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

渡邉 直彦 †　繁富 利恵 ‡　宇根 正志 ‡　大塚　玲 ‡　今井 秀樹 †‡

† 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

†d53330@educ.kc.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

‡{rie-shigetomi,masashi-une,a-otsuka,h-imai}@aist.go.jp

あらまし　本論文では，三浦・長坂・宮武 [1] によって提案された指静脈パターン認証方式における照合アルゴリズムのセキュリティ特性について検討する．本照合アルゴリズムでは，まず被認証物から抽出される静脈パターンの入力照合データと登録照合データの相違度としてミスマッチ率と呼ばれる指標が算出され，ミスマッチ率が判定しきい値以下の場合に一致と判定される．本論文では，本照合アルゴリズムにおいて，どのような登録照合データに対しても一致と誤って判定されてしまう入力照合データが存在することを示す．このような特性を有する入力照合データを「ユニバーサル・ウルフ」と呼び，ユニバーサル・ウルフへの対応策について考察を行う．

Universal Wolves in a Matching Algorithm for Finger Vein Patterns

Naohiko Watanabe †　Rie Shigetomi ‡　Masashi Une ‡　Akira Otsuka ‡
Hideki Imai †‡

†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.chuo-u.ac.jp

‡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

Abstract　In this paper, we will discuss security features of a matching algorithm in a finger vein pattern based authentication method proposed by Miura, Nagasaka and Miyatake[1]. In the matching algorithm, a mismatch ratio is calculated as an index for a degree of the difference between input matching data of a vein pattern extracted from a subject and the corresponding registered matching data. If the ratio is equal to or less than a predetermined threshold, the vein pattern is accepted. Focusing on the matching algorithm, we will show that some specific input matching data are falsely accepted no matter which registered matching data are selected. We name such data “universal wolves.” In addition, we will briefly discuss how to avoid the universal wolves.

1　はじめに

近年，身体的特徴等を用いて個人を自動的に認証するという生体認証方式が金融や交通等をはじめとする幅広い分野において採用されつつある．特に，2004 年央以降，指や手のひらの静脈パターンを利用した生体認証方式 (以下，静脈認証方式と呼ぶ) が，銀行の ATM における顧客の本人確認等に利用されはじめており [2]，今後静脈認証方式のセキュリティの確保が一層重要になると考えられる．

こうした状況下，静脈認証方式のセキュリティ評価手法の開発が急務となっており，セキュリティ評価尺度の開発や，同尺度によって高いセキュリティ・レベルを有することが証明可能な方式の実現が求められている．既存の研究成果をみると，セキュリティ評価手法開発へのアプローチとして，文献 [3] 等で示されている「テスト物体アプローチ」が挙げられる．テスト物体アプローチは，人工的に作製したテスト物体を用いて実際の生体認証システムのふるまいを測定し，各システムの評価を行おうとするものである．

本論文は，上記アプローチとは異なり，論文等において詳細が公開されているアルゴリズムをセキュリティの観点から理論的に評価するというアプローチを採用する．具体的には，三浦・長坂・宮武 [1] で提案されている方式 (以下，MNM 方式と呼ぶ) のセキュリティ特性について検討を行う．その結果，認証時に撮影される指静脈画像から特徴を抽出して得られるデータ (以下，入力照合データと呼ぶ) と，予め登録されているデータ (以下，登録照合データと呼ぶ) の照合を行うアルゴリズム[1](以下，MNM 照合アルゴリズムと呼ぶ) において，どのような登録照合データが照合の対象となったとしても誤って一致と判定してしまう入力照合データが存在することを示す．このような入力照合データを「ユニバーサル・ウルフ (universal wolves)」と呼ぶこととする[2]．本論文では，MNM 照合アルゴリズムのユニバーサル・ウルフの対応策について考察する．

逆に，ユニバーサル・ウルフが登録照合データとなった場合には，どのような入力照合データも当該登録照合データに対して誤って一致と判定してしまうことになる．この逆の場合は，入力照合データと登録照合データを入れ替えるだけで発生するので，以下本論文では，この逆の場合を述べず，自明として扱う．

ただし，本論文の検討は，MNM 照合アルゴリズムを対象としており，実際の静脈認証システムを対象とするものでない点を強調しておく．

以下，**2 章**では MNM 方式の全体像を，**3 章**では MNM 照合アルゴリズムを説明するとともに，**4 章**では MNM 照合アルゴリズムの検討を行い，ユニバーサル・ウルフの存在を示す．**5 章**では対応策について考察を行い，**6 章**において今後の課題を述べて締めくくる．

2　MNM 方式とは

本章では，MNM 方式の手順を示す．MNM 方式は，登録フェーズと認証フェーズに分かれる．登録フェーズでは，指静脈画像の獲得と正規化を行ったあと，指静脈パターンの抽出を行い，登録照合データを得る．認証フェーズでは，登録フェーズと同様の操作を行い，入力照合データを得た後，登録照合データと入力照合データの相違度によって，本人であるか他人であるかを判断する．

以上をまとめると MNM 方式の手順は，以下のように大きく (1)〜(5) に分けることが出来る．

(1) 指静脈画像を獲得する．手の甲側から指に赤外光を照射し，掌側に透過してきた光をカメラで撮影し，指静脈画像を得る．指静脈画像は，横 240 画素，縦 180 画素の 256 階調濃淡画像である．

(2) 指静脈画像を正規化する．指の撮像位置や角度は撮像のたびに変化するため，それらを統一する．指輪郭の検出を行い，その結果に基いて正規化する．この結果によって得られたデータを以下，正規化画像と呼ぶ．

(3) 指静脈パターンを抽出する．正規化画像から線追跡処理を行い，指静脈パターンの抽出を行う．この指静脈パターンの抽出を行うアルゴリズムを以下，MNM 抽出アルゴリズムと呼ぶ．線追跡処理とは，任意の点の近傍画素の静脈領域を探し出し，静脈領域を連続した線として抽出する処理である．1 回の線追跡処理

[1]本照合アルゴリズムは [4, 5] においても採用されている．

[2]音声認識の分野では他人の声として受理されやすい話者を “wolf” と呼ぶケースが多く [6]，生体認証分野一般においても，複数のテンプレートに対して高い確率で他人受入を引き起こす照合用の生体情報をもつ利用者を “wolf” と呼ぶことがある [7].

で全ての静脈領域を抽出できないので，この線追跡処理を反復させるのであるが，[1] では予備実験により十分に抽出が行うことができる反復回数の下限値を 3000 回と求め，MNM 抽出アルゴリズムでも反復回数を 3000 回としている．また，静脈領域とは，線追跡の 3000 回の反復回数のうち何回辿られたかを示す追跡回数にしきい値を設けたとき，しきい値より高い追跡回数となった画素の集合のことである．このとき，しきい値より低い追跡回数となった画素の集合は，背景領域となる．

(4) 入力照合データと登録照合データを照合する．登録照合データと入力照合データの相違度を計算する．この入力照合データ，登録照合データ間の照合時のアルゴリズムが，MNM 照合アルゴリズムに対応する．

(5) 認証結果を出力する．(4) で算出された相違度に基づき，認証結果を出力する．相違度を判定しきい値と比べ，相違度が判定しきい値以下ならば本人，そうでないならば他人であると判定し，結果を出力する．

本論文では，(4) の MNM 照合アルゴリズムに焦点を当てる．その MNM 照合アルゴリズムに対し，ユニバーサル・ウルフによるなりすまし耐性の観点から検討を行う．

(1) の指静脈画像の獲得法，例えば画像取得に使うカメラの性能，赤外光の波長などや，(2) の指静脈画像の正規化法については，MNM 方式の論文に詳しく記載されていないので本論文では検討の対象に入れない．(3) の指静脈パターンの抽出については，[1] では 3000 回の線追跡処理の反復により十分に抽出が行えると判断できる，としている．このため本論文でも MNM 抽出アルゴリズムによって指静脈パターンが理想的に抽出されると仮定する．(5) の認証結果の出力については、実装時にある表示装置を用いユーザに結果を表示するという処理であり，正確に動作すると仮定する．

以上の理由により (4) のみに注目する．

3 MNM 照合アルゴリズム

本章では，MNM 照合アルゴリズムの特徴と全体像について述べる．

MNM 照合アルゴリズムは，あいまい領域の定義及び，ミスマッチ率 R_m の定義を特徴とする．

あいまい領域とは，背景画素，静脈画素のどちらともはっきり断定できないような画素の集合である．このあいまい領域を導入した理由は，認証精度の安定化を図るためと考えることができ，[1] では，あいまい領域を除いて照合することによって認証精度の安定化を実現することができるとしている．

R_m とは，入力照合データと登録照合データ間の相違度を示し，大きいほど入力照合データと登録照合データに違いがあり他人である可能性が高く，小さいほど入力照合データと登録照合データに違いが少なく本人である可能性が高い．

以下，**3.1 節**では MNM 照合アルゴリズムの流れを説明し，**3.2 節**，**3.3 節**で，あいまい領域，R_m について説明をする．

3.1 MNM 照合アルゴリズムの流れ

MNM 照合アルゴリズムは，以下のように大きく 3 つの Step に分かれる．

A 線追跡処理の結果を用いて，正規化画像の 256 階調の各画素を，静脈画素 (画素値 255) と背景画素 (画素値 0) の 2 値に振り分ける操作を行い，2 値の画像データ (以下，2 値画像データと呼ぶ) を獲得する．

B 2 値画像データを縦横共に 1/3 に縮小する．縮小前の 3 × 3 画素の 9 画素の画素値の平均値を求め，その平均値により，縮小後の画像データの各画素を静脈領域，背景領域，あいまい領域のいずれかに振り分ける．平均値が 84 以下となる画素を静脈領域として画素値 255 を，平均値が 171 以上となる画素を背景領域として画素値 0 を，これら以外の画素をあいまい領域として画素値 128 を割り当てる．この結果，3 値の画像データ (以下，照合データと呼ぶ) を獲得する．1/3 に圧縮することにより，照合データの大きさは，横 80 画素，縦 60 画素となる．あいまい領域については，**3.2 節**で詳しく述べる．

C 入力指静脈画像を 3 値画像化させた画像データ (これが入力照合データである) と登録指静脈画像を 3 値画像化させた画像 (これが登録照

合データである) から，静脈領域，背景領域のみを用いて R_m を求め，入力照合データと登録照合データの相違度を評価する．R_m については，**3.3 節**で詳しく述べる．

3.2 あいまい領域

あいまい領域について，[1] では，縦横共に 1/3 に縮小する際,「単純に 128 をしきい値として再 2 値化すると，背景と指静脈の境界では，平均を取る領域の位置により結果が変動する．そこで中間的な画素値となった領域は，背景，指静脈のどちらでもないあいまい領域と定義する」と述べられている．

安定化の障害になるのは，指の置き方や明るさなどの入力毎のむらである．このむらを排除するためには，静脈領域，背景領域の画素のみを照合に用い，むらの影響がある可能性が高い画素を照合に用いなければ良い．そこであいまい領域を定義し，縮小後に中間的な値になった画素を照合時に排除する．あいまい領域とは，縮小前の 9 画素の画素値の平均値 $\overline{P}$ が，256 階調を 3 等分した 85 から 170 までとなる画素の集合と定義している．

3.3 ミスマッチ率 R_m

R_m の計算法について説明する．R_m の計算法は以下のように大きく 3 つの Step に分かれる．

- $\boldsymbol{\alpha}$ 登録照合データと入力照合データに座標を設定し，登録照合データの中心部分を切り出し，テンプレートを作る．
- $\boldsymbol{\beta}$ 入力照合データからはみ出さないようにテンプレートを重ね合わせ， 入力照合データとテンプレートの位置合わせを行う．入力照合データとテンプレートの画素値の相違量としてミスマッチ数 $N_m(s,t)$ を定義し，テンプレートの位置を変えながら $N_m(s,t)$ を順次計算する．$N_m(s,t)$ が最も小さい場所でテンプレートを固定する．固定された場所での $N_m(s,t)$ を最小ミスマッチ数 N_m とする．

  $N_m(s,t)$ を算出するときにあいまい領域を用いず，背景領域，静脈領域のみを用いる．
- $\boldsymbol{\gamma}$ R_m を，N_m と，登録照合データと入力照合データの静脈領域の画素総数の比として求める．

まず$\boldsymbol{\alpha}$について説明する．登録照合データと入力照合データを (x,y) 座標で考える．登録照合データと入力照合データのそれぞれの各画素の位置に座標が合うように座標を設定する．左上の画素を (0,0) とし，右方向を x 座標の正方向，下方向を y 座標の正方向とする．座標 (x,y) の登録照合データと入力照合データの画素値をそれぞれ $R(x,y)$，$I(x,y)$ とする．これらの値は，**3.1** の **B** で割り振られたように，0,128,255 のいずれかとなる．

テンプレートを登録照合データを切り出して作る．縮小後の登録照合データとして，[1] では横 66 画素，縦 44 画素としている．テンプレートは横 66 画素，縦 44 画素の登録照合データの中心部の横 50 画素，縦 30 画素を切り出している．その結果，テンプレートの左上隅の座標は (8,7)，右下隅の座標は (58,37) となる．これらの定数は，[1] が指の大きさを考慮して設定している．

次に$\boldsymbol{\beta}$について説明する．$N_m(s,t)$ は，$R(8,7)$ と $I(s,t)$ とが重なる位置での画素値の相違量として，次のように定義される．

$$N_m(s,t) = \sum_{y=0}^{29}\sum_{x=0}^{49}\{\phi(I(s+x,t+y),R(8+x,7+y))\} \quad (1)$$

ϕ は，B_1 と B_2 を画素値としたとき，これらが背景と静脈領域との重なりであるか否かを判定する関数であり，次のように定義される．

$$\phi(B_1,B_2) = \begin{cases} 1 & if \mid B_1 - B_2 \mid = 255 \\ 0 & otherwise. \end{cases} \quad (2)$$

B_1，B_2 の一方が背景領域で，他方が静脈領域であるときのみ 1 を出力する．B_1，B_2 のどちらかがあいまい領域である場合は 0 を出力する．

$N_m(s,t)$ から N_m を次のように定義する．

$$N_m = \min_{0\le s<16, 0\le t<14} N_m(s,t)$$

次に$\boldsymbol{\gamma}$について説明する．R_m は，次のように定義される．

$$R_m = \frac{N_m}{\sum_{j=t_0}^{t_0+29}\sum_{i=s_0}^{s_0+49}\phi(I(i,j),0) + \sum_{j=7}^{36}\sum_{i=8}^{57}\phi(0,R(i,j))} \quad (3)$$

ただし，s_0，t_0 は N_m を生じる s，t である．

4 MNM照合アルゴリズムのユニバーサル・ウルフ

本章では，MNM 照合アルゴリズムにおけるユニバーサル・ウルフの存在を示す.

式 (3) の R_m の定義を見ると，R_m の値を小さくさせるためには N_m が小さければよいことがわかる．式 (1) の $N_m(s,t)$ の定義を見ると，$N_m(s,t)$ の値を小さくさせるためには ϕ をカウントさせなければよいことがわかる．式 (2) の ϕ については，$I(x,y)=128$ を満たす画素が増えると，ϕ が小さくなることがわかる.

そこで例えば，全ての $I(x,y)$ が 128 となる場合を考える．入力照合データとテンプレートの重なりのどの画素においても $\phi=0$ となり，

$$\begin{aligned} & N_m(s,t) \\ = & \sum_{y=0}^{29}\sum_{x=0}^{49}\phi(I(s+x,t+y),R(8+x,7+y)) \\ = & \sum_{y=0}^{29}\sum_{x=0}^{49}\phi(128,R(8+x,7+y)) \\ = & 0 \end{aligned}$$

となり，$R(x,y)=255$ を満たす (x,y) が存在するとの前提の下で，

$$\begin{aligned} & R_m \\ = & \frac{N_m}{\sum_{j=t_0}^{t_0+29}\sum_{i=s_0}^{s_0+49}\phi(I(i,j),0)+\sum_{j=7}^{36}\sum_{i=8}^{57}\phi(0,R(i,j))} \\ = & \frac{0}{\sum_{j=t_0}^{t_0+29}\sum_{i=s_0}^{s_0+49}\phi(128,0)+\sum_{j=7}^{36}\sum_{i=8}^{57}\phi(0,R(i,j))} \\ = & \frac{0}{0+\sum_{j=7}^{36}\sum_{i=8}^{57}\phi(0,R(i,j))} \\ = & 0 \end{aligned}$$

となる．したがって，静脈画素を少なくとも一つは有するどのような登録照合データに対しても，正の判定しきい値の下で一致と判定させることができることとなり，この例で取り上げた入力照合データがユニバーサル・ウルフであることがわかる.

次に，入力照合データの全ての $I(x,y)$ が 128（以下，全あいまい画像) となる場合，こうした入力照合データを作製出来る縮小前の 2 値画像データは存在するかを考える.

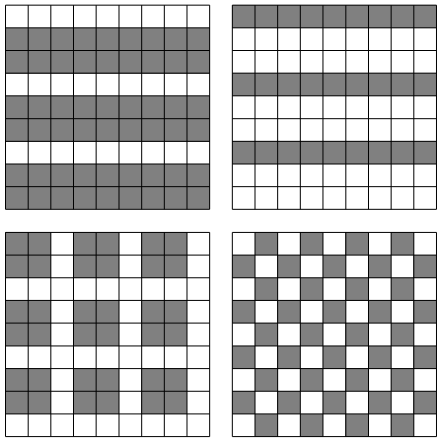

図 1: 2 値画像データ例

$\overline{P}$ があいまい領域に割り振られる値 ($85 \le \overline{P} \le 170$) になるように，静脈領域，背景領域が一定の割合であればよい．以下のように $\overline{P}$ の計算を行い，静脈領域，背景領域の割合を調べると，縮小前の 9 画素のうち，静脈画素数が 3 から 6 個の場合，縮小後の 1 画素はあいまい画素になることがわかる．$\overline{P}$ の添え字は静脈領域の画素数を示す.

$$\begin{aligned} \overline{P_3} &= \frac{1}{9}(255\times 3+0\times 6)=85 \\ \overline{P_4} &= \frac{1}{9}(255\times 4+0\times 5)=113.3 \\ \overline{P_5} &= \frac{1}{9}(255\times 5+0\times 4)=141.6 \\ \overline{P_6} &= \frac{1}{9}(255\times 6+0\times 3)=170 \end{aligned}$$

以上の計算から，全あいまい画像を作製出来る縮小前の 2 値画像データ例を図 1 に示す.

図 1 のような画像データを用いると，どの 3×3 画素の 9 画素を縮小しても縮小後はあいまい画素となるため，ユニバーサル・ウルフを作製することができる.

5 ユニバーサル・ウルフへの対応策に関する考察

本章では，MNM 照合アルゴリズムにおけるユニバーサル・ウルフに対する対応策について述べる.

ユニバーサル･ウルフが照合アルゴリズムに入力されたとき，そういった画像を排除する機能を照合ア

ルゴリズムに持たせれば良い．**4 章**で述べた $R_m = 0$ のときについては，対策は簡単で，入力照合データの全ての画素があいまい領域であるかを調べ，該当した際にその入力照合データを排除させればよい．

しかし，一部があいまい領域でないようなユニバーサル・ウルフについては適切に排除することができない可能性がある．そこで，通常の使用時に想定される，R_m がある正数である場合を考える．この時攻撃法として，全あいまい画像となる入力照合データを用いずに，画像の一部分があいまい領域とならない入力照合データを用い，高い確率で本人と判断させることが出来る画像を作る，という方法が考えられる．

この攻撃法の対応策の 1 つとして，静脈領域の画素数に対するあいまい領域の画素数の割合を登録照合データと入力照合データについて計算し，両者の差が一定値以上の場合には，その入力照合データを排除するという方法が考えられる．照合データのあいまい領域の画素数を A，静脈領域の画素数を V とし，その比 $\rho = A/V$ を計算する．登録照合データは R の添字，入力照合データは I の添字で表すことにし，以下の通り ρ の差の絶対値がしきい値 T_h 以上ならば排除するという方法が考えられる．

$$\mid \rho_R - \rho_I \mid > T_h$$

T_h の値であるが，実験により適切な値を設定する必要がある．

6　まとめ

本論文では，三浦・長坂・宮武 [1] の指静脈パターンを利用した認証方式における照合アルゴリズムのセキュリティ特性について検討を行った．その結果，どのような登録照合データに対しても誤って一致と判定されてしまう入力照合データが存在することを示した．このような特徴を有する入力照合データをユニバーサル・ウルフと呼び，ユニバーサル・ウルフへの対応策について簡単な考察を行った．

今回の検討は MNM 照合アルゴリズムを対象としたものであり，現状利用されている製品・システムにユニバーサル・ウルフが存在するとは限らない．また，ユニバーサル・ウルフを一致と誤って判定するのを防ぐには，照合アルゴリズムを改良する以外にも様々な手法が考えられるので，今回検討したユニバーサル・ウルフが実際の製品・システムでなりすましにつながる可能性については，別の検討が必要である．

今後は，**5 章**の考察を踏まえ，ユニバーサル・ウルフへの対策を施した照合アルゴリズムについて検討を行う方針である．また，MNM 方式にどのようなユニバーサル・ウルフが含まれるのかを検討し，そのパターン全体を明らかにしていく方針である．

参考文献

[1] 三浦直人，長坂晃朗，宮武孝文，“線追跡の反復試行に基づく指静脈パターンの抽出と個人認証への応用，” 信学論 (D)，vol.J86-D-Ⅱ no.5，pp.678-687，May 2003.

[2] 外昌弘，“我が国金融機関におけるバイオメトリック認証技術の活用について，” 情報処理，47 巻 6 号，pp.577-582，June 2006.

[3] 松本勉，“生体認証システムのセキュリティ設計とセキュリティ測定，” ユビキタスネットワーク社会におけるバイオメトリクスセキュリティ研究会・第 7 回研究発表会予稿集，p.57-64，June 2006.

[4] N. Miura, A. Nagasaka, T. Miyatake, “Extraction of Finger-Vein Patterns Using Maximum Curvature Points in Image Profiles,” Proceedings of the ninth IAPR Conference on Machine Vision Applications, pp.347-350, May 2005.

[5] 比良田真史，高橋健太，三村昌弘，“画像マッチングに基づく生体認証に適用可能なキャンセラブルバイオメトリクスの提案，” 信学技報，vol. 106, no.176, ISEC2006-67，pp.205-210，July 2006.

[6] G. Doddington, W. Liggett, A. Martin, M. Przybocki, D. Reynolds, “SHEEP, GOATS, LAMBS and WOLVES: A Statistical Analysis of Speaker Performance in the NIST 1998 Speaker Recognition Evaluation,” Proceedings of ICSLP 98, pp.1351-1354, Nov. 1998.

[7] 日本バイオメトリクス認証協議会，“バイオメトリクスシステムの脆弱性に関する報告書，” Version 0.6，2003.