

指先署名における時間経過のロバスト性に関する考察

中島もも子[†] 鹿嶋雅之[†] 佐藤公則[†] 渡邊睦[†]

バイオメトリクスにおいて、行動的特徴は時間経過による経時変化によって、本人認証ができなくなる恐れがある。本論文では、手形状と指先署名によるマルチモーダル個人認証システムにおける時間経過のロバスト性を調査する。2週間ごとに認証と、毎日認証の2通りの認証実験を行った。認証実験の結果、2週間ごとに認証を行ったとき書き直しが1, 2回発生するが本人認証できた。また、毎日認証の方は書き直しをせずに本人認証できた。本システムでは、リファレンスの更新及びサイン認証に用いるパラメータの更新が行われており、それらによって特徴の経時変化への対応が可能である。本システムは時間経過に対してロバスト性があることを示す。

Consideration about the robustness for the time progress in a fingertip signature

MOMOKO NAKASHIMA[†] MASAYUKI KASHIMA[†]
KIMINORI SATOU[†] MUTSUMI WATANABE[†]

In biometrics, it is the aggressive feature may be unable to be corroborated over time. In this paper, the robustness for the time progress in the multimodal verification system using fingertip signature and the shape of a hand is investigated. We experimented in two types, one is the experiment in every 2 weeks, and other is the experiment in every day. The result was able to be attested every two weeks, although rewriting occurred once or twice. In the case of each day, they were able to verification without a rewrite. Since a reference and a parameter are updated, even if this system passes time, it can be used. Therefore, it turned out that this system has robustness for time progress.

1. はじめに

近年、セキュリティの高さから生体認証の普及が進んでおり、広く研究されている。生体認証は身体的特徴を用いたものと行動的特徴を用いたものに大別される[1]。

しかし、指紋認証や虹彩認証といった身体的特徴を用いた生体認証は、人工物による偽造の可能性が指摘されている[2]。一方、行動的特徴を用いた生体認証は身体的特徴を用いたものよりも成りすましに強いという特徴があるが、行動的特徴のみを用いた生体認証には、パターンが漏えいすることによって偽造が発生する可能性がある[3]。

さらに、生体認証では経時変化によって本人認証ができなくなるという恐れがある。

本研究では、サインを登録した後の時間経過による認証率について検証を行い、手形状と指先署名によるマルチモーダル個人認証における時間経過のロバスト性について考察する。

2. 関連研究について

身体的特徴を用いたシステムとしては、指紋、虹彩、静脈などを用いるものが提案され、一部は販売されている。顔認証などの身体的特徴を用いたシステムは、経時変化による認証率低下が起きるため、経時変化への対応を行って

いるものがある[4]。また、行動的特徴を用いたシステムには、署名、声、歩容などの特徴を用いているものがある[5]。

署名を用いた認証には、タブレットやペンなどを用いているものが多い。本研究ではwebカメラを用いて署名を取得しており、タブレットなどの特殊な機器を必要としないという利点がある[6][7]。

マルチモーダル個人認証には、複数の身体的特徴を用いたものや、身体的特徴と行動的特徴を組み合わせたものがある[8][9]。本研究のシステムは、身体的特徴の手形状と行動的特徴のサインを組み合わせるマルチモーダル個人認証システムである。

3. マルチモーダル個人認証システムについて

本システムは、カメラから得た動画像から手形状画像およびサイン情報を取得し、身体的特徴と行動的特徴の両面から認証を行うマルチモーダル認証システムである。2つの異なる性質の特徴を組み合わせることで偽造可能性を大きく下げっており、評価実験の結果 FRR=1.5%, FAR=0%を得ている[10]。

処理手順は大別してデータ取得フェーズ、登録フェーズ、認証フェーズから成る。システムの手順を図1に示す。

3.1 データ取得フェーズ

データ取得フェーズでは、カメラによる動画像から手形状画像およびサイン筆記動作を取得する。データを取得するためのシステムの外観を、図2に示す。箱の上に取り付けられたwebカメラから撮影領域の動画像を取得する。

[†] 鹿児島大学 工学部

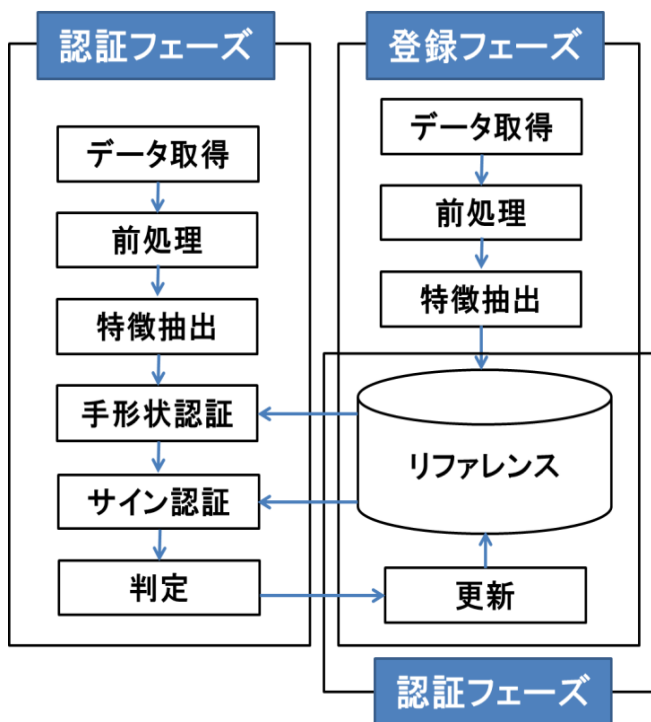


図1 システムの手順

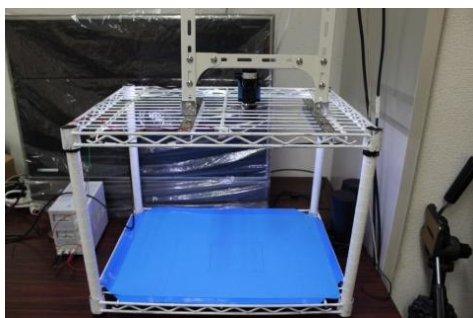


図2 システムの外観

手形状画像は、サイン筆記動作取得の際、書き始めとなるフレームの画像を取得して用いている。取得した画像は24ビットカラー画像として保存を行う。取得した手形状画像の例を図3に示す。

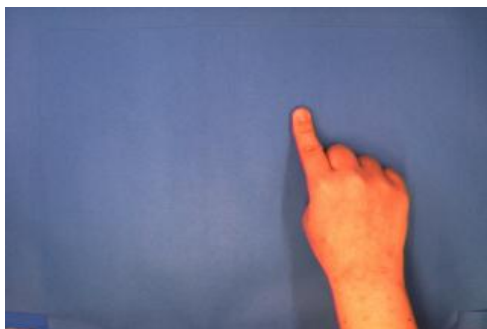


図3 取得した手形状画像の例

サインは、指先点をペンとして指先点の軌跡として取得する。ペンとなる指先点位置の決定には、HSV表色系の

Hue値(色相)を用いている。この抽出手法は崎田ら[11]によって提案されたものである。そのため、論文中で前提とするサインデータはカメラから取得した画像中の指先点の位置を記録したものである。

図4に実際に取得したサインの例を示す。このサインデータには区切り情報を含まないため、図4のような一筆書きのサインとなる。

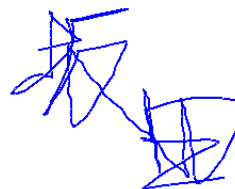


図4 取得したサインの例

取得したサインデータには筆記開始前、終了時の静止状態の指先点座標がノイズとして含まれている。筆記開始時、筆記終了時の指先静止状態において、ノイズとして取得された指先点座標は分散が小さいことが自明である。これを利用して、ノイズを除去する。

3.1.1 手形状特徴抽出

筆記に用いる指に関して、長さ、幅、面積の3つの特徴を抽出する。特徴の抽出は、手形状をHueによって2値化した肌色マスク画像(図5)を用いて以下を行う。

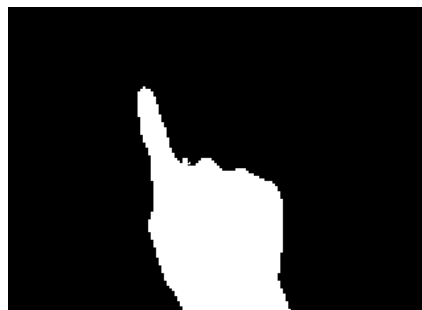


図5 肌色マスク画像

指先点と I_{hand} の重心を求め、2点を結ぶ直線の傾きを求める。次に、この直線に直交する直線の傾きを求め、この傾きを持つ直線を走査線として指先点から重心まで図6のようにスキャンし、指の付け根となる点を求める。

以上の処理によって得た指の付け根の位置と、走査時の指幅によって、次のように特徴を抽出する。

指の長さ：指先点から指の付け根点までの距離

指の幅：指幅の中央値

指面積：走査線が走った肌色領域の画素数の合計

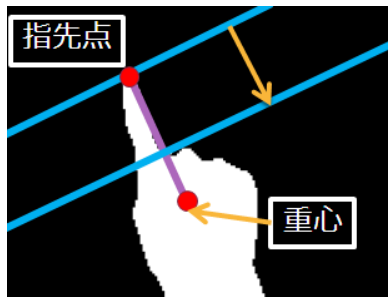


図6 指のスキニング

3.1.2 サイン特徴抽出

前処理によって得られたサインデータから3つの特徴を抽出する。

座標列: 指先点座標であるサインデータ (x_t, y_t) そのものを用いる。 t は、筆記開始から終了までのフレーム数に相当する。

角度列: サインデータ (x_t, y_t) のフレーム間角度を逆正接によって求めたものである。それぞれの値は $0 \sim 360$ の度数法で表したものをを用いている。

筆記時間: サインデータの総フレーム数 t を用いる。

3.2 登録フェーズ

各ユーザのリファレンスデータを登録する。リファレンスには手形状画像データとサインデータを含む。登録されたリファレンスデータは、認証フェーズにおいて入力データと比較し、手形状認証、サイン認証に用いられる。

本システムで用いるリファレンスデータは、特徴の経時変化に対応するためにキュー構造をとり、本人認証時にリファレンスの追加を行う。リファレンスには最大 $N_{\max}$ 件のデータを保持するようにし、 $N_{\max}$ 件のデータがすでにリファレンスに含まれる場合、先頭のデータの除去を行ってから追加する。本システムでは実験的に求めた値として $N_{\max}=5$ としている。

3.3 認証フェーズ

システムに対して入力を行った人物が、登録者本人かを判別する。

認証フェーズは図7のように、手の形状認証を行い、手の形状認証をパスしたものにサイン認証を行うといった、論理レベル (AND) の統合を行っている。つまり、手の形状が本人で、サインも本人のときのみ、認証成功とする。

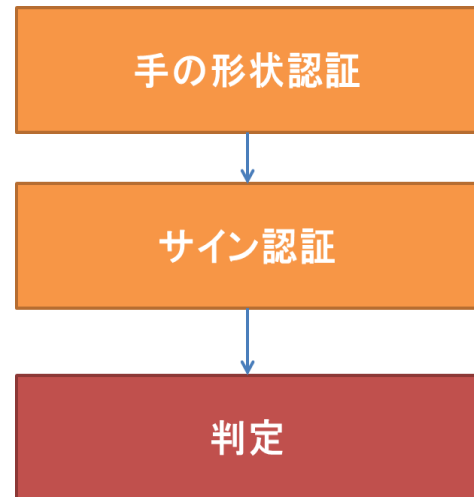


図7 認証フェーズの流れ

3.3.1 手形状認証

手形状認証では、3つの特徴についてリファレンス上のデータと、入力データとの距離を差の絶対値によって計算する。そして、それぞれの特徴に対して与えられた閾値によって判定を行う。すべての特徴の差が閾値未満であった場合、そのリファレンスデータと入力データは同一であるとみなす(式(1))。

$$Result = \begin{cases} \text{Genuine} & \text{if } vote \geq \frac{N}{2} \\ \text{Forgery} & \text{otherwise} \end{cases} \quad (1)$$

3.3.2 サイン認証

サイン認証は、図8のような手順で行われる。入力データとリファレンス上のデータ間で各特徴についてマッチング、スコア化を行い、それぞれから計算したスコアから類似度計算をして判定する。

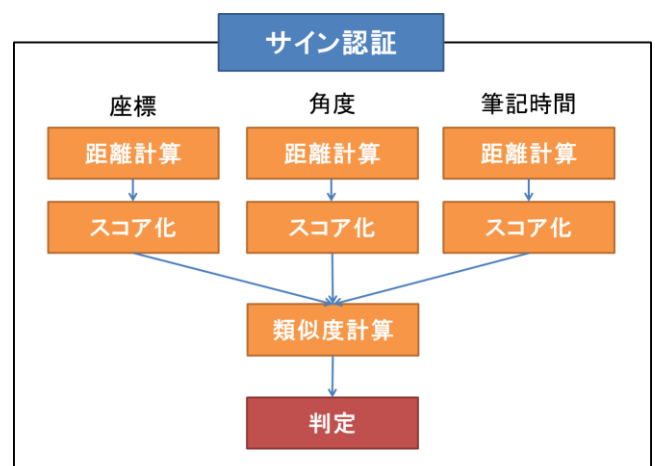


図8 サイン認証の流れ

(i) マッチング

座標列、角度列の特徴に対しては DP マッチングによって特徴ベクトル間の距離を算出する。DP マッチングはパ

ターン間距離をエネルギーとし、このエネルギーを動的計画法により最小化したものを距離とする。

(0,0)から(I,J)までの経路(パターン長が I,J である場合)をたどる時、局所距離を $d(i,j)$ とすると、(0,0)から(i,j)までの累積距離 $g(i,j)$ は次の初期値(式(2))及び漸化式(式(3))で表される。

$$g(0,0) = d(0,0) \quad (2)$$

$$g(i,j) = \min \begin{cases} g(i-1,j) + d(i,j) \\ g(i-1,j-1) + 2d(i,j) \\ g(i,j-1) + d(i,j) \end{cases} \quad (3)$$

ここで、 $g(I,J)$ がパターン間の最適距離となる。

なお、DP マッチングを行う際、 $g(I,J)$ を直接用いるとパターンの過適合の問題が発生する。なので、最適距離に対し、最適経路の移動回数 $path_{all}$ のうちギャップとなる経路数 $path_{gap}$ の割合を乗じたものを距離 $distance$ とすることで、パターンの過適合による影響を低減する(式(4))。

$$distance = (1 + \frac{path_{gap}}{path_{all}})g(I,J) \quad (4)$$

座標列、角度列の特徴は式(4)の手法で距離を計算し、筆記時間は特徴量の差分の絶対値を距離とする。

(ii) スコア化

マッチングによって求めた距離は、各特徴で確率分布の異なる値のため、これを正規化するために[0.0,1.0]の値にスコア化を行う。スコア化は式(5)の関数で行う。

$$score = \exp(-\frac{distance^2}{2c^2}) \quad (5)$$

$distance$ は DP マッチングによって得たパターン間距離、 c は分散であり、これをスコア変換パラメータと呼んでいる。スコア変換パラメータは各特徴それぞれに与えられ、また各ユーザは個別のスコア変換パラメータを持つ。これは、ユーザごとに安定して得られる特徴や、ばらつきを含む特徴が存在するためこの差異を補正し、安定した認証制度を保つために導入している。パラメータの更新については後述する。

図9は関数の形状の変化を表したものである。スコア変換パラメータの値が大きくなるほど、緩やかに変化をするようになる。

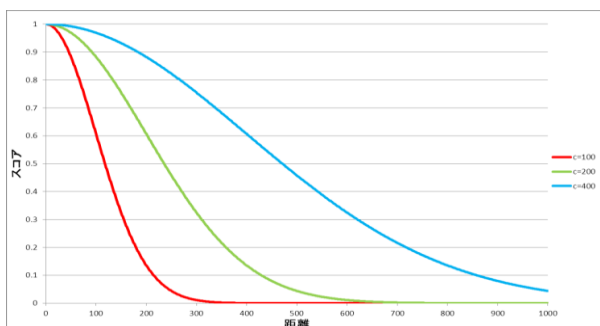


図9 距離のスコア化

(iii) 類似度計算

前項で述べたスコア化によって、座標列のスコア ($Score_{point}$)、角度列のスコア ($Score_{angle}$)、筆記時間のスコア ($Score_{length}$) を求める。このスコアの総積をとることで、類似度 $similarity$ を算出する(式(6))。

$$similarity = score_{point} \times score_{angle} \times score_{length} \quad (6)$$

(iv) 判定

類似度 $similarity$ が閾値以上であった場合、本人と同一とみなす。以上の処理はすべてのリファレンス上のデータについて行い、判定結果は手形状認証と同様に、式(1)により多数決で判定する。

(v) リファレンス・パラメータ更新

更新処理では、判定処理において入力データが本人と同一と判定された場合、キュー構造へ入力データの追加を行う。

パラメータ更新では、登録時と本人認証成功時にスコア変換パラメータ c の補正を行う。パラメータの更新には、マッチングによって得られた $distance$ と理想のスコア $score_{ideal}$ を用いて式(7)によって得られる理想のパラメータ c_{ideal} を用いる。

$$c_{ideal} = \sqrt{-\frac{distance^2}{2c^2}} \quad (7)$$

この理想のパラメータを用いて、現在のパラメータ c_{now} から更新を行う。更新は式(8)のようにして行う。

$$c = c_{now} + k(c_{ideal} - c_{now}) \quad (8)$$

k は調節の度合いを示す定数であり、 $k=0$ の時 $c=c_{now}$ 、 $k=1$ の時 $c=c_{ideal}$ となる。

4. 評価実験・結果

鹿児島大学内で行ったデータ取得実験により収集したデータを用いて、マルチモーダル認証の時間経過に関するロバスト性について評価する。また、サインの成りすましについても評価する。

学生実験の際に協力してもらい、以下の2通りの実験を行った。

- ① 登録後すぐに認証を行う実験
- ② 成りすましの実験
- ③ 毎日認証を行う実験
- ④ 2週間ごとに認証を行う実験

の2通りの実験を行った。

本実験では、類似度の閾値を0.7とした。

なお、評価実験で使用したPCのスペックや使用言語を表1にまとめる。

表 1 使用 PC スペック・言語

CPU	Intel® Core™ 2 Duo
メモリ	3.00GB
OS	Windows XP
使用言語	C#(visualstudio)
使用ライブラリ	OpenCV2.2

4.1 実験結果

4.1.1 登録後すぐに認証

(i) 評価に用いたデータ

データは 63 人分収集した。登録時は被験者自身の苗字、フルネーム、ひらがな、ローマ字、記号の 5 種類を登録するよう指示を行い、一回登録を行った。

登録後、すぐに本人認証を行った。

(ii) 結果

結果は表 2 のようになり、63 人全てで本人と認証できた。

表 2 実験結果(登録後すぐに認証)

	苗字	フルネーム	ひらがな	ローマ字	記号
本人	63	63	63	63	63
他人	0	0	0	0	0
類似度平均	0.89	0.88	0.90	0.90	0.91

(iii) 考察

図 10 を見ると、登録時のサインと認証時のサインにほとんど違いは見られない。登録してからほとんど時間が経っていないため、何をどういう風に筆記したかを覚えているからだと考える。

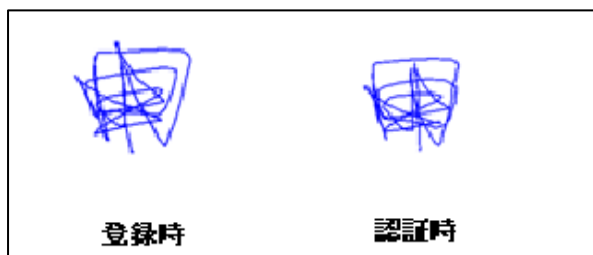


図 10 登録直後の結果の例

また、類似度の平均に着目する。類似度の平均は 0.9 程度と非常に高くなっている。つまり、登録時にサインを書いたものと認証時に書いたもの的大差ないということである。まだ登録したサインを覚えているため、このように高い類似度が出たのだと考えられる。

よって、登録直後は本人認証が確実にできると判断する。

4.1.2 成りすまし

(i) 評価に用いたデータ

あらかじめ登録しておいた二つのサインを用いて、他人の成りすましについて実験を行った。

今回、

- ① 登録してあるサインのみを教え、書き順などを公開せず、サインの成りすましを行う実験
- ② 登録している様子の動画を 1 回見せ、何と書いてあるかを考えて成りすましを行う実験

の 2 つの実験を行った。

データ数は、①が 63 名、②が 28 名である。

(ii) 結果

結果は、表 3、表 4 のようになった。サインのみを教えた時は全員成りすましに失敗した。動画を見せた時は、1 人成りすましに成功した。

表 3 成りすまし結果(登録してあるサインのみを教えた時)

	人数	類似度平均
成功	0	
失敗	63	0.05

表 4 成りすまし結果(動画を見せた時)

	人数	類似度平均
成功	1	0.77
失敗	27	0.15

(iii) 考察

表 3 の結果から、登録してあるサインだけを教えても本人と成りすますことはできなかったという事が分かる。この認証システムでは、一つでも低いスコアが出ると他人と判定されるようになっている。したがって、認証する際は座標・角度・筆記時間のすべてのスコアで高い数値を出さなければならない。今回の実験の場合、書いてある物の形は分かるもののそれ以外の情報は何もなく、書き順や大きさ、筆記時間などが全く分からない。したがって、書いてあるものだけをわかっていても本人と認証することはほぼできないと考える。

表 4 を見ると、1 人本人と認証されている。類似度平均を見てみると、0.77 となっている。閾値が 0.7 であるため、少し超えていることが分かる。動画提示の場合、動いている大きさや早さは分かる。さらに動体視力が良かった場合、何を書いているかまで分かる可能性がある。また、今回実験に用いたサインは苗字を書いたものであった。したがって、苗字のように単純なサインであれば何を書いているか容易に判断出来ていた可能性がある。

今回の実験では、動画を見せた際に 1 人成りすましに成

功していた。しかし、サインを登録する際に名前といった単純なものを登録するのではなく、記号などと組み合わせた複雑なものを登録することで、今回のような成りすましはできなくなると考えられる。

4.2 時間経過のロバスト性に関する実験

4.2.1 毎日の認証実験

(i) 評価に用いたデータ

データは 5 人分収集した。登録時は被験者自身の苗字、フルネーム、ひらがな、ローマ字、記号の 5 種類を登録するよう指示を行い、一回登録を行った。

登録後、毎日登録したデータそれぞれとの本人認証実験を 2 週間(10 回)行った。

認証する字種の順番は、以下のように決めた。

- ① 苗字
- ② フルネーム
- ③ ひらがな
- ④ ローマ字
- ⑤ 記号

(ii) 結果

類似度平均の推移のグラフは、図 11 のようになった。この認証の際、書き直しが発生することはなかった。

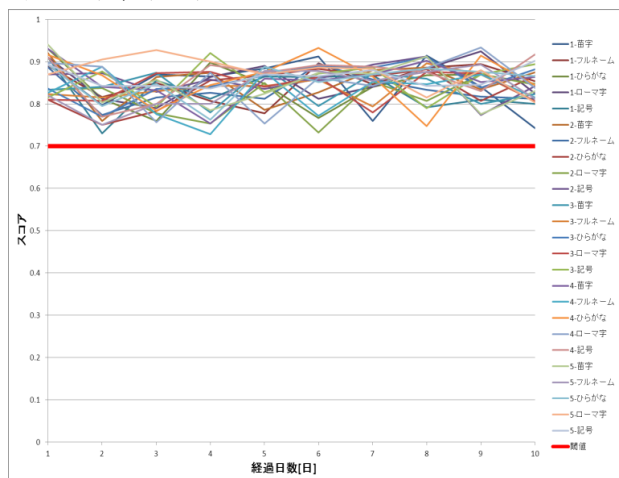


図 11 本人認証試験(毎日実験を試行)

(iii) 考察

図 11 のグラフは、5 人 5 種類のサインの類似度を平均にして表示したものである。全ての結果が閾値を超えていることが分かる。

図 11 を見ると、グラフは上下にスコアが変動していることが分かる。字種ごとに類似度の変化を見たところ、図 12 のようになっていた。

類似度の変化を見たところ、苗字やローマ字の類似度の変化にばらつきが多い。今実験では、毎回苗字の認証から始めていた。毎日最初に認証を行っていたため、サインが安定しなかったのではないかと考えられる。また、ローマ字は日常生活で毎日書くようなものではないので書き慣れ

ていなかったと考えられる。

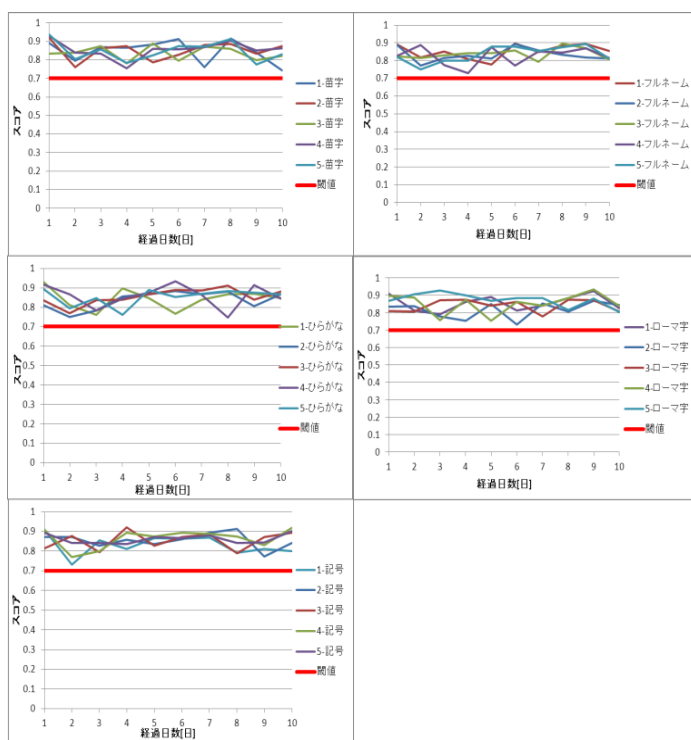


図 12 類似度の変化(字種ごと)

一方、比較的簡単なひらがなや記号は前のものに比べると安定しているように考えられる。やはり簡単なサインだと書き順や大きさなどを覚えやすいため、類似度を安定して出すことができると考える。

本実験では 2 週間に渡り認証実験を行った。今実験では期間が短かったものの、認証を毎日続けることでサインを確実に覚え、どの字種でも類似度がある程度安定してくるのではないかとと思われる。

したがって、毎日認証を行うことで、本システムが安定して個人認証できることが分かった。

4.2.2 2 週間ごとに認証

(i) 評価に用いたデータ

データは 30 人分収集した。登録時は被験者自身が書きやすいもの(苗字、記号等)を登録するように指示を行い、登録を行った。

その後、2 週間ごとに登録したデータとの本人認証実験を 1 か月間行った。さらに登録から 3 か月後に 25 人に対して実験を行った。本人認証は認証に成功するまで複数回行った。

(ii) 結果

結果は表 5 のようになった。その際のスコアの変化は図 13 に示す。

表 5 実験結果(2週間毎に認証)

	登録時	2週間後	1ヶ月後	3ヶ月後
成功	30	30	30	25
失敗	0	0	0	0
類似度平均	0.84	0.81	0.83	0.83
書き直し平均	0	1.5	0.8	1.4

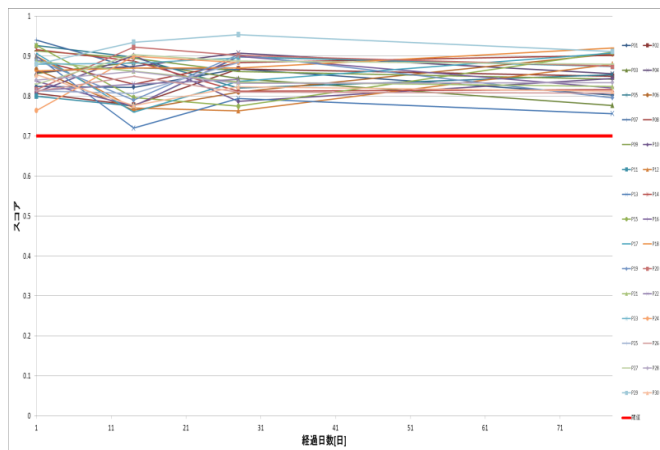


図 13 本人認証試験(2週間毎に認証)

全ての被験者で、3か月後の時間経過に関わらず本人認証できた。

(iii)考察



図 14 実験結果の例

図 14 のように、サインは 2 週間ごとに少しずつ変化をしている。形が変わると、筆記時間も少しずつ異なってくる。よってサインのデータごとにずれが発生し、他人と判定されてしまうことがあった。

表 6 認証結果の例

登録直後	2週間後	1ヶ月後	3ヶ月後
0.94	0.74	0.91	0.79
0.93	0.70	0.84	0.77
0.83	0.53	0.76	0.77
	0.49	0.74	0.73
		0.72	0.72

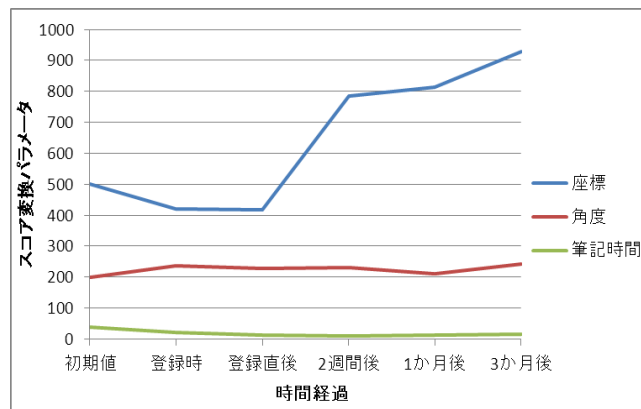


図 15 スコア変換パラメータ変化の例

スコア変換パラメータの変化に着目する。表 6 の結果が出た際のスコア変換パラメータの変化が図 15 である。

登録から 2 週間後の結果が悪かったため、スコア更新の際に座標が大きく変化したことが分かる。2 週間後にあまり良くない類似度が出ているが、これは登録時の認証で優れた結果が出たので、スコア変換パラメータが小さい値に更新されて判定が厳しくなったためである。1 ヶ月後の結果では類似度が高く出ているが、類似度にばらつきがあるためスコア変換パラメータはあまり変化しなかった。3 ヶ月後にもう一度書いたところ、類似度が低かったため、スコア変換パラメータはさらに大きい値に変化した。

図 15 を見ると、座標のスコア変換パラメータは大きくなっているが、角度・筆記時間のスコア変換パラメータは小さい値へと変化している。これにより、座標の変化には緩く対応するようになったが、角度・筆記時間の変化に対して厳しくスコアをつけるようになっている。全てのスコア変換パラメータが緩くなるわけではないので、他人受入れをする恐れは変わっていないと考えられる。

本システムでは、変化に対応するようスコア変換パラメータが変更されているが、初期値は大きい値に設定し本人拒否が起らないようにしているため、登録後の認証によってスコア変換パラメータが厳しくなり、2 回目の判定が厳しくなり、表 5 のように書き直しの回数が増えている。ただし、書き直しの平均は 1.5 回で、妥当な書き直し数と考える。2 回目の判定が厳しいため 3 回目になるとスコア変換パラメータが前より大きい値に変化し、判定が通りやすくなっている。よって表 4 のように書き直し回数が減っている。3 ヶ月後の判定では、やはりどのようなサインを登録していたのか覚えていない人が多かったため、書き直しの回数は増えていた。しかし、書き直しの回数は増えたもののすべての被験者で本人と認証することが出来ていた。

また、リファレンスデータも更新が行われる。これによって、前のデータから次々直近のデータに更新されていくため、スコア変換パラメータと合わせて特徴の経時変化に対応できるのではないかと考えられる。

2週間ごとに実験を行った結果、書き直しが発生する場合もあるが、2週間ごとに認証を行うことは可能だと判断する。

また、2か月程度認証に期間が空いた場合でも認証ができることが確認できた。

5. まとめ

手形状とサインのマルチモーダル個人認証では、リファレンスの更新及びサイン認証に用いるパラメータの更新が行われており、それらによって特徴の経時変化への対応が可能である。

そこで本研究では、サインと手形状を用いたマルチモーダル個人認証において時間経過のロバスト性があるかについて検証を行った。

登録直後のサイン認証の実験を行い、63人全てを本人と認証した。よって登録直後の本人認証率は100%であったと判断する。また、2週間ごとにサイン認証の実験を行い、書き直しが発生したものの全員を本人と認証できた。さらに、毎日サイン認証の実験を行い、5人5種類の字種で毎日認証することが出来ることを確認した。

よって、サインと手形状を用いたマルチモーダル個人認証システムにおいて時間経過のロバスト性があると判断した。

6. 参考文献

- [1] 内田薫, “バイオメトリクスによる個人認証:さまざまなバイオメトリクス技術”, 映像情報メディア学会誌:映像情報メディア, Vol.55, No.2, pp.172-175, (2001)
- [2] 松本勉, “バイオメトリック認証の脆弱性:身体的特徴の偽造問題”, 情報処理, Vol.47, No.6, pp.589-594, (2006)
- [3] 松本勉, 宇根正志, “バイオメトリクス認証の実用におけるぜい弱性と対策”, 電子情報通信学会誌, Vol.90, No.12, pp.1051-1055, (2007)
- [4] 岡倉太郎, 荒川薫, “ブロックマッチングによる経年変化顔画像人物認証法の特性改善:ブロック位置補正の導入”, 電子情報通信学会技術研究報告. SIS, スマートインフォメディアシステム, Vol.111, No.210, pp.69-74, (2011)
- [5] 篠原克幸, “バイオメトリクス認証”, 画像電子学会誌, Vol.39, No.6, pp.877-879, (2010)
- [6] 村松大吾, 本郷保範, 松元勉, “ユーザ共通 Fusion モデルを用いたオンライン署名認証”, 電子情報通信学会論文誌 D, Vol.90, No.2, pp.450-459, (2007)
- [7] M.E. Munich and P. Perona, “Visual identification by signature tracking,” IEEE Trans. Pattern Anal. Mach. Intell., Vol.25, No.2, pp.200-217, 2003.
- [8] 中村陽一, 亀井俊男, “BT-7-10 マルチモーダル指認証”, 電子情報通信学会総合大会講演論文集, “SS-90”, (2009)
- [9] 中野健, 兵頭潤, 立石朋也, “手指の摩擦信号を利用し

たバイオメトリクス認証法”, 日本トライボロジー学会誌, Vol.50, No.8, pp.612-619, (2005)

[10] 佐藤公則, 中島章博, 鹿嶋雅之, 渡邊睦, “手形状と指先署名によるマルチモーダル個人認証システムの開発”, 画像電子学会誌, Vol.41, No.4, pp.371-376, (2012)

[11] 崎田隆行, 鹿嶋雅之, 佐藤公則, 渡邊睦, “指先トラッキングとその軌跡抽出を用いた個人認証に関する研究”, 電子情報通信学会技術研究報告, PRMU2007-146, Vol.107, No.384, pp.56-64, (2007)