

# 筆圧タブレットによるオンラインサイン認証の改良

小南 嘉史<sup>1</sup>・西村 広光<sup>2</sup>・富川武彦<sup>2</sup>

- 1 大学院工学研究科電気電子工学専攻(kominami@ele.kanagawa-it.ac.jp)  
2 情報メディア学科(nisimura,tomikawa@ic.kanagawa-it.ac.jp)

## Integrated Online Sign Detection using Writing Stroke and Writing Pressure

Yoshifumi KOMINAMI<sup>1</sup>, Hiromitsu NISHIMURA<sup>2</sup>, Takehiko TOMIKAWA<sup>2</sup>

### Abstract

In the field of user detection, many detection methods using biometrics attracts are reported in recent years. We reported an online sign detection system using writing stroke and writing pressure. Our system is improved to be able to distinguish similar online sign form using differences of the number of writing strokes. In this paper, we investigate better relationship between writing stroke and writing pressure for sign detection. Improving our user detection system based on these considerations, user detection performances were evaluated.

From our evaluation results, proposed method correctly detected registrants and non-registrants. Comprehensive evaluation results show that our system would perform high capability on user detection.

Key Words: User detection, User identification, On-line sign, pen pressure, pen stroke

### 1. はじめに

インターネットのブロードバンド化に伴い、誰でも気軽に電子商取引が利用できるようになっている。その一方で、コンピュータの高性能化が進み不正なパスワード解析などが比較的容易かつ短時間に行われ、本人を偽った詐欺や個人情報の流出などのインターネット犯罪も増加している。よって、これらの犯罪から身を守るためにも個人認証の高精度化が求められている。そこで、個人認証の分野において、解析され難い方法として指紋や声紋などのバイオメトリクスによる認証が注目され、研究が進められている<sup>1)</sup>。本研究では動的なバイオメトリクス認証である、サインを用いた認証について検討した。

本研究で提案する個人認証システムでは、タブレットから取得したデータをそのまま比較するのではなく、座標データと筆圧データをそれぞれ画数ごとに Code 化処理を行い、類似度によって認証を実現する。このようなシステムの研究が昨年まで行われてきた。<sup>2)</sup>そのシステムを改良することで個人認証の精度を向上させることが目的である。特に登録されたサインを他人が書いた場合など、間違ったサインを認証しないように改良した。そのため大きな改良点として筆圧情報の取り扱い方を変更した。

また、個人認証の精度の向上を図るために登録ユーザー一人当たりの登録サイン数を増やすこともあわせて実験、検討を行った。

提案した手法の評価として、本研究では登録ユーザーが正しく認証されることだけでなく、不正サインの拒否性能の評価として未登録ユーザーのサインがシステムで拒否されること、登録者のサインを他者が真似て筆記したサインをシステムが拒否することの3つの性能を評価した。

独自に採取したサインデータベースを用いて、登録ユーザーのサインと不正サインの認証実験を行い、登録者が正しく認証されることだけでなく、登録者以外の不正サインを正しく拒否することを確認し、登録者数が増加しても高い認証性能を実現できることを確認した。

## 2. オンラインサイン認証

本章では本研究で行う個人認証で利用するオンライン文字の概要や、オンライン文字を利用した個人認証方式について具体的に説明する。

### 2.1 オンライン文字

オンライン文字とは時系列の概念が含まれた文字情報であり、文字の形状だけでなく筆記情報や書き順、筆圧などの情報を含んでいる。筆圧はペンを紙に押し付ける力のことで一般的には線の色の濃さで表される。

本研究で取り扱うのは書き順と筆圧を含むオンライン文字である。

### 2.2 個人認証

個人認証とは、システム利用者が登録されてある人物かを確認し、登録されてある人物だけに利用許可を与える処理でありセキュリティにおいて最も重要な処理である。

従来使用されている個人認証には記憶によるものや所有物によるものなどがある。これはパスワードによる認証や鍵を用いたものなどが挙げられる。

近年ではバイオメトリクスを利用した認証も使用されている。バイオメトリクスを利用した認証とは声紋や指紋、網膜など生体的な特徴を利用した認証のことをいう。バイオメトリクスを利用した認証では生体的な特徴を利用するため忘却、紛失、盗難の恐れが少ない。

### 2.3 オンライン文字を利用したオンライン個人認証

オンライン個人認証とはネットワーク回線上で行われる個人認証で、電子商取引などでよく行われる。現在、オンライン個人認証で主に使用されるのはパスワードである。しかし、パスワードでは解析される可能性が高くなっている。

本研究ではパスワードより多くの情報量を持ち、忘却、紛失、盗難の恐れが少ないサインがオンライン個人認証に適しているのではないかと考え、研究を行うこととした。

## 3. 筆圧タブレットを利用したサイン入力システム

本研究ではバイオメトリクスによる個人認証のひとつであるサインを利用した認証方法の検討を行う。本章では、タブレットを利用したサイン入力システムの解説をする。

### 3.1 筆圧タブレット

タブレットとはペン入力型の入力装置で、コンピュータを利用して絵を描いたり、画像を加工したり、音楽編集に使われたりと繊細な操作を必要とする処理に適した入力インターフェースである。近年はタブレットの機能も向上し、高精度でサンプリングできるだけでなく、ペンを紙面に押し付ける力である筆圧やペンの傾きの情報を採取できるものが販売されている。なかでも筆圧検出機能はほとんどのタブレットに搭載されている。

本研究では筆圧検出タブレットを利用して文字情報を取得し、認証を行うこととした。本研究では筆圧を検出できるタブレットならどれでも対応できるような仕様としたが、筆記者の作業負担の少ない WACOM 社製 Cintiq を利用してデータ入力を行うことにした。Cintiq は図 1 の写真で分かるように一般のタブレットとは違い、ディスプレイと一体となっている。筆記者は専用ペンを使い、ディスプレイに直接書き込むことができるので、タブレットに不慣れな人でも負担をあまり感じることなくサインを書くことができると考えられる。また、一般的なタブレットは図 2 のようなものである。

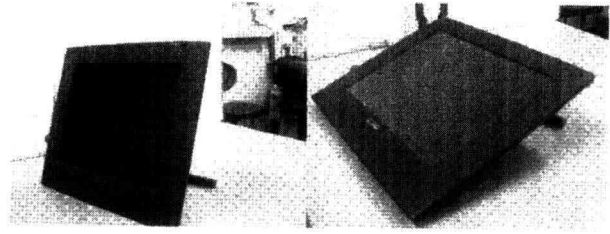


図 1 Cintiq

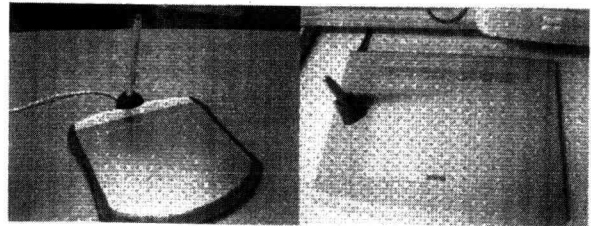


図 2 その他のタブレット

タブレットによって採取できる筆圧レベルが異なるため、Wintab<sup>2)</sup>を利用する。Wintab とは、米国 LCS/Telegraphics 社が開発したタブレットの標準インターフェースで、ペンの出力する座標を遅滞無くコンピュータに入力し、筆圧やペンの傾きなどもこれによって取り入れることが可能である。Wintab は筆圧を取込む際、タブレットの筆圧レベルがいくつであっても 1024 レベルに調整する。これによって筆圧レベルの異なるタブレットでも同様に使用することができる。今回利用した Cintiq では 512 レベルで筆圧を検知する能力があるが、この Wintab を利用することで値が 2 倍にされ、1024 レベルで筆圧情報を取得した。

### 3.2 サイン採取プログラムの概要

サイン採取プログラムは、及川幸一氏の“オンライン文字データ採取システムの作成と筆圧情報を利用したオンライン文字認識”<sup>4)</sup>のなかで作成した文字採取プログラムを改良して利用した。このプログラムは、Wintab を利用して、Microsoft Visual C++ によって作成したものである。サインを採取するにあたって、サイン取得画面のサイン描画範囲を 768×256 pixel とし、さらにサイン筆記時の補助線を設けた。被験者がサインを補助線の外に書いた場合や、サインの途中で補助線の枠をはみ出してしまった場合には、警告メッセージが現れ、もう一度最初からサインを書き直してもらうようなシステムとなっている。

サインデータを取得するプログラムを実行したときに表示されるダイアログは図 3 のようなものである。枠内にサインを書いてもらい、途中で間違えた場合は左側に表示されてある CLEAR ボタンを押すことで何度でも書き直すことができる。きちんと書いた場合は右側に表示されてある NEXT/END ボタンを押すとサインの取得は完了となる。

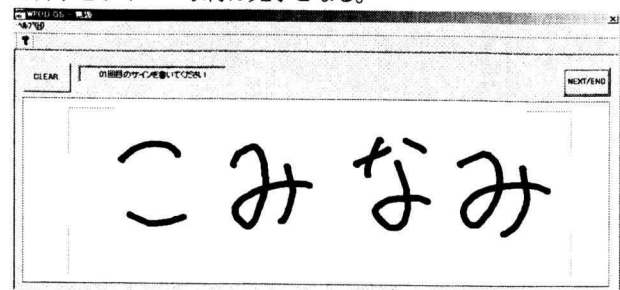


図 3 サイン採取プログラムのダイアログ

### 3.3 サインデータの採取

前節で説明したプログラムを用いサインデータの採取を行った。サインデータの採取の際以下の点に注意してもらいサインを書いてもらった。

- (1) タブレットをねかせた状態で筆記する。
- (2) 椅子に座って筆記する。
- (3) 丁寧な字ではなく普通のサインを筆記する。
- (4) 複数回筆記する場合すべて同じ書き方をする。
- (5) 間違えた場合、CLEAR ボタンを押し、書き直す。

このプログラムはタブレットから、ストローク、筆圧、 $x$ 座標、 $y$ 座標を1パケットとしてコンピュータに取り入れる。採取したサインデータの範囲は筆圧が0~1023までの1024レベル、 $x$ 座標は0~767までの768レベル、 $y$ 座標は0~255までの256レベルとする。このとき $x$ 座標は横軸を、 $y$ 座標は縦軸を指している。そのほかプログラムの制限によりサンプリング点が膨大な数になると不具合を生じる。

### 3.4 サインデータベースの構築

現在サイン認証の研究において基準として自由に使用できる筆圧を含むデータベースは存在しない。そこで、本研究で採取したサインを研究評価用に自由に利用できるものとして <http://www.tomy.ic.kanagawa-it.ac.jp/~kosd/>にて公開する。

## 4. オンライン筆記情報の Code 化

採取したサインデータは座標情報と筆圧情報であり、そのままの数値系列のデータを比較しても位置ずれや大きさの差異により同一人物が同じサインを書いたとしても精度の高い認証を行う事は難しい。そのため採取したサインデータを Code 化し認証を行いやすくする必要がある。

### 4.1 筆跡データの Code 化

同一人物であっても同じ場所にサインを書くことは非常に困難である。さらにサインを比較する際、何処に書いたということよりどのような軌跡を書いたかが重要であると考えられる。そこで、採取した座標情報を座標の位置情報を相対的な動きの情報に変換し、Code 化する。このとき、単純に方向ベクトル化したのでは、筆記速度の情報を利用することができなくなるため、単位方向ベクトルを利用して、同一方向のベクトルが複数出ている場合に、その長さにより筆記速度を表現できるようにした。

座標情報を動きの情報に変換するとき Freeman - Code<sup>3)</sup>と呼ばれるものを用いて Code 化する。

Freeman - Code とは、サインを書いたときに移動するペンの座標データを8方向の単位方向ベクトル系列に変換した Code をいう。移動する座標との対応は図4のようになっており、方向に対して1から8までの数字を割り当てて表す。また、矢印の長さを1単位方向ベクトルとすることで、長さについても示すことができる。具体的には、図5のような筆跡情報を Freeman - Code 化すると図6のようになる。

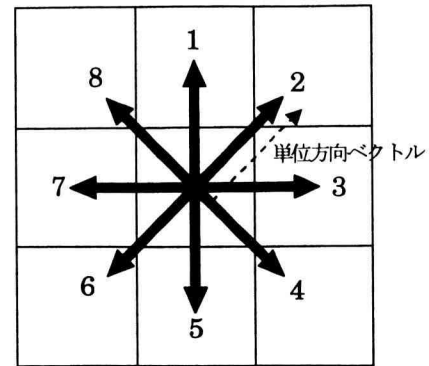


図4 Freeman - Code

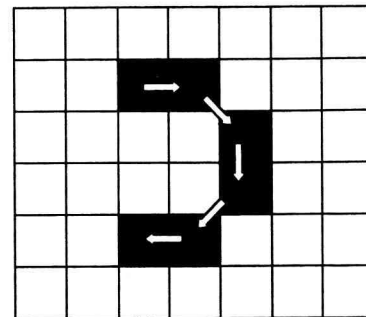


図5 Code 化例(Code 化前)

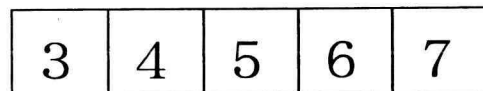


図6 Code 化例(Code 化後)

### 4.2 筆圧データの Code 化

1024レベルでサンプリングされた筆圧情報は8レベルに変換する処理を行い、これらの処理から得られたデータを繋ぎ連続させることにより Code 化処理を行う。これは、人間が完全に同じ筆圧のサインを筆記することができないためである。そこで、サインを書いた人の筆圧変化の傾向を取り出すために、この変換 Code 化処理を行う。また8レベルとしたのは、前節で説明した筆跡データと同レベルだからである。これによりデータの取り扱いが容易になると考えた。

1024レベルから8レベルに変換したことにより筆圧情報の特徴が損なわれないことは実験により確認されている<sup>5)</sup>

### 5. Code の類似判定と認証方法

本研究では前章の処理によって Code 化されたサイン情報を比較して類似度を求めることにより個人認証を行う。この章では認証システムの基本となる類似度の算出方法と個人認証の判定方法について詳しく説明する。

#### 5.1 Code の類似性比較

Code の比較には、対象となる信号系列がどれだけ類似しているかという値、類似度を決定する必要がある。本研究で利用した類似度はストロークごとに以下の(5.1)式で求める。ここで、a は認証対象者の 1 ストロークの信号系列、b は登録ユーザの 1 ストロークの信号系列を表している。

$$\text{類似度}[\%] = \left( 1 - \frac{\sum_{k=1}^n |b_k - a_k|}{\|a_k\| \cdot \|b_k\|} \right) \times 100 \quad (5.1)$$

$$\|a_k\| = \sqrt{\langle a_k, a_k \rangle}, \quad \|b_k\| = \sqrt{\langle b_k, b_k \rangle}$$

このとき認証対象者の Code 列と登録ユーザの Code 列に Code 長の差があるとき、単純に類似性を求めることはできない。そこで Code 長を同じにするため次の方法を用い Code の補間を行う。

二つの Code 列を比較し Code 長に差があった場合、短い Code 列に対し足りない数だけ Code を 1 から 8 までの乱数によって補間する。これは同一筆記者であっても筆記速度にばらつきが多いためにコード長が異なることが多く、補間せずに照合を行うと本人を正しく認証することが難しくなることに加えて、Code の数字には方向性や個人の特徴といった情報も入っているため、何か決まった数字で補間処理をしてしまうと、一方向に偏ったサインデータとなってしまうため、本研究では一様乱数で補間することとした。

また、ストローク差がある場合は 1 ストローク分の Code 列全てを乱数で補間する。

図 7 は Code 列の補間の例である。上の Code 列の長さが 5、下の Code 列の長さが 4 だったとき下の Code 列に 1 から 8 までの乱数を 1 つ加えて両方の Code 長を 5 にそろえるようにする。

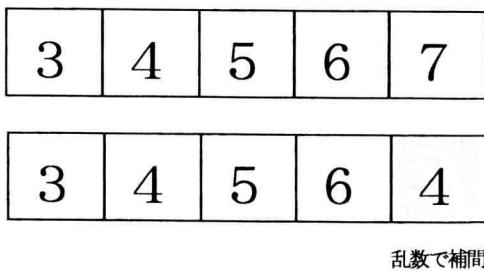


図 7 長さの異なる Code 列

#### 5.2 閾値決定と認証判定

本研究では閾値は小数点以下第一位までを設定できるようにし、手動で決定する。

認証判定としては認証対象者の Code と登録ユーザの Code を比較し、類似度を算出、その類似度が閾値以上で一番高かった登録ユーザを認証対象とすることで認証を行う。このとき、どの登録ユーザと比較しても閾値以上の類似度を得られなかった場合は認証対象なしと判断される。以後このことを **Reject** と呼ぶ。

### 6. 既存のシステム

本研究は、過去に研究、開発されたシステムの改良を目的としている。そこで本章では評価の比較対象となる既存システムの説明をする。

#### 6.1 システムの流れ

このシステムは、データ処理部と認証部に分けられる。データ処理部ではサインデータをタブレットから採取し、座標データは Freeman - Code 化する。筆圧データは、1024 レベルから 8 レベルに変換し Code 化した上で 0 画目のストローク情報として、筆跡データと合わせて認証対象の Code 列とする。データ処理部のシステムの流れを図 8 に示す。認証部では前もって Code 化しておいた登録ユーザの Code 列とデータ処理部において決定した認証対象の Code 列を比較しストロークごとの類似度を算出し、その平均類似度を判定値として、個人認証を行う。認証では、登録ユーザの Code と認証対象者 Code を比較し、設定した閾値以上で、登録ユーザの中で最も高い類似度を獲得したものが、その登録ユーザとして認証される。認証部のシステムの流れを図 9 に示す。

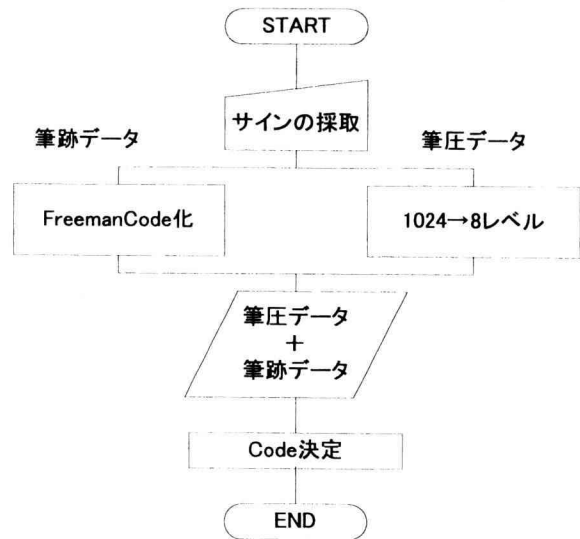


図 8 個人認証システムのフローチャート(1)

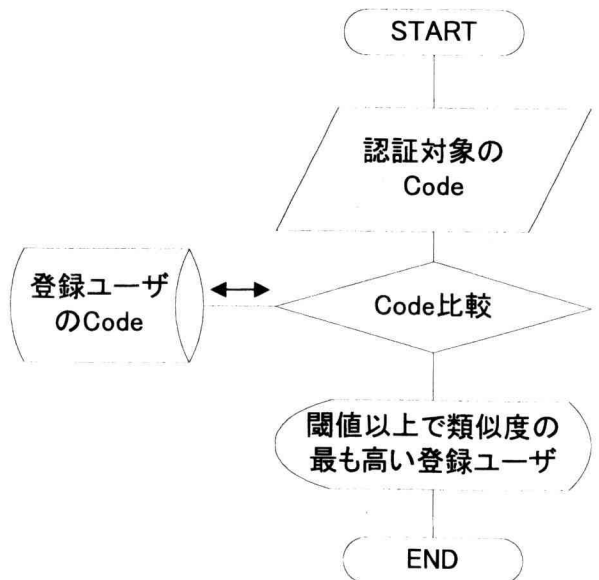


図 9 個人認証システムのフローチャート(2)

### 6.2 類似度決定法とその有効性

このシステムにおいて類似度の決定法は認証性能に大きく影響する問題である。既存のシステムでは形は似ているが画数の違う文字、例えば「熱」と「勢」の文字を判別するために画数差荷重法という方法を考案し使用している。

ストローク数に差がある場合には1ストローク分の Code 列を1~8 までの乱数で補間するため時として高い類似度を得ることがある。この欠点を補うために考えられたのが画数差荷重法である。

画数差荷重法はストローク数に差がある場合にその差に応じた荷重を単純平均法で求めた類似度にかけて判定値を決定する方法である。判定値を求める式は(6.1)式になる。

$$\text{全体の類似度} = \frac{\text{各ストロークの類似度の総和}}{\text{総ストローク数}} \times p^n \quad (6.1)$$

$$\left( \begin{array}{l} p = \text{荷重の割合} \quad : 0 < p < 1 \\ n = \text{画数差} \end{array} \right)$$

画数差荷重法では、認証対象者本人の筆跡類似度と認証対象者ではない他者の筆跡類似度の分布が荷重をかけない場合と比べ、分布がずれる。これにより、閾値判定が可能となる。

### 7. 認証アルゴリズムの改良

本研究では前章で解説したシステムを改良し、さらに高精度の認証システムの検討を行う。本章では本研究での改良点を挙げる。

#### 7.1 筆圧データのストローク毎での処理

既存のシステムではCode化した筆圧を0画目のストローク情報として取り扱っていたが、筆圧もストローク毎のCode列にするようにした。これは筆圧データには個人の特徴が強く表れているものと考え、全ての筆圧情報をまとめて取り扱うより、筆跡データと同様にストローク毎の Code 列にした方が各個人を判別できると考えたからである。

筆圧データをストローク毎に処理したときの全体の類似度の算出方法は(7.1)式のとおりになる。

$$\text{全体の類似度} = \frac{\sum_{k=1}^n (P_k + S_k)}{2n} \times W^j \quad (7.1)$$

$$\left( \begin{array}{l} P_k: k \text{ストローク目の筆圧の類似度} \quad S_k: k \text{ストローク目の筆跡の類似度} \\ n: \text{総ストローク数} \quad W: \text{荷重の割合} \quad j: \text{ストローク差} \end{array} \right)$$

#### 7.2 Code の比較方法の改良

本システムでは認証対象者のCodeと登録ユーザのCodeの差の絶対値を取ることで2つのCodeの類似性を判断している。ところが、筆跡データはベクトル量であるので単純に差を比較することができない。例えば図10(左)のようにFreeman-Codeの1と4の差は3であり1と6の差は5である。しかし、ベクトルで考えると、どちらも同じ角度の単位方向ベクトルなので類似性は同じだといえる。そこで二つのFreeman-Codeのなす角が同じ場合図10(右)のように差が同じだとするように改良した。

つまり  $|b_k - a_k| \leq 4$  のときは(7.2)式を、  $|b_k - a_k| > 4$  のときは(7.3)式を用いて類似度を算出する。

筆圧データは単純なスカラー量なので、そのまま(7.2)式を用いて類似度を求めることとした。

$$\text{類似度} [\%] = \left( 1 - \frac{\sum_{k=1}^n |b_k - a_k|}{\|a_k\| \cdot \|b_k\|} \right) \times 100 \quad (7.2)$$

$$\text{類似度} [\%] = \left( 1 - \frac{\sum_{k=1}^n |8 - |b_k - a_k||}{\|a_k\| \cdot \|b_k\|} \right) \times 100 \quad (7.3)$$

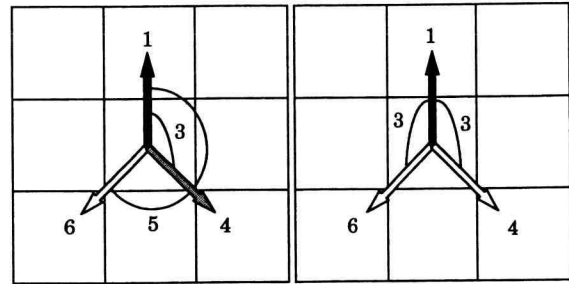


図10 Freeman-Codeの差の改良

#### 7.3 筆圧・筆跡情報の重み付け

今年の改良により筆圧データと筆跡データは独立した変数となったので、それぞれに重み付けをすることで最適な値を検討する。  $W_p, W_s$  を大きくすると類似度の幅を低い方に広げることになる。つまり、同一のサインを比較したときに100%になることに変わりはないが異なるサインを比較した際、マイナスの値をとることも、ありえるということである。重み付けを変えることによりサインの違いを強調できるのではないかと考えられる。

筆圧データと筆跡データのそれぞれに重み付けを行った式を(7.2)式に示す。

$$\text{全体の類似度} = \frac{\sum_{k=1}^n (P_k \times W_p + S_k \times W_s)}{2n} \times W^j \quad (7.4)$$

$$\left( \begin{array}{l} P_k: k \text{ストローク目の筆圧の類似度} \quad S_k: k \text{ストローク目の筆跡の類似度} \\ n: \text{総ストローク数} \quad W: \text{荷重の割合} \quad j: \text{ストローク差} \\ W_p: \text{筆圧に対する重み付け} \quad W_s: \text{筆跡に対する重み付け} \end{array} \right)$$

#### 7.4 登録サインデータ数による認証率の変化

既存のシステムでは認証対象者のサインデータと比較する登録ユーザのサインデータは1ユーザに対して1つしか用意されていなかった。この登録ユーザのサインデータを2つ以上用いることで認証精度をあげることはいかぬかと考え、検討を行った。

## 8. 提案システムの評価実験

提案システムの評価実験として4つの実験を行った。

### 8. 1 Code 比較方法の改良による認証性能評価実験

1つ目にCode比較方法の改良による認証性能評価実験として筆圧データのストロークごとでの処理とCode差の比較方法の改良により既存システムと比較してどの認証性能が改善されるかを比較検討した。

この実験では50人各1回のサインデータを登録ユーザのデータとして用い、その50人のうち誰と認証されたか、もしくは誰とも認証されなかったかによって個人認証を行う。

提案システムの評価を行うために以下の3種類のサインを認証用サインとして入力し、既存のシステムと改良したシステムでどのように変化するか検証した。

#### (1) 登録済みサイン

50人に登録データとして書いたサインと同じサインを各18回書いてもらい認証を行う。

#### (2) 詐称サイン

詐称サインとは、登録データに使用されたサインを登録した人以外が書いたサインをいう。詐称サイン36個を認証用サインとして用いる。

#### (3) 未登録サイン

未登録のサイン72個を登録用サインとして用いる。

### 8. 2 筆圧・筆跡情報重み付けによる認証性能検討実験

2つ目として筆圧・筆跡情報重み付けによる認証性能検討実験を行った。

この実験では筆跡に対する重み付けは1~4の間で変化させ、筆圧に対する重み付けは0~3の間で変化させた。これにより認証率がどのように変化するかを改良したシステムを使い比較検討した。

### 8. 3 提案システムの認証能力検証実験

3つ目は提案システムの認証能力検証実験を行った。

実用的システムに向けた検討として、登録ユーザ数の増加による認証率の変化を調査。また、あわせて登録ユーザー一人当たりの登録データ数を増加させたときの認証率の変化を検討した。このような認証法の評価は従来まであまり行われていないが、実用化に向けた検証として極めて重要であると考えた。

登録人数による認証率の変化と登録ユーザー一人当たりの登録データ数による認証率の変化をみるために登録ユーザー10人のサイン各9個を用いて認証率の変化を調べた。このとき登録人数を10から50に、登録ユーザー一人当たりの登録データ数を1から10に変化させた。

### 8. 4 最適パラメータによる認証性能評価実験

最後に3つの実験により得られた結果をもとに最適な値を用いた認証システムを構築し、その認証性能の評価を行った。

## 9. 実験結果・考察

本章では3つの実験の結果とその結果をもとに最適な値を用いた認証システムの認証性能の評価結果を示す。

### 9. 1 Code 比較方法の改良による認証性能評価実験

50人各18個のサインを用いて行った登録済みサインの認証結果は既存のシステムで90.3%、改良をしたシステムで80.0%となった。このとき、どちらのシステムでも誤認証が発生しているため誤認証をなくすために閾値の設定を上げた。このときの閾値を既存のシステムは88.6%、改良をしたシステムは93.3%とした。既存のシステムで77.8%、改良をしたシステムで65.3%となった。

36個の詐称サインの認証結果は既存のシステムは4個をRejectし、改良をしたシステムでは36個全てをRejectした。このときの閾値は、登録済みサインの認証で語認証なしのときの閾値を使用した。

72個の未登録サインの認証結果は既存のシステム、改良をしたシステムともに72個全てをRejectした。このときの閾値は、登録済みサインの認証で語認証なしのときの閾値を使用した。

3種類のサインの認証結果を表1に示す。

表1 Code比較方法の改良による認証実験の結果

	既存のシステム	改良したシステム
登録済みサインの認証率	77.8%	65.3%
詐称サインのReject率	4/36	36/36
未登録サインのReject率	72/72	72/72

登録済みサインの認証において改良したシステムは既存のシステムより認証率が下がった。しかし、登録者単位でみると既存のシステムよりも認証率が上回っている場合もあり、そのことからそれぞれのシステムにおいて得意なサインがあると考えられるので今後更なる研究が必要だと考えられ一概に今年のシステムが悪いとはいえない。

特に誤認証の多かった例として図11、図12の二つのサインを挙げる。このサインはその形状を見た場合一目で違うサインとわかる。しかし、ストロークごとに筆跡の動きを見ると非常に似ていることがわかる。このように形状の異なる文字でも動きの要素において高い類似度を示すことがわかった。

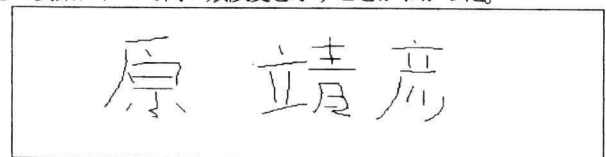


図11 誤認証をしたサインの例(1)



図12 誤認証をしたサインの例(2)

不正サインデータの拒否実験において、未登録サインは両システムともすべてRejectしたが、詐称サインでは既存のシステムでは4個しかRejectできなかったのに対し改良をしたシステムでは36個全てをRejectできた。これにより改良をしたシステムは詐称サインに対し精度の高い認証ができることがわかった。

図 13、図 14 は詐称サインの拒否実験に用いたサインの例である。このように形状の似たサインでも改良したシステムでは拒否することができる。

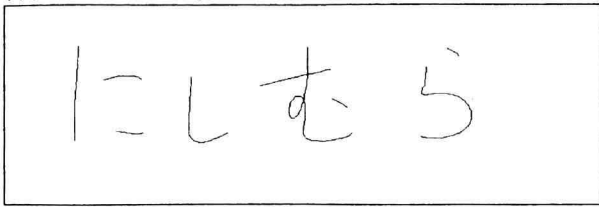


図 13 登録ユーザのサインの例

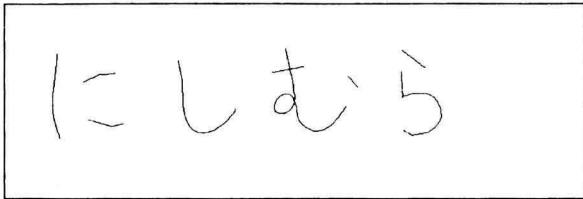


図 14 詐称サインの例

### 9.2 筆圧・筆跡情報重み付けによる認証性能検討実験

筆圧・筆跡に対する重み付けによる認証率の変化を図 15 に示す。閾値は誤認証無しとなるように設定しているため 100-認証率が Reject 率になる。

図 15 で基準となるのは、筆圧 1 倍、筆跡 1 倍のときであり、これは前節の実験のパラメータと等価である。結果から、いくつかの点で基準より高い認証率を得ることに成功した。傾向としては、筆跡は筆圧よりも高い倍率にした方が、認証率が上がることがわかる。また、筆圧の倍率を過度に低くした場合や筆跡の倍率を過度に高くした場合には、認証性能が著しく低下することがわかる。検討結果から筆跡 3 倍、筆圧 0.5 倍の重み付けが適しているといえる。

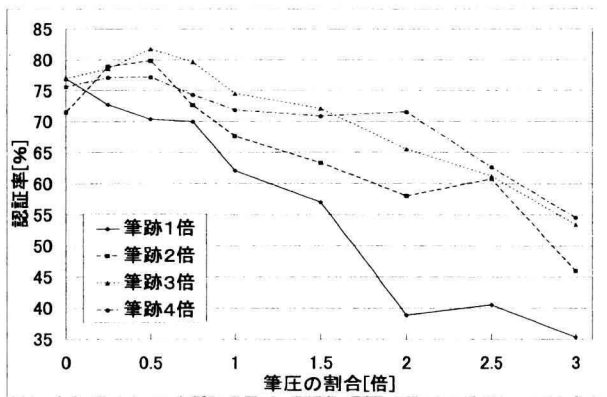


図 15 筆圧・筆跡の重み付けによる認証率の変化

### 9.3 提案システムの認証能力検証実験

登録データ数 1 のときに登録人数を 10 から 50 に増加させたときの認証率の変化は図 16 のようになった。図 16 より登録人数が増加すると認証率が下がることがわかる。

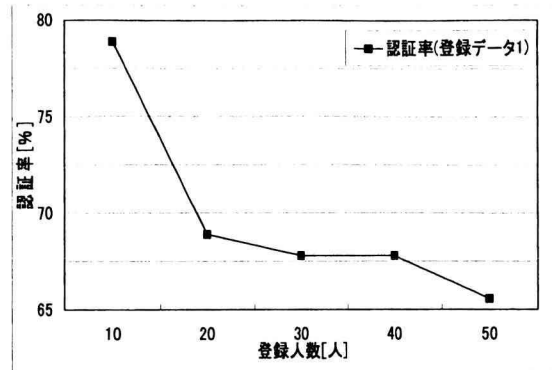


図 16 登録人数による認証率の変化

登録人数が 50 人のときに登録データ数を 1 から 10 に増加させたときの認証率の変化は図 17 のようになった。図 17 より登録データ数が増加すると認証率が上がることがわかる。

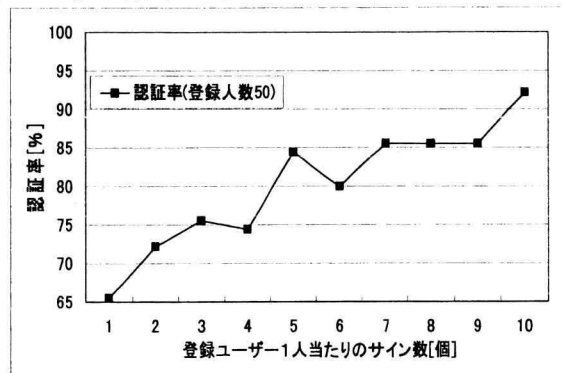


図 17 登録サイン数による認証率の変化

図 18 は登録データ数、ユーザ数を変化させたときの結果である。図 18 より登録人数の増加により認証率が下がるが一定数に達すると認証率の低下も緩やかになることが分かる。また登録データ数も 7 から 10 の間では大きな変化はなかった。

この結果から、登録データが 7 から 10 のとき登録人数が増加しても 80%以上の認証率が維持できると考えられる。

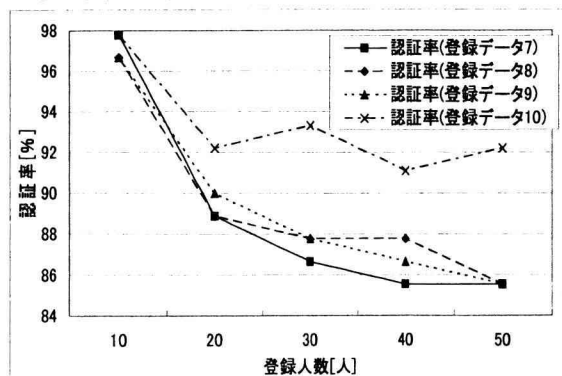


図 18 登録人数・サイン数による認証率の変化

#### 9.4 最適パラメータによる認証性能評価実験

前節までの実験により筆跡・筆圧の倍率と一人当たりの登録サイン数の最適と思われる値がわかった。そこでその値を改良したシステムに用いて認証実験を行った。実験は一人当たりの登録サイン数を10個、筆跡の倍率3.0、筆圧の倍率0.5として登録人数10から50人に変化させ、登録人数分各9個のサインデータを用いて認証を行った。

表2は登録人数を10から50人に変化させたときの誤認証率の変化である。表2を見てわかるように登録人数の増加による認証性能の低下はほとんどみられない。これは前節の実験結果とも一致する。

表2 登録人数による誤認証率の変化

登録人数	誤認証率
10人	3/90
20人	3/180
30人	5/270
40人	5/360
50人	5/450

図19は登録人数50人のときの、閾値を80から90%のときの認証率、誤認証率、Reject率である。閾値80%のとき認証率は98.9%と高い認証率になっている。また、誤認証率が0%となる閾値87%においても95.8%となっている。

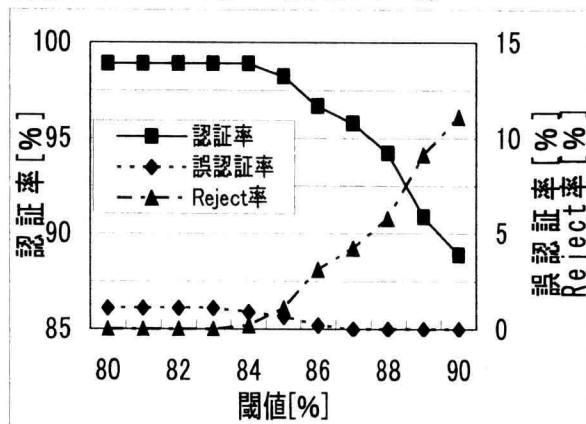


図19 最適パラメータによる認証実験の結果

#### 10. まとめ

既存のシステムは登録済みサインの認証や未登録サインの拒否では性能が高いことが分かる。しかし、詐称サインに対しては非常に低い精度の認証しかできない。これは既存のシステムが形状の判別に重点がおかれているからだと考えられる。よって登録されてない形状のサインを拒否することができても、登録されている形状のサインだと他人が書いたものと区別することができない。

改良したシステムは詐称サインの拒否や未登録サインの拒否は高い性能を示すが、登録済みサインの認証は既存のシステムに劣る。これは形状の判別と同時に他者との区別ができるように改良したためである。個人の特徴が出ていると思われる筆圧の情報量を多くしたために形状の判別能力は低下したが、個人の判断ができるようになった。

個人認証システムにおいて一番大事なのは誤認証をしないことである。そのことから既存のシステムで詐称サイン36個全てをRejectするためには閾値の設定を93.1%にする必要があり、そのときの認証率は56.6%となる。この認証率は改良したシステムを下回ることになるので個人認証システムとしては改良し

たシステムの方が有効であるといえる。

また、筆跡・筆圧情報に重み付けと登録サイン数の増加という2つの改良を加えることで90%以上と高い認証率を得ることができた。

以上のことより提案手法により既存システムの性能向上ができたといえる。

#### 謝辞

サインデータの採取に御協力戴いた、富川研究室及び電気電子工学科の皆様様に心より感謝をいたします。

#### 参考文献

- 1) 笹倉康明 浜本隆之“顔画像の輝度値変化形状に基づく個人認識”,情報科学技術フォーラム 一般講演論文集 Vol.3 pp153-154,(2003)
- 2) R.Poyner, “Wintab Interface specification 1.1”, LCS/Telegraphics, (1996)
- 3) 安居院猛 中嶋正之, “画像工学の基礎”,昭晃堂,(1986)
- 4) 及川幸一, “オンライン文字データ採取システムの作成と筆圧情報を利用したオンライン文字認識”,神奈川工科大学工学部情報工学科 卒業論文,(2001)
- 5) 中島洋行, “筆圧検出タブレットを利用したオンライン個人認証システムの試作”,神奈川工科大学工学部電気電子工学科 卒業論文(2002)
- 6) 菊地真美 赤松則男, “高速筆記者のための高感度筆圧ペンの試作と筆者認識実験”,電子情報通信学会論文誌 Vol.83 No.8 pp1763-1772,(2000)