社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2007－ＡＶＭ－59（３）
2007／12／13

Fuzzy Vaultを用いた音声データへの指紋データ埋め込み法の検討

李 在熙† 姜 錫† 坂本 雄児†

†北海道大学大学院 情報科学研究科 〒060-0814 北海道札幌市北区北14条西9丁目
E-mail: †leejaehee@mcm.ist.hokudai.ac.jp

あらまし Fuzzy Vaultを用いた音声データへの指紋データ埋め込み法の検討.

キーワード Fuzzy vault, 電子透かし, 指紋認証

An Investigation of an Embedding Technique of Fingerprint data into Sound Data using Fuzzy Vault

JaeHee Lee† Seok Kang† and Yuji Sakamoto†

† Graduate School of Information Science and Technology, Hokkaido University N14, W9, Kita-ku, Sappro, 060-084, Japan
E-mail: †leejaehee@mcm.ist.hokudai.ac.jp

Abstract An investigation of an Embedding Technique of Fingerprint data into Sound Data using Fuzzy Vault.

Keyword Fuzzy vault, Watermark, Fingerprint

1. まえがき

音楽配信とはネットにより音楽を販売するサービスで,簡便性と値段の安さ,1曲ずつ買えるなどのメリットがあり,利用者が増え続いている.

一方,このように配信された音楽は不法コピーなど著作権を侵害する事に対して無防備とも言え,配信後の音楽に対して新たな著作権保護技術が求められている.

また,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バイオメトリクス認証(Biometrics Authentication)の導入が進んでいる.

バイオメトリクス認証とは,人の身体的な特徴の指紋,顔,手の甲の静脈などを用いて認証を行う事を言い,最近はキャッシュカード偽造などを防ぐために多く使われている.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,利便性が高いという利点がある.しかし,生体情報データを紛失し,悪用される可能性があり,生体情報その物を暗号化する必要がある.

本研究では音楽のネット配信サービスと生体認証である指紋認証を融合する事でより,新たな音楽の著作権保護法を提案する.

2. Fuzzy Vault Scheme

2.1. Fuzzy Vault Schemeの概要

Fuzzy vault Scheme[1]とは,完全に一致しない情報を用いて隠したい情報を秘匿する暗号方式の事である.

Fuzzy Vaultには符号化であるロック過程と復号であるアンロック過程があり,以下にその過程について述べる.

2.2. 符号化(ロック過程)

秘密情報sと任意の情報$A=\{a_1,a_2,\cdots,a_n\}$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$\{a_1,a_2,\cdots,a_n\}$に対する射影を求めて,式(1)を求める.[5]

$$(x_i,y_i)=(a_i,p(a_i)) \quad \text{但し,} \quad p(0)=s \qquad (1)$$

さらに,$i=\{n+1,\cdots r\}$について,式(2)の条件をみたす,擬似データ群(x_i,y_i)のチャフというのを加える.

$$x_i \notin A, \quad y_i \notin p(x_i) \qquad (2)$$

最後にAから得られた値とチャフの順番を混ぜ,判別がつかないようにし,ロック情報とする.

2.3. 復号化(アンロック過程)

Aと同じ形式を持つ情報$B=\{b_1,b_2,\cdots,b_n\}$を用いて,ロック情報から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. 指紋認証

3.1. 指紋認証の概要

指紋は人それぞれ異なる特徴があり，一生変わらないので，他の人と区別する重要な個人情報の一つとして用いられる．

指紋認証はバイオメトリクスセキュリティの中で最も普及されており，他のバイオメトリクスセキュリティより，多様な分野で応用されている．身近な例として，クレジットカードや，携帯電話，家の鍵という所にも用いられている．

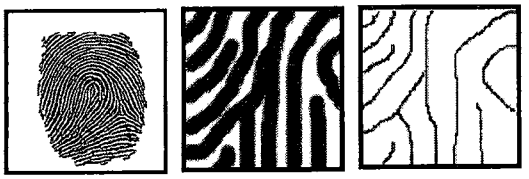
また，指紋認証は他のバイオメトリクスセキュリティに比べて，端末機が比較的小型である事と，初期設置費用が安く済むという利点がある．

現在，指紋認証では指紋の特徴点情報を用いて認証を行う特徴点方式が最も一般的である．まず，特徴点方式を用いた指紋認証法について述べる．

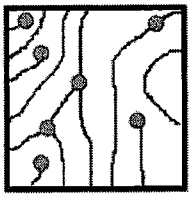
3.2. 指紋認証の過程(特徴点の抽出)

ここでは，指紋認証で最も一般的である指紋の端点や分岐点の特徴点情報を用いて認証を行う特徴点方式について説明を行う．

指紋認証を行うには以下の図１のように大きく４つの過程がある．まず，図 1-(a)認証で使う指紋の撮影からはじめ，撮影されて画像を膨張や収縮し，図１-(b)のように２値化過程を行う．



(a) 指紋撮影　(b) 2 値化画像　(c) 細線化



(d) 特徴点の抽出

図１特徴点抽出処理の流れ

そして，図１-(c)の細線化を行い，できるだけ指紋の特徴点を抽出するのに必要な画像情報だけを残す．これらの過程より図１-(d)のように特徴点を選択することが出来る．

3.3. 指紋認証の問題点

これまでの説明では，指紋がどのように使われ，どのような特徴を持っているかについて述べた．

近年，個人情報が悪用されて金銭的な問題などの被害が起きたというニュースも少なくなく耳にする．指紋は個人特有の個人情報でも言え，悪用される可能性が非常に高いのである．また，指紋は住所や電話番号の個人情報とは異なり，一生変わらない個人情報であるので，指紋情報が一度盗まれてしまうと一生その個人情報は使えなくなるのではなく，自分がいる限り開悪用され続けるのである．

図２はテンプレートマッチング法と言う指紋認証法である．

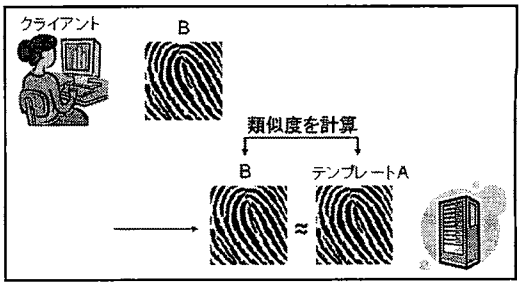


図２テンプレートマッチング法

図２のテンプレートマッチング法は事前にサーバー側に登録しておいた指紋データと認証を行う指紋との類似度検査を行い，２つの指紋が一致すれば認証できる仕組みである．しかし，この方法だと，サーバー側に指紋をそのまま登録したり，送信したりするので万が一その指紋データが盗まれてしまうと非常に危険度が高いのである．指紋データが盗まれても元の指紋は特定できない指紋その物を暗号化する技術が求められる．

4. Fuzzy Vault を用いた指紋認証

指紋その物が盗まれて悪用される対策として Fuzzy Vault を用いた指紋認証法の考え方が考案されている．

図３は Fuzzy Vault を用いた指紋認証法の全体的な流れを示したものである．秘密情報となる指紋の特徴点データをそのまま公開したり，登録するのではなく，chaff と呼ばれる偽の特徴点情報を加える事で元の指紋データを推測できなくなる方法である．指紋の特徴点データ(秘密情報)に chaff の偽情報を加えたデータを Vault といい，この Vault 値をサーバー側に登録したり，認証を行う時，通信するデータとして用いられるのである．

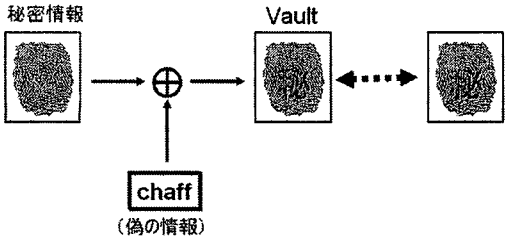


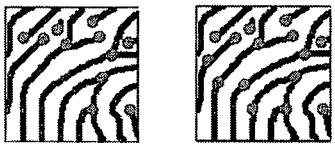
図 3 Fuzzy Vault を用いた指紋認証

4.1. 指紋認証の条件

携帯音楽プレイヤーなどの計算能力が低い端末で指紋認証を行う事と，指紋を電子透かしとして用いるという事には多くの制約がある．ここではその制約を満たす指紋認証の条件について述べる．

(A) 認証を行うたび，特徴点選択の変化が少ない事である．これは指紋認証の精度に関わる問題で指紋認証を行うたび，選択される特徴点が異なってしまうと正しく認証が行えない．

(B) 特徴点が偏れないようにする事である．図 4 -(a)は指紋の特徴点が左側と上の方に偏っている例でこの場合は，図 4 -(b)のように特徴点が分布して例に比べて元の指紋データを推測されやすくなるので機密性が落ちてしまう．



(a) 特徴点が偏る　(b) 特徴点が偏らない

図 4 特徴点の選択

(C) 計算量(計算時間)を少なくする．計算を行なうが能力が非常に低い携帯音楽プレイヤーとなるので可能な限り，計算量を少なくする指紋認証法を考案する必要がある．

(D) Vault 値を小さくする．音楽への電子透かしデータとして用いられるのは Vault 値である．電子透かしの基本的な考え方でもあるが，透かしデータ埋め込み前後の変化が出来るだけ少ない方が安全である．しかし，Vault 値を小さくする事は指紋認証の機密性と関わる問題なので，適正な値を求める必要がある．

5. RS(Reed Solomon)符号

RS 符号は巡回符号の一つで，数学的にバースト誤りを訂正する事が出来る訂正符号である．

RS 符号は高い訂正能力を持っていて，CD や DVD のような記録装置に用いられている．近年は RFID や QR などにも用いられているが，他の誤り訂正符号に比べて複雑な演算が必要で計算時間が非常にかかってしまう問題がある．

6. 音声への指紋データ埋め込み

6.1. 特徴量の計算

4.1 で述べた指紋認証の条件を満たす特徴の計算を次のように求める．

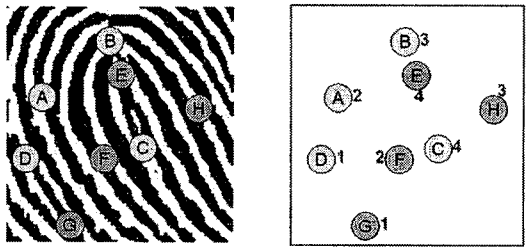
まず，特徴点は端点と分岐点の 2 つとした．端点と分岐点というのは指紋の特徴を示す一番大きな要素であり，確実に特徴点を選択できる利点がある．また，特徴点を 2 つの要素に限った事によって，出来るだけ計算量を少なく出来る．

この特徴点の(x, y)座標から特徴量を求めることとした．特徴量を計算するのに当たって，出来るだけ単純にする事により，誤りを少なくするのが目的である．

6.2. 秘密情報の復元

指紋情報である秘密情報を復元するのに RS(Reed Solomon)符号を用いた．RS 符号は複雑な演算を行なうため，計算時間が多くかかってしまう問題点があったのだが，計算する要素が少ないため復号の計算時間は全体としては大きくないのである．それに，RS 符号は訂正能力が非常に高いとう利点がある．

しかし，RS 符号で指紋の秘密情報の復元をするのには問題がある．認証を行う時，読み込む特徴点の順番と復元を行う時の順番が同じでないと，うまく復元が行なわれないという事である．



(a) 指紋の特徴点と chaff　(b) 順番を示す情報

図 5 秘密情報の復元

そこで，図 5 のように，秘密情報である指紋の特徴点と偽情報である chaff に順番を示す情報を加える事によってこの問題を解決する．

6.3. 特徴点選択の問題点

指紋の特徴点を選択するのに当たって，指紋のひげや，指についた埃，撮影画像のノイズや画質などにより，特徴点がうまく取れない問題がある．特徴点の選択が正しくないと，余計な計算を行なったり，認証率が大きく低下する場合がある．図６は指紋のひげやノイズを示した画像である．

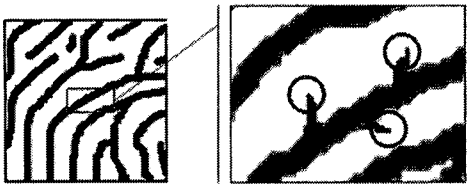


図６指紋のひげ，ノイズ

このような指紋の撮影画像から，正しし指紋を選択するのは困難であると言える．

そこで，指紋のひげや画像のノイズのように非常に短い要素が認識されないようにしきい値を決める事で問題の解決を図った．

7. 指紋認証実験

7.1. 実験環境

認証実験を行ったシステムの環境は以下の表１に示す．

表１実験環境

- システム：Intel Pentium 2.8GHz (1.5GB RAM)
- O.S：Windows XP (SP2)
- 特徴点の計算：NFIS2
  (NIST Fingerprint Image Software 2)

また，秘密情報と chaff 情報は同じ数とし，RS 符号の復元能力を４ブロックとした．

指紋は 10 枚の指紋画像をそれぞれ 5 回ずつ実験を行なった．

これらの環境で計算時間と認証率などを評価する．

7.2. 認証率の評価

表２に認証率の実験結果を示す．指紋Ａ’は上記で説明した指紋のひげや画像のノイズに対して対策を行なってない方法で対策を行なったＡより，認証率が低い．その他の指紋に対しては指紋のひげや画像のノイズ対策を行なった結果である．

表２認証率

	1回目	2回目	3回目	4回目	5回目
指紋Ａ’	○	×	×	×	○
指紋Ａ	○	○	○	○	○
指紋Ｂ	×	○	○	○	○
指紋Ｃ	○	○	○	○	○
指紋Ｄ	○	○	×	○	×
指紋Ｅ	○	○	○	×	○
指紋Ｆ	○	○	○	○	○
指紋Ｇ	○	○	○	○	○
指紋Ｈ	○	○	○	×	○
指紋Ｉ	○	○	○	○	○
指紋Ｊ	○	×	○	○	○

全体の認証率は９２％となった．

7.3. 計算時間の評価

指紋認証にかかった計算時間を図７に示す．

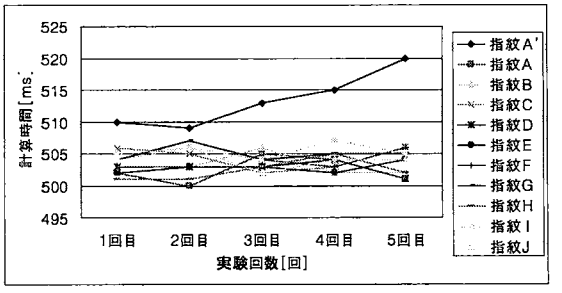


図７計算時間の評価

図７の計算時間の結果によると，指紋のひげや画像のノイズ対策を行なってない指紋 A’は他の指紋に比べて計算時間が長いという結果だった．この理由として，指紋 A’の場合は余計な特徴点まで選択されて他の指紋より計算時間が長くなったと見られる．

8. おわりに

Fuzzy Vault を用いて指紋認証法の実験を行った．撮影画像の状態や指紋の拡大具合により，指紋のひげがはっきりしている指紋に対してはうまく認証がお行えなっかたが，認識される線の長さにしきい値を決めることにより，正しく認証が出来た．また，この調整により，計算時間も短縮された結果となった．

しかし，撮影された画像の状態により，しきい値を決めないと，うまく認証は行えなかった．今後，指紋の状態により，自動的にしきい値が決まるシステムを考える必要がある．また，これらの指紋のデータをどう音声に埋め込むかを考察する．

文　献

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

[2] A. Malickas and R. Vitkus, "Fingerprint Registration Using Composite Features Consensus", Informatica, Institute of Mathematics and Informatics (Vilnius),vol. 10, no. 4, pp. 389-402, 1999.

[3] B. Schoenmakers, F. Boudot, and J .Traor_e. A fair and e_cient solution to the sociaset millionaires' problem. Discrete Applied Mathematics, 2000. To appear.

[4] T. C. Clancy, N. Kiyavash, and D. J. Lin, "Secure Smartcard-Based Fingerprint Authentication", ACM SIGMM 2003 Multimedia, Biometrics Methods and Applications Workshop, pp. 45-52, 2003.

[5] U. Uludag"Fuzzy Vault for Fingerprints",Proc. of Audio- and Video-based Biometric Person Authentication (AVBPA) 2005, pp. 310–319, Rye Brook, NY, July 2005.

[6] 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.