2006年度 卒業論文

指紋がキーとなる金庫
“Indexed Fuzzy Vault ”の開発

電子情報学部 情報メディア学科

3ADM1117　大貫 泰紀
3ADM3225　高橋 佑介

指導教員 菊池 浩明

目 次

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から，パスワードに代わって生体認証の利用が進んできた．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，生体情報から不変の情報を得ることは難しく，常に不完全な情報から認証しなければならない．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 [1]．Fuzzy Vault Scheme は以下の特徴を持つ．

1. 登録情報は任意に選ぶことが出来る．
2. 登録情報，認証時の情報は順序を気にする必要がない．
3. 登録情報と認証時の情報の大部分が一致していれば抽出が出来る．
4. 秘密情報はシステムに保管しないため安全性が高い．

指紋認証に Fuzzy Vault Scheme を適用する場合，指紋画像から得られた情報を RS 符号により復号する．生体情報から得られる情報の順番は一定でなく，認証時は登録情報と同じ順番で得られるとは限らない．しかし，RS 符号は登録情報と同じ順番に情報を並べないと復号することが出来ない．

Uludag らは誤り訂正符号を使用せず，ラグランジェ補間法を用いた手法を提案している [2]．しかしながら，多項式補間のために複数のマニューシャ候補の中から総当たりによる復号処理の必要があり，相応の計算時間を要する．

一方，大木らは符号多項式の情報ビットを全て破棄し，検査符号とマニューシャを対応付けることでテンプレートの安全性を高めている [3]．しかしながら，大木らの方式には特徴量の抽出方法に 4.6 節で述べる問題があり，認証精度が低い．

そこで本稿では，インデックスの付加と最小距離マニューシャマッチングによる Fuzzy Vault Scheme を提案する．マニューシャにインデックスを付加することで情報ビットの入れ替わり問題に対応でき，RS 符号の適用を可能とする．また，ユークリッド距離が最小となるデータを抽出することで，計算時間が短縮される．

本論文では，Juels らによる基本となる Fuzzy Vault Scheme の概要を述べ，提案方式の実装に基づいて特徴量抽出法，マッチング方式の評価を行う．

2 Fuzzy Vault Scheme

2.1 概要

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秘匿する暗号方式である．秘密情報 s を任意の情報 A を用いて暗号化 (ロック) する．復号 (アンロック) には，A と同様な形式を取る情報 B を用い，A と B の大部分が一致していた場合のみ，誤り訂正符号により s を復元する．

Fuzzy Vault Scheme は，多項式復元問題とチャフの付加によって情報理論的に安全性が保たれている．Vault R の値から元の多項式を復元するのは，[1] によると，サイズ r の Vault R から正しく t 個の組 (マニューシャ) を選ぶには，$\mu > 0$ について，

$$\frac{\mu}{3} q^{k-t} \left(\frac{r}{t}\right)^t$$

個の場合の数 (多項式数) が存在し，たとえば体の大きさ $q = 10^4$ から $t = 22$ 個の正しい点を選ぶには，2^{86} 通りの組み合わせが存在し，困難である．

2.2 ロック過程

まず，秘密情報 s と任意の情報 $A = \{a_1, a_2, \ldots, a_n\}$ を用意する．s から生成したランダムな多項式 p の，A の要素 $\{a_1, \ldots, a_n\}$ に対する射影を求めて，

$$(x_i, y_i) = (a_i, p(a_i))$$

を得る．ここで $p(0) = s$ とする．さらに，$i = n+1, \ldots, r$ について，$x_i \notin A$，$y_i \neq p(x_i)$ となるような，チャフと呼ばれる擬似データ群 (x_i, y_i) を追加する．最後に，A から得たデータとチャフの判別を困難にするように順番をシャッフルする．これを Vault(ロック情報) R とする．

2.3 アンロック過程

A と同じ形式を持つ情報 $B = \{b_1, b_2, b_3, \ldots, b_n\}$ を用いて，Vault R から b_i と一致するデータ x_j を探索し，これを (b_i, y_j) の組を集合 Q に追加する．このとき，A と B の値の大部分が一致していた場合，Q からアンロックが行われ，s を得る．

3　誤り訂正符号

元のデータに冗長なデータを付加することで，元のデータの一部にエラー (誤り) が起きてもエラーを訂正し元のデータを復元できる符号を誤り訂正符号という．信頼性が要求されるサーバのシステムや，信頼性の低い通信手段などに用いられている．

3.1　Reed-Solomon 符号

Reed-Solomon 符号 (以下，RS 符号) は巡回符号の一つで，数学的にバースト誤り (連続した誤り) を訂正することが出来る誤り訂正符号である．高い訂正能力を持っており，CD や DVD などの記憶装置，ADSL などの通信分野などに用いられている．近年では RFID や QR コードなど幅広い場面で利用されているが，他の誤り訂正符号に比べ複雑な演算が必要になるため計算に多くの時間がかかってしまうという難点がある．

3.2 誤り訂正の処理過程

RS 符号は大きく分けて符号化，復号の処理に分かれる．

3.2.1 符号化

RS 符号では全ての計算を，2 を法とした次数 p のガロア拡大体 $GF(2^p)$ 上で行う．ガロア体とは要素が有限で四則演算が閉じている集合のことで，例えば 2^p の要素を持つ体を 2^p のガロア拡大体と呼ぶ．ガロア拡大体を生成方法はいくつかあるが，ここでは割愛する．

RS 符号は，(n, k)RS 符号と定義できる．n はブロック長，k は情報符号長とする．$n-k$ が検査符号長となり，$t = (n-k)/2$ が誤り訂正可能最大数となる．符号化には原始多項式と呼ばれる既約多項式の中の特別な多項式を用いる．また，原始多項式とは別に生成多項式と呼ばれる訂正能力に大きく関わる多項式を用意する必要がある．生成多項式は GF の元が根となるような多項式であり，$(x-\alpha)(x-\alpha^2)(x-\alpha^3)\cdots$ のように表すことが出来る．符号化したい情報を $V(x)$，生成多項式を $G(x)$ とすると，符号多項式 $W(x) = x^{2t} \cdot V(x) + R$ となる．ただし $R = x^{2t} \cdot V(x) \bmod G(x)$ とする．

3.2.2 復号

まず，受け取った多項式 (受信多項式) に誤りがあるかチェックし，誤りがある場合は復号を行う．誤りのチェックには受信多項式 $Y(x)$ に生成多項式の根を代入し，全ての根において値が零となれば誤り無しであることが分かる．ひとつでも非零となる場合は受信多項式に誤りが存在する．

誤りを訂正する場合は，x^{2t} を根を代入した値を多項式表現したシンドローム多項式と呼ばれる多項式で除算し，剰余などから誤り位置を特定する誤り位置多項式，誤り数値を特定する誤り数値多項式をそれぞれ生成する．これらの多項式から誤りの位置，数値を特定し訂正することで，符号多項式を復元することが出来る．

3.3 予備実験

3.3.1 “誤り訂正符号を用いた指紋復元君の開発”

RS 符号を用いた予備実験として，誤り訂正符号を用いた指紋復元君 (以下，指紋復元君) を開発した．これは指紋画像から特徴点を抽出し，これらを情報符号として符号化する．このとき得られた検査符号を保持しておく．次に改ざんを施した指紋画像を用意し，同様に特徴点を抽出する．これを情報符号として，保持していた検査符号を組み合わせることで復号を行う．改ざんが誤り訂正能力以内であれば復号が成功し，元の指紋画像から得られた特徴点を復元できる．図 1 に指紋復元君の実行画面を示す.

3.3.2 プログラム概要

プログラムは以下のファイルからなる．なお，NFIS2 については 5.1.2 節にて詳述する．

- RS.java
  RS 符号の計算を行うプログラム．GF の大きさ，誤り訂正能力，秘密情報数などを任意に設定できるようにした.

- Point.java
  NFIS2 のパッケージ MINDTCT を使って生成される MIN ファイルを読み込み，指紋画像に分岐点には緑、端点には赤をつけた画像を出力するプログラム．MIN ファイルとは特徴点の座標や特徴点の種類などが書かれたテキストファイルである．

- MainFrame.java
  上記 2 つのプログラムを統合し，GUI で改ざんを施した画像の特徴点の誤りを訂正するプログラム．プログラムの流れとして，指紋画像の特徴点を抽出し，画像を 5×5 の合計 25 のエリアに分割する．次に各エリア内の特徴点をカウントする．これら 25 エリアの特徴点の数を情報符号とし，符号化することで検査符号を得る．そして、改ざんした指紋画像にも同様の処理を行い，得られた情報符号と検査符号を組み合わせて復号を行うことで誤りの位置と数値を求め，訂正する．なお RS 符号は，(31,25)RS 符号と (63,25)RS 符号を選択可能にした.

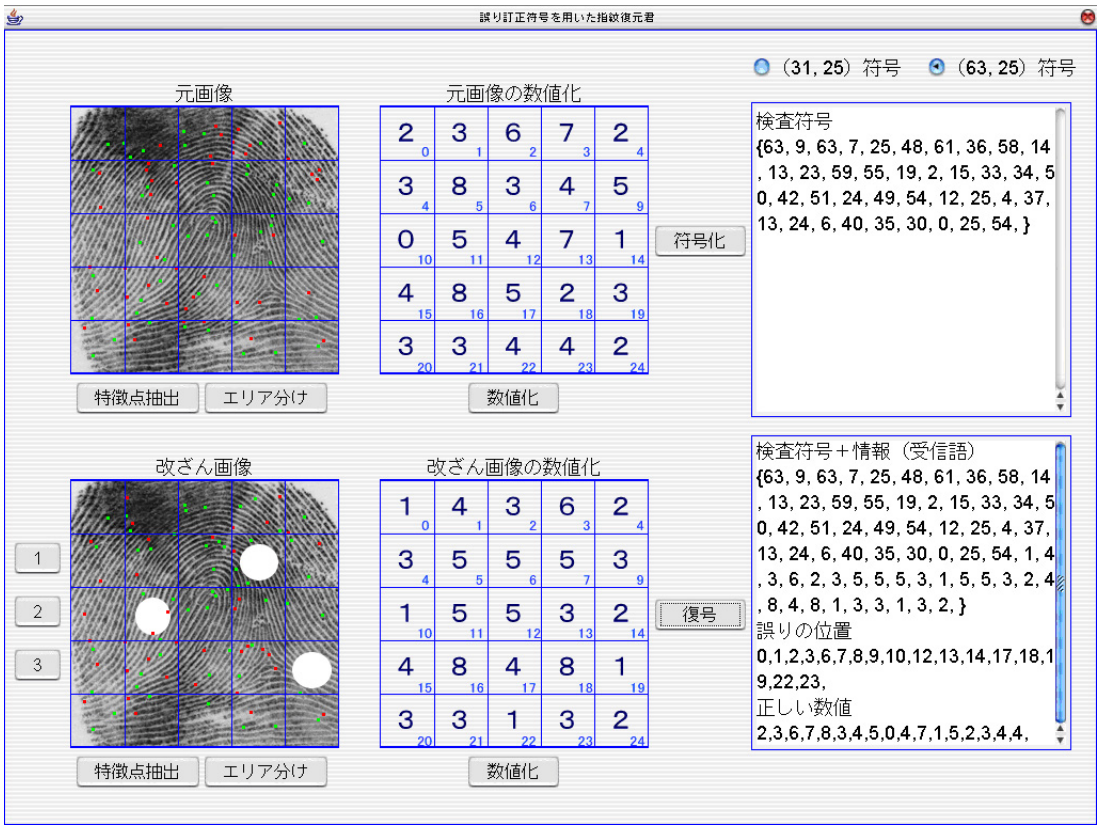

図 1: 指紋復元君の実行画面

次に，各ボタンの機能について説明する．

- 「特徴点抽出」ボタン
  指紋画像の特徴点の抽出を行う．今回は特徴点の抽出アルゴリズムに NFIS2 を使用し，分岐点と端点にそれぞれ緑，赤の点をつけて表示した．分岐点とは指紋の隆線が分かれている部分，端点とは隆線が途切れている部分のことを指す．図 2 に分岐点，端点の例を示す．

- 「エリア分け」ボタン
  指紋画像を 5 × 5 の合計 25 のエリアに分割する．今回は 1 つのエリアを 50 × 50 ピクセルに分割した．エリア分割の例を図 3 に示す．

- 「数値化」ボタン
  エリアごとの特徴点を数える．このとき分岐点，端点の区別はつけずに数える．

- 「符号化」ボタン
  「数値化」ボタンで得られた数値を情報符号とし，RS 符号で符号化することで検査符号を得る．

- 「復号」ボタン
  改ざん画像から得られた情報符号と検査符号を用いて誤りを訂正する．

- 「１」・「２」・「３」ボタン
  改ざん画像の切り替えを行う．

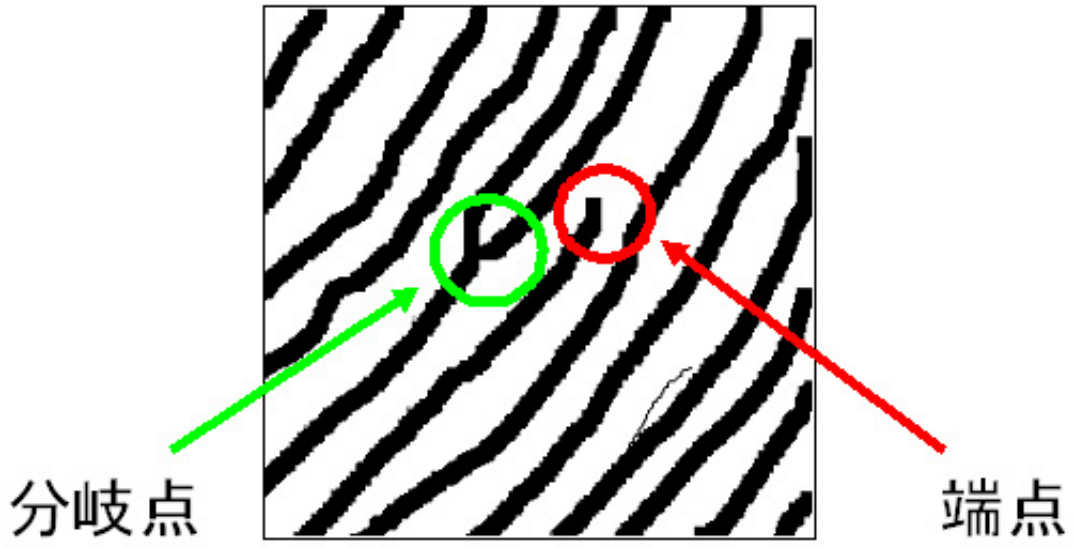

図 2: 分岐点，端点の例

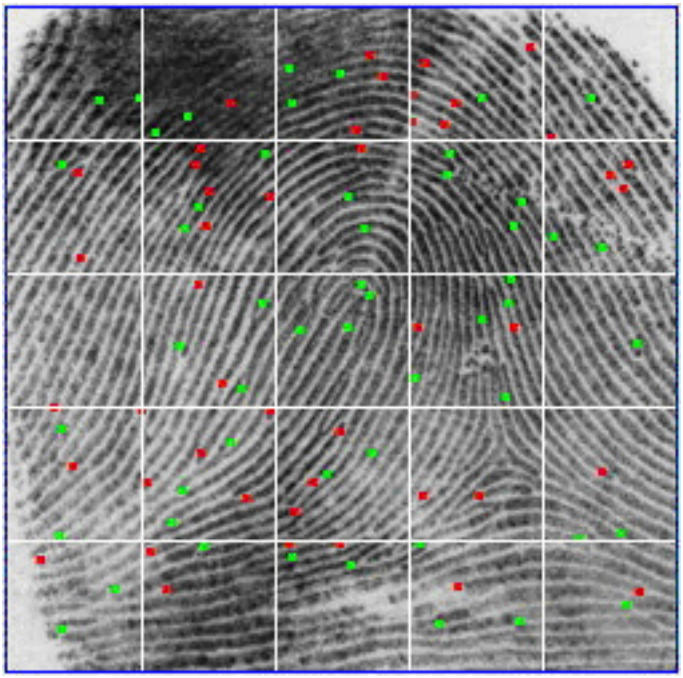

図 3: エリア分割の例

3.3.3 特徴量計算

特徴量として，エリアごとのマニューシャ数を用いた．マニューシャの抽出にはNFIS2を使用した．一つのエリアを一つのブロックとし，25ブロックの情報符号とした．

3.3.4 実験環境

予備実験は以下の環境で実験をした．

表 1: 諸元

元指紋画像	1枚
改ざん指紋画像	3枚
誤り訂正符号	RS符号
誤り訂正可能エリア	3，19エリア
マニューシャ抽出	NFIS2[6]
指紋リーダー	Digital Persona U.are.U4000
開発ソフト	Digital Persona Gold SDK 2.5.0 Java version 1.5.0_06

3.4 評価

用意した3種類の改ざん画像のうち，3エリアまで訂正可能な符号では訂正できず，19エリアまで訂正可能な符号のとき2枚が訂正可能だった．19エリア誤り訂正符号を用いても訂正できなかった理由として，マニューシャの変動が激しいことが挙げられた．改ざんを加えた画像を保存した際に，画質が劣化したため，正しくマニューシャ抽出が行えなかったと思われる．なお指紋復元君ではNFIS2で用意されているサンプル画像を使用しているが，U.are.Uで取得した画像に対して同様の処理を行った場合，この様な現象は確認されなかった．

4 Indexed Fuzzy Vault

4.1 概要

本方式では，情報 A としてマニューシャの x 座標，y 座標の値を連結した値を使用する．Fuzzy Vault Scheme で RS 符号を適用するには，情報 A と B の一致したデータを元の符号語の順に並べ替える必要がある．この問題を解決するために，登録情報のマニュ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．マッチング処理は，Vault R と特徴量 B でユークリッド距離を最小の距離となるデータの組を選ぶ．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復元できる．

4.2 処理方式

提案方式は登録 (ロック) と認証 (アンロック) の 2 つのフェーズより構成される．

4.2.1 登録 (ロック)

Step 1. 指紋マニューシャの x 座標，y 座標を取得し，これらの座標を連結し，サイズ n の特徴量 $A = \{a_1, a_2, \ldots, a_n\}$ とする．

Step 2. 秘密情報 s を RS 符号で符号化した多項式 p と特徴量 A から，$(x_i, y_i) = (a_i, p(a_i))$ とする．各マニューシャ $i = 1, \ldots, n$ について，y_i にインデックス i を付加し，Vault $R = \{(1, x_1.y_1), \ldots, (n, x_n, y_n)\}$ とする..

Step 3. $i = n+1, \ldots, r$ について，チャフとして $x_i \notin A$，$y_i \neq p(x)$ となる (x_j, y_j) をランダムに生成し，Vault R を

$$R = R \cup \{(i \bmod n, x_i, y_i)\}$$

と更新する．この Vault R の大きさ $|R| = r$ がセキュリティパラメータとなる．ここで，同じインデックスの要素が r/n 個存在し, その内 $(r/n) - 1$ 個がチャフである．

Step 4. 最後に Vault R の要素をシャッフルし，ロック情報とする．

4.2.2 認証 (アンロック)

認証時には Vault R と (自分の) 新たな特徴量 $B = \{b_1, b_2, \ldots, b_n\}$ を用いて，s をアンロックするための Q を次のように求める．

Step 5. $i = i, \ldots, n$ について，b_i と R の要素中の $\{x_1, \ldots, x_r\}$ との間の全てのユークリッド距離

$$d(b_i, x_j) = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}$$

を求める．(j^*, x_{j^*}, y_{j^*}) を $d(b_i, x_{j^*})$ が最小でかつ (j^*, x_{j^*}, y_{j^*}) となる R の要素とする．そして Q を

$$Q = Q \cup \{(i^*, x_{j^*}, y_{j^*})\}$$

と更新する．$r \gg n$ なので，この条件を満たす要素は必ず存在する．

Step 6. 得られた Q をインデックス i 順に並べ替えて符号語とみなし，RS 符号の復号計算を行う．

Step 7. 復号したデータに対し，ラグランジェの補間式を適用し，秘密情報 s を取り出す．

5　実装，評価

5.1　実装

5.1.1　環境

表 2 に実装環境を示す．マニューシャの抽出には NFIS2 を用いた．RS 符号は独自に実装した．

表 2: 実装環境

ツール	仕様
指紋リーダー	Digital Persona U.are.U4000
開発ソフト	Digital Persona Gold SDK 2.5.0 Java version 1.5.0_06 NIST NFIS2[6]

5.1.2　特徴量抽出

特徴量は NFIS2 より生成される MIN ファイルを用いた．MIN ファイルは指紋画像の特徴点の情報が記録されたファイルで，特徴点の座標は MIN ファイルから参照して開発した．

NFIS2（NIST Fingerprint Image Software 2）とは NIST が開発した指紋画像に関するソフトウェアで 7 つのパッケージからなる．本研究を進めるに当たり使用したパッケージは，指紋画像の特徴点を抽出する MINDTCT，画像のフォーマットの変換をする IMGTOOL である．

以下に NFIS2 で MIN ファイルを作成する方法を示す．

1. 指紋画像のファイルを U.are.U から取得する．ただし，画像の縦横のサイズは等しくする.U.are.U から得られる指紋画像は 500 × 550 の BMP ファイルなので，ペイント等で調整するか別途プログラム等を作る必要がある．

2. TeraTerm などで noisy にログインする．

3. 以下のコマンドで BMP ファイルを JPG ファイルに変換する．
   /usr/local/nfis/bin/cjpeg -grayscale [入力 BMP ファイル] [出力 JPG ファイル]
   なお，その他の NFIS のコマンドを実行する際にもコマンド名の前に

/usr/local/nfis/bin/
と記述すること．

4. 特徴点の座標が書かれた MIN ファイルを作る．
/usr/local/nfis/bin/mindtct [入力 JPG ファイル] [保存ファイル]
mindtct を実行すると (保存ファイル名).brw や.min など複数のファイルが作成される．

例：
/usr/local/nfis/bin/mindtct finger.jpg finger
finger.brw･･･指紋画像を二値化した画像のファイル．ファイル形式は RAW
finger.min･･･抽出した特徴点の情報 (座標など) が記されたファイル．

MIN ファイルは特徴点 1 つに対し，情報が 1 行で記され次のようになる．
MN：MX，MY：DIR：REL：TYP：FTYP：FN：NX1，NY1；RC1:...
以下に主なものの説明を示す．
MN･･･特徴点の識別番号
MX･･･特徴点の X 座標
MY･･･特徴点の Y 座標
DIR･･･特徴点の方向．0〜31 の 32 段階で表され，1 つのエリアの角度は 11.25 °となる．0 が上方向，8 が右方向，16 が下方向，24 が左方向を示す．
REL･･･特徴点の信頼度．0.0〜1.0 で表され，この値が大きいほど信頼できる特徴点である．
TYP･･･特徴点の属性．BIF は分岐点，RIG は端点を示す．

その他詳細は /home/share/Biometrics/NFIS2/doc/nfis2.pdf を参照．

5.2 評価方法

5.2.1 精度

訂正能力 t を固定し，チャフの比率 r/n を変化させた場合と，r/n を固定し t を変化させた場合の 2 つのパターンについて，他人受入率 (FAR)，本人拒否率 (FRR) の変化を求める．ここでは本人の指紋 50 枚を使い，FRR を求めた．FAR については，$i = 1, \ldots, n$ について，r/n 個の候補の中からランダムに 1 要素を選んだときの受理率で算出した．図 4 にチャフの数 $r = n$ としたときの訂正能力 t についての誤り率を，図 5 に訂正能力 $t = 6$ としたときのチャフの比 r/n についての誤り率を，図 6 に FAR と FRR の関係を各々示す．

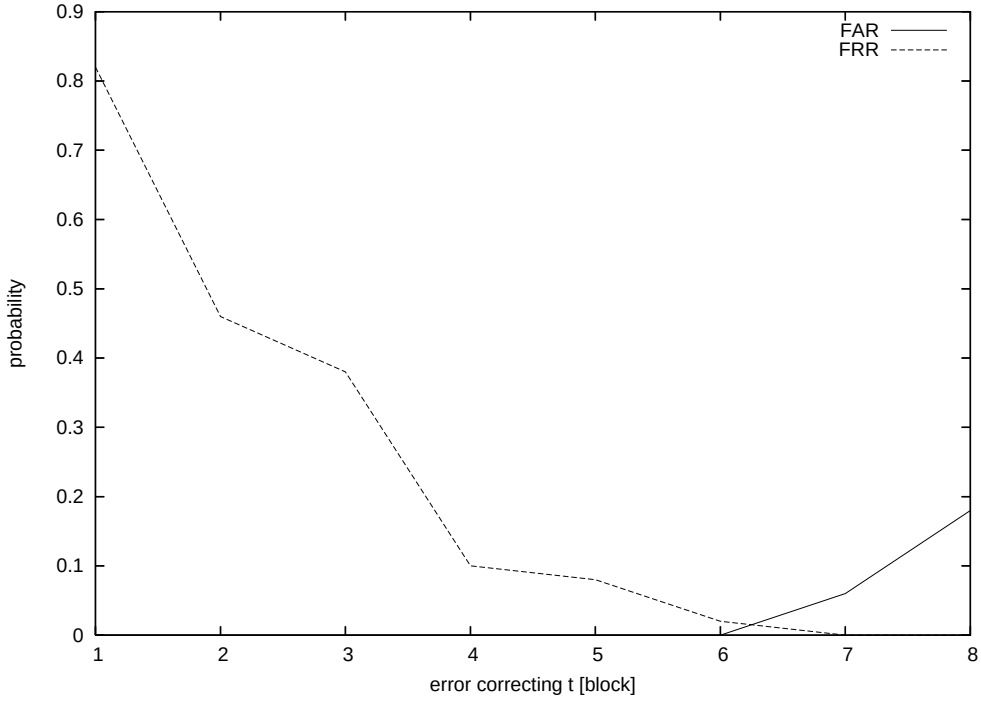

図 4: 誤り訂正能力 t についての誤り率

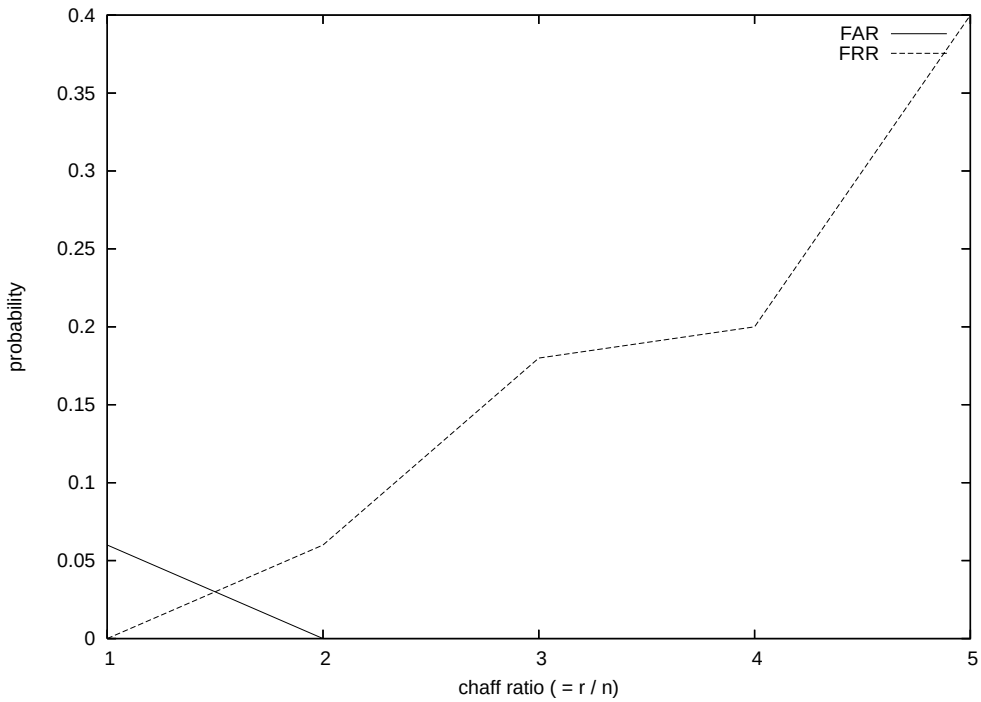

図 5: チャフ比 r/n についての誤り率

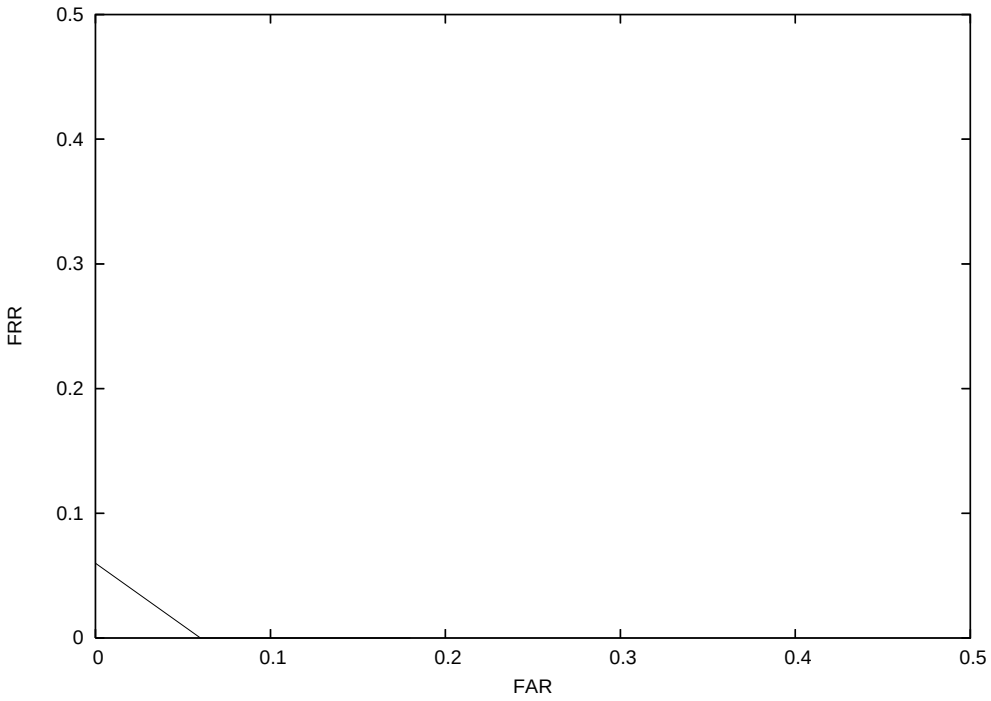

図 6: FAR と FRR の関係

5.2.2 精度の比較

指紋リーダー U.are.U 4000 と指紋認証システム開発キット DigitalPersona SDK に指紋認証機能が提供されている．本提案方式との制度を比較するため，この機能を用いて精度実験を行った．実験方法は以下の通り．

- 被験者 10 人の指 10 本，計 100 本を U.are.U に登録する．
- ひとつの指で 5 回認証を行い，他人受入，本人拒否の回数を求め，FAR，FRR を算出する．

表 3 に各個人の認証率を，表 4 に各指の認証率を示す．また表 5 に U.are.U の認証精度と本方式との精度の比較を示す．

表 3: 各個人の認証率

	他人受入		本人拒否	
名前	FAR(%)	回数	FRR(%)	回数
被験者 A	0	0	0	0
被験者 B	0.0021	21	4	2
被験者 C	0	0	0	0
被験者 D	0	0	8	4
被験者 E	0	0	0	0
被験者 F	0	0	2	1
被験者 G	0	0	0	0
被験者 H	0	0	2	1
被験者 I	0.0010	1	2	1
被験者 J	0	0	0	0
平均	0.0013	13/9900	1.8	9/500

表 4: 指ごとの認証率

	FAR(%)	FRR(%)
親指	0	0
人差し指	0.0010	0
中指	0.0025	4
薬指	0.0015	3
小指	0.0060	2
平均	0.0013	1.8

表 5: Indexed Fuzzy Vault との認証精度比較

	FAR(%)	FRR(%)
Indexed Fuzzy Vault	0	0.02
U.are.U 実測値	0.0013	1.8
U.are.U 公表値	0.001	0.0064

5.2.3 処理時間

最適なガロア拡大体 GF の位数を求めるため，本方式の認証時における処理時間を検証する．図 7 に訂正能力 t[block] についての位数の異なるいくつかのガロア拡大体での処理時間を示す.

図 8 に Uludag らの方式 [2] と提案方式の計算時間の比較を示す．Uludag らの方式は n 個のマニューシャから多項式の次数 $+1$ 個を選ぶすべての組合せを総当りで試行し，正しい秘密情報が復元できるまで繰り返す手法である．マッチングの際に得られた点が 22 個のときの組合せ数は $\binom{22}{n}$ で表せる．一回あたりの試行時間を T[ms] とすると，復号時間は $T\binom{n}{t}$ に比例する．スターリングの近似式を用いると，上限

$$y = \alpha e^{\beta x}$$

で与えられる．ただし，ここで α，β は定数である．すなわち，Uludag らの方式では訂正能力が増えるにつれて処理時間が指数関数的に増加する.

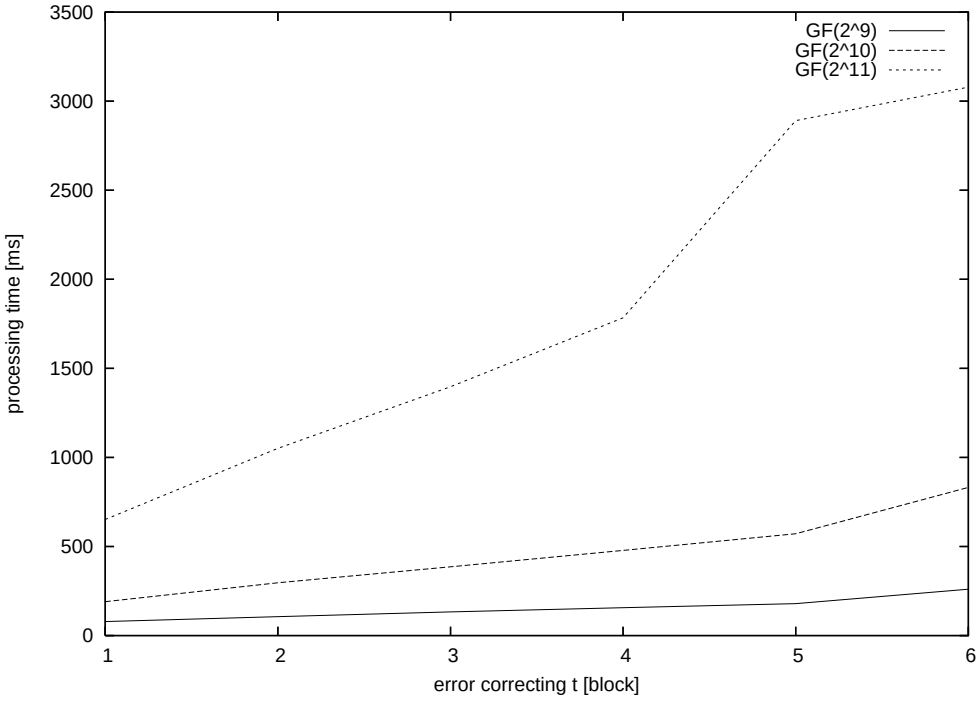

図 7: 誤り訂正ブロック数 t についての処理時間

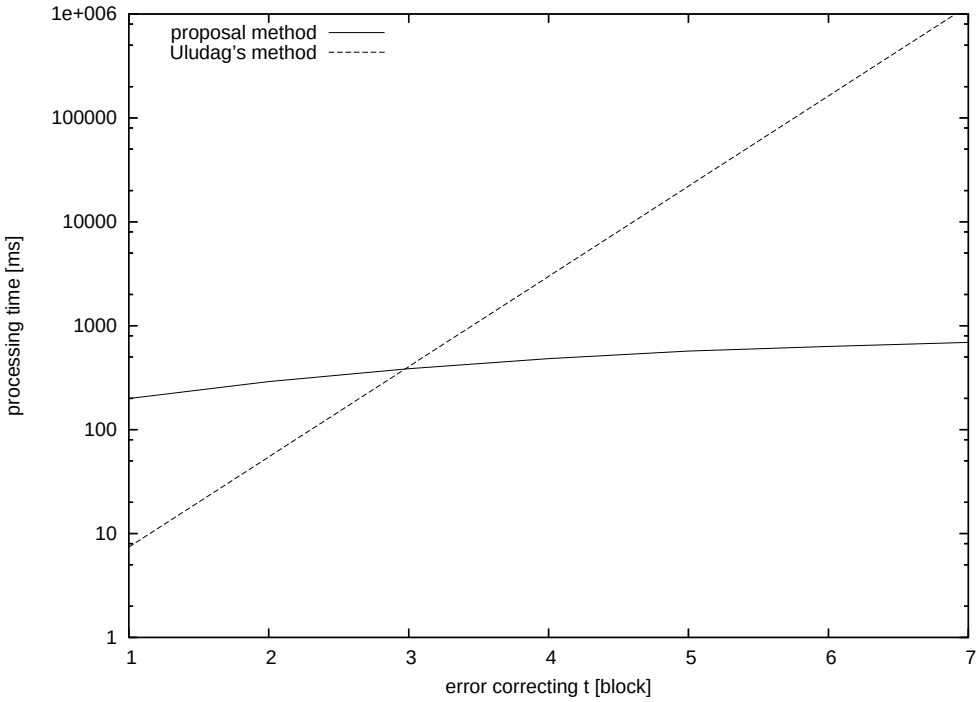

図 8: Uludag 方式 [2] との処理時間の比較

5.2.4 安全性

本方式の安全性はマニューシャ数 n，チャフ数 r，訂正能力 t に依存して決定され，攻撃者がなりすましを行うことができる確率 (FAR) は

$$\left(\frac{1}{r/n+1}\right)^{n-t}$$

となる．したがって，本方式の評価において最も誤りが小さかったときのパラメータは $n=22$，$r=22$，$t=6$ であるので，安全性は 2^{16} となる．公開鍵暗号の安全性は 2^{1024} ということを考えると，安全性は十分とはいえない．今後総当り攻撃への対策としてチャフの数を増やしていく必要がある.

5.2.5 特徴量

大木らの提案する方式 [3] は，マニューシャの成分をビット列で表現しそれらを組み合わせて一つの特徴量として用いている．データは 1 個当たり 8 ビットで表現され，端点 or 分岐点，隆線ベクトル方向，交差隆線数をから計算している．一方，Uludag らは特徴量として x 座標，y 座標をビット列で表現し，それらを連結したものを特徴量として用いている．特徴量は 16 ビットで表現され，x，y 座標をそれぞれ 8 ビットで表現している．図 9 に実験で用いた同一マニューシャ70 個の座標の分布を示す．今回の実験では Uludag らの方式に条件を合わせ，各座標を 5 ビットに正規化し，特徴量を 10 ビットで表現する．実験は同じ指の画像 70 枚に対し 3 つのマニューシャの特徴量をそれぞれの方式で求めた．図 10 に大木ら，図 11 に Uludag らの各方式で計算した特徴量のヒストグラムを示す.

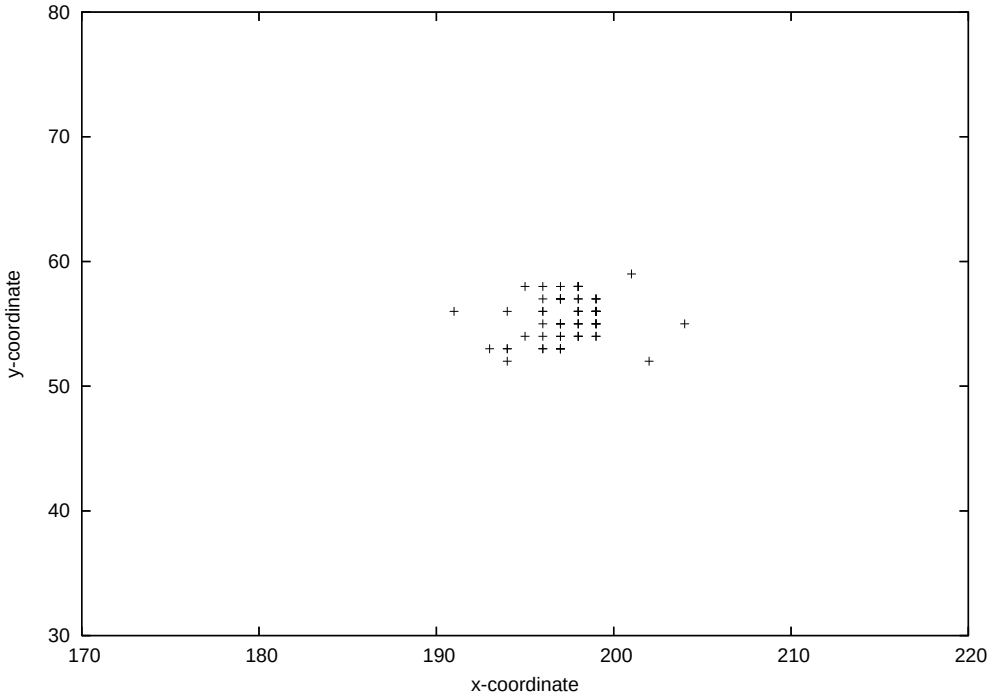

図 9: マニューシャの座標の分布

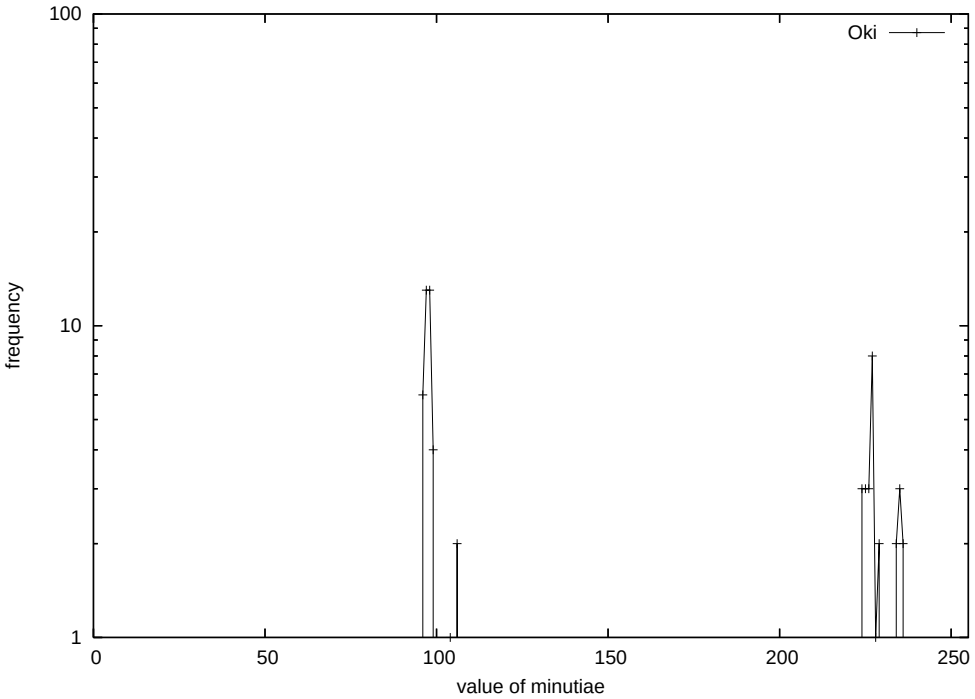

図 10: 大木らの方式 [3] の特徴量のヒストグラム

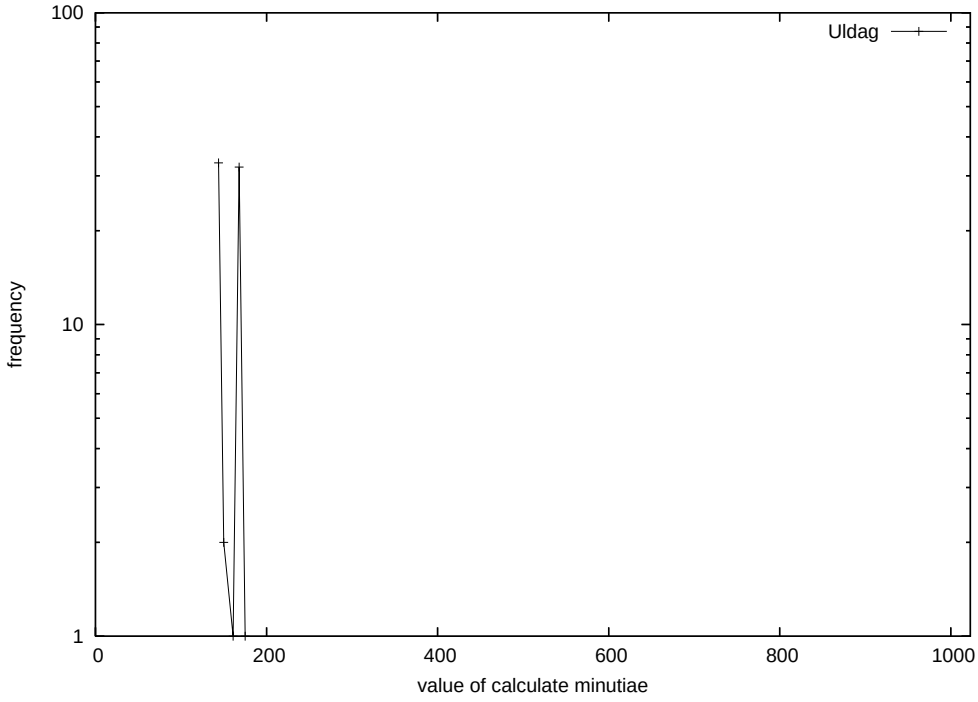

図 11: Uludag らの方式 [2] の特徴量のヒストグラム

5.3 考察

本実験の範囲で最も誤りが小さかったのは$r/n = 1$, $t = 6$のときであり，FAR=0, FRR=0.02 が得られた．ただし，これはマニューシャ1 個に対するチャフの数は 1 個を意味するため，総当り攻撃に対する耐性は十分ではない．

また，表 5 から本方式と U.are.U との認証精度の比較結果は次のようになった．FAR は，U.are.U が 0.0013 に対して本方式は 0 という結果が得られた．FRR は，U.are.U が 1.8 に対して本方式は 0.02 という結果が得られた．ただし，実験環境，すなわち認証回数や使用した指紋画像の枚数などが違うので一概に比較はできない．表 6 に各方式の比較したものを示す. 大木らの方式と Uludag らの方式の 2 つの特徴量は，Uludag らの方式が安定した特徴量を得ることがわかった．大木方式では，マニューシャの端点，分岐点の属性値を MSB としているが，これらの変動が大きいことが原因と考えられる．

表 6: 各方式の比較

方式	特徴量計算	秘密情報復元
Uludag ら	x，y 座標	複数回の秘密分散
大木ら	マニューシャ情報 (分岐 or 端点，隆線等)	複数回の秘密分散
提案方式	x，y 座標	誤り訂正符号 秘密分散

6 おわりに

符号語にインデックスを付加し，データの抽出にユークリッド距離を利用することで，従来の Fuzzy VaultScheme を指紋認証に適用を可能にした “Indexed Fuzzy Vault ” を開発し，評価を行った．その結果，FAR=0，FRR=0.02，このときの処理時間は平均 530[ms] となった．今後の課題として，安全性を高めるために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．また，先行研究の Fuzzy Extractor の調査や指の状態変化を考慮した認証実験を行うことなどが挙げられる．

参考文献

[1] A. Juels, M. Sudan, “A Fuzzy Vault Scheme”, International Symposium on Information Theory, p. 408, IEEE Press, Lausanne, Switzerland, 2002.

[2] U. Uludag, S. Pankanti and A. Jain. “Fuzzy Vault for Fingerprints”, Proc. of Audio- and Video-based Biometric Person Authentication (AVBPA) 2005, pp. 310–319, Rye Brook, NY, July 2005.

[3] 大木，田島，赤塚，小松，笠原，“Fuzzy Biometric Vault Scheme によるテンプレートの安全性に関する一考察”，暗号と情報セキュリティシンポジウム SCIS2005，pp.547-552，2005.

[4] 今井 秀樹，“符号理論”，電子情報通信学会，1990.

[5] 星守，小野令美，吉田利信，“入門数値計算”，オーム社，1999.

[6] “NIST FINGERPRINT IMAGE SOFTWARE 2 (NFIS2)”, http://fingerprint.nist.gov/NFIS/

[7] 大貫，高橋，永井，菊池，“インデックス付マニューシャによる 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.

謝辞

本研究を遂行するにあたって，多くの方々から御指導，御激励を受け賜りました．特に，多大なる御指導を賜りました，東海大学電子情報学部情報メディア学科 菊池浩明教授に深甚なる感謝を申し上げます．

また，多大なるご指導を賜り，本研究を導いて頂きました永井慧氏に深くお礼申し上げます．最後に，本研究に協力して下さった菊池研究室の皆さんに感謝の意を述べると共に，謝辞とさせて頂きます．