SCIS 2007 The 2007 Symposium on Cryptography and Information Security
Sasebo, Japan, Jan. 23-26, 2007
The Institute of Electronics, Information and Communication Engineers

マニューシャマッチングのウルフに関する理論的考察

A Theoretical Study on Wolves in Minutiae Matching Algorithm

河上 梨恵 * Rie Kawakami
繁富 利恵 † Rie Shigetomi
美添 一樹 * Kazuki Yoshizoe
宇根 正志 † Masashi Une
大塚 玲 † Akira Otsuka
今井 秀樹 * † Hideki Imai

あらまし 本論文では，マニューシャマッチング方式におけるなりすましへの耐性について理論的に考察する．とりわけ，ある与えられたテンプレートとランダムに生成された入力データにおいて，一定数以上の特徴点が一致する確率（マニューシャ衝突率）に着目する．セキュリティ評価方法の一つとして生体認証におけるブルートフォースアタックを前提としたマニューシャ衝突率は，Ratha らによって既に検討されている．ただしその検討では，ランダムに生成した入力データに制限がされている．そこで本論文では，Ratha らの検討結果をもとに，正確なマニューシャ衝突率を導出する．次に，Ratha らが設定した入力データについての制限を外し，マニューシャ衝突率が最大となるような入力データの探索を行う．その結果として，マニューシャ衝突率が Ratha らの検討によって示された値よりもはるかに大きな値となることを示す．

キーワード 生体認証，指紋認証，マニューシャマッチング方式，マニューシャ衝突率，ブルートフォースアタック

1 はじめに

マニューシャマッチング方式とは，生体認証においてテンプレートと入力データの特徴点を照合するアルゴリズムである．指紋認証に用いられる一般的なマニューシャマッチング方式では，隆線の端点や分岐点を特徴点として，その特徴点に 2 次元座標および隆線角度のデータを与え，入力データとテンプレート間におけるこれらのデータを比較するケースが多い．一致する特徴点の数に基づいて類似度を計算し，その値が閾値以上である場合に一致を出力し，それ以外の場合は不一致を出力する．

こうした方式に対して，テンプレートの情報は持たず，入力データを総当りで提示してなりすましを試みる（ブルートフォースアタックと呼ぶ）という状況を考える．ブルートフォースアタックへの耐性を評価する検討としては，ある与えられたテンプレートに対して，ランダムに選ばれた入力データの特徴点が一定数以上一致する確率（マニューシャ衝突率と呼ぶ）が，Ratha らの論文 [1] で既に検討されている．ただし，Ratha らの検討においては，入力データの特徴点数がテンプレートデータの特徴点数と同等の場合のみに制限されており，想定される全ての入力データの集合の，ある部分集合から入力データが選択されるケースに焦点を当てている．また，導出されたマニューシャ衝突率は概算値に過ぎず，正確な確率を示すものではない．

そこで，本論文では，まず Ratha らの式をもとに正確なマニューシャ衝突率を求める式を導出する．また，攻撃に用いられる入力データについての Ratha らの課した条件を外し，マニューシャ衝突率が最大となる入力データを探索する．そうした入力データを用いて，マニューシャ衝突率を計算した結果，Ratha らの検討によって示された概算値に比べ，はるかに大きな値となることを示す．攻撃者が，想定される全ての入力データの集合から最も有利な入力データを選択して，なりすまし試みるという攻撃（ウルフ攻撃と呼ばれる [2]）を採用することを前提とした場合，今回の検討結果は，なりすましが成功する可能性が，Ratha らによる結果から示唆されるものよりも高まる可能性を示しているといえる．

* 中央大学理工学部電気電子情報通信工学科今井研究室，〒 112-8551 東京都文京区春日 1-13-27，Imai lab., Dept. of Electrical, Electronic, and Communication Engineering, Faculty of Science and Engineering, Chuo University, 1-13-27 Kasuga, Bunkyo-ku Tokyo 112-8551, Japan, {d53330@educ.kc,yoshizoe@tamacc}.chuo-u.ac.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 1102 号室, Research Center for Information Security, National Institute of Advanced Industrial Science and Technology 1-18-13 Sotokanda Chiyoda-ku Tokyo 101-0021,Japan, {rie-shigetomi,masashi-une,a-otsuka,h-imai}@aist.go.jp

本論文の構成は以下のとおりである．**2 章**において指紋認証におけるマニューシャマッチング方式について説明する．**3 章**において Ratha らによるマニューシャ衝突率を紹介し，その検討の問題点を示す．**4 章**において正確なマニューシャ衝突率を導出する．**5 章**において **4 章**で導出した正確なマニューシャ衝突率と Ratha らの示したマニューシャ衝突率との比較と，ウルフについての考察をおこなう．**6 章**でまとめる．

2　マニューシャマッチング方式とは

本章では，一般的な指紋認証におけるマニューシャマッチング方式について説明する．

マニューシャマッチング方式とは指紋の隆線から特徴点を抽出し，照合データとテンプレート間の特徴点を照合することで個人を認証するアルゴリズムである．以下でマニューシャマッチング方式のアルゴリズムについて説明する．

指紋認証におけるマニューシャマッチング方式のアルゴリズムは大きく分けて以下のフェーズに分けることができる．

- **指紋画像の獲得** 指紋認証装置に提示された指の指紋画像を獲得する．
- **特徴点抽出** 獲得した画像から隆線の端点や分岐点を特徴点 M_i，$(i = 1, 2, ..., n)$ として抽出する．各特徴点には特徴点データとして，2 次元座標 (x_i, y_i)，と隆線の方向角 d_i を与える．
- **画像登録** 特徴点 $M_{ri} = (x_{ri}, y_{ri}, d_{ri})$ を抽出した画像をテンプレートとして登録する．テンプレートの特徴点の集合を $M_r = M_{r1}, M_{r2}, ..., M_{rn}$ とする．
- **照合** 特徴点 $M_{qi} = (x_{qi}, y_{qi}, d_{qi})$ を抽出した入力データと，テンプレート間の特徴点データの類似度を算出する．入力データの特徴点の集合を $M_q = M_{q1}, M_{q2}, ..., M_{qn}$ とする．
- **結果出力** 算出した特徴点データの類似度の結果が，閾値以上である場合は一致を出力し，それ以外の場合は不一致を出力する．

3　Ratha らによるマニューシャ衝突率

3.1　マニューシャ衝突率の定義

テンプレートの特徴点データが入力データの特徴点データと一致する確率をマニューシャ衝突率とする．本章では，Ratha らの論文による指紋照合におけるテンプレートと入力データのマニューシャ衝突率の計算について紹介する．

3.2　マニューシャ衝突率計算における仮定

Ratha らは，**2 章**で説明したマニューシャマッチング方式を前提に，以下のパラメータ設定の下で分析を行っている．

- テンプレート・入力データの画像サイズ
  $S = 300 \times 300$ 画素.
- 隆線の幅と谷の幅の合計値
  $T = 15$ 画素.
- 特徴点の数の最大値
  $K = S/T^2 = 20 \times 20 = 400$.

3.3　マニューシャ衝突率の導出

まずテンプレートの特徴点を $M_{ri} \quad (i = 1, 2, ..., N_r)$ とする．M_{ri} の各特徴点は，それぞれ 2 次元座標データ (x_{ri}, y_{ri}) と隆線方向角データ d_{ri} を持っている．同様にランダムに選択した入力データの特徴点を M_{qi} $(i = 1, 2, ..., N_q)$ とする．M_{qi} の各特徴点は，それぞれ 2 次元座標をデータ (x_{qi}, y_{qi}) と隆線方向角データ d_{qi} を持っている．このとき，ランダムに生成した入力データの 1 つの特徴点と，テンプレートの特徴点の一致する確率は下記のように表すことができる．

$$p_{est} = \frac{N_r}{K \times d} \tag{1}$$

そこで，入力データの各特徴点がテンプレートに含まれているか否かを順番に検査した結果，N_{q-1} 個の特徴点がテンプレートに含まれていなかったとする．このとき，N_q 番目の特徴点がテンプレートに含まれている確率は下記のようになる．

$$p = \frac{N_r}{(K - N_q + 1) \times d} \tag{2}$$

このため，ランダムに選択した入力データに含まれる 1 つの特徴点がテンプレートに含まれる確率が (2) 式で与えられるとみなしたとき，入力データの t 個の特徴点がテンプレートに含まれる確率は下記のようになる．

$$P_{exact} = \left(\begin{array}{c} N_r \\ t \end{array} \right) p^t \left(1 - p\right)^{N_q - t} \tag{3}$$

(3) 式よりテンプレートとランダムに選択した入力データ間で，ある一定の数 m 個以上の特徴点が一致する確率は，次のように表すことができる．

$$P_{ver} = \sum_{t=m}^{N_q} \left(\begin{array}{c} N_r \\ t \end{array} \right) p^t \left(1 - p\right)^{N_q - t} \tag{4}$$

上記の (4) 式によって表される確率を，Ratha らは本章において定義したマニューシャ衝突率とみなしている．さらに Ratha らは，$N_q = N_r$ において P_{ver} を計算し，以下の近似式を得ている．

$$P_{ver} = \frac{e^{-N_p}}{\sqrt{2\pi m}} \left(\frac{eNp}{m} \right)^m \tag{5}$$

Ratha らは各パラメータに具体的な値を代入して，(5) 式によって示される P_{ver} の値を計算している．

3.4 Ratha らによるマニューシャ衝突率の問題点

本節では，上記で紹介した Ratha らによるマニューシャ衝突率について検討する．まず (2) 式において p は，$N_q - 1$ 個の特徴点がテンプレートと一致しなかったときに N_q 番目の特徴点がテンプレートに含まれる確率を表している．そのため，p の関数である P_{ver} は本論文で定義したマニューシャ衝突率の正確な値を示すものではない．マニューシャ衝突率は P_{ver} を超えることはないため，Ratha らは，P_{ver} をマニューシャ衝突率の概算値を簡便に計算するために用いたものと考えられる．

さらに，$p \leqq 1$ であるから，ランダムに生成する入力データの特徴点数 N_q は (3) 式から $N_q \leqq K - \frac{N_r}{d} + 1$ となり，N_q の値に制限が生じる．また，$N_q = N_r$ という制約も加えている．

ブルートフォースアタックにおいて，攻撃者は全入力データを準備することが可能なので，Ratha らのマニューシャ衝突率はブルートフォースアタックによるウルフの評価ではなく，他人受け入れ率（FAR）の評価となる．

4 正確なマニューシャ衝突率の導出

本章では **3.2 節**の仮定のもと，より正確なマニューシャ衝突率を導出する．

4.1 特徴点の 2 次元座標データのみが一致する確率

まず，入力データをテンプレート間の 2 次元座標についてのみ考える．

テンプレートのある 1 つの特徴点 M_{ri} の 2 次元座標データ (x_{ri}, y_{ri}) と，入力データの特徴点の 2 次元座標データが一致する確率について考える．(x_{ri}, y_{ri}) と入力データのある特徴点の 2 次元座標データが一致する確率は，以下のように表すことができる．

$$\frac{N_q}{K} \tag{6}$$

次に，テンプレートの全特徴点のうち，$n-1$ 個の特徴点の 2 次元座標データ $(x_{ri}, y_{ri}) \quad (i = 1, 2, ..., n-1)$ が，入力データの $n-1$ 個の特徴点の 2 次元座標データと一致したとする．このとき，n 番目の特徴点の 2 次元座標データ (x_{rn}, y_{rn}) が，入力データの特徴点の 2 次元座標データと一致する確率は，以下のように表すことができる．

$$\frac{N_q - (n-1)}{K - (n-1)} \tag{7}$$

以上より，テンプレートの特徴点 M_r の内，n 個の特徴点の 2 次元座標データと，入力データの特徴点 M_q の内、n 個の 2 次元座標データが一致する確率は以下のように表すことができる．

$$\begin{aligned} &\frac{N_q}{K} \times \frac{N_q - 1}{K - 1} \times \cdots \times \frac{N_q - (n-1)}{K - (n-1)} \\ &= \prod_{i=0}^{n-1} \frac{N_q - i}{K - i} \end{aligned} \tag{8}$$

同様に，テンプレートの全特徴点のうち n 個の特徴点の 2 次元座標データが，入力データの特徴点の 2 次元座標データと一致した場合に，残りのテンプレートの $N_r - n$ 個の特徴点の 2 次元座標データが一致しない確率は，以下のように表すことができる．

$$\begin{aligned} \frac{K - N_q}{K - n} \quad &\times \frac{K - N_q - 1}{K - n - 1} \times \cdots \\ &\times \frac{K - N_q - (N_r - n - 1)}{K - n - (N_{\mathrm{r}} - n - 1)} \end{aligned}$$

$$= \prod_{i=n}^{N_r - 1} \frac{K - N_q - (i - n)}{K - i} \tag{9}$$

以上より，各特徴点の 2 次元座標データのみに着目したときに，テンプレートの n 個の特徴点が入力データの特徴点と一致し，残りの $N_r - n$ 個の特徴点が入力データの特徴点と一致しない確率は以下のように表すことができる．

$$P_n = \left(\prod_{i=0}^{n-1} \frac{N_q - i}{K - i} \right) \left(\prod_{i=n}^{N_r - 1} \frac{K - N_q - (i - n)}{K - i} \right) \tag{10}$$

これより，テンプレートと入力データの特徴点の照合を行ったときに，その 2 次元座標データについて N 個以上の特徴点が一致する確率 P_N は，以下のようになる．

$P_N =$

$$\begin{pmatrix} N_r \\ N \end{pmatrix} \left(\prod_{i=0}^{N-1} \frac{N_q - i}{K - i} \right) \left(\prod_{i=N}^{N_r - 1} \frac{K - N_q - (i - N)}{K - i} \right) \tag{11}$$

4.2 特徴点の方向角データのみが一致する確率

次に，入力データとテンプレート間の方向角についてのみ考える．

まず，テンプレートのある 1 つの特徴点と入力データのある 1 つの特徴点が，方向角データについて一致する確率は，以下のように表すことができる．

$$\frac{1}{d} \tag{12}$$

次に，テンプレートの n 個の特徴点が，入力データと一致する確率は，以下のように表すことができる．

$$\left(\frac{1}{d}\right)^n \tag{13}$$

同様に，テンプレートの $N_r - n$ 個の特徴点が，入力データと一致しない確率は，以下のように表すことができる．

$$\left(1 - \frac{1}{d}\right)^{N_r - n} \tag{14}$$

以上より，テンプレートの全特徴点のうち n 個の特徴点が一致し，$N_r - n$ 個が一致しない確率は，以下のように表すことができる．

$$P'_n = \left(\frac{1}{d}\right)^n \left(1 - \frac{1}{d}\right)^{N_r - n} \tag{15}$$

これより，テンプレートの特徴点のうち m 個以上が一致して，残りが一致しない確率 P'_N は，

$$P'_N = \sum_{t=m}^{N} \left(\begin{array}{c} N \\ t \end{array} \right) \left(\frac{1}{d}\right)^t \left(1 - \frac{1}{d}\right)^{N-t} \tag{16}$$

となる．

4.3 2 次元座標データと方向角データの両方を考慮した確率

P_N および P'_N より，ランダムに選択した入力データとあるテンプレートを照合したときに，m 個以上の特徴点が，2 次元座標と方向角の両方一致する時のマニューシャ衝突率は，

$$P_{ver} = \sum_{N=m}^{N_r} (P_N \times P_{N'}) \tag{17}$$

と表すことができる．

但し，$N_r + N_q - K \leqq N \leqq N_r - 1$ である．

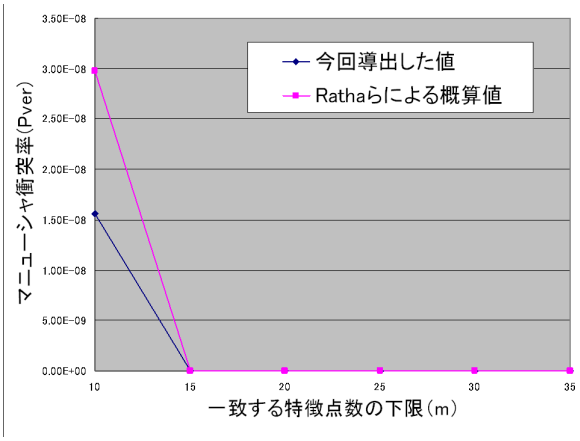

図 1: マニューシャ衝突率（$N_q = 40$ の場合）

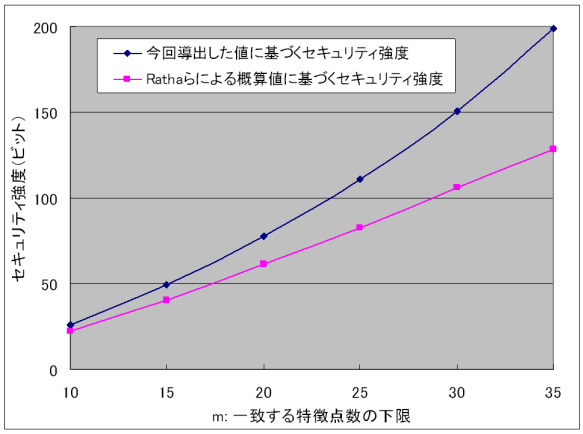

図 2: セキュリティ強度（$N_q = 40$ の場合）

5 マニューシャ衝突率についての検討

本章では Ratha らの検討したマニューシャ衝突率の概算値と **4 章**で導出したマニューシャ衝突率の値を比較する．

5.1 Ratha らの概算値と今回導出した値の比較

まず，Ratha らの検討において，ランダムに選択した入力データの特徴点 N_q は，$N_q \leqq K - \frac{N_r}{d} + 1$ と限定されている．その条件のもと，入力データの特徴点数を $N_q = 40$，テンプレートの特徴点数を $N_r = 40$，方向角データのバリエーションとして $d = 4$ と設定した場合，両者の値は図 1 のとおりになる．例えば，$m = 10$ 以上の特徴点が一致する確率は，Ratha らの概算値では約 2.8×10^{-8} となっている．これに対して，今回導出したマニューシャ衝突率は約 1.6×10^{-8} となった．Ratha らは一定数以上の特徴点を確率 1 で一致させるために必要な入力データの提示回数 $log\, 1/P_{ver}$ を「セキュリティ強度」と呼んでいる．この指標をベースに比較すると図 2 のようになる．

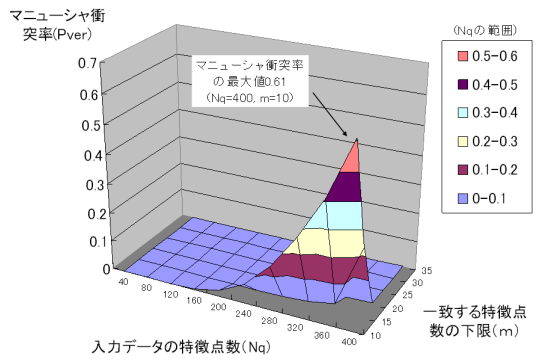

図 3: マニューシャ衝突率（N_q と m を変動させた場合）

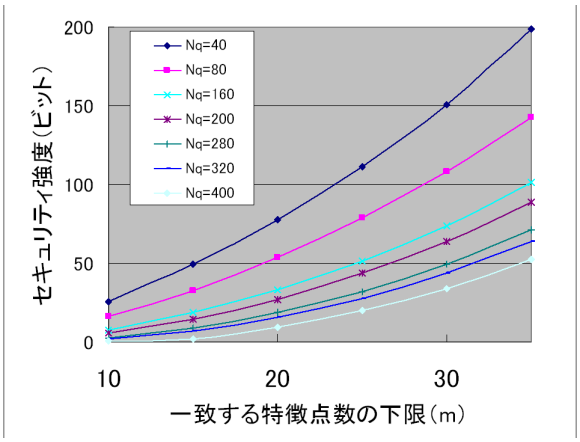

図 4: セキュリティ強度 (N_q=40〜400)

5.2 $N_q = 40$ の制約を外した場合のマニューシャ衝突率

次に，Ratha らが設定した $N_q = 40$ の条件を外した場合について計算する．**4 章**において導出したマニューシャ衝突率では，ランダムに選択した入力データの特徴点 N_q の値は最大 400 である．そこで，導出したマニューシャ衝突率の式において，テンプレート特徴点数 $N_r = 40$，方向角データ $d = 4$ と設定した上で，入力データ N_q を変化させたときに一定数 m 以上の特徴点が一致する時のマニューシャ衝突率を求めた（図 3 参照）．

その結果，入力データ特徴点 N_q を最大値の 400，テンプレート特徴点 $N_r = 40$，方向角データ $d = 4$ としたときの，$m = 10$ 以上の特徴点が一致するマニューシャ衝突率は，約 0.6 となった．これは Ratha らの検討による $N_q = 40$ の場合の約 4.0×10^7 倍である．

また，導出したマニューシャ衝突率の式において，テンプレート特徴点数 $N_r = 40$，方向角データ $d = 4$ と設定した上で，入力データ N_q を変化させたときに一定数 m 以上の特徴点が一致する時の強度 ($= log\, 1/P_{ver}$)（図 4 参照）は，$N_q = 40$，$m = 35$ としたときに最大値約 200bit であるのに対し $N_q = 400$，$m = 10$ としたときは最小値約 0.7bit となった．そのときのグラフを m 軸に平行に切断したときの値が図 5 である．

以上のことより，マニューシャ衝突率を最大化するという意味で，攻撃者に最も有利となる入力データは，入力データを $N_q = 400$ としたものであると言える．

5.3 考察

なりすましへの耐性を考える場合，ブルートフォースアタックだけでなく，攻撃者にとって最も有利な入力データが選択された場合の攻撃（ウルフ攻撃と呼ばれる [2]）についても想定することが求められる．こうした状況を考えると，今回導出したマニューシャ衝突率においては，N_q の制約を除き，同衝突率が最大となるような入力データを攻撃に利用した場合についても想定することが求められるといえる．

今回のマニューシャマッチング方式においては，実際に Ratha らの概算値よりもマニューシャ衝突率がはるかに大きくなることが明らかとなった．したがって，評価対象となるアルゴリズム次第ではあるが，ウルフ攻撃によってなりすましが成功してしまう可能性が Ratha らの検討によって示された結果よりも高い場合も考えられるといえる．

6 まとめ

本論文では，マニューシャマッチングにおけるランダムに選択した入力データとテンプレート間の，正確なマニューシャ衝突率を求めた．その結果からランダムに選択した入力データの特徴点 N_q を 400 とすることで，特徴点 10 以上の特徴点が一致するときのマニューシャ衝突率の値が 0.6 となるウルフの存在を示した．

参考文献

[1] N. K. Ratha, J. H. Connell and R. M. Bolle, “Enhancing security and privacy in biometrics-based authentication systems,” IBM System Journal, Vol.40, No.3, pp.614-634, 2001.

[2] 宇根正志・大塚玲・今井秀樹, “ 生体認証システムにおける新しいセキュリティ評価尺度：ウルフ攻撃確率，”2007 年暗号と情報セキュリティ・シンポジウム予稿集，電子情報通信学会，2007 年

[3] 渡邉直彦・繁富利恵・宇根正志・大塚玲・今井秀樹, “ 指静脈パターン照合アルゴリズムにおけるユニバーサル・ウルフ，”コンピュータセキュリティシンポジウム 2006 予稿集，情報処理学会，pp.621-626，2006 年

[4] 渡邉直彦・繁富利恵・美添一樹・宇根正志・大塚玲・今井秀樹, “ 指静脈パターン照合アルゴリズムにおけるユニバーサル・ウルフ－特徴抽出過程を含めた考

察一，”2007 年暗号と情報セキュリティ・シンポジウム予稿集，電子情報通信学会，2007 年