Vol.2011-CVIM-177 No.1
2011/5/19

ペン持ち方特徴を用いたバイオメトリック個人認証

村松　大吾[†1,*1]　橋本　侑樹[†2]　小方　博之[†1]

筆記をする際のペン持ち方に注目し，カメラで撮影したペン持ち方画像を用いて個人を認証する手法を検討する．ペンの持ち方は，手の大きさ等の人の身体的特徴に由来する個人性とともに，どのようにペンを持つのか，という人の癖に由来する個人性が存在すると考えられ，個人認証に有効なモダリティだと考えられる．本研究ではその有効性を確認するために，ペン持ち方を撮影した画像（ペン持ち方データ）から多数の特徴を抽出し，各特徴から計算される非類似度を統合することで認証を行う．本研究では 33 個の特徴から計算される非類似度スコアを realAdaBoost を用いて統合し，ユーザ依存しきい値と比較することで認証を行った．30 人から取得したペン持ち方データを用いた評価実験では，他人の握り方を真似したなりすまし攻撃に対して等誤り率 4.1% という結果を得た．

Biometric Person Authentication Method Using Pen Holding Feature

Daigo Muramats,[†1,*1] Yuki Hashimoto[†1]
and Hiroyuki Ogata[†1]

We focus on a biometric person authentication method using features of pen holding style. The manner of holding pen can be distinctive among persons and be useful modality for person authentication, because the manner is affected by both the physical features and habitual behavior. In order to evaluate the efficiency, we extract several features from the pen-holding image, and fuse them for verification. In this paper, realAdaBoost algorithm is used for the fusion, and user-dependent threshold is applied for a decision making. The developed algorithm is evaluated using the database collected dorm 30 persons. The algorithm achieved an EER of 4.0% against the impersonation attacks.

1. はじめに

個人の権利多様化に伴い，人物を自動的に特定する技術がこれまで以上に重要となってきている．バイオメトリクス（生体認証）はヒトから取得される特徴を用いて個人を自動的に認証する技術であり，近年盛んに研究され，また実際に導入されている[1)]．例えば銀行 ATM で用いられている静脈認証やパソコンや携帯端末で用いられている指紋認証はそれらの代表的なものである[2)]．

バイオメトリクスは身体的特徴を用いた手法と行動的特徴を用いた手法に大別することができる．身体的特徴としては前述した静脈や指紋，虹彩，掌形，顔などが良く知られており，行動的特徴には筆記動作（署名）や歩行，キーストロークなどがある[1)]．バイオメトリクスにおいて，これらの身体的特徴や行動的特徴はモダリティと呼ばれるが，前述した以外にも様々なモダリティが研究・検討されている．その一つの理由としては，安全性や利便性，コスト等を考慮した場合，どのような場面においても完璧なモダリティが現状存在せず，どのモダリティにも長所・短所が存在するためである．

バイオメトリクスの安全性（認証精度）を改善する手法としてマルチモーダル認証と呼ばれる手法が研究されている[3)]．マルチモーダル認証は一つのモダリティ（例えば指紋だけ，虹彩だけ）で認証を行うのではなく，複数のモダリティを組み合わせて認証を行うものであり，例えば指紋と指静脈[4)]，顔と声[5)]，発話と唇動作[6)]，歩行と顔[7)] など様々な手法が研究されている．

マルチモーダル認証は認証精度の改善という安全性の点から非常に有効な手法であると考えられるが，複数の取得デバイスが必要となる場合や，利用者に複数回のデータ入力を要求する場合などがあり，組み合わせるモダリティにおいてはコストや利便性の観点からは必ずしも好ましい手法ではない．コストの観点からはデータ取得デバイスが同じ（一つ）であることが好ましく，利便性の観点からは，利用者に要求する動作が増えないことが好ましい[⋆1]．一方，単一デバイス，単一動作，で取得できる特徴を用いたマルチモーダル手法の場

†1 成蹊大学理工学部エレクトロメカニクス学科
Department of Electrical and Mechanical Engineering, Seikei University
∗1 現在，大阪大学 産業科学研究所
Presently with The Institute of Science and Industrial Research, Osaka University
†2 成蹊大学大学院理工学研究科
Graduate School of Science and Technology, Seikei University
⋆1 同時に取得される特徴を利用することでなりすましの難易度も上がるという利点もある

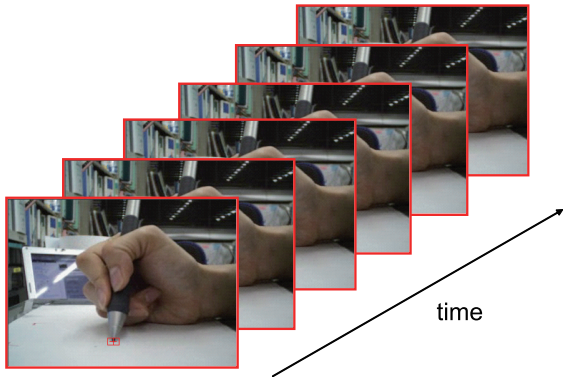

図 1 カメラを用いて撮影された筆記動作

合（例えば文献[4]）は，デバイス設置コスト増加や利便性を損ねることなく精度を向上させることができる．これは既存のバイオメトリックシステムにおいて，データ取得に用いられているデバイスにより，既存特徴と同時に取得できる特徴を用いて認証システムを構築することができれば，認証精度を向上させられる可能性があることを意味している．

図 1 は署名筆記動作をカメラで撮影したものである．カメラを用いたオンライン署名認証手法[8),9)] では，映像からペン先を追跡することでペン先の移動軌跡を抽出し認証に利用するが，画像中のペン先以外の情報は認証に利用されず，実質捨てられている．そこで，この利用されていない情報も活用することで，より高精度の筆記動作認証を開発したいと考えている．本研究ではその最初のステップとして，利用されず捨てられている情報を用いた認証手法，ペン持ち方特徴を用いた認証手法[10)–12)] に焦点をあて，精度の改善を目指す．

本論文では，抽出したペン持ち方特徴から得られる複数の非類似度を，realAdaBoost[13)] を用いることで統合し，認証を行った．またユーザの個人性を考慮したしきい値を設定することで精度改善を目指した．30 人から取得したデータを用いた評価実験では，本人データを真似たなりすましデータに対して等誤り率 4.1% となり，文献[12)] と比較し精度改善に成功した．

2. 関 連 研 究

手の幾何的な特徴を利用したバイオメトリクスとしては掌形認証がある．掌形認証では，手の静止画像や 3 次元イメージを取得し認証に利用するもので，指の長さや幅，手の大きさなどを取得し認証する手法である[14)]．この手法は手そのものの身体的特徴を用いた認証であり，行動的な要素は考慮されない．それに対し Ogihara らは ATM 操作時の手の動きを動画像としてカメラで取得して認証を行う手法を提案している[15)]．この手法は，ATM 操作時の手形状と操作タイミングを考慮した手法であり，手形状特徴として上方から撮影した手の画像から 10 種類の特徴を抽出し認証に用いている．これらの手法は，基本的に手をある程度開いていることを前提としている．

一方，ペンを握ることを前提としている認証手法として，ペンに圧力センサを取り付け，把持力を用いた認証手法[16)] や，データグローブを用いて筆記時の各関節の曲がり方などを計測し認証に利用する手法[17),18)] が提案されている．これらの手法は筆記との相性は非常に良いと考えられるが，専用のデータ取得デバイスが必要になる．

それに対し Gluhchev らは筆記動作中の手を上方からカメラで撮影し，取得した動画から肌の色や手の幾何的特徴などを抽出し，利用する手法を提案している[19)]．この手法は本研究で検討する手法と非常に似ている手法であるが，カメラを設置する場所等が異なるため，利用できる特徴も異なる．著者らはペンを持つ手を上方から撮影するよりも，親指側から撮影した画像の方がペン持ち方の特徴が現れやすいと考えている．また将来的にオンライン署名との組合せを考えた場合にも，ペン先追跡精度やオンライン署名認証精度を考慮すると，親指方向から撮影した方が有利であると考えている[⋆1]．ただし，文献[19)] はペン筆記動作中の動的データを用いているのに対し，本研究の手法は現状筆記開始時の持ち方（静止画）にしか対応していない[⋆2]．なお，著者らのこれまでの研究としては文献[10)–12)] などがあるが，本研究は特徴量追加や認証アルゴリズムの改良により，これらの手法よりも良い精度を実現した．

3. アルゴリズム

図 2 にアルゴリズムの概要を示す．バイオメトリクスでは認証を行うために，正しい人物の特徴をユーザ ID とともに事前に登録する必要がある．本手法も例外ではなく，アルゴリズムは本人の特徴を事前に登録する登録フェーズと，実際に認証を行う認証フェーズとに分かれる．登録フェーズでは，登録する人物の生体特徴を取得，そこから本人識別に有効な特

⋆1 上方から撮影をすると，ペン先が手で隠されてしまうことがあり，カメラ位置の変更等が必要になる[8)]．また第一著者は研究[9),20)] でオンライン署名認証の精度とカメラ位置の考察を行ってるが，横側（親指側）から撮影した画像を用いた認証精度が良いという結果を得ている．
⋆2 動画像への対応は今後の課題である

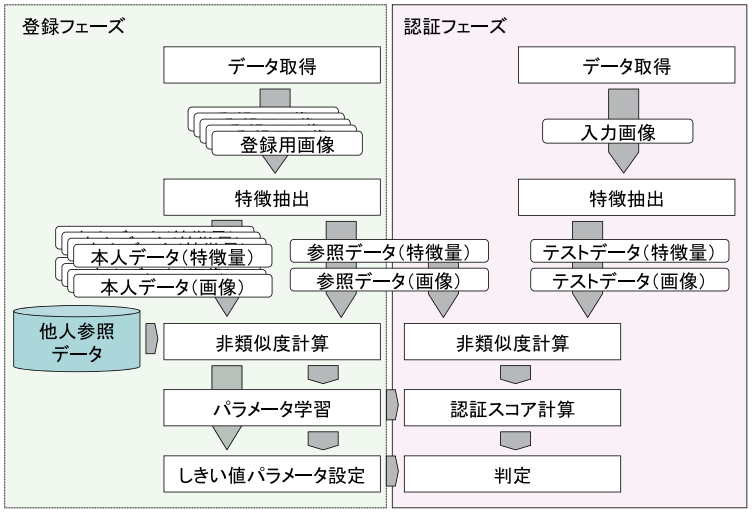

図 2 ペン持ち方認証アルゴリズム

徴を抽出し，参照データとして登録する．また本研究では，登録された本人データと，他人データとのスコアを計算し，これらのスコアを利用して認証時に必要なパラメータの学習・設定を行っている．

認証フェーズでは，データ取得によって得られた画像から登録フェーズ同様特徴を抽出し，抽出した特徴を用いて非類似度を計算する．その後計算された非類似度を統合して認証スコアを計算し，しきい値と比較することで認証を行う．本章の残りの部分では，これらのフェーズを構成する個々の処理について説明を行う．

3.1 データ取得

カメラを用いてペンを持った手を撮影する．撮影方向はいくつか考えられるが，ペン持ち方の違いがわかりやすいよう本研究では図 3 に示すように，ペンを持つ手を親指側から撮影する．これにより図 5 のような画像が取得される．親指側から撮影することにより，親指の位置や人差指の曲げ方の違いに関係する特徴を画像から取得できる．

3.2 特 徴 抽 出

取得された画像データから，個人性が現れると思われる特徴を抽出する．図 5 は異なる 9 人から取得したペン持ち方の画像である．これらの図よりペン持ち方にはかなり個人差があ

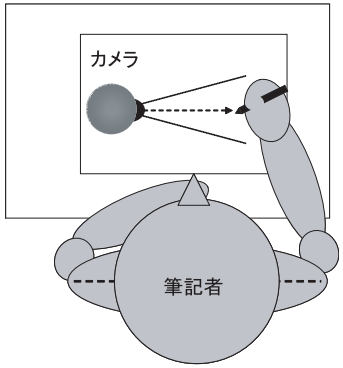

図 3 撮影設定

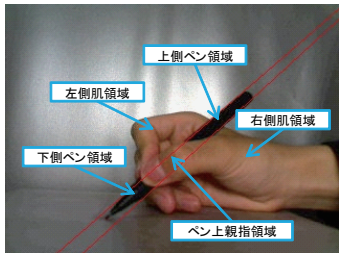

図 4 取得画像

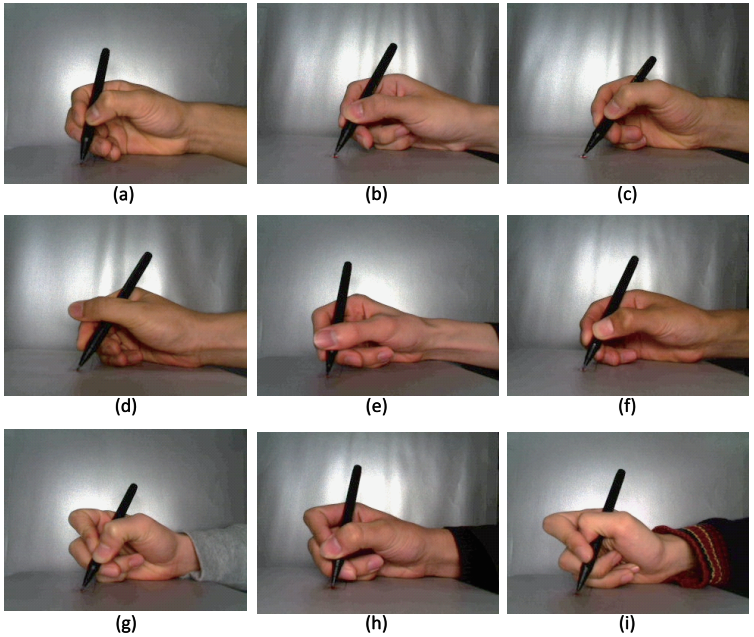

図 5 様々なペン持ち方

Vol.2011-CVIM-177 No.1
2011/5/19

ることが見てとれる．例えば，ペンの傾きや，人差指の曲げ方，ペンを支える親指の位置などにその違いが見られる．本研究ではこのように個人性が現れそうな領域に注目し，部位の位置や面積などの特徴量及び親指領域などの画像データを特徴として抽出する．本研究では手に関連する領域を図 4 に示すように（1）上側ペン領域,（2）下側ペン領域,（3）左側肌領域,（4）右側肌領域,（5）ペン上親指領域，に分類し，それらの領域から，次に示す領域の面積や長さ，位置といった特徴量（数値）や特定領域の画像を抽出して利用する．

- 特徴量
  - （1） ペン傾き
  - （2） ペン長さ
  - （3） ペン先からペンを持つ位置までの距離
  - （4） 上側ペン領域面積
  - （5） 下側ペン領域面積
  - （6） 左側肌領域：面積
  - （7） 左側肌領域：周囲長
  - （8） 左側肌領域：左上の位置（x 座標，y 座標）
  - （9） 左側肌領域：円形度（2 種類）
  - （10） 左側肌領域：周囲長さ-ペンと接している長さ
  - （11） 左側肌領域：重心位置（x 座標，y 座標）
  - （12） 左側肌領域：最も上の点位置（x 座標，y 座標）
  - （13） 左側肌領域：最も左の点位置（x 座標，y 座標）
  - （14） 左側肌領域：最も下の点位置（x 座標，y 座標）
  - （15） 右側肌領域：最も上の点位置（x 座標，y 座標）
  - （16） ペン上親指領域：重心位置（x 座標，y 座標）
  - （17） ペン上親指領域：重心のペン方向における位置
  - （18） ペン上親指領域：面積
  - （19） 上側ペン領域・下側ペン領域・ペン上親指領域の比率
  - （20） 親指の位置（x 座標，y 座標）
- 画像
  - （1） 親指周辺領域画像
  - （2） 左側肌領域画像

特徴量は，対象となる領域や部位に関する数値データであるのに対し，親指周辺領域画像と

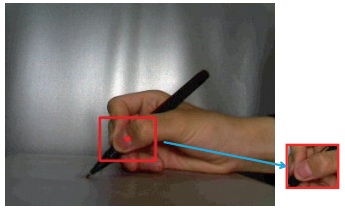

図 6 親指周辺領域画像

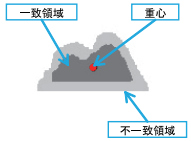

図 7 2 つの重ねられた左側肌領域画像（ペンと接する部分が水平になるように回転し，重心で位置合わせが行われている）

左側肌領域画像は図 6，7 に示すような画像特徴である．

3.3 比較・非類似度計算

二枚の画像 A および B から抽出された特徴量を $F_a = (fa_1, fa_2, ...fa_{N_v}), F_b = (fb_1, fb_2, ..., fb_{N_v})$ をしたとき，n 番目の特徴量に関する非類似度を

$$dis_n(A,B) = |fa_n - fb_n|, n = 1, 2, ..., N_v \quad (1)$$

と計算する．本研究では $N_v = 31$ である．

親指周辺領域に関する非類似度は次のように求める．親指周辺画像を $I_r(i,j)_{,1\leq i\leq W,1\leq j\leq H}$，入力画像を $I_v(i,j)_{,1\leq i\leq W_F,1\leq j\leq H_F}$ $(H < H_F, W < W_F)$ としたとき，親指周辺領域の非類似度は次のように計算する：

$$dis_{thumb} = \frac{1}{W \times H} \min_{(x,y)\in Region} \sum_{i=1}^{W}\sum_{j=1}^{H} |I_r(i,j) - I_v(x+i, y+j)| \quad (2)$$

ここで，$Resion$ は参照データの親指位置を (x_g, y_g) としたとき $(x_g - W/2 - 10, y_g - H/2 - 10) - (x_g + W/2 + 10, y_g + H/2 + 10)$ で決まる矩形領域である．つまり，親指周辺領域に関する非類似度は，親指がありそうな領域を参照データの親指位置± 10 ピクセルのエリアに限定し，その中で最小となる非類似度として計算する．

左側肌領域の非類似度は図 7 に示すように，左側肌領域のペンと接している部分が水平になるように回転し，重心で重ね合わせた場合に一致していない画素数として定義する．

これらにより，31 種類の特徴量に関する非類似度と，2 種類の画像に関連する非類似度を合わせた $N_{dim} = 33$ 次元の非類似度ベクトルが作成される．

3.4 認証スコア計算

33 個の非類似度を組み合わせて認証スコアを計算する．あるユーザ $id \in \{1, 2, ..., N_{ID}\}$ の参照データ $R_{img}^{(id)}$ とテストデータ Q_{img} から計算された非類似度ベクトルを $Dis(R_{img}^{(id)}, Q_{img}) = \{dis_n(R_{img}^{(id)}, Q_{img})\}_{n=1}^{N}$ としたとき，本研究では，次の手順で認証スコアを求める：

Step 1

非類似度ベクトルを正規化し，正規化非類似度ベクトル $\overline{Dis}(R_{img}^{(id)}, Q_{img})$ に変換する．

$$\overline{Dis}(R_{img}^{(id)}, Q_{img}) = (\overline{dis}_1(R_{img}^{(id)}, Q_{img}), ..., \overline{dis}_{N_{dim}}(R_{img}^{(id)}, Q_{img}))$$
$$\overline{dis}_n(R_{img}^{(id)}, Q_{img}) = \frac{dis_n(R_{img}^{(id)}, Q_{img})}{norm_n^{(id)}}, n = 1, 2, ..., N_{dim} \quad (3)$$

Step 2

正規化非類似度ベクトルの各要素が値域 $[-1, 1]$ をとるベクトル S に変換する．

$$S(R_{img}^{(id)}, Q_{img}); a, b) = (s_1(R_{img}^{(id)}, Q_{img}; a, b), ..., s_{N_{dim}}(R_{img}^{(id)}, Q_{img}; a, b)$$
$$s_n(R_{img}^{(id)}, Q_{img}; a, b) = g(\overline{Dis}(R_{img}^{(id)}, Q_{img}); a, b) \quad (4)$$

ここで関数 $g(s; a, b)$ は

$$g(s; a, b) = 1 - \frac{2}{1 + exp(-a(s - b))} \quad (5)$$

であり，a, b はパラメータである．この関数により全ての要素は $[-1, 1]$ の範囲をとる．

Step 3

Step2 で計算されたベクトル S の各要素 s_n は，n 番目の特徴を個別に用いた場合の認証スコアと考えることができる．そこで s_n を組み合わせることにより最終的な認証スコア $Score$ を次のように計算する：

$$Score(R_{img}^{(id)}, Q_{img}; \Theta) = \sum_{n=1}^{N_{dim}} \alpha_n s_n(R_{img}^{(id)}, Q_{img}; a, b) \quad (6)$$

ここで $\Theta = \{\alpha_n\}_{n=1}^{N_{dim}}$ であり，α_n は n 番目の特徴から計算された認証スコアの信頼度である．本研究ではこの Θ を realAdaBoost[13] を用いて設定する．

3.5 しきい値パラメータ設定

バイオメトリクスにおいてはユーザ依存しきい値をうまく設定することにより認証精度が改善するという報告がなされている（例えば[21]）．そこで，本研究では，ユーザ依存しきい値を次のように設定する：

$$Threshod_{id}(c) = Th_{id} + c \times dev_{id} \quad (7)$$

ここで，Th_{id} と dev_{id} はユーザ id に依存する項であり，これによりユーザ依存が実現される．良く利用される手法としては Z-norm[3] がある．本研究では，いくつかの考えられるユーザ依存正規化法を比較検討する．

3.6 比　　較

Q_{img} が，自分は人物 id と主張する X から取得されたデータの場合，認証は次のように行う：

$$X = \begin{cases} \text{Accepted} & \text{if } Score(R_{img}^{(id)}, Q_{img}) > Threshold_{id}(c) \\ \text{Rejected} & \text{otherwise} \end{cases} \quad (8)$$

4. 評 価 実 験

4.1 データベース

30 人の被験者から 1 人につき本人データ 10 枚，計 300 枚のペン持ち方画像を取得した．取得手順は次の通りである．

[step 1] ペンを持つ
[step 2] 1 文字筆記する
[step 3] ペン先を撮影台に置く
[step 4] 撮影する（このデータが実験用に利用される）
[step 5] ペンを置く
[step 6] step 1 に戻り繰り返す

今回の収集では図 8 に示すようにカメラを固定し，カメラに対するペン先位置も固定となるようにデータを収集した．またなりすましへの耐性を評価するために，本人データを提供した被験者 30 人の中から 8 人，本人データを提供していない人物 1 人の計 9 人に協力を依頼し，協力者に撮影された 30 人分の本人データを順番に提示し，ペンの持ち方が似るようにペンを持ってもらい，5 回ずつ撮影を行いなりすまし画像を収集した．その結果なりすまし画像 $(30 - 8) \times 9 \times 5 + 8 \times 8 \times 5 = 1310$ 枚が得られた[⋆1]．

⋆1 本人データを提供した人物は自分自身のデータへのなりすましは行わない

図 8 データ取得の様子

4.2 実験設定

ユーザ id の本人データを $Gd_l^{(id)}, 1 \leq id \leq 30, 1 \leq l \leq 10$，ユーザ id に対するなりすましデータを $Ad_k^{(id)}, 1 \leq k \leq K_{id}, K_{id} \in \{40, 45\}$ とする．本実験では，各ユーザから最初に撮影された本人データ $Gd_1^{(id)}$ をテンプレート画像とする（$R_{img}^{(id)} = Gd_1^{(id)}$）．次に，$Gd_l^{(id)}, 2 \leq l \leq 5$ を登録時に利用する本人データ，$Gd_l^{(m)}; m \neq id, 1 \leq l \leq 10$ を他人参照データとして登録フェーズで利用した．精度評価用データ（Q_{img}）には，ユーザ id に対しては本人データ $Gd_j^{(id)}, 6 \leq j \leq 10$ 及びなりすましデータ $Ad_k^{(id)}, 1 \leq k \leq K_i$ を用いた．したがって，評価に用いた本人データは $N_G = 150$，なりすましデータは $N_I = 1310$ である．

4.3 評価指標

認証システムの精度を評価するために，本人拒否率（False Reject Rate（FRR））と他人受入率（False Accept Rage（FAR））を計算し，バイオメトリックシステムの代表的な評価指標である等誤り率（Equal Error Rate（EER））を用いて評価を行う．各エラーは次のように計算する：

$$FRR(Threshold(c)) = \frac{1}{N_G} \sum_{id=1}^{30} \sum_{l=6}^{10} \delta \left(Score(Gd_1^{(id)}, Gd_l^{(id)}; \Theta) < Threshold(c) \right)$$

$$FAR(Threshold(c)) = \frac{1}{N_I} \sum_{i=1}^{10} \sum_{k=1}^{K_i} \delta \left(Score(Gd_1^{(id)}, Ad_k^{(id)}; \Theta) \geq Threshold(c) \right)$$

表 1 しきい値設定パラメータと等誤り率

設定 No.	Th_{id}	dev_{id}	EER [%]
1	学習用本人スコア平均値	学習用本人スコア標準偏差	12.0
2	学習用他人スコア平均値	学習用他人スコア標準偏差	10.7
3	学習用全員スコア平均値	学習用スコアの標準偏差	8.7
4	学習用本人スコア平均値	-	11.4
5	学習用他人スコア平均値	-	12.0
6	学習用全員スコア平均値	-	12.0
7	学習用本人スコア平均値	学習用全員スコア平均値	6.0
8	学習用他人スコア平均値	学習用全員スコア平均値	4.1
9	学習用全員スコア平均値	学習用全員スコア平均値	4.1
10	設定なし		11.3

ここで $\delta(x)$ は次のような関数である：

$$\delta(x) = \begin{cases} 1 & \text{if } x \text{ is true} \\ 0 & \text{otherwise} \end{cases} . \tag{9}$$

また EER は次のように求める:

$$EER = \frac{FAR(Threshold(c^*)) + FRR(Threshold(c^*))}{2} \tag{10}$$

$$\text{where } c^* = \underset{c}{argmin} \left| FAR(Threshold(c)) - FRR(Threshold(c)) \right| \tag{11}$$

4.4 実験結果

式（7）のユーザしきい値設定用パラメータを変更した場合の実験結果を表 1 に示す．表の中で「全員」とは「本人＋他人」のことである．また設定 10 は，ユーザ依存しきい値を利用せず，計算された認証スコアをそのまま利用した場合の結果である．

図 9 には今回の実験で結果の良かった設定 8 のエラートレードオフカーブを示す．今回最も結果の良かった設定においてはなりすましデータに対する等誤り率は 4.1%という結果になった[⋆1]．

5. 考　　察

本研究の特長は，筆記時のペン持ち方に注目し，カメラで撮影された画像から抽出される

⋆1 参考までに FAR 計算になりすましデータではなく，他人データを用いた場合の等誤り率はなりすましデータよりも小さくなる．今回他人データを用いた評価実験も行ったが実験設定に問題がある可能性があるため，数値の報告は控える

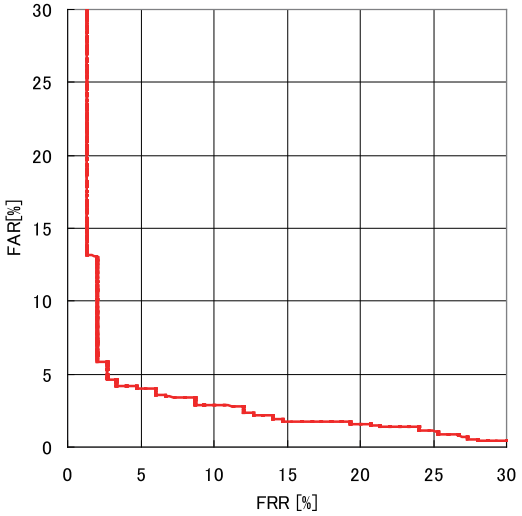

図 9 エラートレードオフカーブ（設定 8）

特徴を用いて認証を行う点である．また今回検討した手法では，多数の特徴を抽出し，特徴毎に簡単な（弱い）認証手法をつくり，それらを realAdaBoost アルゴリズムで統合を行った．これにより出力されるスコアは個人毎に精度評価を行えばある程度の良い結果が得られたが，全体で共通のしきい値を用いると，精度があまり良くなかった．そこで，ユーザ依存のしきい値パラメータを設定し利用した．その結果なりすましデータに対する等誤り率 4.1%という結果となった．一般にスコア正規化には Znorm 等（設定 1-3）がよく利用されるが，今回は Znorm を用いたものはあまり良い精度とはならず，正規化には平均値のみを利用するもの（設定 8-9）が良いという結果となった[⋆1]．同様の結果がカメラを用いたオンライン署名認証[9] でも確認されている．

認証精度については，本結果は著者らグループの以前の手法[12] の精度 EER=5.6%を上回るものであった．今回新しい特徴の追加，realAdoBoost の導入及びユーザ依存しきい値の導入など変更を加えたことがプラスに働いたと考えられる．しかしながら，アルゴリズムにはまだまだ改良の余地があるため，改良を加え，精度を改善してきたい．例えば今回用いたアルゴリズムについては，各特徴から計算された非類似度ベクトルを変換する関数にパラメータが存在するが，それらの最適化をおこなっていないため，それらにより精度の改善が可能だと考えられる．さらに，本研究は現在まだ静止画としての特徴しか利用していない．動的な特徴を利用することにより，精度の改善が見込めるため，動的特徴の対応を進めることが非常に重要な課題と考える．また動的特徴への対応とともに，オンライン署名認証とのマルチモーダル化を行い，より精度の高い認証アルゴリズムを構築したいと考える．

⋆1 設定 7 も平均のみを用いたものであるが，個人毎には学習用本人データが十分にないため，あまりよい推定値になっていないと考えられる

参 考 文 献

1) Jain, A. K., Flynn, P. and Ross, A. A.: *Handbook of Biometrics*, Springer Science+Business Media, LLC. (2008).
2) 湯浅秀一，和田山豊，藤井明宏：実用化が進む生体認証技術，沖テクニカルレビュー，Vol.207, No.3, pp.62–65 (2006).
3) Ross, A. A., Nandakumar, K. and Jain, A. K.: *Handbook of Multibiometrics*, Springer Science+Business Media, LLC. (2006).
4) 中村陽一，亀井俊男：マルチモーダル指認証，画像ラボ， Vol.21, No.1, pp.41–46 (2010).
5) Brunelli, R. and Falavigna, D.: Person identification using multiple cues, *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, Vol.17, No.10, pp.955–966 (1995).
6) 市野将嗣，坂野　鋭，小松尚久：唇動作と音声を用いたカーネル判別分析による個人認証方式，電子情報通信学会論文誌 D， Vol.J92-D, No.8, pp.1363–1372 (2009).
7) Zhou, X., Bhanu, B. and Han, J.: Human Recognition at a Distance in Video by Integrating Face Profile and Gait (2005).
8) Munich, M.E. and Perona, P.: Visual Identification by Signature Tracking, *IEEE Trans. Pattern Analysis and Machine Intelligence*, Vol.25, No.2, pp.200–217 (2003).
9) Yasuda, K., Muramatsu, D., Shirato, S. and Matsumoto, T.: Visual-based online signature verification using features extracted from video, *Journal of Network and Computer Applications*, Vol.33, pp.333–341 (2010).
10) 村松大吾，阿部貢士，堀内翔，小方博之：ペン持ち方情報を用いたバイオメトリック個人認証，電子情報通信学会論文誌 A， Vol.J92-A, No.5, pp.392–396 (2009).
11) Hashimoto, Y., Muramatsu, D. and Ogata, H.: Biometric person authentication method using features extracted from pen- holding style, *Proc. SPIE*, Vol.7708.
12) Hashimoto, Y., Muramatsu, D. and Ogata, H.: カメラを用いたペン持ち方認証，映

像情報メディア学会技術報告，Vol.34, No.54, pp.1–4 (2010).
13) Schapire, R.E. and Singer, Y.: Improved Boosting Algorithms Using Confidence-rated Predictions, *Machine Learning*, Vol.37, No.3, pp.297–336 (1999).
14) Sidlauskas, D.P. and Tamer, S.: Hand Geometry Recognition, *Handbook of Biometrics* (Jain, A.K., Flynn, P. and Ross, A.A., eds.), Springer Science+Business Media, LLC., chapter5 (2008).
15) Ogihara, A., Matsumura, H. and Shiozaki, A.: Biometric verification using keystroke motion and key press timing for ATM user authentication, pp.223–226 (2006).
16) 和田直哉，半谷精一郎: 筆記時の把持位置・把持力に含まれる個人性に関する一検討，電子情報通信学会大会講演論文集 (2009)
17) Hangai, S. and Higuchi, T.: Writer Identification Using Finger-Bend in Writing Signature, *Proc. BioAW2004, LNCS*, Vol.3087, pp.229–237 (2004).
18) Kamel, N., Sayeed, S. and Ellis, G.: Glove-Based Approach to Online Signature Verification, *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, Vol.30, No.6, pp.1109 –1113 (2008).
19) Gluhchev, G., Savov, M., Boumbarov, O. and Vasileva, D.: A New Approach to Signature-Based Authentication, *ICB*, Lecture Notes in Computer Science, Vol.4642, Springer, pp.594–603 (2007).
20) Shirato, S., Muramatsu, D. and Matsumoto, T.: Camera-based online signature verification system: effects of camera positions, *World Automation Congress (WAC), 2010*, pp.1 –6 (2010).
21) Jain, A.K., Griess, F.D. and Connell, S.D.: On-line signature verification, *Pattern Recognition*, Vol.35, pp.2963–2972 (2002).