

修士論文

手形状特徴の時間的変化を
有効利用した個人認証

平成 23 年度修了
三重大学大学院 工学研究科
博士前期課程 情報工学専攻

一ノ瀬 辰也

目次

はじめに	1
第1章 生体認証	2
1.1 静的特徴を用いた個人認証	2
1.1.1 指紋	2
1.1.2 静脈	3
1.1.3 顔	3
1.1.4 虹彩	3
1.2 行動的特徴を用いた認証	4
1.2.1 歩容	4
1.2.2 声紋	4
1.2.3 署名	4
1.2.4 ジェスチャ	5
1.3 生体認証における問題点	5
第2章 従来研究	6
2.1 システム全体の概要	6
2.2 認証方法	6
2.2.1 類似度算出	7
2.2.2 信頼限界と閾値	7
2.3 従来手法のまとめ	8
2.4 本研究の目的	9
第3章 提案手法1	10
3.1 類似度計算方法	10
3.2 追加する特徴量について	11
3.3 認証方法	12
3.4 SVMについて	13

第4章 提案手法2	17
4.1 形状特徴抽出	17
4.1.1 輪郭のマッチング	17
4.2 認証方法	19
第5章 評価実験	22
5.1 対象とする動画像について	22
5.2 実験結果	22
5.3 考察	23
おわりに	26
謝辞	28
参考文献	29
付録	30

はじめに

近年, 携帯電話に様々な機能が搭載され, それぞれの用途に合った柔軟な認証方式が求められている. そのため, 多く使われていた数桁の暗証番号やパスワードを用いた認証方式以外にも, 漏洩, 忘却, なりすましなどの危険性に対して頑強な認証方式として, 生体認証の研究が盛んに行われている.

生体認証には静的特徴による認証(指紋, 顔, 静脈等)と動的特徴による認証(ジェスチャ, 声紋, 歩容等)が存在し, それを実用化するための研究が行われている. 静的認証については, 多く実用例が存在する. しかし, 指紋, 静脈等については, 汚れ, 外傷, 乾燥などに弱いという欠点がある. また, 顔認証についても, ディスプレイで登録者の顔を拡大表示することで照合できてしまうという欠点がある.

それに対し, 動的特徴を用いた認証では個人の癖を利用して個人認証を行うため, パターンが盗まれた場合でも真似するのは困難である. しかし, こちらの認証は技術的, 社会的な問題から実用化された例は少ない.

動的認証の研究の中にジェスチャ認証がある. この認証では, 手形状の動きを撮影した動画像からその動きにおける個人の癖を利用することで個人認証を行う. さらに, その中の一つにグー, チョキ, パーを順番に提示した動画から個人の癖を利用する研究 [1] がある.

この方法では, 登録者本人の手形状(グー, チョキ, パーの形状)と手形状の遷移の時間差を参照パターンとして登録しておき, 認証に利用する. しかし, この方法を追試した結果, 本人以外でも手形状の類似度が高く形状変化が似ている場合があり, 認証に利用するには不十分な認識精度であった.

そこで本研究では, 数ある特徴量の中からさらに有効な特徴量を, 実験, 考察を行うことで見つけ, その特徴量を認証に用いることで従来手法よりも認証精度を改善することを目的とする.

本稿では, 第1章では生体認証について, 第2章では従来研究について, 第3章では提案手法について, 第4章では提案手法の有効性を示す実験について述べる.

第1章

生体認証

バイオメトリクスとは、人間の生体的特徴を用いて個人認証を行う方法のことである。生体的特徴といっても、人間には様々な特徴があるため、どの特徴を利用するかにより手法が分けられる。バイオメトリクスの目的は個人を特定、確認することであるため、その特徴は個人性を持つ必要がある。それ以外にもバイオメトリクスに必要な条件はいくつか挙げられている。一般にバイオメトリクスに適している生体特徴とは以下の条件を満たすものであるとされている。[3][4]

- 不遍性 (Universality): 全ての人を持つ特徴であること
- 唯一性 (Uniqueness): 他人と特徴が異なること
- 永続性 (Permanence): 時間の経過とともに変化しないこと
- 収集可能性 (Collectability): 数値的に計ることが出来ること (客観的データに置き換えられること)

バイオメトリクスは大きく分けると、静的特徴を用いた認証と動的特徴を用いた認証に分けることができる。以下にそれぞれの代表的な認証方法とそこで使われている技術、特徴量について述べる。

1.1 静的特徴を用いた個人認証

1.1.1 指紋

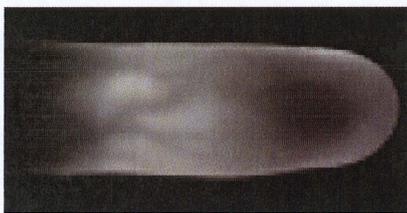
人の指紋は、隆線とその間に形成された谷の紋様がその個人を特徴づける。指先の皮膚紋様は、弓状紋、蹄状紋、渦状紋に大別できる。紋様の山の部分を隆線、隆線の間を谷と呼ぶ。精度良く判別しようとする、その紋様の詳細に着目し特徴を抽出する必要がある。特徴には、いくつかあるがこれらをまとめてマニューシャと呼ぶ。1つの指には150程度のマニューシャ(図1)があるとされている。



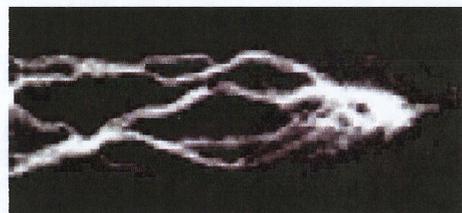
図1 指紋のマニューシャ

1.1.2 静脈

静脈には、指の静脈を用いたものと手の甲の静脈を用いた認証技術と存在する。指、手の甲の静脈パターンは千差万別であるため、個人の識別に利用できることが示唆されている。手の甲の静脈分布パターンについては、左右の手によっても異なると言われている。指静脈パターンの認証技術は、近赤外光を指に照射し、その透過光から得られる指の静脈画像を撮影し指静脈画像から指静脈パターンを抽出してあらかじめ登録された指静脈パターンデータと照合して個人を識別する技術である。近赤外線には、生体組織に対して透過性が高い一方、血液中のヘモグロビンには吸収されるという特徴があるため近赤外光を指に照射すると、図2に示すような指の静脈が影となって画像に現れる。この影が静脈パターンとなる。指静脈画像はカメラにより撮影され、指静脈画像に対して画像処理を施すことにより指静脈パターンが得られる。



(a) 近赤外光による指の透過画像



(b) 画像処理後の指静脈パターン

図2 指静脈パターン

1.1.3 顔

人間は顔によって相手を認識しており、バイオメトリクスの中では顔が人間にとって最も馴染みやすい技術と言える。顔認証技術の特徴としては、登録情報としての顔画像と、認証時に撮影される提示情報としての顔画像とは撮影条件が異なるため、単純なマッチングではなく、様々な特徴を抽出して照合する必要がある。画像処理で人間が行うのと同レベルの認証精度を実現するのは難しい。一卵性双生児などの識別可能性、めがね、髪型などの認証精度への影響が不十分であり、成りすましなどに弱い問題がある。

1.1.4 虹彩

虹彩と網膜は混同されることが多い。黒目の内側で瞳孔より外側のドーナツ状の筋肉質部分を虹彩という。網膜は、レンズに相当する水晶体の奥にある視神経の集まった部分である。同一人物の左右の眼でも異なり、一卵双生児でも異なる。眼の充血や、眼の不自由な方の多くは視神経の障害であ

り,ほとんどの場合,虹彩認証精度の劣化にはならない.虹彩認証では,虹彩画像からアイリスコードという特徴量を用いる.アイリスコード間における判定は,統計的な決定理論と信号処理を使い,任意の2つの虹彩コードの排他論理和から計算されるハミング距離に基づいて行われる.(図3)

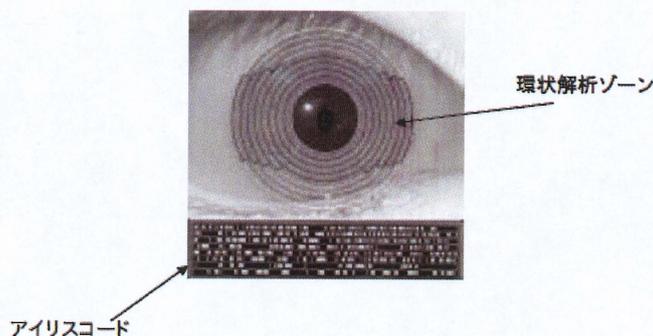


図3 虹彩パターン(分布帯とアイリスコード)

1.2 行動的特徴を用いた認証

1.2.1 歩容

歩容認証では,個人ごとで体型や歩行パターン(歩幅,手足の振り,姿勢等,無意識下で現れる周期的な動き)が異なることに着目して認証を行う.歩容認証の特徴としてカメラから離れた場所での認証が可能であるという点が挙げられる.そのため,防犯カメラを用いた広域監視への応用が期待されている.しかし,設置されているカメラの視点の違いに伴う見えの変化が挙げられる.そのため,この問題を解決するための研究が多く行われている.

1.2.2 声紋

音声信号の周波数成分から声紋データを抽出し,事前に登録した同じ言葉の声紋データと照合することで話者認証する方式.音声の個人差を用いて,誰の声であるかを自動的に判定することを声紋認識あるいは話者認識(Speaker Recognition あるいは Voice Verification)という.

1.2.3 署名

署名認証には,静的と動的署名認証の2つがある.静的署名認証はオフライン署名認証,動的署名認証はオンライン署名認証とも呼ばれる.オフライン署名認証は,既に書かれた純正署名(本物の署名)データと新し提出された署名データを比較判定するもので,一般的には,一般的には二次元座標値の類似性で個人認証を行う方式である.一方,オンライン署名認証は,タブレットなどの座標入力装置上に筆記された署名を利用する個人認証方式である.ペン先の座標,筆圧などを一定時間間隔で

サンプリングして得られる時系列情報を署名の運筆情報として捉え、あらかじめ登録した基準となる署名データと入力署名の運筆情報を照合することにより本人の書いた署名であるかを判定する。

1.2.4 ジェスチャ

手指動を用いた個人認証の方法. 手指の形状および動作はカメラより撮影する。「じゃんけん」のように、手指の動作にそれぞれ個人固有の特徴が含まれていることに着目して、この手指動情報を特徴量として用いている。動作であるため静止物と違い、真似ることが難しく、行動パターンの変更も可能な特徴を持つ。

1.3 生体認証における問題点

ここまで、代表的な認証方法で用いられている技術とその特徴について述べてきた。バイオメトリクスによる認証には、最初にあげた、普遍性、唯一性、永続性、収集可能性、といったもの以外にも必要とされるものがある。それは、安全性、経済性、社会的受容性、さらにバイオメトリクス特有の問題である認証精度である。さらに言えば、認証精度だけからではわからない盗難や偽造に強いという条件も必要となる。

銀行の ATM で手のひら静脈認証を行う場合の精度を例としてあげると、非接触型手のひら静脈認証を開発した富士通研究所によると、認識精度の評価実験では 7 万 5000 人、15 万人の手のひらデータを用い、本人受入率 99.99 % のとき、他人受入率は 0.00008 % 以下となっている。これを見て分かるように、生体認証は現在の認証技術としては優れているといえる。そのため、金融機関の ATM のようによりレベルの高いセキュリティーが求められるケースから、セキュアな情報へのアクセス権限の管理、入退室管理などに至るまで広く利用されるようになりつつある。

しかし、一方でリスクもある。生体情報という情報は本人しか持ち得ない固有不変の情報であるために、一度漏洩した場合にその認証が利用不可能になってしまうということである。これに対し、認証パターンが簡単に変更可能な動的特徴を用いた認証も利用され始めている。こちらの認証では個人のクセというものが非常に重要となってくるため、クセの出ないような単純な動作を登録した場合には認証エラーが頻繁に起きるなど、利用者が登録する動作によってセキュリティーや認証精度が左右されてしまうという問題に注意する必要がある。

第2章

従来研究

現在, 動作のクセから個人認証を行う方式が多く存在する. 動作には, 様々なものが存在するが, 本研究では手や指の動きに注目し, 高精度な認証アルゴリズムを構築することを目的とする. 手を動かし, そこから個人認証する技術には, 「閉じた手から V サインを作る」「1 から5 まで指を折って数える」といったものが存在する.[6] その中の1 つにグー, チョキ, パーと変化させたときの個人の癖から個人認証を行う研究 [1] がある.

次に, その研究での認証方式を述べ, 最後に問題点と本研究の目的についてまとめる.

2.1 システム全体の概要

手指動に含まれる個人の「くせ」をりようした手指動による個人認証システムを提案している. この認証方式では, 秘密情報として変更可能な動的パターンをもち, バイオメトリクスとして変更の難しく再現性が容易な個人的特徴(手形状, くせ)があり, 二つの性質をもった個人認証方式といえる.

2.2 認証方法

従来研究では, はじめにユーザの手指動を登録し, そのデータを用いて認証を行う. 登録過程, 認証過程は以下ようになる.

登録過程

1. 登録者の秘密情報となる手形状の組合せ(パスパターン)を選ぶ
2. 各手形状のテンプレートを1枚ずつ登録する
3. カメラの前で手指動を行う
4. 動作中の手形状と全登録テンプレートとを比較し, 一連の動作が終了するまで類似度を算出する
5. 何度か一連の動作を行い, 類似度の時刻変移データ(動きデータ)を算出し, これを登録する
6. 複数個の動きデータから認証時に用いる閾値を算出し, これを照合ように登録する.

認証過程

1. カメラの前で手指動を行う
2. パスパターンに相当する手形状の瞬間にキーを押す
3. 一連の動作と全登録テンプレートを比較して動きデータをとる
4. パスパターンの一致不一致, 及び動きデータの一致度のある閾値と比較し登録者どうかを判定する.

2.2.1 類似度算出

得られた動画像から手領域を抽出し, 登録してあるユーザの各テンプレートとの類似度を算出する. そのときの, 定義式 (1) (2) を以下に示す. このとき, 大きさや傾きについての正規化を行い, m, n は画像サイズ, V_{ij}, V'_{ij} は正規化後の比較対象の画素 (i, j) 成分である.

$$\|V\| = \sqrt{\sum_{i,j=0}^{i=n,j=m} V_{ij}^2} \quad (1)$$

$$\text{Similarity} = 1 - \frac{\|V - V'\|}{\|V\| + \|V'\|} \quad (2)$$

2.2.2 信頼限界と閾値

ユーザのパターンを登録する際, サンプル数が多いほど正確な認証が可能となる. しかし, 実用性を考えた場合, 登録者の負担となるため, 比較的少ないサンプル数で高い認証率を実現する必要がある. そこで, 従来研究では信頼限界を用いている. 以下に, 標本数が少ない場合に閾値を決定するための手法を述べる. 母集団の標準偏差 σ が未知で標本が n のとき, 標本の標準偏差 s は n が大きい場合には $\sigma \approx s$ となるが, n が小さいときの統計量 t は,

$$t = \frac{\bar{x} - \mu}{s/\sqrt{n}} \quad (3)$$

と定義され, この分布はスチューデントの t 分布と呼ばれる (図 4). 式 3 で, μ は母集団の平均であり, \bar{x} は標本平均である. s/\sqrt{n} の項は標本標準誤差と呼ばれ, ここでは $SE(\bar{x})$ と書く. 自由度が $n - 1$ のとき t 値の $(1 - \alpha) \times 100\%$ が $-t_{\alpha/2} \sim t_{\alpha/2}$ の範囲内にあるとすると, $(\alpha \times 100)\%$ 信頼限界の式は,

$$\bar{x} - t_{\frac{\alpha}{2}} SE(\bar{x}) \leq \mu \leq \bar{x} + t_{\frac{\alpha}{2}} SE(\bar{x}) \quad (4)$$

と求めることができる.

例えば, グーの手形状のときキーを押した瞬間の類似度が 5 回の試行でそれぞれ 0.800, 0.850, 0.820, 0.835, 0.810 だったとすると, このときの 99% 信頼限界は, 自由度 4, $t_{0.005} = 4.60$

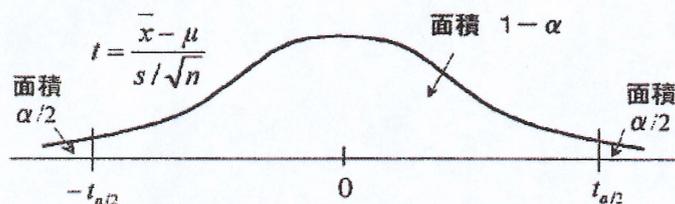


図4 tの分布

であるため

$$0.785 \leq \mu \leq 0.861 \quad (5)$$

となる。

2.3 従来手法のまとめ

ここまで、従来手法についての簡単な説明を述べた。次に、ここでは従来手法の問題点について述べる。

従来手法では、動画像の各フレームとユーザがあらかじめ登録しておいたグー、チョキ、パーの3つのテンプレートとの類似度(図5)のうち各フレームにおける最大類似度(図6)とその変化の仕方を利用している。

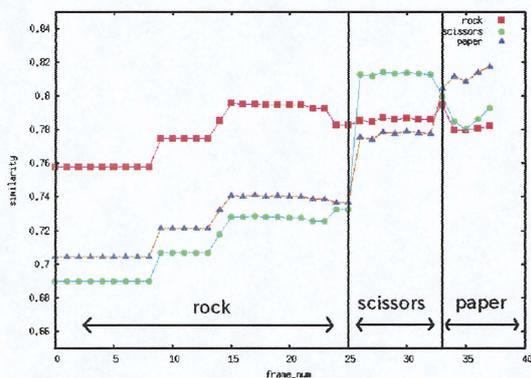


図5 類似度算出結果

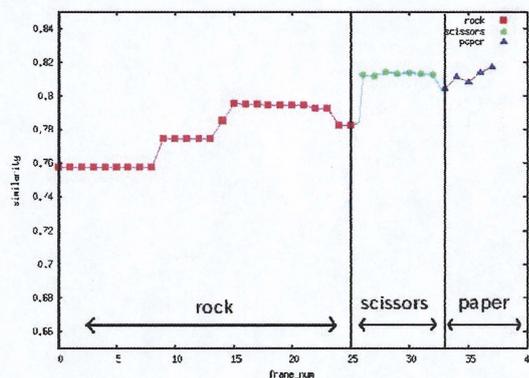


図6 各フレームにおける最大値

さらに動きデータとしては、以下の6つの特徴量を抽出する。

1. グーの手形状にし、キーを押した瞬間(認証開始)における登録テンプレートとの類似度
2. 現在の手形状と登録テンプレートの類似度が98%信頼限界に達するまでの時間
3. 1から類似度の99%信頼限界に達するまでの時間

4. チョキの手形状でキーを押した瞬間における登録テンプレートとの類似度
5. 4 から類似度の 99% 信頼限界に達するまでの時間
6. パーの手形状でキーを押した瞬間(認証終了)における登録テンプレートとの類似度

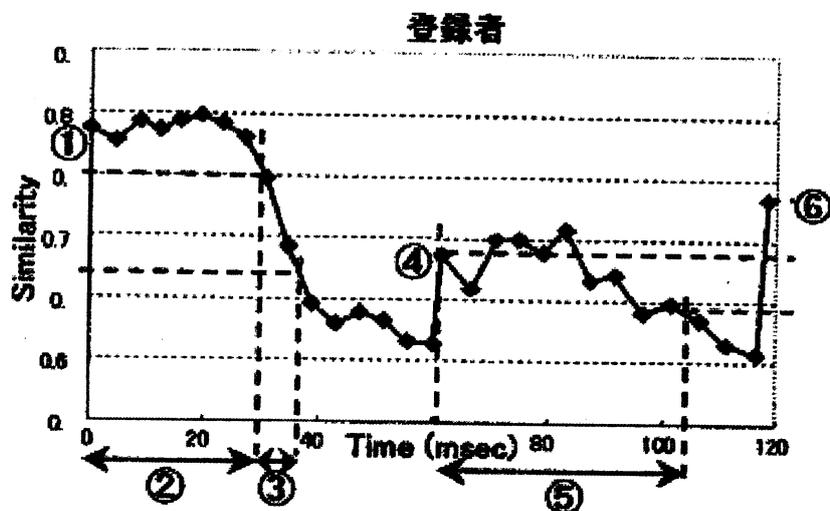


図7 動きデータ (6箇所)のデータを抽出

2.4 本研究の目的

従来手法の追試を行った結果,より類似したパターンを識別するには不十分であった.そこで本研究では,グー,チョキ,パーの一連の動作による認証方式に有効な特徴量が何かを検討し,その特徴量を用いることで認証精度を上げることを目的とする.

第3章

提案手法 1

認証精度を高めるためにはより有効な特徴量, 認証方法を検討する必要があった. そのため本研究では登録テンプレートとの類似度を上げるために, 類似度計算には相関係数を使い, 得られた類似度からより多くの有効な特徴量の抽出を行う. さらに識別には SVM を用いることで本人と他人の特徴量を学習させ, より精度の高い認証システムを提案する.

以下に類似度計算方法, 追加する特徴量, 認証方法について述べる.

3.1 類似度計算方法

従来研究と同様に, 撮影画像とユーザが登録しておいたテンプレート画像との類似度を算出する. ただし, 定義式は以下の正規化+ 相関係数の式とする.

$$R_{X,Y} = \frac{1}{S_{X,Y}} \sum_{y=0}^{h-1} \sum_{x=0}^{w-1} (T_{x,y} - \langle T \rangle) (I_{X+x,Y+y} - \langle I_{X,Y} \rangle)$$

このとき

- $R_{x,y}$
探索対象画像 (X, Y) 位置の演算結果
- (w, h)
テンプレートの幅と高さ
- $T_{x,y}$
テンプレートの (x, y) ピクセル値 $x = [0, w-1], y = [0, h-1]$
- (W, H)
探索対象画像の幅と高さ
- $I_{X+x,Y+y}$ 探索対象画像の (X+x, Y+y) ピクセル値 $x = [0, W-w+1], Y = [0, H-h+1]$
- $S_{X,Y}$

$$\sqrt{\sum_{y=0}^{h-1} \sum_{x=0}^{w-1} (T_{x,y})^2 \sum_{y=0}^{h-1} \sum_{x=0}^{w-1} (I_{X+x,Y+y})^2}$$

- $\langle T \rangle$

$$\frac{1}{wh} \sum_{j=0}^{h-1} \sum_{i=0}^{w-1} T_{ij}$$

- $\langle I_{X,Y} \rangle$

$$\frac{1}{wh} \sum_{j=0}^{h-1} \sum_{i=0}^{w-1} I_{X+i,Y+j}$$

3.2 追加する特徴量について

ここでは、追加する特徴量について説明する。まず、下に示す図上で記した類似度計算方法によりある被験者試行に対し、各フレーム画像と登録テンプレートとの類似度を計算しプロットしたものが以下の図 8,9,10 となる。グーを提示しているときはグーテンプレートとの類似度、チョキを提示しているときはチョキテンプレートとの類似度、パーを提示しているときはパーテンプレートとの類似度がそれぞれ最大になる。

基本的には、図 8 のように最大類似度と 2 番目、3 番目の類似度は離れた値になるのだが、人によっては、図 9 のようにチョキ提示時において最大類似度となるチョキテンプレートとパーテンプレートとの類似度が近い値になったり、パー提示時において、最大類似度となるパーテンプレートとチョキテンプレートとの類似度が近い値になるといったように、各フレームにおける最大類似度だけでなく、フレーム毎における、2 番目、3 番目の類似度にも有効な特徴量があると判断したため、本研究ではこちらの特徴量についても有効利用する方法を提案する。

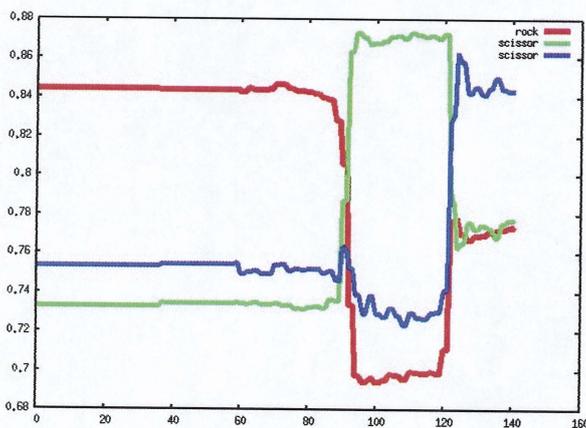


図 8 被験者1

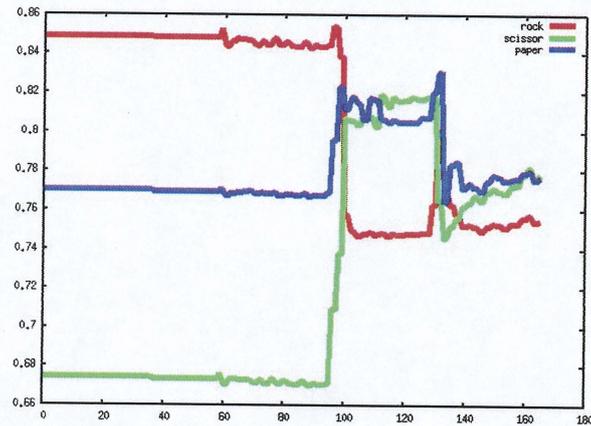


図9 被験者2

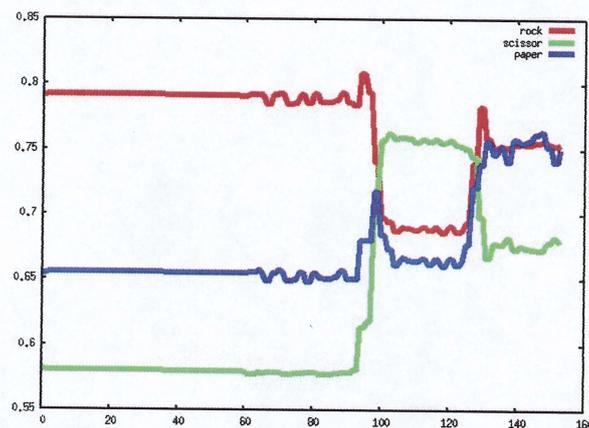


図10 被験者3

3.3 認証方法

ここでは、認証の際、判定に用いる特徴量について述べる。それらの特徴量を算出後、求めた値をSVMに学習させ、識別を行う。

次に追加する特徴量、後にSVMを用いた認証方法について述べる。

前の節で述べたように判定基準には、最大類似度のみではなく、2番目、3番目の特徴量も用いる。①、④は、従来手法でも用いていたので、具体的には以下の図11の②、③、⑤、⑥を判定基準に用いる特徴量として追加する。

①、②、③、④、⑤、⑥はそれぞれ次に示す特徴量となっている。

- ① 認証開始時にキーを押した瞬間から、ゲーテンプレートとの類似度が99%信頼限界に達するまでの時間

- ② 認証開始時にキーを押した瞬間から、パーテンプレートとの類似度が 99 % 信頼限界に達するまでの時間
- ③ 認証開始時にキーを押した瞬間から、チョキテンプレートとの類似度が 99 % 信頼限界に達するまでの時間
- ④ 手形状をチョキにした瞬間から、チョキテンプレートとの類似度が 99 % 信頼限界に達するまでの時間
- ⑤ 手形状をチョキにした瞬間から、パーテンプレートとの類似度が 99 % 信頼限界に達するまでの時間
- ⑥ 手形状をチョキにした瞬間から、グーテンプレートとの類似度が 99 % 信頼限界に達するまでの時間

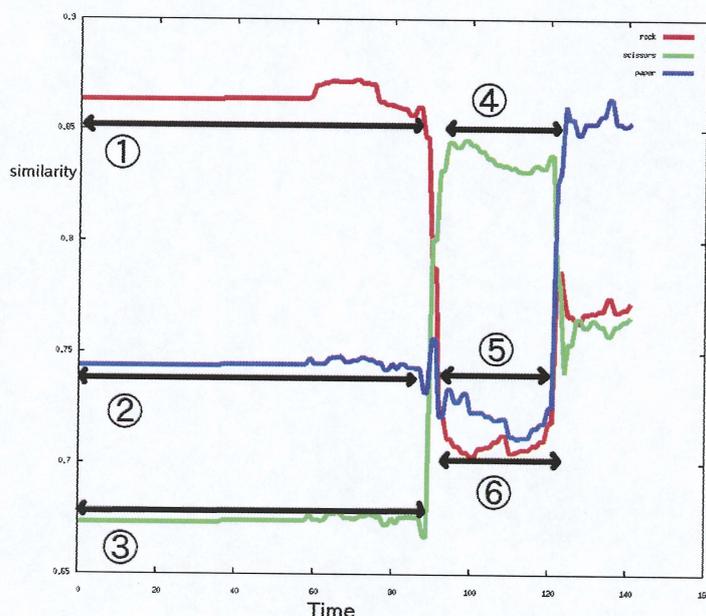


図 11 追加した特徴量

それらの値を求めた後、従来手法で用いられていたグーになった瞬間の最大類似度、チョキになった瞬間の最大類似度、パーになった瞬間の最大類似度の3つを求め、計9個の値を個人の動きデータとして SVM に学習させ識別を行う。識別を行う前に次の節では、まず SVM について簡単に述べる。

3.4 SVM について

サポートベクターマシン (SVM) は、教師あり学習を用いる識別手法の1つである。パターン認識や回帰分析へ適用できる。

サポートベクターマシンは、未学習データに対して高い識別性能を発揮することができる。[5] 基本的には、線形入力素子を利用して2クラスのパターン識別器を構成する手法である。訓練サンプルから、各データ点との距離が最大となる分離平面を求めるマージン最大化という基準で線形入力素子のパラメータを学習する。

本実験では、SVMのプログラムとして <http://www.csie.ntu.edu.tw/~cjlin/libsvm/> からダウンロードしたものをを用いる。

その中で主に使用したプログラムは以下の3つである。

- svm-scale 学習させたいデータを正規化するプログラム
- svm-train 学習データから予測のためのモデルを生成するプログラム
- svm-predict 予測を実行するプログラム

さらに、以下のようなオプションが指定できる。

`-s svm_type`: SVMタイプの指定(デフォルト 0)

タイプには以下のものを指定できる。

- 0 C-SVM
- 1 nu-SVC
- 2 one-class SVM
- 3 epsilon-SVR
- 4 nu-SVR

`-t kernel_type` : カーネル関数の指定(デフォルト 2)

- 0 線形(linear)
- 1 多項式 (polynormial)
- 2 RBF (radial basis function)
- 3 シグモイド (sigmoid)

`-d degree`:カーネル関数の degree の指定(デフォルト 3)

`-g gamma`:カーネル関数の gamma の指定(デフォルト $1/k$, k は訓練セットのインデックスの最大の値, つまり入力ベクトルの次元)

`-r coef0`: カーネル関数の coef0 の指定(デフォルト 0)

`-c cost`:コストパラメータの指定(C-SVC, epsilon-SVR, nu-SVR で使用, デフォルト 1)

`-n nu`:nuパラメータの指定(nu-SVC, one-class SVM, nu-SVR で使用, デフォルト 0.5)

- p epsilon: set the epsilon in loss function of epsilon-SVR(デフォルト 0.1)
- m cachesize:使用キャッシュメモリサイズの指定(単位 MB, デフォルト 40)
- e epsilon: 終了の閾値の設定(デフォルト 0.001)
- h shrinking:whether to use the shrinking heuristics,0 or 1(デフォルト 1)
- wi weight:クラス i に対するコストパラメータの重み, $weight * C$ (デフォルト 1)
- v n: n -fold のクロスバリデーションを実行

オプションについて本研究では,SVM のタイプ, カーネル関数の指定についてはデフォルトのままで行うものとする.SVM を用いることで, 図 12 のように本人と他人を識別するための閾値を自動で決めることができる.

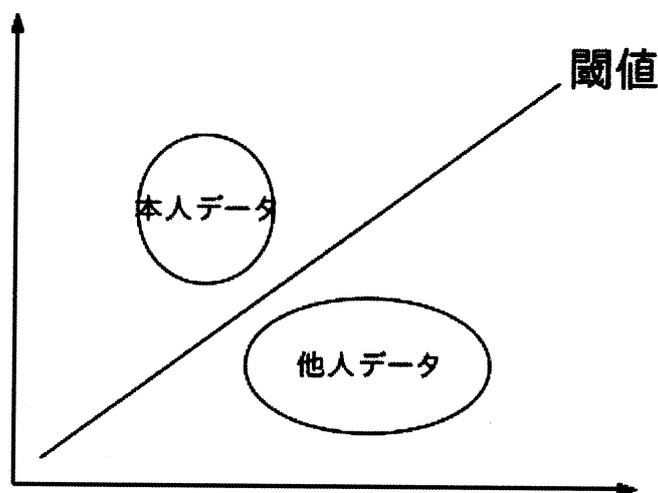


図 12 SVM による識別

次に SVM 使用時に, 学習フェーズ, 認証フェーズそれぞれについて具体的にどのようなことを行うのかについて述べる.

• 学習フェーズ

1. 動画像の各フレームと, 登録しておいた各テンプレート画像と比較し, 類似度算出する.
2. その後, 本人, 他人それぞれで算出された類似度から, 動き特徴を抽出し, 学習させる.

• 認証フェーズ

1. 新しく撮影された動画像についても, 学習時と同様に動き特徴を抽出する.
2. その後, 登録してある学習モデルと分類器により本人かどうかを判定

図は次に示す図 13,14 となる.

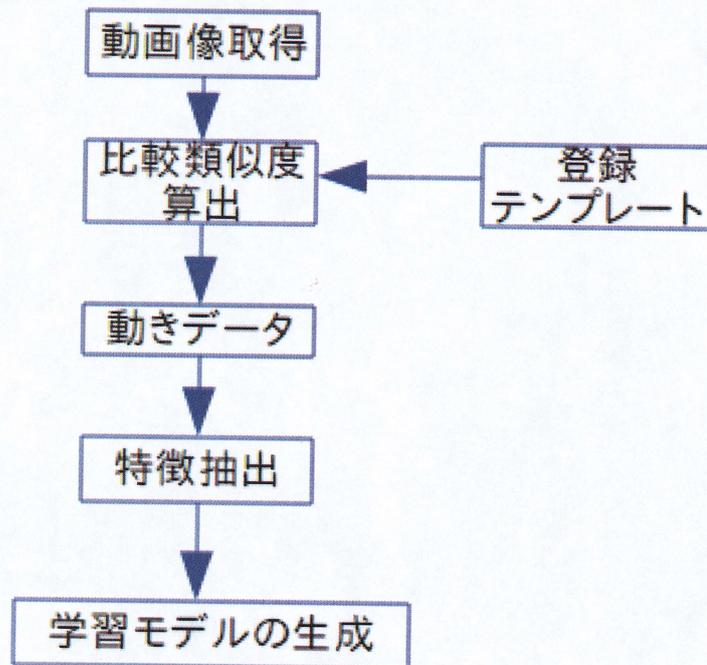


図 13 学習フェーズ

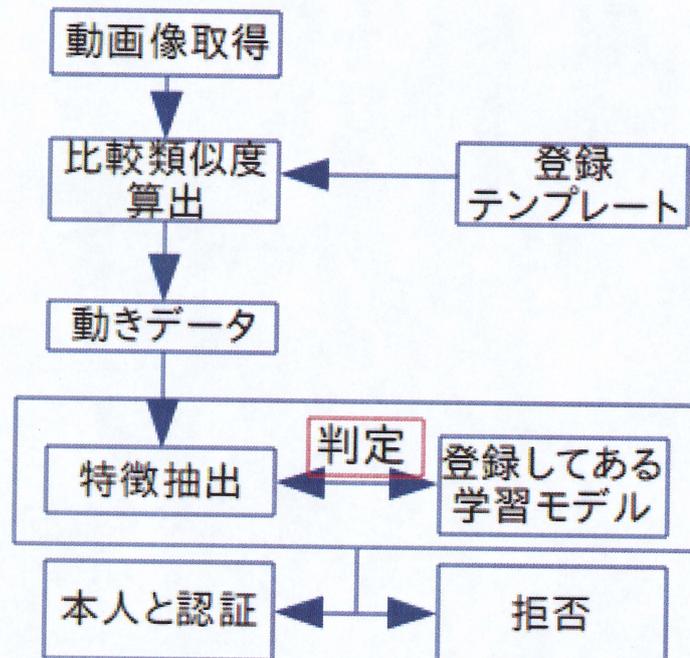


図 14 認証フェーズ

第4章

提案手法2

登録テンプレートとの類似度ではなく、撮影した動画像で変化を観察した所、類似度が高い場合でも手の形状に差が認められることから、この章ではそれらに関する特徴量の追加、さらに類似度の値をそのまま利用するのではなく類似度の差(比)を利用することでより精度の高い認証を行う方法を提案する。大まかな認証手順は以下のようになる。

1. 動画像取得
2. 各フレーム画像と登録テンプレートでの形状の相似度と類似度を算出
3. 形状の相似度を用いて、登録してある本人パターンに近いものを取り出す
4. 本人候補として選ばれたパターンについてのみ、類似度から得られる動きデータ(類似度の比)を利用し学習させておいた SVM により識別を行う

次に形状に関する特徴量の求め方、後に類似度の比の利用方法と認証方法の詳細について述べる。

4.1 形状特徴抽出

算出された類似度が、登録ユーザと似ている場合でも、手形状(輪郭)の差が認められることから、提案手法では、これに関する特徴量も追加する。

4.1.1 輪郭のマッチング

2つの輪郭を比較する最も簡単な方法は、輪郭モーメントを計算することである。モーメントとは、簡単に説明するとその輪郭のピクセルすべてを積分することで、計算される輪郭の全体的な特徴だといえる。

本研究では、いくつかあるモーメントの中でも Hu 不変モーメントと呼ばれるものを用いてマッチングを行う。こちらについて説明する前に、モーメント、中心モーメント、について簡単に説明をする。輪郭(p,q)モーメントは一般的に以下のように定義される。 $m_{p,q} = \sum_{i=1}^n (x,y)x^p y^q$ ここで p は x の次数で q は y の次数。ここで、次数は、対応する要素がここで示した合計を計算するのに取られるべき乗を意味している。この合計は、輪郭境界のピクセル全体(この式内では n で表現)に及ぶ。そのため、p と q が両方とも 0 である場合、 $m_{0,0}$ は実際には輪郭ピクセルの長さになる。

今説明したモーメントの計算は、2つの輪郭の比較に使うことができる輪郭の基本的な特徴を与え

る.しかし,この計算から得られるモーメントはほとんどの実践的なケースでは,比較を行うのに最もよいパラメータではない.特に,正規化されたモーメントを使うことがほとんどである.

こちらを使うことで,サイズの違い,傾きについて正規化された特徴を得ることができる.正規化されたモーメントは, m_{00} を適切にべき乗したものですべて除算される点を除いて中心モーメントと同じとなっていて,中心モーメントについては,以下の定義式より算出される.

$$\mu_{p,q} = \sum_{i=0}^n I(x,y)(x-x_{avg})^p(y-y_{avg})^q \quad (6)$$

このとき, x_{avg}, y_{avg} は次のようになっている.

$$x_{avg} = m_{10}/m_{00}, y_{avg} = m_{01}/m_{00}$$

以下は正規化されたモーメントの定義式

$$\eta_{p,q} = \frac{\mu_{p,q}}{m_{00}^{(p+q)/2+1}}$$

そして,最後にHu不変モーメントについて説明する.Hu不変モーメントは中心モーメントの1次結合となっている.ここでの考え方は,異なる正規化中心モーメントを組み合わせることで,スケーリング,回転,反射に不変なやり方で画像の様々な側面を表現する不変関数を作成することができる.実際に,Huモーメントの定義式について以下に示す.

$$h_1 = \eta_{20} + \eta_{02}$$

$$h_2 = (\eta_{20} + \eta_{02})^2 + 4\eta_{11}^2$$

$$h_3 = (\eta_{30} - 3\eta_{12})^2 + (3\eta_{21} - \eta_{03})^2$$

$$h_4 = (\eta_{30} + \eta_{12})^2 + (\eta_{21} + \eta_{03})^2$$

$$h_5 = (\eta_{30} - 3\eta_{12})(\eta_{30} + \eta_{12}) + ((\eta_{30} + \eta_{12})^2 - 3(\eta_{21} + \eta_{03})^2) \\ + (3\eta_{21} - \eta_{03})(\eta_{21} + \eta_{03})(3(\eta_{30} + \eta_{12})^2 - (\eta_{21} + \eta_{03})^2)$$

$$h_6 = (\eta_{20} - \eta_{02})((\eta_{30} + \eta_{12})^2 - (\eta_{21} + \eta_{03})^2) + 4\eta_{11}(\eta_{30} + \eta_{12})(\eta_{21} + \eta_{03})$$

$$h_7 = (3\eta_{21} - \eta_{03})(\eta_{21} + \eta_{03})(3(\eta_{30} + \eta_{12})^2 - (\eta_{21} + \eta_{03})^2) \\ - (\eta_{30} - 3\eta_{12})(\eta_{21} + \eta_{03})(3(\eta_{30} + \eta_{12})^2 - (\eta_{21} + \eta_{03})^2)$$

4.2 認証方法

ここまで、新しく追加する形状に関する特徴量について述べた。本節では、その形状特徴と類似度を使用して認証を行う方法について述べる。まず、入力されたパターンを形状特徴を利用し、本人と似ているかそうではないかの2つのグループに分ける。図で示すと以下の図15,16となる。

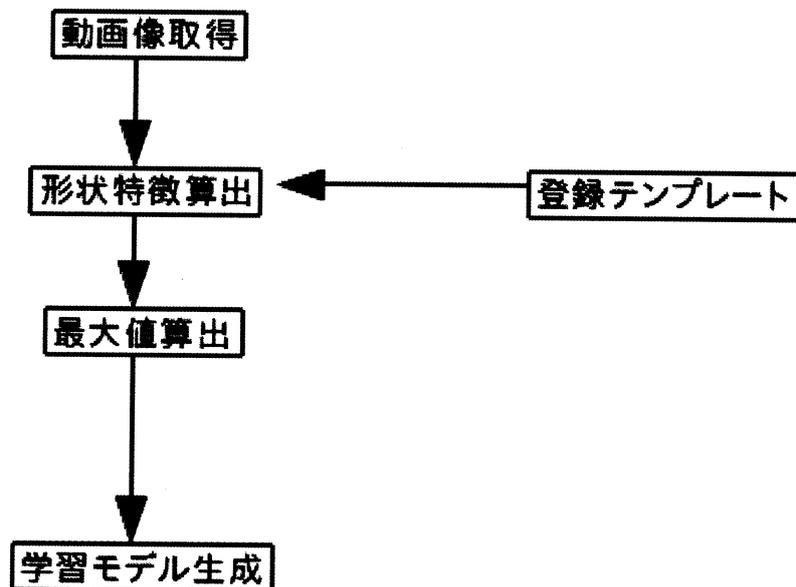


図15 学習フェーズ

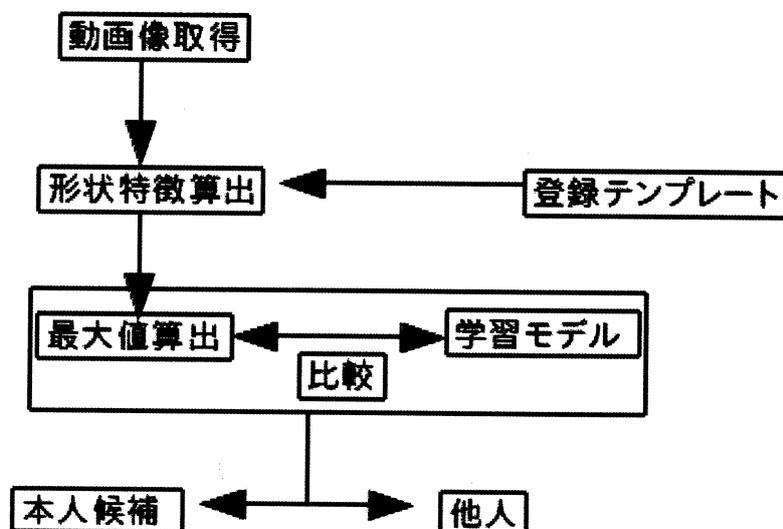


図16 認証フェーズ

● 学習フェーズ

1. 現在の動画像と登録テンプレートとの2枚の画像について、上で紹介した方法によりマッチングを行い相似度を算出する
2. 算出後、グー、チョキ、パーとそれぞれ手形状が変化した際の、最大値を3つ取り出す
3. 3つの最大値を学習させる

● 認証フェーズ

1. 学習時と同様に相似度を算出し、最大値を取り出す
2. 最大値を使い、学習モデルにより識別

本人候補として分類されたパターンについては、次に類似度の変化の仕方から得られた特徴量を学習後、本人か他人かの識別をする。その際の詳細について、次に示す。

本人候補のパターンを、本人か他人かで識別するのに用いる特徴量は以下の9つである。

特徴量1 グーになった瞬間の類似度

特徴量2 チョキになった瞬間の類似度

特徴量3 パーになった瞬間の類似度

初期フレームにおけるパーテンプレートとの類似度を1とした場合の

特徴量4 チョキ提示時のグーテンプレートとの類似度を比で表したもの

特徴量5 パー提示時のグーテンプレートとの類似度を比で表したもの

初期フレームにおけるチョキテンプレートとの類似度を1とした場合

特徴量6 チョキ提示時のチョキテンプレートとの類似度を比で表したもの

特徴量7 パー提示時のチョキテンプレートとの類似度を比で表したもの

初期フレームにおけるパーテンプレートとの類似度を1とした場合の

特徴量8 チョキ提示時のパーテンプレートとの類似度を比で表したもの

特徴量9 パー提示時のパーテンプレートとの類似度を比で表したもの

図 17,18,19 に示す差がそれぞれ特徴量となっている。

提案手法2 では、この9個の特徴量を算出後、それらを SVM に学習させることで識別を行う。

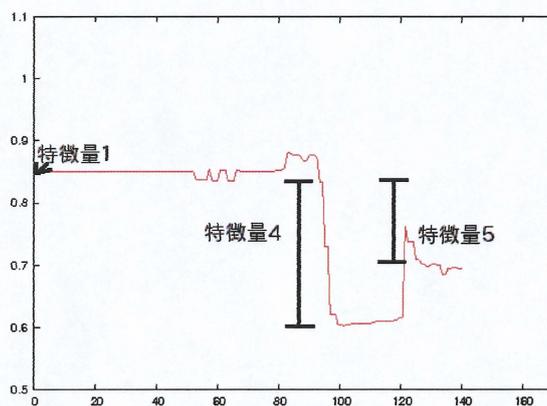


図 17 グーテンプレートとの類似度から得られる特徴量

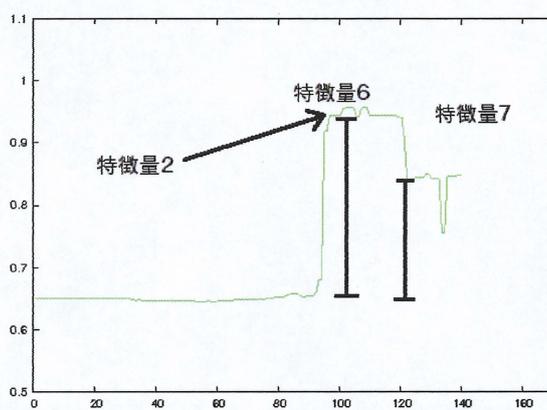


図 18 チョキテンプレートとの類似度から得られる特徴量

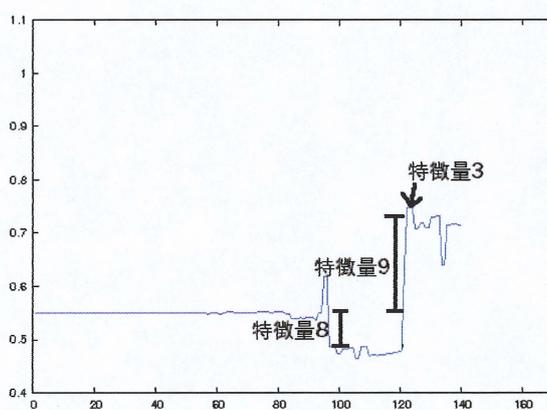


図 19 パーテンプレートとの類似度から得られる特徴量

第5章

評価実験

この章では、実験を行うことで提案した認証方法の有効性を確かめる。比較を行うために、従来手法、提案手法の両方について精度を求める。

5.1 対象とする動画像について

評価データとしては、本人30(個)、他人17(人)×10(個)の計200個の動画を対象とする。動画の内容はグー、チョコキ、パーを順番に10回ずつ提示してもらい、それをUSBカメラで撮影したものとする。(カメラのフレームレートについては30fps)

5.2 実験結果

実験結果を示す前にまず、本研究で用いる認証の精度について述べる。今回、認証精度には本人受入率と他人拒否率で用いることとする。それぞれは以下を意味する。

- 本人受入率 本人データを本人として受け入れる割合
- 他人拒否率 他人データを他人であると拒否する割合

つまり、本人受入率が低くなるほど、本人であるのにも関わらず拒否されてしまうということになり使いづらいシステムとなる。それに対し、他人拒否率が低くなると、他人であるのにも関わらず本人と判定されてしまい、他人が「なりすまし」しやすくととも危険なシステムとなってしまう。この二つはどちらかの精度を上げると、どちらかの精度が下がるといったようなトレードオフの関係にあり、このバランスを上手く取る必要がある。

精度評価については、2分法を使用するものとする。つまり、手持ちのデータを学習用と評価用に2分し、交換することによって2回実験を行い総合評価する。次に、従来手法、提案手法1、提案手法2のそれぞれについての結果を示す。

本人受入率	30個中26個	86%
他人拒否率	170個中167個	98%

表1 従来手法結果

本人受入率	30 個中 24 個	70 %
他人拒否率	170 個中 167 個	98 %

表 2 提案手法 1 結果

本人受入率	30 個中 29 個	96 %
他人拒否率	170 個中 167 個	98 %

表 3 提案手法 2 結果

5.3 考察

図 20~25 は各テンプレートとの類似度算出後、その変化をプロットをしたものとなっている。1 人につき 10 回分の試行をプロットしたもので、横軸が時間軸(フレーム数)、縦軸が各テンプレートとの類似度の大きさを表している。その中でも、赤線はグーテンプレートとの類似度、緑線はチョコキテンプレートとの類似度、青線はパーテンプレートとの類似度を表している。グラフにより、6 人のデータを比較してみると、6 人ともグーからチョコキへの変化は、80~100 フレームまでの間に变化しており、チョコキからパーへの変化は、120 フレーム前後で同じように変化している。また被験者 1, 3 を見ても分かるように本人間の試行でも、その時間差にバラツキがありに手形状の遷移時間差にそれほど違いがないことが分かる。そのため、図 26 のような状態になってしまい閾値の決定が難しかったこと、さらにそのようなあまり違いの出ない識別に有効でない特徴量を増やしてしまったため、結果として提案手法 1 が従来手法よりも精度が低下したと考えられる。

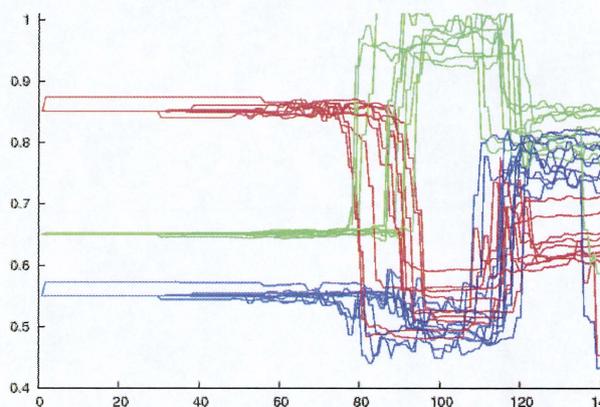


図 20 被験者 1

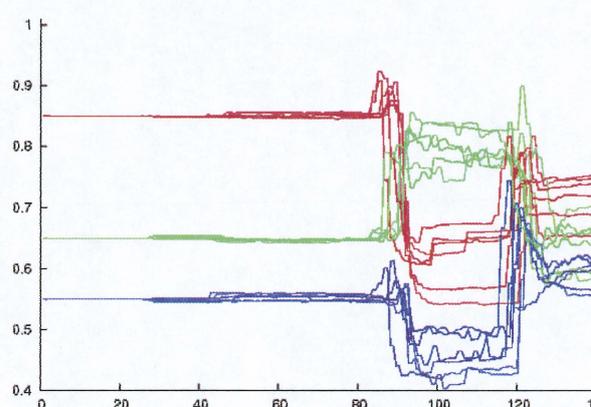


図 21 被験者 2

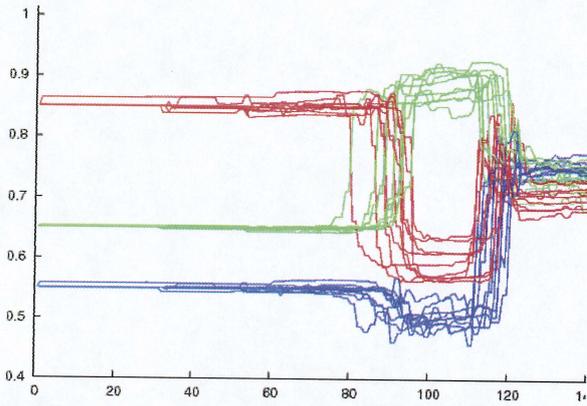


図 22 被験者3

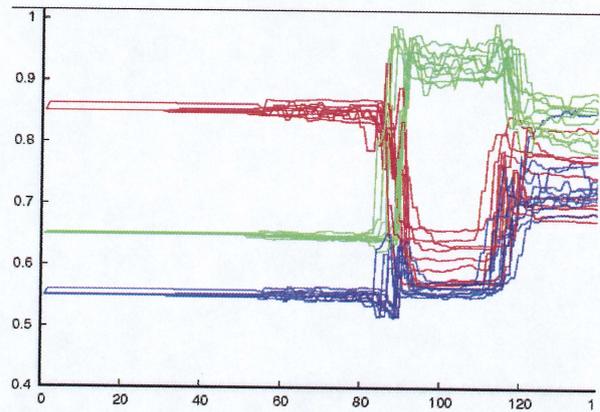


図 23 被験者4

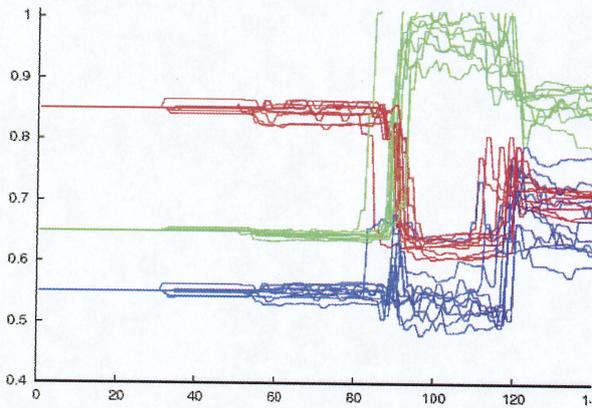


図 24 被験者5

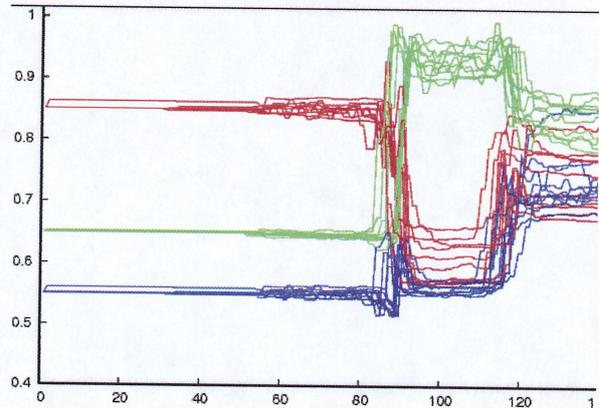


図 25 被験者6

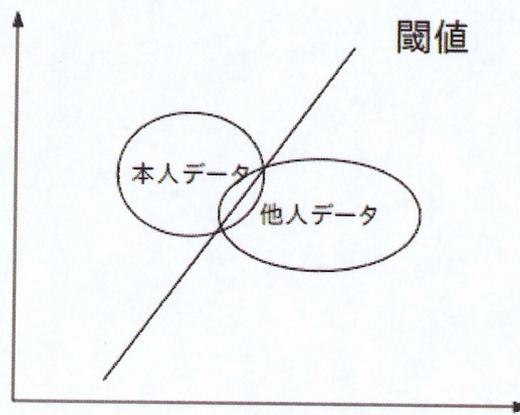


図 26 本人間バラツキが他人間のバラツキと重なってしまう場合

提案手法2 の本人受入率の精度が従来手法よりも向上した要因としては、以下の2 つが考えられる。

- 提案手法1 であまり有効ではなかった、時間遷移の差を省き、手形状間に関する類似度の違いを特徴量として用いたこと
- 手の形状に関する特徴量を追加したこと

まず、図 27 を見ると、被験者 1 と被験者 2 について、手形状の類似度の変化の仕方が似ていることが分かる。しかし、図 28,29 を見てみると、グーの形状においては握り方の違い、パーの形状においては指の開き方が少し異なることが分かる。この形状の違いを特徴量として利用するために、4 章で述べた輪郭のマッチングを使う。マッチング後その相似度をプロットしたものが図 30 となる。

このとき、図 27,28,29,30 はそれぞれ次を表している。

図 27 被験者 1, 2 にそれぞれ 10 回の試行を行ってもらい、その類似度変化を重ねて表示したもの

図 28,29 被験者 1, 2 についてそれぞれ試行を行ってもらったときの、任意のフレーム画像

図 30 被験者 1, 2 にそれぞれ 10 回の試行を行ってもらい、その形状変化を重ねて表示したもの。

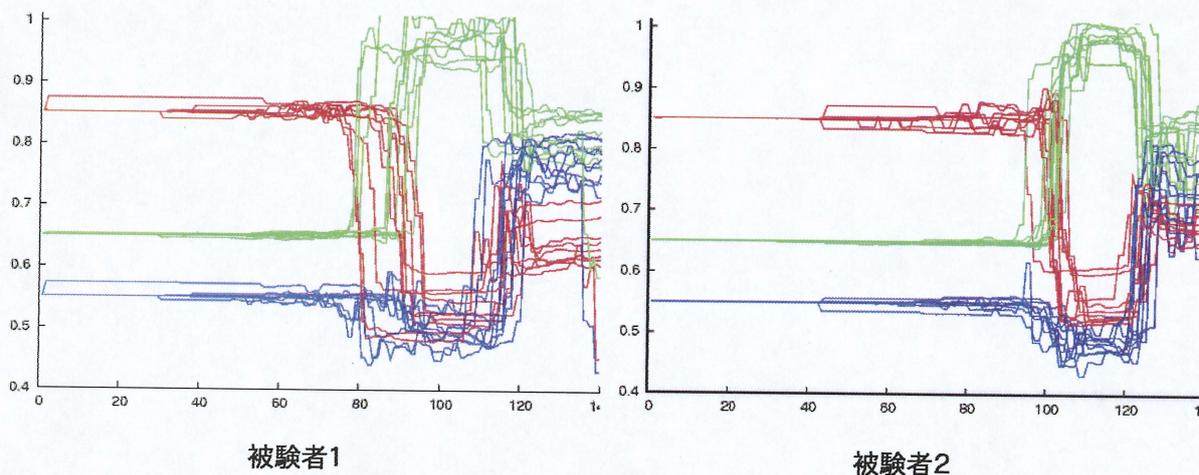


図 27 類似度の変化の仕方が近い例

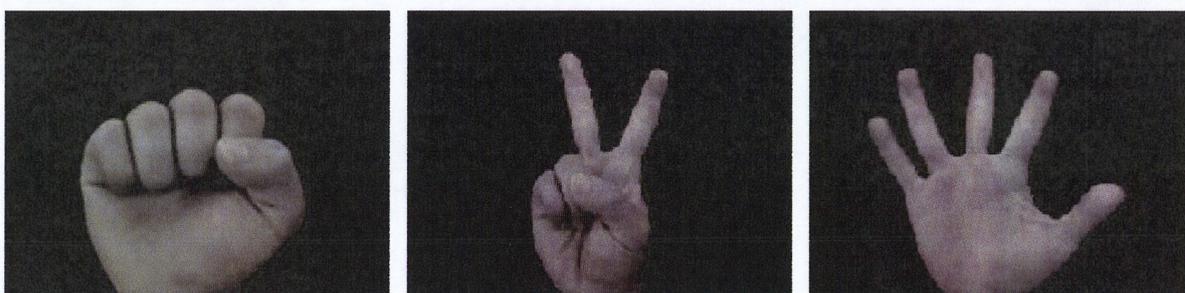


被験者1 のグー

被験者1 のチョキ

被験者1 のパー

図 28 被験者1 の各手形状

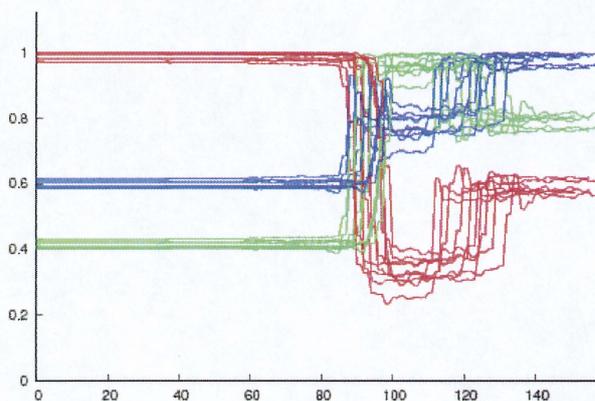


被験者2 のグー

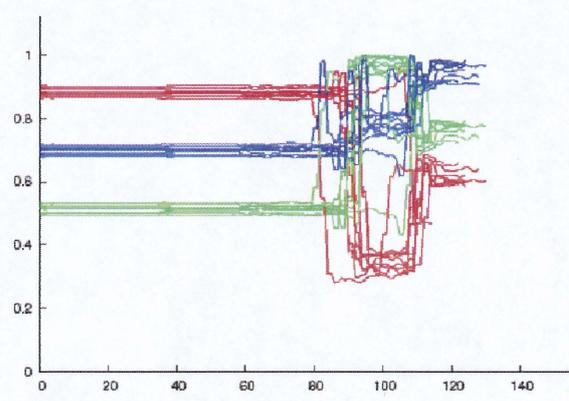
被験者2 のチョキ

被験者3 のパー

図 29 被験者2 の各手形状



被験者1



被験者2

図 30 手形状の変化の違い

おわりに

本研究では、グー、チョキ、パーによる個人認証において、より有効な特徴量を検討し、その特徴量を用いた認証方式を提案し実装した。そして、提案手法の有効性を確かめるために、18名の被検者に対して、10回撮影したものを評価データとして実験を行った。実験では、1名の動画から典型的な手形状のフレームを取り出し、手領域の抽出をしてサイズや正規化をした後、上記でそれぞれ提案した特徴量を本人のパターンとして登録する。その後残りの17名について同様にして特徴量を計算し、登録パターンとの差異に基づいて、本人か他人かの識別を行う。このとき、識別にはSVMを使用した。この結果、本人受入率96%、他人拒否率98%を得ることができ、従来手法よりも認証精度を改善することができた。

この手法の精度と安定性をさらに向上させ、他の手形状動作に適用可能とすることにより、撮影機能をもつ機器の認証法として有効なものの一つになると期待される。

謝辞

日ごろから多くの御指導を頂きました太田義勝教授，鈴木秀智准教授に深く感謝いたします。そして，日頃何かとお世話になりました落合美子事務員に感謝いたします。また，本論文作成にあたって特にお世話になりました鈴木秀智准教授に深く感謝いたします。最後に，日頃から熱心に討論して頂いた研究室の諸氏に感謝いたします。

参考文献

- [1] 長田 礼子, 尾崎 哲, 青木 輝勝, 安田 浩, "手指動からの特徴抽出によるリアルタイム個人認証", 電子情報通信学会論文誌.D-2, 情報・システム, 2-パターン処理 J84-D-2(2), 258-265, 2001
- [2] 堀 隆之, 大谷 淳, 棚沢 順, "テンソル分解に基づく人物の歩行動作を用いた個人認証", 電子情報通信学会技術研究報告.PRMU, パターン処理・メディア理解 108(363), 87-92, 2008
- [3] Anil K. Jain, Arun Ross, and Salil Prabhakar, 2004. An Introduction to Biometric Recognition. IEEE Trans. on Circuit and System for Video Technology, Special Issue on Image and Video-Based Biometrics, 14(1), 4-20
- [4] 瀬戸洋一, 2002. サイバーセキュリティにおける生体認証技術, 共立出版株式会社.
- [5] サポートベクターマシン wiki <http://ja.wikipedia.org/wiki/サポートベクターマシン>
- [6] http://www.ntt-east.co.jp/whats_up/08/kanren01.html

付録

実験に使用したプログラム

実験に使用したプログラムは/home/ichinose/tmp/OpenCV-2.0.0/samples/c/shuuron_program/finger_ディレクトリの下においてある.

- 類似度算出するプログラム janken_g3eff.cpp
- コンパイル方法 g++ -ggdb 'pkg-config opencv --cflags --libs' -o 実行ファイル名 janken_g3eff.cpp LabelingW.h
- 実行コマンド ./実行ファイル 読み込む動画(.avi) 類似度を書き出すためのファイル名 各フレームについて最大値を書き出すためのファイル名 キーを押したときの類似度を書き出すためのファイル名 切り出す画像の位置設定 画像サイズ

学習と識別には, さらにその下のディレクトリである libsvm-3.1 においてあるプログラムを使用する.