じものを選ぶことができれば，攻撃成功とする．このとき，登録時の生体情報 $A$ と同じものを得ることができるので $V$ と $A$ を用いてなりすますことができる．

Fuzzy commitment scheme の場合, $E(A, s) = C = g - A$ である (3.1.1 を参照)．攻撃者は $C$ から $g$ を推測し，これと $C$ から $A$ を復元する (攻撃②)．登録時の $g$ と同じものを選ぶことができれば，攻撃成功とする．このとき，登録時の生体情報 $A$ と同じものを得ることができるので $C$ と $A$ を用いてなりすますことができる．

攻撃①の成功確率を $P^V$，攻撃②の成功確率を $P^C$ とする．

**定義**

$P^V \leq \epsilon$ や $P^C \leq \epsilon$ となる認証システムを $\epsilon$ 安全と呼ぶ．

$\epsilon$ が十分小さい値であるとき，認証システムは安全であるという．

# 6　既存研究の認証精度と安全性

大木ら [4]，Jain ら [5] によって提案された Fuzzy vault scheme を用いたマニューシャマッチング方式の手法の本人拒否率 (FRR)，他人受入率 (FAR) と $P^V$ の値を表 1 に示す．表 1 より，大木らの手法も Jain らの手法も下に示したパラメータ設定ではオフライン攻撃の成功確率が 1 となり安全ではない．

$$P^V = \frac{q^{r-k}}{\binom{r}{t}(q-1)^{r-t}} \quad (1)$$

$q$ :RS 符号のガロア体の位数
$k$ : 秘密情報 $s$ の要素数
$t$ : vault $V$ の正しい情報の要素数
$r$ : vault $V$ の要素数 (ダミーを含む)
$(k \leq t \leq r \leq q)$
大木らの手法:$(q, k, r, t)$=$(2^8, 4, 270, 20)$
Jain らの手法:$(q, k, r, t)$=$(2^{16}, 7, 224, 18)$

表 1: 既存研究における認証精度と安全性

| | 大木らの手法 | Jain らの手法 |
|---|---|---|
| FRR | 0.055 | 0.09 |
| FAR | 0.004 | 0.0013 |
| $P^V$ | 1 | 1 |

# 7　提案手法

## 7.1　提案手法

Fuzzy Commitment Scheme を指紋マニューシャマッチングに適用した手法を述べる．

$q = 2^m$ として指紋画像を $q$ 個の小長方形画像に分割し，各小長方形画像から最も信頼度の高いマニューシャをひとつ選ぶ．小長方形画像にマニューシャが存在するときはマニューシャ情報を 2 値データ $m-1$ ビットであらわし，最後に 1 を付加する．マニューシャが存在しないときはランダムな 2 値データ $m-1$ ビットであらわし，最後に 0 を付加する．各小長方形画像に対して作られた $m$ ビットの 2 値データを小長方形画像情報と呼ぶ．よって小長方形画像情報は，マニューシャの存在と不在で最下位ビットが異なるため値が一致することはない．認証指紋 $A'$ の各小長方形画像情報は，マニューシャ存在小長方形画像は登録時と同様であるが，不在小長方形画像は消失記号とする．よって $A'$ の要素 $a'_i$ が消失記号であるとき，得られる $g'$ の要素 $g'_i$ も消失記号となる．このとき，$g'$ が復号条件を満たせば秘密情報 $s$ が復元される．

## 7.2　実験

指紋リーダ U.are.U 4500 を用いて，学生 15 人の右手人差し指の指紋画像 (225 pixels× 313 pixels) を各 5 枚採取する．次に NIST の特徴点抽出ソフトウェア NBIS[6] を用いてマニューシャに関する情報を取得し，信頼度 50 以上のマニューシャの角度 (3 ビット)，隆線数 (3 ビット) の情報を用いる．

指紋画像を 28 pixels × 19 pixels の小長方形画像 120 個と 28 pixels × 18 pixels の小長方形画像 8 個に分割する．分割のときは，指先を上にして左上隅から順番に左から右へと 8 個ずつ，重なりやすき間がないように分割し，下のほうに降りてきながらこれを繰り返す．一番最後の小長方形画像は用いない．よって 127 個の小長方形画像を得る．小長方形画像情報を分割した順序に従って並べ，長さ 127 の $m$ ビット 2 値データの列を得る．本稿の実験では，画像を $x$ 方向に ±14 pixels ずつ ±56 pixels まで，$y$ 方向に ±10 pixels ずつ ±40 pixels まで平行移動させて位置補正を行った．

実験環境を表 2 に示す．自作したマッチングアルゴリズムにおいて Fuzzy commitment scheme の適用前は EER= 0.11 であった．適用後の FRR, FAR, $P^C$ を表 3 に，Fuzzy commitment scheme の適用前後の ROC カーブを図 2 に示す．

$$P^C = \frac{(2p^p(1-p)^{1-p})^q}{q^k} \quad (2)$$

$p$ : 各小長方形画像のマニューシャの出現確率

ここで commitment 生成に用いられたマニューシャの個数の平均値は 40 であった．よって我々は，各小長方形画像のマニューシャ出現確率の平均値で $p$ を近似し，$p = \frac{40}{127}$ として $P^C$ を計算した．

表 2: 実験環境

| ツール | 仕様 |
|---|---|
| 指紋リーダ | Digital Persona U.are.U 4500 |
| 開発ソフト | Core2Duo CPU 3.16GHz 4GB<br>MATLAB R2009a |

表 3: 提案手法における認証精度と安全性

| | $k=1$ | $k=2$ | $k=3$ | $k=4$ |
|---|---|---|---|---|
| FRR | 0.29 | 0.42 | 0.55 | 0.66 |
| FAR | 0.0045 | 0.0012 | 0.0006 | 0 |
| $P^C$ | 1 | $2^{-1}$ | $2^{-5}$ | $2^{-12}$ |

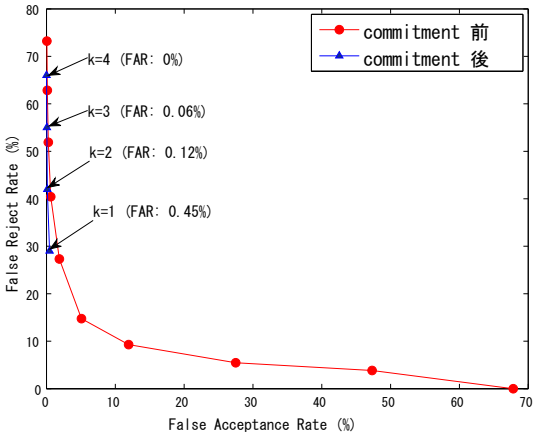

図 2: ROC カーブ

表 1，表 3 に示した結果から，提案手法は大木ら [4]，Jain ら [5] の手法よりも認証精度が大きく低下することがわかる．また，安全性においても高い攻撃成功確率を示しており，決して安全であるとは言えない．ただし，本実験の過程において，認証精度低下の原因や安全性向上のためのいくつかの知見を得ることができた．簡単にではあるが，次章以降でそれらについて述べたい．

## 8 実験結果に対する考察

本実験において，高い認証精度は得られなかった．この原因として以下が考えられる．

(1) 位置補正の最大 (±56pixels)×(±40 pixels ) を上回るずれや，回転によるずれには対応できなかったこと．

(2) 分割する小長方形画像の大きさや採用マニューシャの信頼度情報が最適ではないこと．

(1) に関しては，ソフトウェアに MATLAB を用いたため，RS 符号の復号処理速度が極端に遅くなり，これ以上の範囲では位置補正が困難であった．今後はより高速なソフトウェアを用いて実装し，十分な位置補正を行えるようにしたい．

(2) に関しては，マニューシャの各情報分布などの統計を取り，最適な画像分割方法やマニューシャの信頼度情報の適用方法を検討したい．

また，マニューシャ分布の統計から $p \approx \frac{1}{2}$ となるような小長方形画像を用いることで，安全性は向上すると考えられる．

## 9 まとめと今後の課題

本稿では，Fuzzy commitment scheme を指紋マニューシャマッチングに適用した実験と評価を行った．その結果，認証精度，安全性ともに満足のいく結果とはならなかった．しかしながら，提案手法もマニューシャの情報や分布の統計をもとに，適切に画像分割や位置補正を行うことで，認証精度と安全性の向上が望める．よって今後は，マニューシャに関する統計調査を行い，提案手法が安全で性能のよい認証アルゴリズムになりうるかどうか検証していく．

## 参考文献

[1] A. Juels and M. Wattenberg, “A fuzzy commitment scheme,” 6th ACM conference on Computer and communications security, pp.28-36, 1999.

[2] A. Juels and M. Sudan, “A Fuzzy Vault Scheme,” IEEE International Symposium on Information Theory, pp. 408, 2002.

[3] 武藤祐貴, 井沼学, 今井秀樹, “指紋認証における Fuzzy Commitment Scheme と Fuzzy Vault Scheme の安全性の評価と比較,” SCIS2009, 1E2-4, Jan 2009.

[4] 星勇輔, 大木哲史, 山崎恭, 小松尚久, 笠原正雄, “Fuzzy Fingerprint Vault Scheme におけるダミーデータ生成手段に関する考察,” SCIS2007, 3C1-3, Jan 2007.

[5] K. Nandakumar, A. Jain and S. Pankanti, “Fingerprint-based Fuzzy Vault: Implementation and Performance,” IEEE Transactions on Information Forensics and Security, Volume 2, Issue 4, pp.744-757, 2007.

[6] “NIST Biometric Image Software,” http://fingerprint.nist.gov/NBIS/