平成 12 年度

学士学位論文

電子ペンによる個人認証システムにおける前処理の改善に関する研究

Research on improvement of preprocessing in individual attestation system with electronic pen

学籍番号　1010423　　氏名　長尾　崇

指導教員：　竹田史章

年月日：　2001 年 2 月 5 日

所属：情報システム工学科

要旨

近年、バイオメトリクスを用いた種々の個人認証システムがインターネットビジネスの展開と相まって、多数提案されている。本論文では、動的な個人を特徴づける情報である筆圧に着目し、これを用いた個人認証システムを提案する。特に認証システムではニューラルネットワークを使用しており、学習データとして、本人と本人外のデータが必要となる。ここでは、本人外のデータを本人から作成する方法を検討し、その有効性をシミュレーションで確認する。

These days, the many authentication system that use of biometrics are proposed with development of the internet business. In this paper, we pay attention to writing pressure what have the dynamic intelligence for characterize of the individual. We propose of authentication system using writing data. Specially, Neural Network (NN) is adopted in the engine of authentication system. The authentication system needs personal data and others data. Others data are generated from personal data. Finally, the effectiveness of data generation method, while is preprocessing for the authentication system, is show by simmulation.

キーワード：ニューラルネットワーク、個人認証、筆圧波形、抑制データ

目次

1　はじめに

近年の情報化社会の拡大にともない、我々の行動範囲はネットワークを通じて今後さらに拡大しつづけるであろうと予測される。情報化の進歩と共に、情報の電子化やネットワークシステム上での非対面での価値の交換といったものが、一般生活において日常化しつつある。それにともない、データの改ざんやユーザの「なりすまし」といった不正や犯罪が多くなってしまう。このような社会の変化において、ますます個人を特定するための個人認証手法の重要性が高まっている。

現在、我々が持つ個人認証手法の主流といえばクレジットカードを代表とする所有物による認証や、パスワード・暗証番号など知識による認証となっている。しかしながら、これらはカードを紛失したり、パスワードを忘れてしまうと本人であっても使うことができないという不便さがある。また、盗難や偽造、盗み見により容易に他人がなりすませるという問題もある。このため、ユーザ側には大きな負担がかかってしまい、決してこれらは万全の手法とは言えない。そこで今後の個人認証では、クレジットカードのような個人と独立した存在のものではなく、個人と不可分な生体情報（バイオメトリクス）を用いた個人認証技術が主流となっていくと推測される。

現在までにバイオメトリクスによる個人認証技術はいくつか存在しており[4]、その中で指紋や虹彩によるものは特に有名である。これらの技術は従来、警察や官庁分野など限られた応用において大規模システムを用いてのみ利用可能であったものである。しかしながら、近年のパターン処理技術の進歩と、コンピュータの性能の向上のため、パーソナルコンピュータを使ってユーザが不便を感じない時間で個人認証処理が行えるようになった。現在では、入門管理など物理アクセス制御、さらにはパーソナルレベルでの情報セキュリティ分野へと応用を広げ、実用化が進みつつある[5]。

バイオメトリクスによる個人認証システムは、基本的に入力センサでユーザが提示したバイオメトリクスを取得し、そこから特徴を抽出する。そして、あらかじめ登録していたテンプレートと比較し、登録者と同一人物であるか否かを決定するという動作を行う。一般に指紋に関しては犯罪捜査を連想してしまい、また虹彩においては眼球内に光を直接照射するという事への心理的な抵抗がある。また、音声を用いた個人認証システムでは前者のような抵抗はないものの、音声処理において多大な計算量が必要となる[4]。これらのバイオメトリクスを用いた認証システムは充分な精度での運用が可能であったとしても、適用可能な範囲が限定されると予測される。

高知工科大学情報システム工学科（竹田研究室）とG社とJ社の共同研究により、これらのバイオメトリクスに代わるものとして、筆記による情報を認証に用いることに着目している[2]。

筆記という行為は日常化した行為であるため、心理的な抵抗による拒否反応はなく、また多大な計算量を必要とする音声による個人認証[6]に比べ、情報量がすくないため計算量を少なくすることが可能である。

現在ではこの筆記による個人認証システムのプロトタイプを完成し、実用可能な段階になりつつある。この認証システムでは、タブレットを使用しない筆圧検知部をペン内部に搭載した電子ペンを用ている。この電子ペンは JSD により開発されたもので、従来の電子ペンに比べ約 30 倍以上の筆跡検知精度を持つ高分解能の筆圧波形を利用した認証を行なうことができる。

本論文では、現在の電子ペンによる個人認証システムの構成を示し、登録・認証エンジンに使用されているニューラルネットワーク（以下 NN と略記）について記述する。とくに、個人認証システムで使用されている NN への学習に用いる入力データの内本人以外としての、抑制データの作成手法について述べる。この個人認証システムでは、従来の手法として、登録者本人以外の別の登録者から採取された筆記データの内、NN への学習に使用される筆記データを抑制データとして使用している。しかしながらこの場合、本人と他人の境界線があいまいになり、誤認証を起こす恐れがある。そこで本人の登録データから正規乱数を発生させ、その発生させた乱数から抑制データを作成する手法を提案する。本論文では、この提案する手法の有効性を、実際に採取された筆記データを用いたシミュレーションによって検討する。

2　筆圧による認証

筆記された文字は、他人が模倣することは非常に困難である。このことから、欧米では古くから個人認証の手法としても用いられている。

筆記情報による個人認証は大別すると、既に書かれた筆跡の静的情報を用いるオフライン方式と、筆記動作に伴う動的情報を用いるオンライン方式とに分けられる。筆記された文字の模倣が困難なものであれば、その文字を生成するための筆記という行為も他人による模倣が困難なはずであり、筆記行為を対象とした認証についてもいくつかの手法が提案されている。

本論文で使用する認証システムでは筆圧情報を用い、それにより個人認証を行なう。筆圧情報は、電子ペンと呼ばれるペン状の入力装置を用いることにより採取される。本論文で使用された電子ペンでは、筆圧分解能 0.1g、時間分解能 4ms という高分解能の筆圧波形を得ることができる。筆圧波形とは、一回の筆跡による筆圧の時間変動を表したものである。本論文で扱う筆圧認証は、この筆圧波形から抽出した特徴量により個人を識別するオンライン方式の個人認証である。

3 筆記情報を用いた認証における他の研究(4)

本章では、筆記情報を用いた認証技術の研究において、筆圧以外の情報を用いたものを示す。以下に示す研究では、大規模な手書き文字認識において、特定の字種にのみ反応する機能をモジュール単位で実現し、手書き文字認識の細分類部に適用できるニューラルネットワーク（NN）である排他的学習ネット(Exclusive Learning neural NETwork 以下 ELNET と略記)の概要と、学習および認証方法を紹介する。この ELNET は、複数の小規模な階層型 NN によって構成される。従来の文字認識への NN の適用法とは異なり、ELNET は各 NN モジュールの出力層の素子を一個とする。そして、NN モジュール毎に強化用データと抑制用データを用いて、排他的に学習を行うという特徴を有する。これにより、各 NN モジュールが特定の 1 字種に対してのみ反応する機能を実現している。また、従来の NN の構成手法では不可能であった、簡単なパターンマッチング法を大分類部として利用することが可能となる。この簡単なアルゴリズムによる大分類と ELNET による細分類法を組み合わせることで、合理的かつ高精度な認識システムが構築できる。

3-1　排他的学習ネット（ＥＬＮＥＴ）

ＥＬＮＥＴでは、以下の図 5.1 に示すようなモジュールを使用する。このモジュールは、出力層の素子の数が 1 個の三層からなるＮＮである。各モジュールは、それぞれが 1 字種に対応するので、細分類部を構築する際には、対象となる字種数と同数のモジュールで構成される（図 5.2）

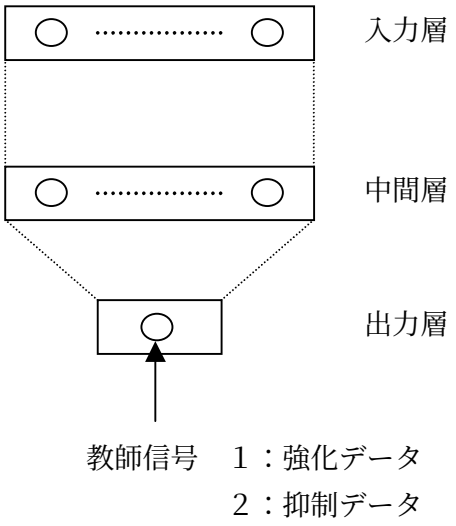


図 5.1　ＥＬＮＥＴのモジュール構成

モジュールの学習において、各モジュールに対応する 1 字種を学習させるだけでは、どのような字種に対しても強く反応してしまうネットワークが形成される恐れがある。これでは、特定の 1 字種にのみ反応するモジュール実現できない可能性がある。そのため、「似て非なるもの」を学ぶことで、類似した文字がそれぞれ何であるかを容易に認識できるのと同じように、学習には各モジュールに対応する字種を強化データとして用い、さらに抑制データとして他の字種も提示して学習を行なっている。前章までで述べてきた署名による個人認証では、学習において強化データに登録者の登録署名データ、抑制データには他人の登録署名データを使用している。モジュールに対応した字種と、それ以外の字種との明確な識別境界を形成させるために、抑制データには各モジュールに対応する字種とパターン空間上近隣に位置する異なる字種のデータを用いることが望ましい。そこでＥＬＮＥＴでは、モジュールに対応するデータを強化データ、抑制データには強化データ以外で大分類で上位候補となる字種のデータを用いることで学習を行なう。

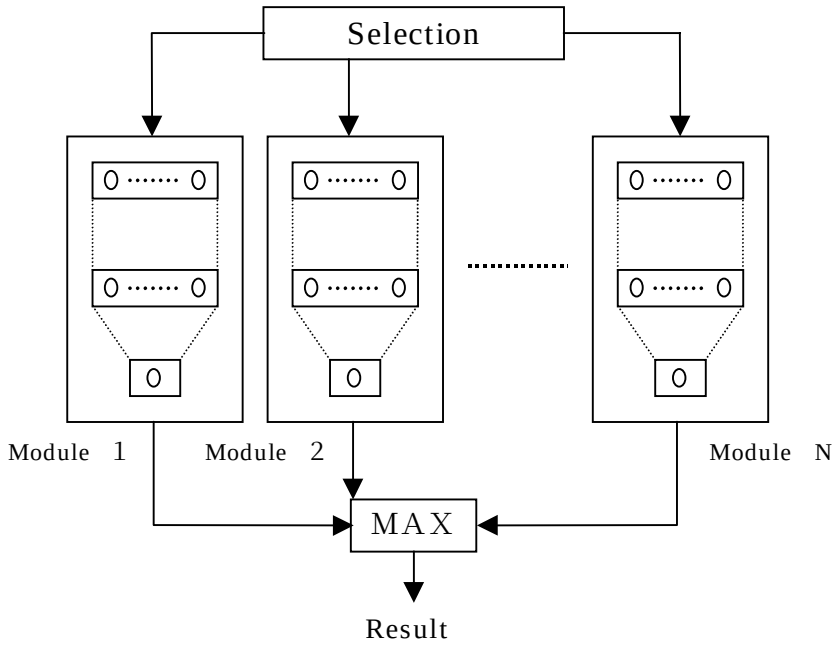


図 5.2　ELNET を用いた細分類部

3-1-1　学習手順

はじめに以下の二つの手順によって、学習データを用いて字種毎に学習データテーブルを作成する。まず、字種Ｔである入力パターンベクトルをｘとする。ｘを入力して大分類を行ない、大分類における ｉ 番目の候補 R_i を求める（i=1,2,…）。そして大分類の結果に基づき、ELNET のモジュール学習用の学習データテーブル作成する。

学習データテーブル作成はまず、Tに対応したモジュール M(T)用の学習データテーブルの左端に入力した文字の字種Tの番号を記述し、次いでそれ以外の上位候補 R_i (≠T)の字種番号を順番にその右に記述する。作成された学習データテーブルにおいて、i 番目に記録されている番号に対応する字種を C_i とする。

作成された学習データテーブルに基づき、続いてモジュールの学習を行なう。字種 C_i のパターンベクトルを $v(C_i)$とし、$v(C_i)$を強化データとして学習させる場合を $v(C_i)\rightarrow E$(Excitement)（5.1)、抑制データとして学習させる場合を $v(C_i)\rightarrow I$(Inhibition)（5.2）で表す。

begin i=1 to K

if(C_i＝T) $v(C_i)\rightarrow E$ (5.1)

else $v(C_i)\rightarrow I$ (5.2)

end

但し K は、1 モジュールの学習に用いるデータ数を表す。上記の学習アルゴリズムにおいて、大分類で上位に出現した回数に応じて、モジュールに学習させる各字種のデータ数が異なる。抑制データの $v(C_i)$は、大分類の上位候補字種の中からランダムに選択される。この際、$v(C_i)$は同じデータが２回選択されないようにする。

3-1-2　認識手順

まず未知入力パターンベクトルに対し、大分類における i 番目の候補 R_i を求める。次に上位 N 個の候補 R_I(１≦i≦N)に対応するモジュールを選択し、各モジュールにｘを入力する。このｘが入力されたモジュールの中から、最大の出力をするモジュール i を決定し、このモジュールに対応する字種を認識結果とする。なお、各モジュールの出力層素子は、学習時には強化データに“１”を、抑制データに“２”が教師信号として割り当てられる。

3-2　認識システムの基本構成

ELNET を使用して認識システムの構成を図 5.3 に示す。大分類部には、偏差付シティブロック距離によるパターンマッチング法を用い、細分類部には ELNET を用いる。

3-2-1　前処理と特徴抽出

ELNET を用いた認証システムでは、入力パターンの前処理として非線型正規化[7]と輪郭線抽出を行なう。特徴抽出においては、まず前処理を施した入力データを 4×4 の領域に分割し、さらに領域数を半分ずつずらしオーバラップさせたけい 7×7=49

の領域に対して、方向性素特徴量[8]を求める。方向性素特徴量は、縦、横、±45°の4方向の線素量を各領域内で重み付けして求める。従って、49×4=196次元の特徴量が抽出される。

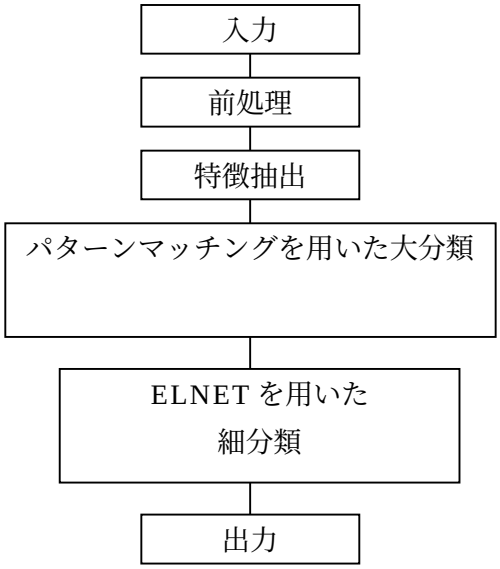


図 5.3　システムの構成

3-2-2　大分類部・細分類部

大分類部の距離尺度として偏差付シティブロック距離を用いている。この距離をDとすると求める式は（5.4）のようになる。

$$D(x, p^i) = \sum_{j=1}^{196} \max\left\{0, |x_j - p_j^i| - a_j^i\right\} \qquad (5.4)$$

ここでxは入力パターンベクトル、P^iはi番目の標準パターンベクトルをあらわす。またx_jは入力パターンベクトルのj次元目を表す。a_j^iはi番目の標準パターンベクトルのj次元目の標準偏差を表す。上記の式により求められた距離により大分類を行ない、$D(x, p^i)$の小さい順に上位候補とする。

細分類部では、上記の大分類部の結果に基づき、ELNETを用いて認証を行なう。認証アルゴリズムについては、本章の第1項で述べたアルゴリズムを用いている。

3-3　ELNET を用いた認証システムによる認証精度

3-3-1　認証実験概要

認識実験には、手書き文字データベース ELT9B の全 3,036 字種を用いる。全 200 セット中、奇数番目の 100 セットを学習データ(Training data)、偶数番目の 100 セットを未学習データ(Unknown data)とする。大分類および細分類の入力特徴量には 196 次元の方向性素特徴量を用いる。大分類には、偏差付シティブロック距離によるパターンマッチング法を用い、細分類には ELNET を用いて行なう。ELNET におけるモジュールの学習には、係数変化型学習法（以下 DCLA 法と略記）を用いる。DCLA 法は、学習係数を出力値に応じて動的に変化させるという特徴を有し、BP 法に比べ収束性が高い[9]。なお、モジュールの入力層素子数は入力特徴量の次元に従って 196 とし、中間層の素子数は 5 に設定して実験を行なう。

3-3-2 性能評価

ELNET の性能評価実験において、1 モジュールあたりの強化データを 100、抑制データ数を 300 として学習を行ない、認証実験を行う。実験の結果、大分類における未学習データに対する 1 位認識率は 92.42%を示した。これに対し、大分類の上位 2 個の候補を対象にして、ELNET により細分類を行なった場合、93.11%の認識率が得られており、ELNET を用いることで向上している。また、NN での学習回数も少なく、認識速度も高速である。しかしながら、学習データ、未学習データともに細分類の対象とする候補数が３以上の場合、認識率が低下してしまう。また、“ 鳥 ”と“ 烏 ”等の類似文字が存在する字種の認識率も低くなってしまう。平仮名と漢字の認識率については、漢字の認識率の方が高い。これは特徴抽出部で求められた方向線素特徴量が、曲線成分の多い平仮名より、直線成分の多い漢字の認識に適していることと、ストローク数の多い漢字の方が、ストローク数の少ない平仮名に比べ、文字の変動が少ないことが原因として考えられる。

4　ＮＮによる筆圧認証システムの構成

ニューラルネットワークを用いた筆圧認証システムでは、筆圧検知部がペン軸に内臓された電子ペン（DP１０００）を使用し、個人認証を行なう。登録された筆圧データから特徴抽出を行ない、ＮＮにより学習を行なう。ＮＮをテンプレートマッチングの代わりとして使用し、本人か本人以外のデータであるか、あるいは書かれた筆記データが誰のものであるかを認識する。

本章では、この電子ペンによる筆圧情報を用いた個人認証システムの構成を述べる。システムの基本構成は大まかに分類すると、登録処理部、学習部、そして認証処理部に分かれる。

4-1　入出力機器

筆圧による個人認証システムでは、認証を行なうにあたり個人情報として、筆圧情報を必要とする。ここでは、この筆圧情報であるソースデータを登録者より採取するため、図 4.1 に示す入力機器を用いる。

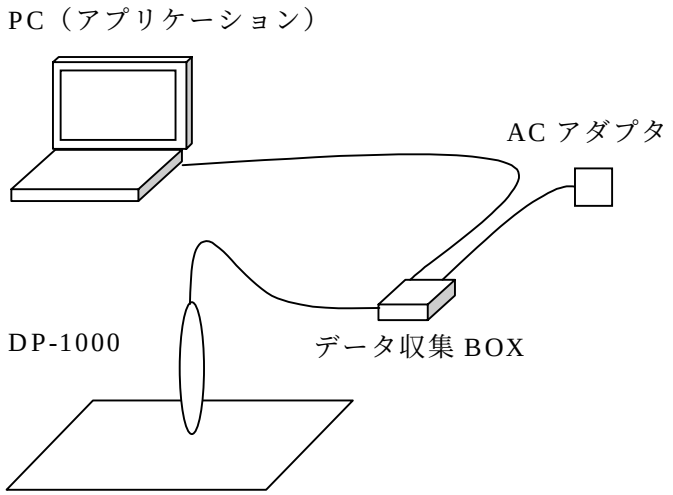


図 4.1 入力機器の全体構成

システムが Windows95 上で動作するため、PC には Windows95/ 98 対応のパソコンを使用している。データ収集 BOX は H83048 マイコンを搭載し、PC とはシリアルポート(19,200bps)で接続されている。電源は AC アダプタによって得ている。デー

タ収集 BOX に電子ペンが５芯ケーブルによって接続される。データ収集 BOX と電子ペンを図 4.2 に示す。

図 4.2　電子ペンとデータ収集 BOX

4-2　電子ペン「DP1000」

前述された機器の中で使われている電子ペン「DP1000」は、JSD によって開発されたものである。この電子ペンは、従来品のようなタブレット（下敷き）を必要としないタイプの電子ペンである。下に電子ペンの構造及び、この電子ペンによって採取された、筆圧の波形を図 4.3 に示す。

使用されているペン軸は市販のものであり、弾性体にはばねを使用する。筆記の際にペン軸が筆記面に押し付けられると、ペン内部にある金属面が押し上げられる。図中では金属面とコイル面の間にはある程度の隙間があるが、ペン先に荷重がかかるとこ二面間の距離が狭くなる。この二面間の距離を IC センサーで感知し、その距離を基に筆圧値を求める。この電子ペンの筆圧分解能は 4[msec]で、1 秒間に 250 個の筆圧値を検出することができる。初期反応荷重は 20ｇからとなっており、小さなペンタッチや書き癖を逃さず感知することが可能である。また、最大反応荷重は 500ｇとなっており、幅広い筆圧測定範囲を持つ。

4-3　登録処理機構

登録処理機構では、電子ペンによってサインを行ない、採取されたデータを処理することで生成された登録用データを、NN に入力し学習させることにより認証システムに登録を行なう部分である。登録処理には「新規追加」、「追加登録」、「再登録」の３種類が存在する。新規登録は未登録の者が電子ペンによって採取されたデータを認

証システムに登録する。追加登録は既に登録している者が既存の登録データに新しい登録データを追加して学習を行なう。そして、再登録は既に登録している者が既存のデータを一旦全て破棄し、新しく採取したデータを用いて学習を行なう。

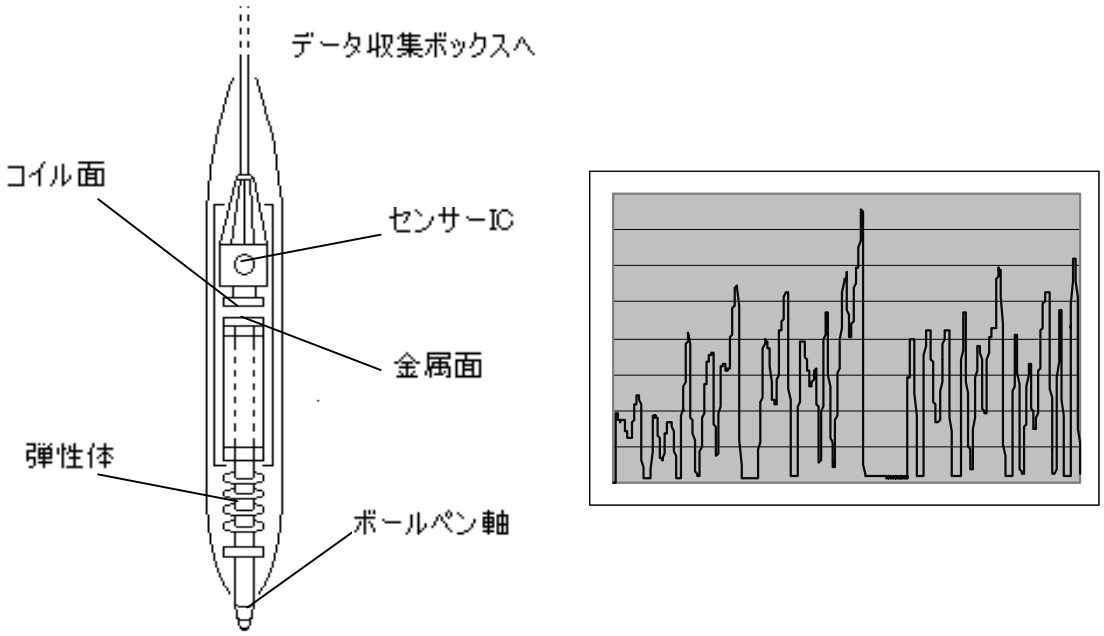


図 4.3　電子ペンの構成及び筆圧波形

4-3-1　登録ソースデータ入力

登録処理機構において新規登録では、まず登録者 ID が自動で割り当てられる。登録者 ID は 0001～1000 の４桁となっており、0000 は使用しない。またこの与えられた ID はユーザが変更することはできない。

認証システムに登録を行なう為に各筆記者毎に 3 回毎のソースデータを学習に使用する筆記データとして採取する。

ソースデータ入力処理の最初での書き始めの検出は、最新 10 個の筆圧カウント値データから、その分散値を計算し、値が 10.0 を超えれば書き始めとみなし、この書き始め検出直前のカウント値を基準カウント値として、筆圧カウント値をソースデータ用配列に格納していくのがソースデータのサンプリングである（図 4.4）。

書き終わり検出では、50 未満の筆圧カウント値が連続で何個サンプリングされたかを計算し、その連続値が規定値を超えれば書き終わりとみなす。書き終わり検出をすると共にまた次のソースデータの入力処理を始め、すでに３回終了しているならばサンプリングの終了として次の処理である登録データの適正チェックを行なう。

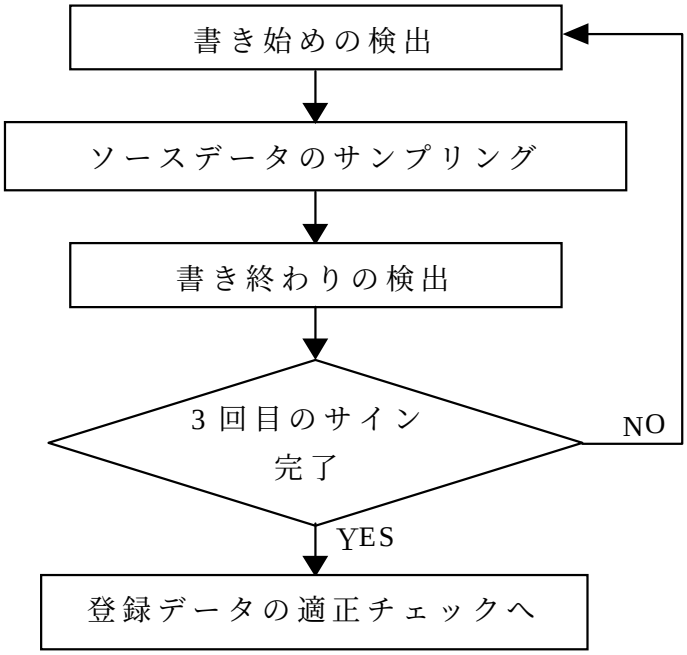


図 4.4 登録ソースデータの入力

4-3-2　適正チェック

この登録データの適正チェックでは NN への学習を行なう前に、採取された登録データの中に、他の登録データとの相違点が多く、学習効率を低下させる恐れのあるものがあるかをチェックする。理由としては、登録データは、ある程度のばらつきがあると学習の効率が良いが、登録データの情報がが大きく異なる場合、後の学習効率の低下や認証処理においても不具合が生じる原因になりかねないからである。チェックによって不適切なデータが検出された場合には、その学習データを破棄し、再入力を促す。このチェックでは各登録データから抽出した参照データを比較することで行なう。図 4.5 に登録データの適正チェックの処理の流れを示す。

適正チェックでは、登録されたソースデータから参照データの抽出というものを行なうが、抽出される参照データとは以下の２つである。

①電子ペンによってサンプリングされたデータ中、文字を筆記中に得られたものと思われるデータ（筆圧値）のみをカウントし、その数を実画部（実際に筆記を行なっている部分）のデータサイズとして抽出する。
②ソースデータを時系列上に連続に並べ、時間軸をＸ軸、筆圧カウント値をＹ軸にとった際にソースデータ上に現れる筆圧波形（図 4.3 参照）の局所最小値を境界線とした領域を抽出し、その数を領域数として抽出する(図 4.6)。

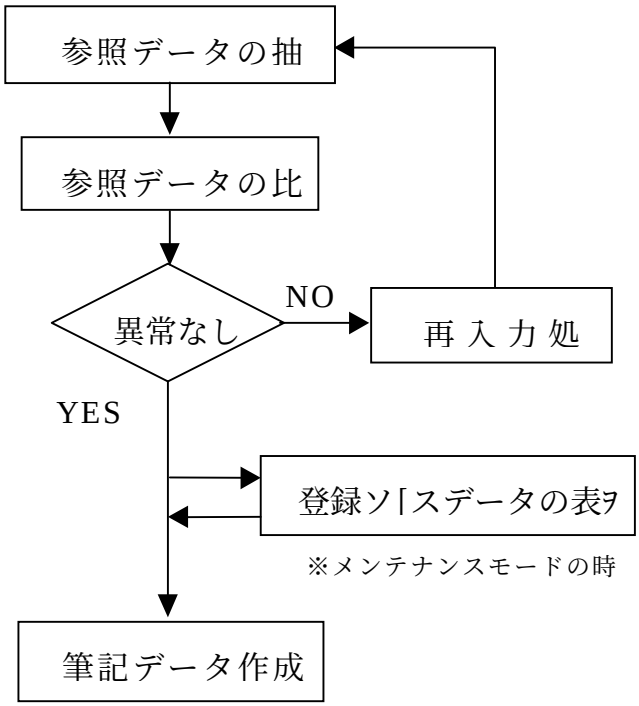


図 4.5 登録データの適正チェック

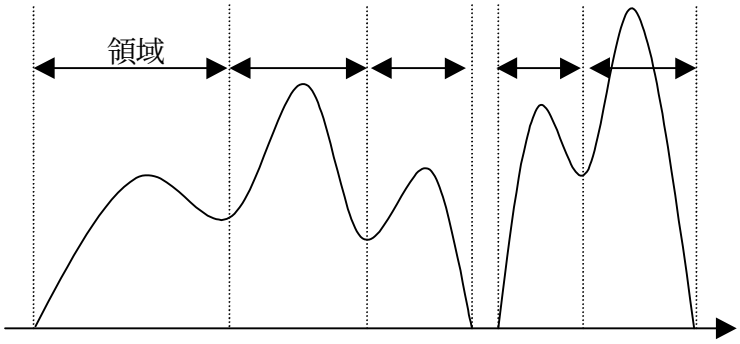


図 4.6　筆圧波形における領域の抽出

なお、参照データは図 4.7 に示す処理手順によって抽出される。

参照データの抽出後、抽出された 2 つの参照データの比較を行なう。抽出された参照データの内、実画部のソースデータサイズを Px(I)、実画部の領域数を Ｐｙ(I)とする。このとき I＝1~3 である。この値に関する各登録ソースデータ間の差⊿Px(I)、⊿Py(I)を求める(4.2)。

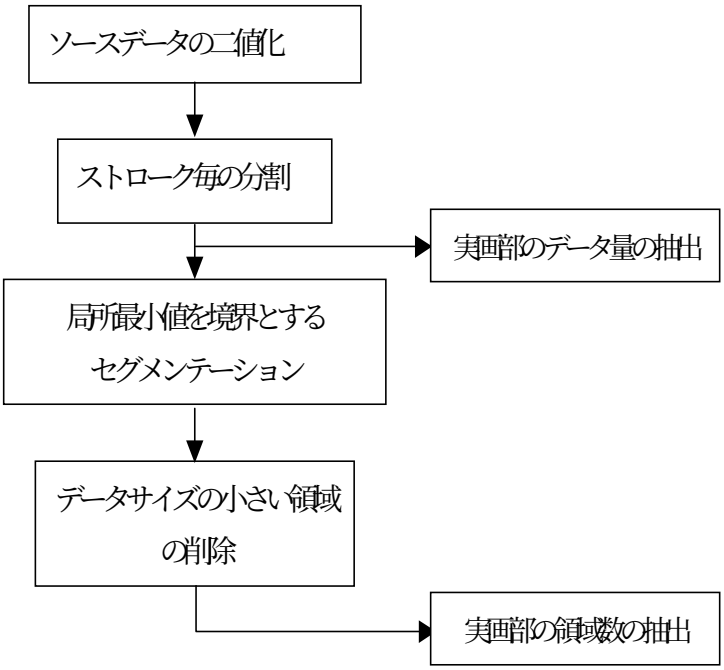


図 4.7　参照データの抽出処理手順

$$\Delta Px(I) = | Px(I) - Px(Mod(I,3)+1) |$$
$$\Delta Py(I) = | Py(I) - Py(Mod(I,3)+1) | \qquad (4.1)$$

（Mod(a,b)は a/b の剰余とする）

式に（4.1）により求められた値が設定された範囲内にあるかどうかのフラグを求める（4.2）。

$$Flag(I) = \begin{cases} 1 \ (\Delta Px(I) < 500) and (\Delta Py(I) < 5) \\ 0 \ \ (\Delta Py(I) \geq 500) or (\Delta Py(I) \geq 5) \end{cases} \qquad (4.2)$$

式（4.2）により求められたフラグに対して、表 4.1（Data1~3 は登録ソースデータを指す）により認証精度の低下を招く恐れのある登録データを決定する。この適正チェックにおいて問題があると判断された場合には、ソースデータの再入力を行ってもらう。再入力が終わればまた登録データの比較が行われ、三回すべての登録データが問題なしと判断されたときのみ次の処理に移ることができる。この適正チェックはあくまで 2 つの参照データを元に判断しているものであるため、その他のパラメータに関する異常を感知する能力は持っていない。

表 4.1　登録データの適正チェック表

Flag(1)	Flag(2)	Flag(3)	Data 1	Data 2	Data 3
0	0	0	NG	OK	NG
1	0	0	OK	OK	NG
0	1	0	NG	OK	OK
0	0	1	OK	NG	OK
1	1	0	NG	OK	NG
1	0	1	OK	NG	NG
0	1	1	NG	NG	OK
1	1	1	OK	OK	OK

OK：問題なし　NG：問題あり

4-3-3　筆記データファイル作成

この個人認証システムにおいて、登録／認証は NN で行なわれる。この NN にデータを入力することにより学習が行なわれる。この時、ソースデータをそのまま渡すのではなく、筆記データへと変換してから NN へ渡される。筆記データ作成において使用する値を以下に定義する。

・ソースデータ　：S_n
・S_n のデータサイズ　：Sv_n
・S_n のソースデータ系列　：$Sd_n(h)$　（$h=0,1,2,\ldots,Sv_n$）
・変換後に生成される筆記データ：N_n
・N_n のデータサイズ　：Nv_n
・筆記データ系列　：$Nd_n(k)$　（$k=0,1,2,\ldots,Nv_n$）

ただし，登録処理時においては，n=1～3 であり，認証処理時においては，n=1 でとなる。筆記データ作成では、まず式（4.3），（4.4）により WinWidth と WinShift をそれぞれ求める。

$$WinWidth = \frac{Sv_n * 2}{Nv_n + 1} \tag{4.3}$$

$$WinShift = 2 * WinWidth \tag{4.4}$$

そして、この二つの値と定義された値によって筆記データを作成する。筆記データ生成までのフローチャートを図 4.8 に示す。

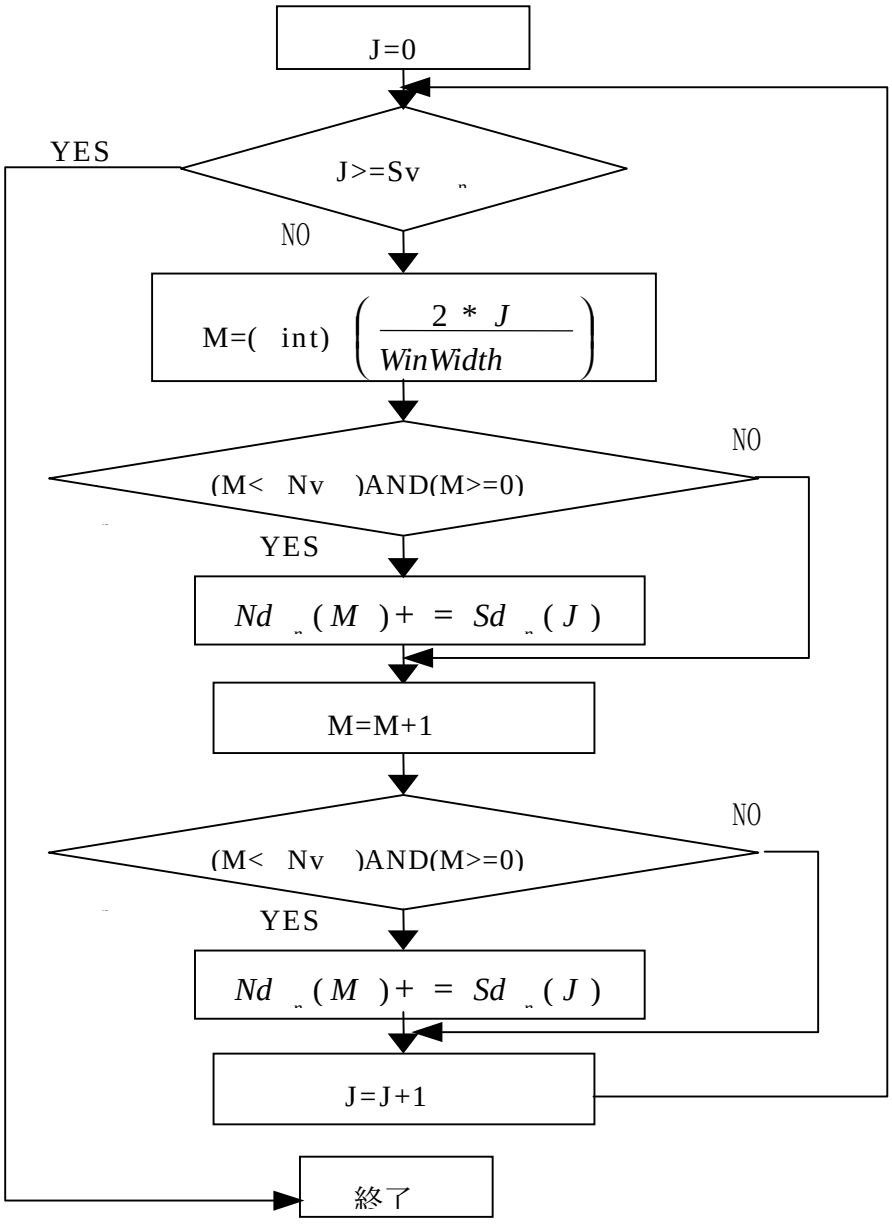


図 4.8　筆記データの作成処理手順

生成された筆記データ（図 4.9）は NN に入力されるために、筆圧波形自身における筆圧カウント値の最大値によって除算を行ない、最大値を 1.0 として 0.0~1.0 の間の数値に正規化される。また、時間軸の数値も NN への入力数に合わせ、50 に圧縮される（図 4.10）。

処理が終了した後に、筆記データをファイルに書きこみ保存する。このファイルが生成される際、登録の種類によってヘッダ内の情報が一部変化する。

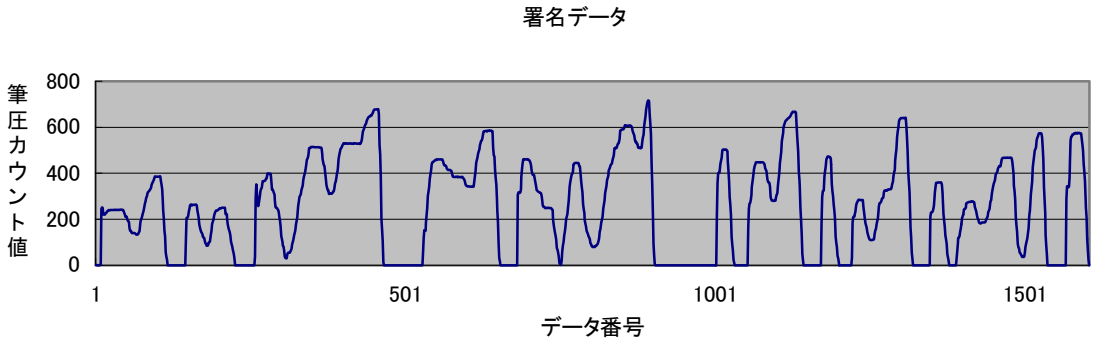


図 4.9　筆記データ

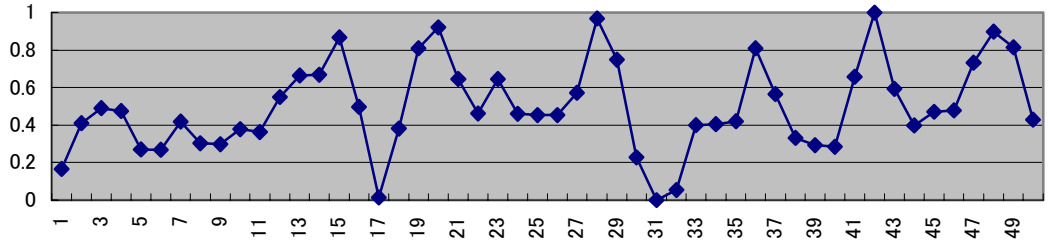


図 4.10　正規化された筆記データ

変化するヘッダ情報の内容は「通し番号」であり、

新規登録または再登録の場合：　1~3
追加登録の場合：(既に登録してあるデータ数＋1~(既に登録してあるデータ数＋3)

となる。NN はここの数値を見ることにより、初期学習（乱数で初期化を行った状態から学習を始める）を行うか、追加学習（現在の状態からさらに学習を行っていく）を行うかを判断する。

4-3-4　登録処理機構定義ファイルの作成

登録処理機構定義ファイルに書き込まれる再認証／再学習を検証する候補者 ID は、4-4-3 で作成された参照データと、マトリクスマップデータを使用して作成される。ここで用いられるマトリクスマップデータとは、参照データの実画部のソースデータサイズを X 軸にとり、実画部の領域数を Y 軸とした 2 次元マトリクスで構成されており、各マトリクスは等間隔に区画化されている。以下にマトリクスマップデータの構成と、それに関する値を示す。

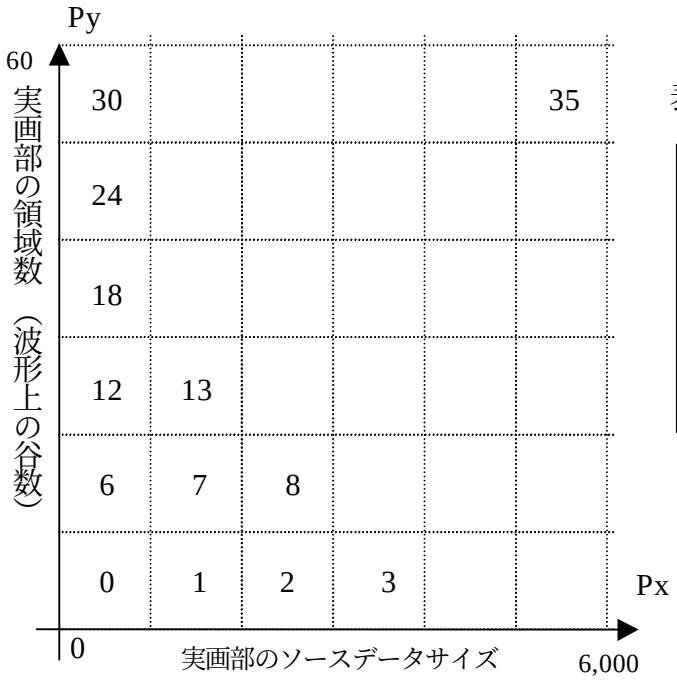


図 4.11 マトリクスマップデータ模式図

表 4.2 マトリクスマップデータ構成値

X軸方向の区画数	Nx
Y軸方向の区画数	Ny
X軸方向の上限値	Lx
Y軸方向の上限値	Ly
マトリクス数	Nx×Ny

図 4.11 のマトリクスマップデータ図においては Nx=Ny=6, Lx=6000, Ly=60 となっており、マトリクス数は 36 である。登録セッション定義ファイルの作成方法は登録の種類によって異なるため、登録の種類別に作成手順を以下に示す。

●新規登録時の処理

①参照データ Px(I), Py(I)（I=1~3）に関して、マップ平面上では重心となる平均値 Gx, Gy を求める(4.5)。

$$Gx=\frac{1}{3}\sum_{I=1}^{3}Px(I),\quad Gy=\frac{1}{3}\sum_{I=1}^{3}Py(I) \tag{4.5}$$

②求められた重心(Gx,Gy)がどのマトリクスに属するかを求める。属するマトリクスの番号を M としたとき、この M は(4.6)式で求められる。

$$M = Div\left((\mathrm{int})Gx, Wx\right)\cdot Nx + \left(Div\left((\mathrm{int})Gy, Wy\right)\right) \tag{4.6}$$

$$\left(Wx=\frac{Lx}{Nx}, Wy=\frac{Ly}{Ny}\right)$$

ただし Div(a,b)は a÷b の商である。

③この M と、平面上で M を囲む８つのマトリクスに登録されている登録者 ID を登録定義ファイルに書き込む。

●追加登録時の処理

①追加登録の際には、既に登録されてある登録データの参照データと、新たに追加した参照データによって平均値を求める。既に登録されている参照データを Qx(K),Qy(K)（K=1~既存登録数（N））として重心を求める（4.7),（4.8)。

$$Gx = \frac{1}{N+3}\left(\sum_{I=1}^{3} Px(I) + \sum_{K=1}^{N} Qx(K)\right) \qquad (4.7)$$

$$Gy = \frac{1}{N+3}\left(\sum_{I=1}^{3} Py(I) + \sum_{K=1}^{N} Qy(K)\right) \qquad (4.8)$$

②新規登録時と同様に求めた重心(Gx,Gy)が属するマトリクス M を求める。

③M の周囲８つのマトリクスに登録されている登録者 ID を登録セッション定義ファイルに書き込む。ただし、追加登録を行なう登録者 ID と、候補者として書き込まれる登録者 ID は重複してはならないため、追加登録を行なった登録者 ID はここには書き込まない。

●再登録時の処理

①新規登録・追加登録と同様にして重心(Gx,Gy)を求める。

②こちらも上記同様にして、マトリクス M を求める。

③求めた M とその周囲の 8 つのマトリクスに登録されている登録者 ID を登録セッション定義ファイルに書き込む。ただし、再登録を行なう登録者 ID と、候補者として書き込まれる登録者 ID は重複してはいけないため、再登録を行なった登録者 ID は書き込まれない。

4-4　認証処理機構

認証処理機構部では、提示用に登録した時と同様の文字をサインし、登録されているデータとの照合を行うことにより筆記者の認証を行う。

認証には大きく分けて入力が指定のカテゴリに属するか（認証）と、入力がどのカテゴリに属するか(識別)に分けられる。前者はある単独のカテゴリに対してのみ判定

処理を行ない、システムに与えられた入力がこのカテゴリに属しているかといった判定を行なう。一方後者は前者の様に単独のカテゴリではなく、システムに登録された全カテゴリが判定処理の候補であり、システムに与える入力に一致するカテゴリがシステムに存在するかという判定を行なうことになる。

今回の実験において使用された電子ペン個人認証システムでは、この二つの認証を単一 ID 指定型, ID 指定無型と称して用いている。前者ではシステムにあらかじめ入力を行う ID を通知しておき、その ID を持った本人かどうかの確認を行う。後者は逆に、ID の通知を行わず、システム自身に登録者の特定を行わせる。以下に認証処理機構における各処理について述べていく。

4-4-1　登録者名･ID の選択

この処理は単一 ID 指定型のみに必要なものであり、どの登録者として提示ソースデータ（以下テストソースデータ）を入力するのかを選択する。個人認証システムでは、ここで登録者 ID を選択しない限り、次の処理に進むことはできない。

4-4-2　テストソースデータ入力

認証時に筆記者から提示される認証用署名データ（テストソースデータ）の入力処理の流れを以下の図 4.12 に示す。ここでサンプリングされる提示用のサインは一回のみである。筆記途中で失敗してもそのまま次の処理にいってしまい、入力失敗はデータ収集ボックスからの信号がこない場合に限られる。

4-4-3　参照データ作成

ここでの行なわれる処理は、登録処理時の参照データの抽出を参照とする。テストソースデータにおける実画部の筆記データサイズと、局所最小値を境界線とする領域数を抽出する。処理手順は登録処理時と同じとなる。（図 4.7 参照）

4-4-4　筆記データファイル作成

こちらも参照データ作成同様、登録時の筆記データファイル作成を参照とする。登録セッション時と異なる点は、①保存されるデータは一個、②登録者 ID が“1001”③通し番号は「1」のみを使用する、の三点となっており、ファイル仕様そのものには変化はない。

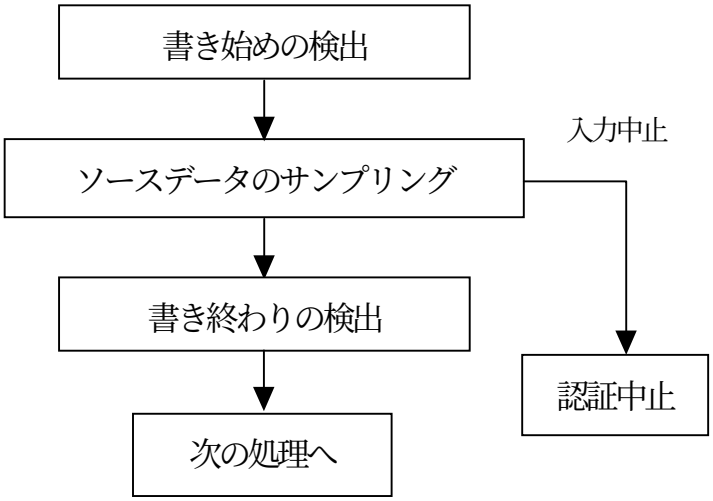


図 4.12　提示ソースデータの入力

4-4-5　認証機構定義ファイル作成

認証機構定義ファイルは、テストデータから抽出された参照データと、登録機構で作成されたマトリクスマップデータを用いて作成される。参照データがどのマトリクスに属するかを調べ、その周囲 8 マスに登録されている登録者 ID を抽出して、認証セッションファイルに書き込まれる。

ファイル作成手順はまず、登録ソースデータから抽出された参照データを T とおき、

T=（Tx,Ty）
（Tx：実画部のソースデータサイズ　Ty：実画部の領域数）

として、マトリクスマップデータに関する設定値を 4-3-4 と同様に
X 軸方向の区画数：Nx
Y 軸方向の区画数：Ny
X 軸方向の上限値：Lx
Y 軸方向の上限値：Ly
マトリクス数　　：Nx×Ny

と定義する。

上記の設定値を用いて、参照データ T が属するマトリクス番号 Tm を式（4.9）により計算する。

$$Tm = Div(Tx, Wx) \cdot Nx + (Div(Ty, Wy) \tag{4.9}$$

$$\left(Wx = \frac{Lx}{Nx}, Wy = \frac{Ly}{Ny} \right)$$

このマトリクス番号 Tm に登録されている登録者 ID、また、マトリクスマップ平面上で、Tm に隣接する周囲 8 つのマトリクスに登録されている登録者の、マップ平面上における座標を（Rx,Ry）とする。そして、

$$Thread\_Range = \sqrt{2} \cdot Wx \cdot Range\_X \tag{4.10}$$

$$Range\_X = 0.1,\ Range\_Y = \frac{Range\_X \cdot Wx}{Wy} \tag{4.11}$$

上記の 3 つを定義し、さらに（4.12）を計算し、

$$D = \sqrt{Dx^2 + Dy^2} \tag{4.12}$$

$$\left(\begin{array}{l} Dx = (Rx - Tx) \cdot Range\_X \\ Dy = (Rx - Ty) \cdot Range\_Y \end{array} \right) \tag{4.13}$$

D を求め、$D \le Thread\_Range$ という条件を満たす登録者 ID のみを認証定義ファイルに書き込む。認証セッション定義ファイルが作成された後に NN モジュールが起動し、登録者数分の認証処理が行われる。しかしながら、候補者となる登録者数が「0 人」となった場合には NN モジュールは起動せず、「該当者なし」と判断して、認証セッションを終了する。

4-4-6　認証結果の表示

認証処理の終了と同時に NN が認証結果ファイルを作成する。この結果ファイルの中には、認証定義ファイルに列挙された各候補者用の NN からの出力値が格納されている。用いられた NN は出力層素子が２つのものを使用しており、それぞれの出力値を OUT1,OUT2 とした場合に、以下の条件を満たす候補者をテストデータの提示者本人と判断する。

(OUT1>THREAD1)　AND
　　((OUT1－OUT2)>THREAD2)

上記の条件式の中で用いられている、THREAD1,THREAD2 は認証における判断基準となる値で設定ファイルから読み込まれる。

5　NN を用いた学習

5-1　学習システム

筆圧認証システムでは、登録処理の中で NN を用いた学習が行なわれる。このシステムでは登録対象のカテゴリ数と同数の NN を並列に配置したシステムを用いている。このシステム構成を図 5.1 に示す[2]。

図 5.1 では分類を行なうカテゴリ数の NN と前処理機構として NN 選択機構、そして NN の出力値の比較部から構成される。登録処理において各筆記者には 1 個ずつの NN が対応し、NN にはそれぞれ独立した ID が与えられる。

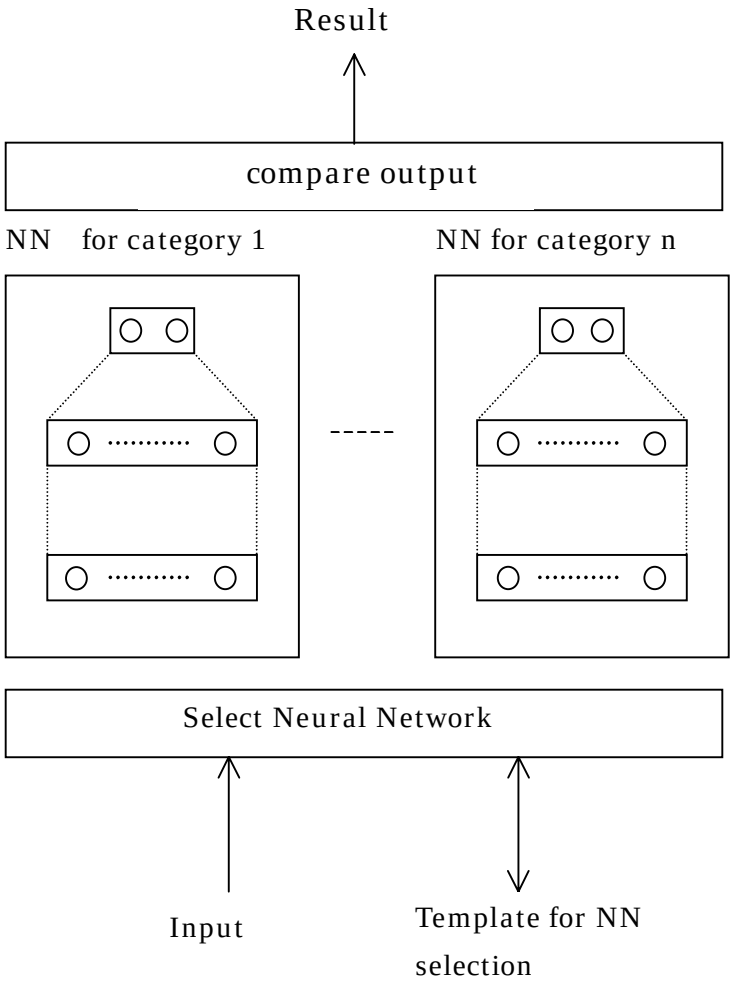


図 5.1　システム構成

カテゴリ毎にNNを独立させることにより個々のNNの規模は小さくなるので学習に用いられる時間は大きく短縮される。また、カテゴリ同士が独立したものであるため、新規にカテゴリ追加のために学習を行なう場合にも、他の学習済みカテゴリの分類能力に影響をおよぼすことなく実行できる。

5-2　ニューラルネットワーク

認証システムでの学習に用いられているニューラルネットワークは、図5.2に示すような三層の階層型ネットワークを使用する。各層の素子の数は最大50個までとなる。下図では例として入力層、中間層、出力層の素子数（○印）がそれぞれ5個、3個、4個と示してあるが、電子ペンによる個人認証システムでは、各素子数が50個、35個、2個なっている。各素子は、それぞれ独立した層に配置している。各層の素子はそれよりひとつ前の層の素子から入力を受け、また、各層間ではすべての素子が結びついている。情報の流れる方向は、入力パターン（下図では5つの入力値）が入力層の各素子に与えられ、中間層で変換され、出力層の各素子から出力パターン（下図では4つの出力値）が得られることになる。

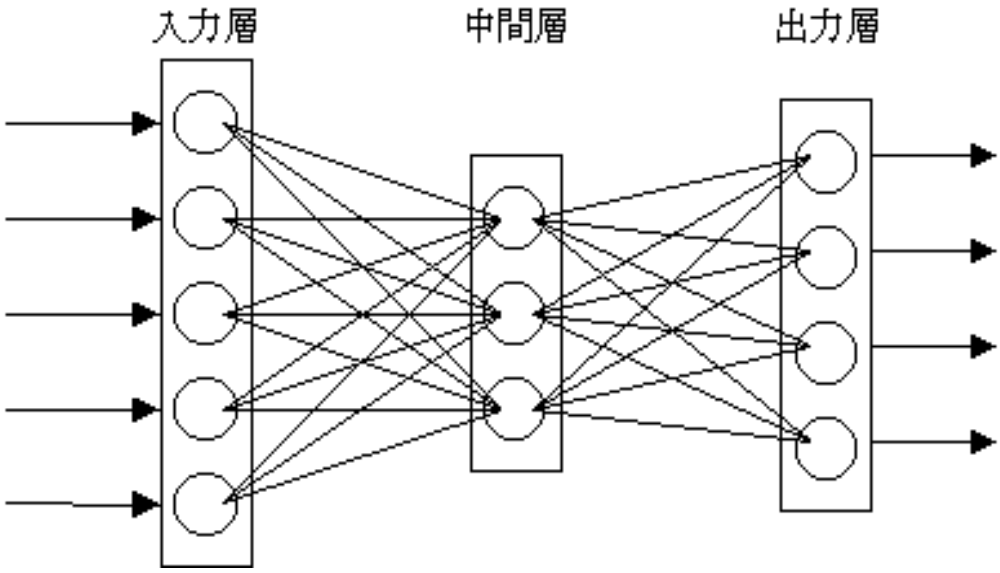


図5.2　ニューラルネットワークの例

ネットワーク構成

ネットワークの構成は環境設定ファイルで設定する。設定項目は入力層の素子数、中間層の数と素子数、出力層の素子数の四つである。入力層の素子数は入力スラブ値

と同数に設定する。電子ペンによる個人認証システムでは 50 に設定されている。また、出力層の素子数は学習パターン数と同数に設定する。中間層の数は現状では必ず“1”としなければならない。

中間層の細胞数は任意に設定することができるが、入力層との素子数と同数程度が適当である。学習が収束しにくい場合には、中間層の素子数を増加させるとよい。

5-2-2　情報の伝達

本項では、ニューラルネットワークにおいて、入力層に与えられた入力パターンが、どの様にして伝達され、出力層から出力されるのかを記述する。

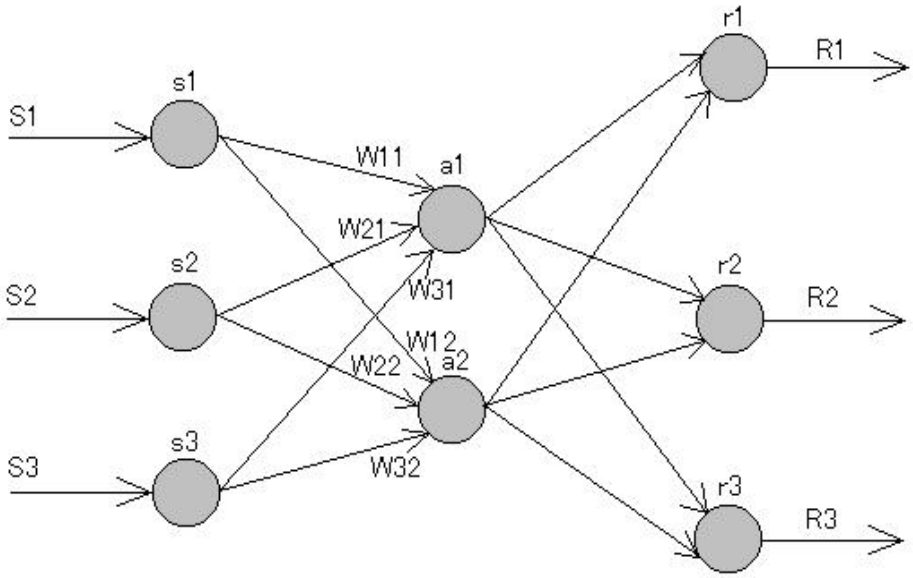


図 5.3　ニューラルネットワークの入出力

図 5.3 においてｓ1，s2，s3 はそれぞれの入力層の第 1，2，3 ユニット、a1，a2 はそれぞれ中間層の第 1，2 ユニット、ｒ1，r2，r3 はそれぞれ出力層の第 1，2，3 ユニットを表す。また、S1，S2，S3 は入力層への入力値（スラブ値)、R1，R2，R3 は出力層の出力値を表す。

入力層の第 i ユニットから中間層の第 j ユニットへの結合の重み（ウェイト）を Wij とする。中間層と出力層の間の情報伝達方法も全く同じであるので、入力層と中間層を例として説明する。

＜ユニットの入力値＞

入力層の第 i ユニットの出力値を Si とすると（入力層のユニットは入力血と出力値が同じ)、中間層の第 j ユニットの入力の総和 Ij は式（5.1）にて求められる。

$$I_1 = W_{11}S_1 + W_{21}S_2 + W_{31}S_3$$
$$I_2 = W_{12}S_1 + W_{22}S_2 + W_{32}S_3 \quad (5.1)$$

となり一般的に、

$$I_j = \sum_i W_{ij}S_i \quad (5.2)$$

とあらわすことができる。

＜ユニットの出力値＞

中間層の第 j ユニットの入力の総和を Ij とすると、中間層の第 j ユニットの出力値 Oj は式（5.3）にて求められる。

$$O_j = f(I_j) \quad (5.3)$$

(f は入出力関数)

このようにして、入力層の各ユニットの出力値と、入力層のと中間層の各ユニット間のウェイトから中間層の各ユニットの出力値を得ることができる。

同様にして、中間層の各ユニットの出力値と、中間層と出力層の各ユニット間のウェイトから出力層の各ユニットの出力値を得ることができる。

5-2-3　中間層･出力層の入出力関数

中間層と出力層の各ユニットの入出力関数として使用される、ロジスティック関数（シグモイド関数）を式（5.4）に示す。

$$f(x) = \frac{1}{1 + \exp\left(\frac{-x+\theta}{T}\right)} \quad (5.4)$$

式（5.4）において、x は各ユニットへの入力値で、f(x)はそのユニットの出力値である。T はネットワークの温度と呼ばれる正の数で、T が大きくなるほどグラフはなだらかなものとなる。θ はユニット単位のしきい値である。

図 5.4 にシグモイド関数のグラフを示す。このグラフでのしきい値 θ は 0 とする。

Tは総合誤差に比例して、1.3 から 0.7 まで変化させる。この操作は学習プログラムが自動的に行なう。また、総合誤差については次項にて記述する。

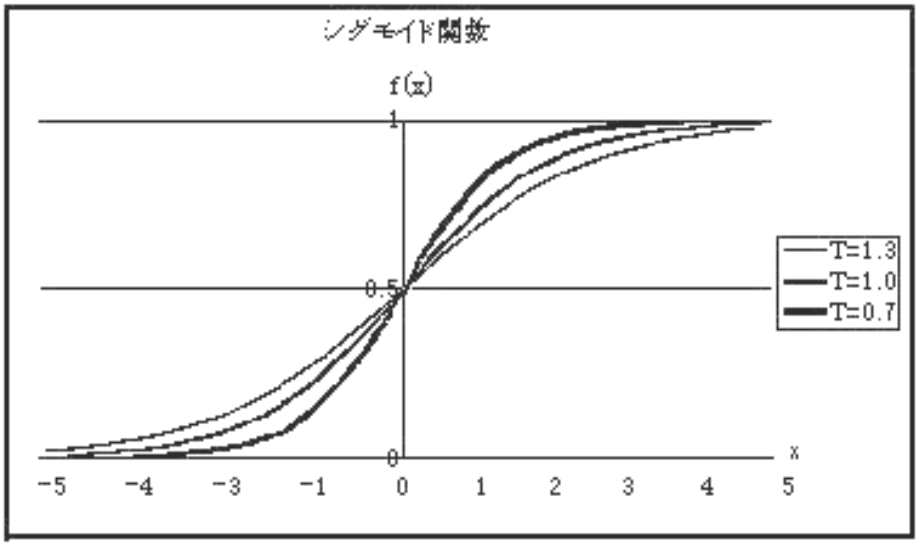


図 5.4　シグモイド関数

5-2-4　学習アルゴリズム

前項の情報の伝達において、入力層に与えられた入力パターンが中間層を経て変換され、出力層から出力パターンが得られることを示したが、入力パターンに対して期待する出力パターンを得るためには、各ユニット間の結合重み（ウェイト）を適切な値しなければならない。このウェイトを適切な値に設定にするために学習を行なう。

学習方法としては、≪誤差逆伝搬(Error Back Propagation)アルゴリズム)≫を使用する。具体的には、いくつかの入力パターンの例（学習パターン）を与え、その時の出力パターンと期待する出力パターン（教師値）との誤差が減少するようにウェイトを修正する。

ある入力パターンを与えた時の出力層の第 j ユニットの出力値を Oj、この時の出力層の第 j ユニットの期待値を Tj とすると、第 j ユニットの誤差 Ej は式（5.5）にて求められる。

$$E_j = \frac{1}{2}\left(T_j - O_j\right)^2 \tag{5.5}$$

したがって、一つの学習パターンＰにおける出力層の誤差 Ep は式（5.6）にて求められる

$$E_j = \frac{1}{2}\sum_j \left(T_j - O_j\right)^2 \tag{5.6}$$

全学習パターンの誤差の総和を E とし、これを総合誤差と記述する（5.7)。

$$E = \sum_p E_p = \frac{1}{2}\sum_p \sum_j \left(T_j - O_j\right)^2 \tag{5.7}$$

上記の総合誤差 E が最小になるように各ユニット間の結合重み（ウェイト）を修正する。修正の方法としては最急降下法を用いる。具体的には、各学習パターン毎に各ユニットの誤差 Ej が最小になる方向へ微妙な変更を加えていく。

第 t 回目の学習における、k－1 層の第 I ユニットから k 層の第 j ユニットへのウェイト Wij の修正量⊿Wij(k-1,k)(t)は（5.8）式にて求められる。

$$\Delta W_{ij}^{k-1,k}(t) = -\varepsilon \delta_j^k O_j^{k-1} + \alpha \Delta W_{ij}^{k-1,k}(t-1) + \beta \Delta W_{ij}^{k-1,k}(t-2) \tag{5.8}$$

上の式において、“ ε ”は学習定数、“ α ”は慣性定数、“ β ”は振動定数をあらわす。また、”δj(k)”は k 層の第 j ユニットの一般化誤差で、k 層が出力層の場合と中間層の場合によって算出方法が異なる。（5.9)，（5.10）に一般化誤差の算出方法を示す。

k 層が出力層の場合、（Ij(k)は k 層の第 j ユニットの入力総和）

$$\delta_j^k = \left(T_j - O_j^k\right) f'\left(I_j^k\right) \tag{5.9}$$

k 層が中間層の場合、（ただし、mは出力層のユニット番号）

$$\delta_j^k = \left(\sum_m W_{jm}^{k,k-1} \delta_m^{k+1}\right) f'\left(I_j^k\right) \tag{5.10}$$

以上が誤差逆伝搬法によるウェイト修正の説明とする。

前項で記述したウェイトの修正式

$$\Delta W_{ij}^{k-1,k}(t) = -\varepsilon \delta_j^k O_j^{k-1} + \alpha \Delta W_{ij}^{k-1,k}(t-1) + \beta \Delta W_{ij}^{k-1,k}(t-2) \tag{5.11}$$

における、学習定数ε、慣性定数α、振動定数のβは環境設定ファイルで設定する。εは大きな値にするとウェイトの修正量が大きくなり、学習は早くなるが、あまり大きくすると逆に学習が収束しなくなる。総合誤差が上下に振動するときは、学習定数を小さくし、誤差の減少速度が小さい時は学習定数を大きくする必要がある。この操作は学習プログラムが自動的に行なう。ユーザは学習開始時の学習定数の初期値を設定する。初期値は（0.1< ε <1.0）の範囲で設定する。デフォルト値は 0.5 である。

慣性定数αは総合誤差の振動を減らし、学習の収束を加速させる働きをする。振動定数βは総合誤差を上下に振動させて極小値から脱出させる働きをする。αとβには関連性があり、以下の図の範囲内（塗りつぶした部分）で設定する[10]。慣性定数のデフォルト値は 0.95、振動定数のデフォルト値は‐0.1 である。

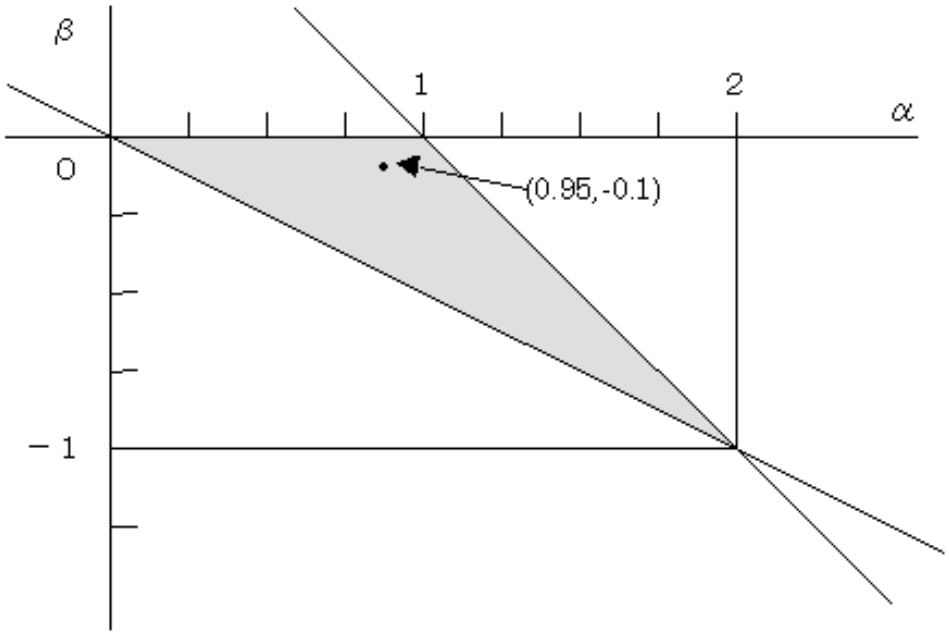


図 5.5　慣性定数と振動定数の範囲

5-2-5　初期学習と継続学習

学習時には、初期学習か継続学習のどちらを行なうかを選択することができる。初期学習では、最初に乱数を用いることでウェイト値の初期化を行なう。それに対して継続学習では、既に存在しているウェイト値を初期値として使用する。継続学習は学習データを追加した時など現状のウェイトを利用したい時に実行する。

5-3　筆記による個人照合に用いられる NN 識別手法

5-3-1　ニューロテンプレートマッチング識別手法[1]

ここでは、本論文で用いた筆圧データによる個人認証用テンプレートマッチング識別手法について説明する。実際に筆記データを使用しての個人認証では、登録者は 10 人、20 人ではなく、非常に多くの識別データを扱うことになる。そこで、本論文で記述する NN による識別手法は、NN とテンプレートマッチングを融合させたニューロテンプレートマッチング識別手法を用いる。この手法では、識別パターンの増加と新規識別パターンの登録を容易に実現することが可能である。

その基本的な構成は、個々の識別パターン毎のテンプレートを NN で構成し、非線型テンプレートによるマッチング処理を行なう。なお、各テンプレートに対応する NN は、目的とする識別パターン（目的パターン）と目的としない識別パターン（目的外パターン）の二つだけを分類する機能を有する。また、NN の出力層の素子の構成法は二種類ある。一つは、出力層は一つの素子を持ち、出力値がある設定したしきい値より大きければ目的データ、それより小さければ目的外データと判定する手法である（以下ＮＮ１と略記)。もう一つは、出力層の素子に目的素子と目的外素子を設定する方法である（以下ＮＮ２と略記)。

NN での学習を行なうためには、教師される信号が１となる場合と、０となる場合のそれぞれの入力が必要となる。この教師信号が１となる入力を強化データ、0 となる入力を抑制データとそれぞれ表記することにする。

5-3-2　NN2 の構成

電子ペン個人認証システムにおける登録処理中で使用するニューラルネットワークは、出力層に二つの素子を持つニューラルネットワーク（以下 NN2）を使用する。出力層にある二つのユニットの一つは目的パターンの提示に反応するユニットであり、もう一つは目的外のパターンに反応するものである。学習において、目的パターンのデータ（本人の筆記データ）を提示した場合には目的パターンに対応するユニットには“１”を、目的外に対応するユニットには“０”を教師する。目的外パターンのデータ（他人による偽筆等）の提示に対しては目的パターンユニットには“０”、目的外パターンユニットに“１”を教師する。

電子ペン個人認証で使用されている NN2 は入力層・中間層・出力層の 3 層からなり、入力層の素子が 50 個、中間層が 35 個、そして出力層が２個となっており、構成は 50×35×２となる（図 5.6)。

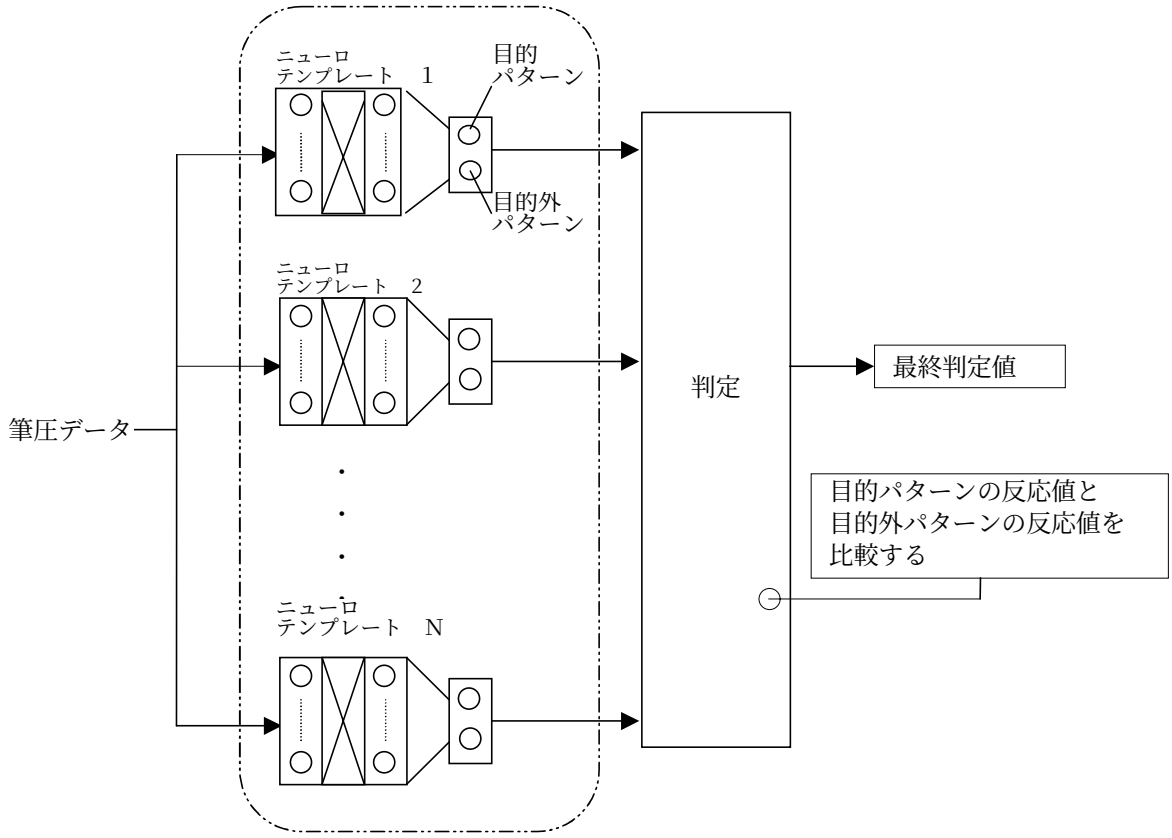


図 5.6　NN 2 の構成

複数のテンプレートの結果から最終判定を得る手続きは以下の通りである。まず、目的パターンの出力ユニット値にしきい値を設定する。さらに、目的外パターンの出力ユニット値と目的パターンの出力ユニット値との差分にも別のしきい値を設定しする。この二つのしきい値を満たした全てのニューロテンプレートからの出力ユニット値の最大値に対応するカテゴリを最終判定候補とする。この候補となる入力値を同じカテゴリの学習データから統計的に作成した上下限値で確認し、この上下限値の範囲内に入力値のすべてが収まっていればそのカテゴリを最終判定としている。

5-3-3　NN 選択機構

筆圧による個人認証システムにおける NN 選択機構では、認証処理において駆動する NN 数をできるだけ少数に抑えることを目的とする。理由としては、各 NN の規模が小さくとも、登録者の増加に伴い NN の数が増加すれば、それにともない動作に必要とされる時間を無視することはできないからである。

従来の NN のみの識別手法では困難であった、識別パターンの増加と新規識別パターンの登録を実現するために、NN とテンプレートマッチングを融合したものを使用する。基本的な構成は個々の識別パターン毎にテンプレートを NN によって作成し、

本来線形処理であったテンプレートを NN との融合により、非線形処理による判定を行なうテンプレートによるマッチング処理を行なうというものである。NN 選択機構により駆動する NN を選択することで、不要な NN の駆動が抑制される。また、それによって学習時間の短縮化が期待できるとともに異常な入力が与えられた場合に、システムが異常動作し、誤った認証を行なうという可能性の低減を図ることができる。テンプレートは学習データを用いることで作成され、学習データの追加毎に更新されるものとする。筆圧波形から画数及び筆記時間を求め、テンプレートに格納された画数及び筆記時間と比較することにより駆動する NN の決定を行なっている。

5-4　現状の筆圧認証システムの特徴

前章で記述されたニューラルネットワークを用いた筆圧による個人認証システムは次のような特徴を有する。

①この認証システムでは、登録処理において登録者一人に対して、一つの NN が割り当てられ、テンプレートの代わりとしている。これにより、登録者の追加毎に NN を再構築しなければならないが、全体を再構築する必要はな。

②登録処理を行なう際に採取した三回の登録署名データの中に、他のデータとの相違点が多い異常なデータが存在すると、学習効率の低下、収束しない原因となる。そこで、登録前にこれらの現象を抑えるために、署名データから抽出された個人情報を軸とした二次元平面を作成し、登録署名データに異常があるかどうかのチェックを行なう。

③NN は学習を行なうために強化データと抑制データを用いる必要がある。本来抑制データに用いるデータは、他人がその登録者を模倣した署名データ（偽筆）を使用するが、実用上偽筆データの採取は非常に困難な為、他人の登録署名データ（他筆）を抑制データとして使用している。

5-5　登録署名チェック手法

筆圧による個人認証システムでは、登録署名に対してチェックを行ない、異常がみられるようであれば、その登録署名に対して再登録を促すようになっている。現在の手法は、署名データから抽出される二つの特徴データそれぞれを軸とする二次元平面を構成するものである。しかしながら、これらの情報は NN への入力データとは直接関係するような情報は使用していない。このため、明らかに異常であるデータでも、チェックに掛からずそのまま NN への入力に使用される恐れがある。本節では従来のチェック手法を詳しく示すものとする。

5-5-1　従来のチェック手法

電子ペンによって採取された N 個の登録署名から二つの特徴パラメータを抽出する。抽出する項目を以下に示す。

①実画部の総データ数

オンラインによって採取された登録データは、実際に文字を書いているときに得られたデータ（筆圧＞０,以降実画と呼ぶ）と文字の画と画の間で採取されたデータ（筆圧＝０,以降空画と呼ぶ）の二種類がある。これらのデータのうち、前者におけるデータの数を抽出する。（2-4-3 参照）

②総領域数

データ番号を横軸、筆圧値を縦軸とした場合に、採取した登録データが描く筆圧波形(図 2.3)が得られる。このとき、画の始点と終点、及び波形の局所最小値を境界線とする区間を領域と呼び、この領域の数を抽出する。

N 個の登録署名データから得られる実画部の総データ数のデータを X(n)、総領域数のデータを Y(n)として（ｎ=1~N)、この二つのデータ間の差を以下の式で求める。ただし、ｎ=1~N, m=1~N, ｎ≠ｍである。求められた dx_{nm}, dy_{NM} で、以下の条件（5.12),（5.13）を満たさない組み合わせがあれば、異常が　あるとみなして、再登録を促す。

$$\left(dx_{nm} \le Th1\right) \cap \left(dy_{nm} \le Th2\right) \tag{5.12}$$

$$\left(dx_{nm}, dy_{nm}\right) = \left(\sqrt{(X(n)-X(m)^2)}, \sqrt{(Y(n)-Y(m)^2)}\right) \tag{5.13}$$

Th1，Th2 は任意の正整数であり、現システムでは現在 Th=500，Th2=５とする。

5-6　学習データの作成

登録処理において、ＮＮを用いての学習を行なう際には、ＮＮに入力するデータとして強化データと抑制データの二種類が必要となる。強化データとは、NN の出力層の二つの素子のうち、目的データを入力した場合に目的素子が活性化するデータであり、登録者本人の署名筆記データをそのまま用いることができる。抑制データは、逆に目的外データを本入力した場合、目的外素子が活性化するデータである。本来ならば、他人がその登録者の署名を模倣した署名データ（偽筆）を使用する。しかしながら、実用上において、その偽筆データを取得するのは非常に困難である。電子ペンによる個人認証システムでは、この偽筆データの代わりとなるものを作成し、それを抑制データとして用いる。

5-6-1　従来の手法による問題点

筆圧認証システムでは、ＮＮをテンプレートの代わりとして使用することにより認証を行なう。NN を認証用テンプレートとして機能させるため、登録者本人の署名データを強化データとし、本人以外の署名データを抑制データとする。本来は、本人の署名データを他人が模倣した署名（偽筆による署名）を抑制データとする。しかしながら、実用上で偽筆による署名を取得するのは非常に困難であるため、現状のシステムでは本人以外の登録署名（他署名）を抑制データとして使用する。そのため、本人（A とする）と本人以外（$\overline{A}$ とする）を区別するために構成される境界線(曲面)が、A の署名データが分布しうる範囲よりも広くなる可能性がある（図 5.7）。

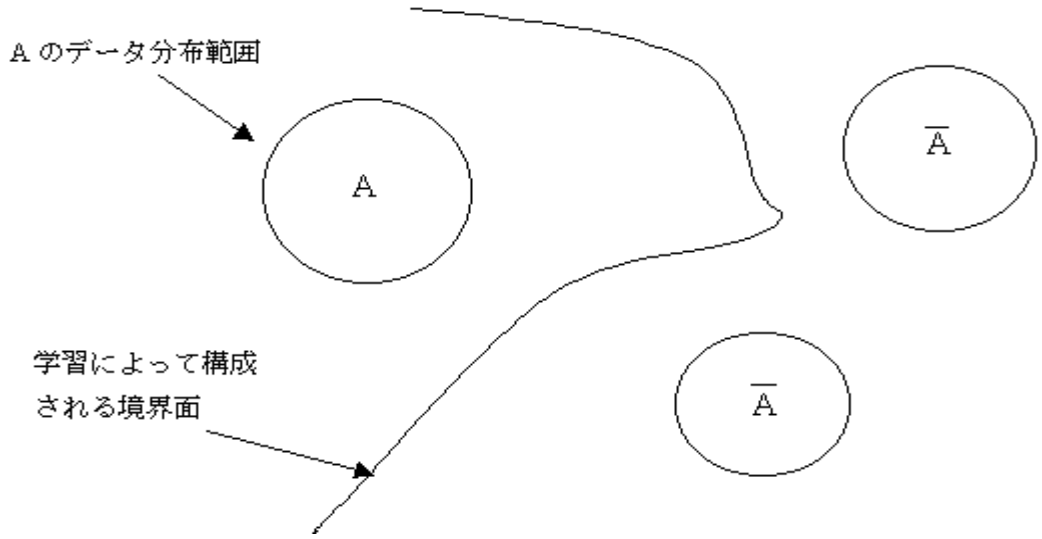


図 5.7　他人の登録署名データを抑制データとして学習する場合

上記のように他人の登録署名で抑制データを作成した場合、照合時に本人が提示した署名データを本人の署名と判断する「本人認証率」は高くなるが、本人以外が提示した署名データを誤って本人の署名と判断する「誤認証率」も同じ様に高くなる。

また、学習に用いられる入力データの作成方法も問題点がある。時間軸を表す横軸方向は、移動平均法を施して固定値として 50 に圧縮しているため、時間情報が消失する。筆圧カウント値を表す縦軸方向も、筆圧波形自身の最大値で除算することで正規化を行なうため、筆圧の強弱情報が消失する。このように入力されるデータの情報が少なくなるため、同一筆記者内の「揺らぎ」には強いが、個人差もなくなってしまい、他人侵入率を高くする要因の一つになりうる。

6　データ作成手法の提案

6-1　抑制データ作成手法の提案

現在の認証アルゴリズムでは、登録者（A）の抑制データ($\overline{A}$)は、他人の署名データを用いるこで作成している。表 6.1 にAとして使用した筆記者のデータを、A の NN に入力した場合（$\overline{A}$の本人署名は、A にとっては他者署名）の誤認率を示す。

この誤認率を求めるために使用した署名データは、竹田研究室に所属する学生の内、7 名を選び、各人から 50 個ずつの筆記データを採取し、その内の任意に選んだ 3 個のデータを、学習に使用する登録データとして使用した。表中の Th1 は認証における出力値が OK か NG のどちらであるかの判定のためのしきい値とする。

表を見る限りでは、良い結果を納めているといえるが、$\overline{A}$として学習していない未知の筆記者のデータをどこまで棄却できるかという疑問が残る。

表 6.1　他人の署名データを抑制データとした場合の誤認率（%）

TH1の値	0.4	0.5	0.6	0.7	0.8	0.9
誤認率(%)	0.65%	0.54%	0.42%	0.30%	0.18%	0.00%

また、$\overline{A}$として学習するデータと A との特徴空間における「距離」が大きい場合、学習によって構成される A と$\overline{A}$の境界線（曲面）が雑になる(図 5.7 を参照とする)。

このような状態では誤認率が高くなる可能性がある。そこで、A（登録者）か$\overline{A}$（抑制データ）かを判定する境界線を、A 自身のデータから作成し、A の本人データが分布しうる限界近くでこの境界線を引くことができれば、誤認証の低下が期待できる。この概念を図 6.1 に示す。

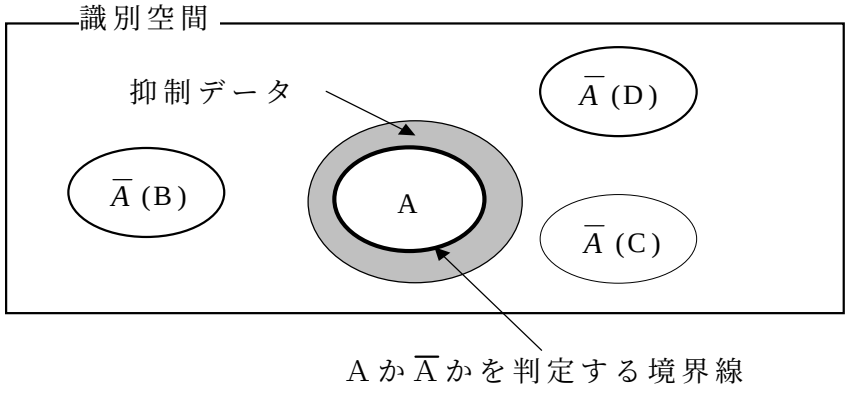


図 6.1　A 自身のデータから抑制データを作成し学習

この抑制データ作成案として行なったのが、A の登録データから得られる標準偏差を元に作成した正規乱数のデータである。正規乱数の生成は、N 個の登録から作成されたスラブデータ（NN への入力用に作成されるデータ）で、同じ番号上にある N 個の値から標準偏差σを求め、平均値 0，標準偏差σの正規分布に従って乱数を発生させる（図 6.2)。発生させたデータに登録署名データの上限値あるいは下限値をオフセットにすることで、抑制データを生成する。こうして作成した抑制データによって学習を行い、認証を行なった結果を以下の表に示す。実験条件は他人の登録データでの抑制データ作成時と同じである。

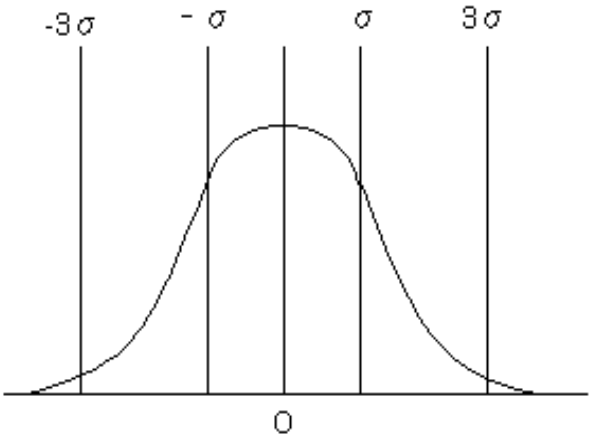


図 6.2　平均 0，標準偏差σの正規分布

表 6.2　正規乱数を抑制データに使用した場合の誤認率(%)

TH1の値	0.4	0.5	0.6	0.7	0.8	0.9
誤認率(%)	4.56%	4.56%	4.20%	3.72%	3.30%	2.82%

判定しきい値を厳しくすれば、誤認率を 0%までに抑えられていることがわかる。しかしながらこの実験では、正規乱数によって生成されたデータは、A のパターンに類似しているかどうかのチェックも行なわずに、全てを抑制データとしている。これでは A とを分ける境界線が A の分布しうる範囲の内側に境界線が引かれ、結果として、実際には A である登録者の筆記データを認証させても本人ではないと判断するといった本人署名の受理率を低下させる原因になると考えられる（図 6.3)。

そこで、正規乱数で生成した抑制データに対しチェックを行ない、登録者本人パターンに近ければ強化データとし、そうでなければ抑制データとするようにすれば、学習効率と認証率の向上が期待できる。

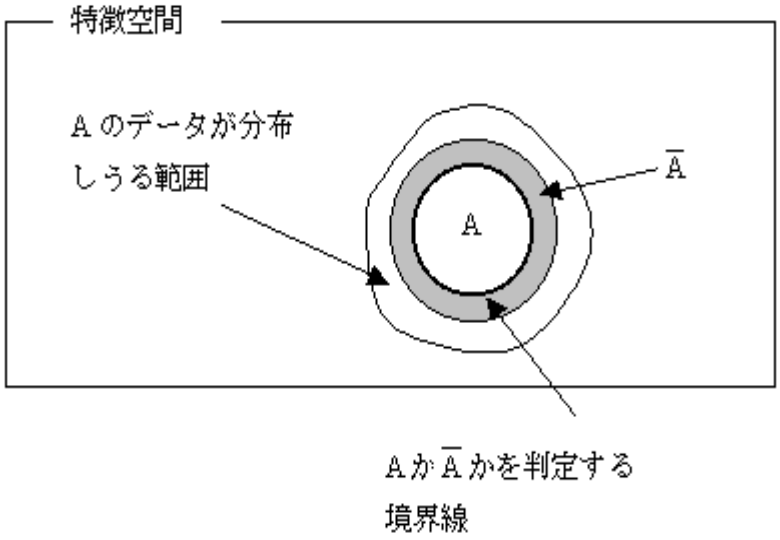


図 6.3　A の分布しうる範囲より内側に構成される境界線

具体案として以下の項目を使用したものが考えられている。

①相関係数：ｒ

データの相関を示す値であり、１に近づく程パターンが近づいていく。

②類似度を表す距離値：ｄ

実際の値を比較して、その距離を求める。値が小さいほどパターンが近づくことになる。この値はテンプレートマッチング等に使用されるものである。

ただし、これらの値は NN への入力データを直接比較して得られるものとする。この二つを使用して図 6.4 に示す手順によって、乱数より生成したデータを強化データとするか、抑制データとするかを選択する。図中の Th_r,Th_dは、選定基準とするしきい値であり、本人 A のデータのばらつき具合によって値を変化させる。どの値が最適であるか、また、どのように変化させると最適なしきい値を設定できるかは、未検証である。

さらに、正規乱数だけでなく、他者の署名データに対しても同じ処理による選定を行ない、混合させて抑制データを作成する方法も考えられる。

ただし、以上の案は、本人 A のデータのばらつきが大きくないことを期待してのものである。登録データに異常なデータが含まれた結果、A の分布範囲が大きくなり、$\overline{A}$ のデータの侵入を許してしまう恐れもある。そのためには、まず登録処理を行なう前にデータをチェックし、異常データが含まれていないかどうかを確認し、含まれるようであれば、再登録を促すような仕組みが必要であると考えられる。

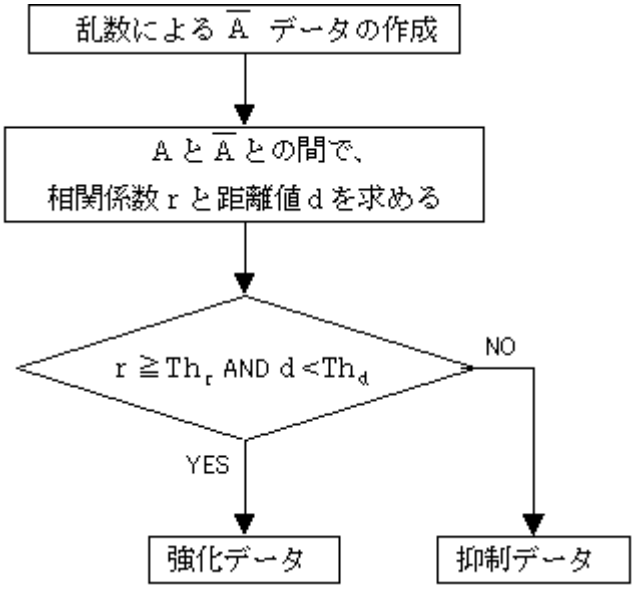


図 6.4　抑制データ/強化データへの選定処理案

6-2　登録処理前の入力データチェックの検討

NN に登録署名データを入力し、学習を行なう場合、登録データにある程度のばらつきを持たせた方が、認証率は向上する。しかしながら、ばらつきが大きすぎると学習の低下や他人排除率の低下を招く恐れがある。また、前項でも述べた通り、抑制データを生成する事にも支障を起こす恐れもある。そこで、登録処理を行なう前に、登録署名データに対するチェック機構を設け、その署名データが登録するに値するかどうかをチェックする。

前項で示した二つのパラメータを使用し、図 6.5 に示すような処理を行なう。この処理の結果によって異常有りと判断されたデータに対しては再登録処理を進める。ただし、全ての登録データを再登録させるのではなく、異常が含まれると思われるデータを検出し、そのデータに対してのみ再登録を行なうようにする。

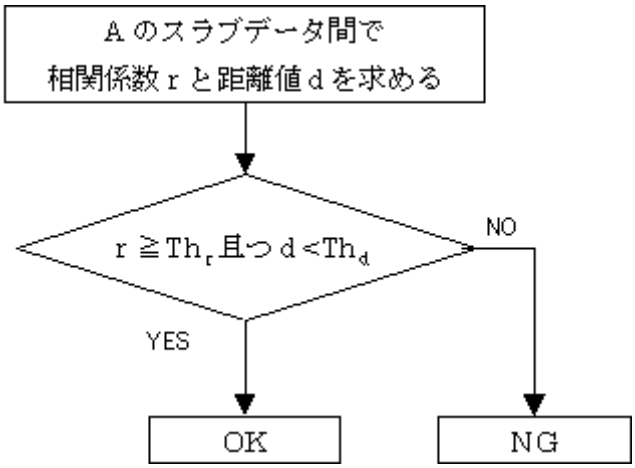


図 6.5　登録署名データのチェック

以下に登録データが３つの場合、チェック後に再登録が必要とされる登録署名データを選定する基準となる表 6.3 を示す。この選定表は、個人認証システムで実際に使用したものである。

表 6.3　チェック後の再登録データ番号選定表

	r、dを求める組み合わせ(数字はデータ番号)			再登録を促すデータ番号
	1-2	1-3	2-3	
チェック結果	OK	OK	OK	なし
	NG	OK	OK	1,2
	OK	NG	OK	1,3
	OK	OK	NG	2,3
	NG	NG	OK	1
	NG	OK	NG	2
	OK	NG	NG	3
	NG	NG	NG	1,2,3

7　認証実験

本章では、現状の電子ペンシステムによって摂取された筆記データを元に学習を行なう。学習に用いられる抑制データの作成手法は、他人の登録データによって作成されるものと、正規乱数によって作成されるものとの二種類を用いる。それぞれの抑制データを用いての学習をおこなった後に、認証実験を行ない、その認証結果を表に示す。それぞれの抑制データ作成手法ごとに表に表し、認証精度の比較を行なう。

7-1　実験手順

7-1-1　実験条件

認証実験は、以下に示すような条件下で行なうものとする。

●実験対象データ

竹田研究室に所属する学生の内、任意に選定した 7 名から採取された本人署名データを使用する。採取されたデータ数は各人 50 個ずつ（50 個/人×７）であり、名前はフルネームで書かれたものを使用する。

また、本人署名の他に、各人が自分以外の署名を単純に模倣した偽筆署名（54 個/人×７）を採取する。偽筆署名の内訳は、自分以外の 6 名に対し、一人につき 9 個の偽筆を採取したということになる。

●筆記データ採取方法

日本システム開発（株）によって開発された、電子ペン DP1000 を用いて筆記データを採取する。筆記環境を同じにするため筆記者は椅子に座った状態で署名を行なう（図 7.2）。用紙は図 7.1 に示すような同じ大きさの記入枠が並んだ筆記データ採取シートを使用する。氏名は一つの枠に一回のみ記入する。図 7.3 に実際に記入枠に書かれた氏名と、それにより得られた筆圧波形を示す。なお、筆記者には、普段書きなれた書き方での署名を心がけるようにする。

●登録データ数

最初に本人より採取された 50 個のソースデータの内、無作為に選んだ 10 個のデータを学習登録データとして NN に入力し、学習を行なう。残りの 40 個のデータは認証テストを行なう際に、入力されるテストデータとする。

●筆記データ作成手法

採取されたソースデータを NN に入力できる状態にするため、筆圧波形筆圧軸に対し、筆圧値の最大値でデータを除算することにより、0.0~1.0 までの値に正規化を行なう。

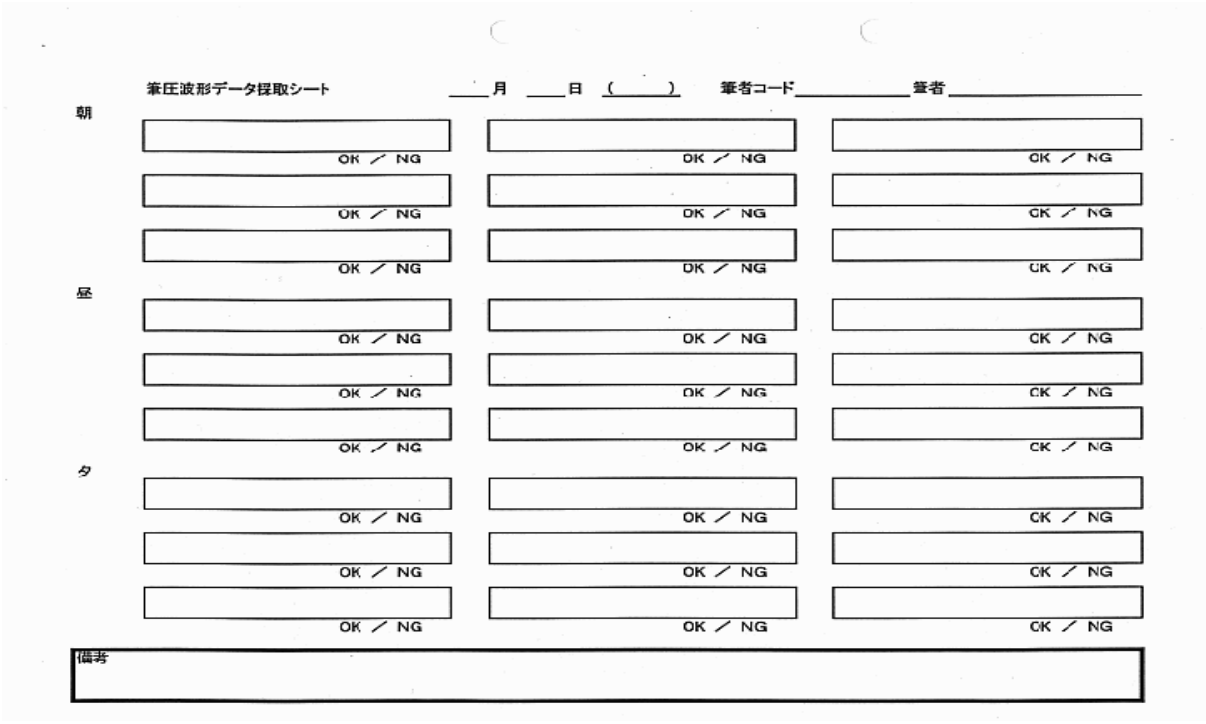
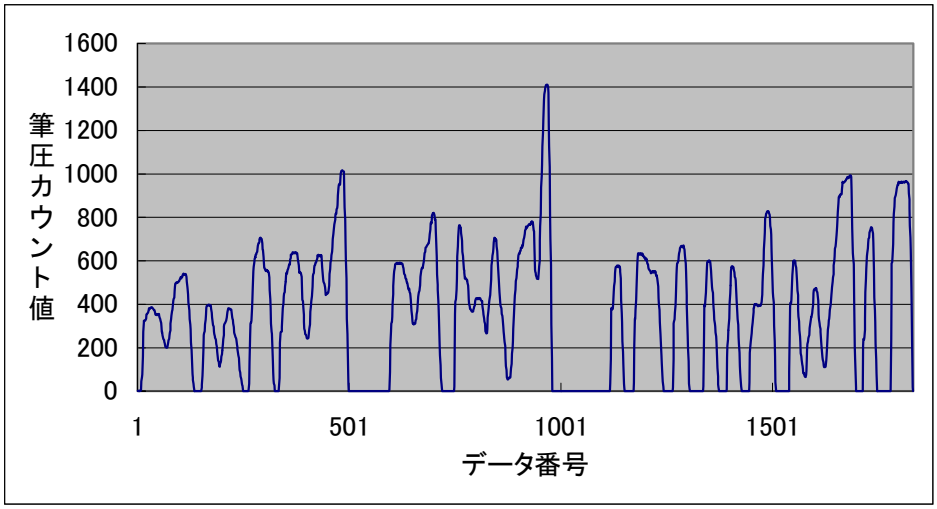


図 7.1　署名データ採取シート

図 7.2　署名データ採取風景

(a)



(b)

図 7.3　枠に記入された実際の署名(a)と得られた筆圧波形(b)

●学習方法

自分以外の 6 名の登録署名データ（計 60 個）を元に作成されたものを抑制データとして使用した場合と、本人による登録署名から得られる標準偏差を元に作成された正規乱数から、抑制データを作成した場合の二種類の学習を行なう。

●認証結果判定用閾値

認証実験後、NN からの出力値から本人か、そうでないかを OK/NG で判定するためのしきい値。値は 0.4~0.9 までの範囲で、0.1 単位で増減させて検証を行なう。OK か NG かの判定方法は、ある筆記者の署名データを NN に入力した場合、出力値 Out が、Out≧Th1（Th1 は判定用しきい値）を満たすとき、その筆記者は登録者本人であると判断するものとする。しきい値が大きいほど、NN からの出力に対する判断が厳しいことになる。

7-1-2　実験結果表示内容

ここでは認証実験による性能比較において、評価の対象となる実験結果を以下に示す。

●認証率

認証率は、登録者本人の登録データによって学習を行なった NN に、登録者本人が筆記した署名を入力した結果、本人として受理された割合をパーセンテージで表したものであり、値が高いほど登録者本人の署名データは受理されやすい。

●誤認率

上記と同様に、学習を行なった NN に、本人以外が署名した他筆署名を入力する。誤認率は、この他筆署名を登録者本人と誤って認識し、受理した割合を表したものであり、値が低いほど登録者以外の署名データを棄却していることとなる。

●偽筆認証率

本人登録データによって学習された NN に、登録者本人以外の 6 人が 9 個ずつ系 54 個登録者の氏名を簡単に模倣した署名（偽筆）を入力する。この入力データを登録者本人と判断し、受理された割合を示したものである。この値が大きいほど偽筆データを誤って受理していることとなる。

7.2 実験結果

表中では判定閾値 TH は、0.4〜0.9 としているが、実際の認証システムでは、0.6 か 0.7 で設定し出力判定を行なっている。性能比較では TH が 0.6、0.7 の場合の認証結果を見ることとする。表 4.1 では、認証率では 8･9 割の認証率を得ることが確認でき、誤認証率も１％を切る程度の精度を得ることができ、共に高い認証精度を得ることができたと思われる。しかしながら、偽筆認証では約 50％の偽筆データに対して、本人であると誤って認証してしまっており、とても良い結果とは言えない。一方、表 4.2 の正規乱数で抑制データを作成した場合、本人認証率は表 4.1 に比べて若干上がっている。また、偽筆認証率も結果的には良いものではないが、40％台の誤認率であり、他人の登録データで抑制データを作成したときより偽筆による誤認証率を抑えることに成功している。しかしながら、誤認率は表 4.1 に比べて精度が低下してしまっている。特に、k0a の誤認率が非常に悪くなっている。これは、k0a のテンプレートに入力した k09 のテストデータ全てを、k0a と誤って認証してしまったためである。

表 7.1 他人の登録データから抑制データを作成した場合の認証・誤認率及び偽筆認証率

登録者名：K05~K0ｂ，TH：判定閾値，登録データ数：10

認証率

TH	0.4	0.5	0.6	0.7	0.8	0.9	0.4	0.5	0.6	0.7	0.8	0.9
K05	40	40	40	40	39	37	100.00%	100.00%	100.00%	100.00%	97.50%	92.50%
K06	31	31	29	29	29	27	77.50%	77.50%	72.50%	72.50%	72.50%	67.50%
K07	40	40	40	40	40	39	100.00%	100.00%	100.00%	100.00%	100.00%	97.50%
K08	40	40	40	40	39	38	100.00%	100.00%	100.00%	100.00%	97.50%	95.00%
K09	37	37	36	36	34	34	92.50%	92.50%	90.00%	90.00%	85.00%	85.00%
k0a	31	31	31	29	28	28	77.50%	77.50%	77.50%	72.50%	70.00%	70.00%
k0b	35	35	34	34	33	30	87.50%	87.50%	85.00%	85.00%	82.50%	75.00%
計	254	254	250	248	242	233	90.71%	90.71%	89.29%	88.57%	86.43%	83.21%

誤認率

TH	0.4	0.5	0.6	0.7	0.8	0.9	0.4	0.5	0.6	0.7	0.8	0.9
K05	1	1	0	0	0	0	0.42%	0.42%	0.00%	0.00%	0.00%	0.00%
K06	1	1	1	1	0	0	0.42%	0.42%	0.42%	0.42%	0.00%	0.00%
K07	1	1	0	0	0	0	0.42%	0.42%	0.00%	0.00%	0.00%	0.00%
K08	0	0	0	0	0	0	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
K09	0	0	0	0	0	0	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
k0a	8	6	6	4	3	0	3.34%	2.50%	2.50%	1.67%	1.25%	0.00%
k0b	0	0	0	0	0	0	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
計	11	9	7	5	3	0	0.65%	0.54%	0.42%	0.30%	0.18%	0.00%

偽筆認証率

TH	0.4	0.5	0.6	0.7	0.8	0.9	0.4	0.5	0.6	0.7	0.8	0.9
K05	21	21	21	19	19	13	38.89%	38.89%	38.89%	35.19%	35.19%	24.08%
K06	29	29	28	27	26	18	53.71%	53.71%	51.86%	50.00%	48.15%	33.34%
K07	17	17	15	14	13	8	31.49%	31.49%	27.78%	25.93%	24.08%	14.82%
K08	41	41	40	36	35	31	75.93%	75.93%	74.08%	66.67%	64.82%	57.41%
K09	25	25	25	23	22	15	48.08%	48.08%	48.08%	44.24%	42.31%	28.85%
k0a	26	26	24	24	24	23	48.15%	48.15%	44.45%	44.45%	44.45%	42.60%
k0b	35	35	35	32	30	26	67.31%	67.31%	67.31%	61.54%	57.70%	50.00%
計	194	194	188	175	169	134	51.87%	51.87%	50.27%	46.79%	45.19%	35.83%

表 7.2　正規乱数を抑制データとして使用した場合の認証・誤認率及び偽筆認証率

登録者名：K05~K0ｂ，TH：判定閾値，登録データ数：10

認証率

TH	0.4	0.5	0.6	0.7	0.8	0.9	0.4	0.5	0.6	0.7	0.8	0.9
K05	39	39	39	39	38	36	97.50%	97.50%	97.50%	97.50%	95.00%	90.00%
K06	33	33	33	33	32	31	82.50%	82.50%	82.50%	82.50%	80.00%	77.50%
K07	47	47	47	46	46	46	100.00%	100.00%	100.00%	97.88%	97.88%	97.88%
K08	39	39	39	39	39	39	97.50%	97.50%	97.50%	97.50%	97.50%	97.50%
K09	32	32	32	32	31	28	80.00%	80.00%	80.00%	80.00%	77.50%	70.00%
k0a	37	36	36	35	33	29	92.50%	90.00%	90.00%	87.50%	82.50%	72.50%
k0b	36	36	36	36	36	36	90.00%	90.00%	90.00%	90.00%	90.00%	90.00%
計	263	262	262	260	255	245	91.64%	91.29%	91.29%	90.59%	88.85%	85.37%

誤認率

TH	0.4	0.5	0.6	0.7	0.8	0.9	0.4	0.5	0.6	0.7	0.8	0.9
K05	0	0	0	0	0	0	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
K06	1	1	1	1	1	1	0.42%	0.42%	0.42%	0.42%	0.42%	0.42%
K07	3	3	2	1	1	0	1.25%	1.25%	0.84%	0.42%	0.42%	0.00%
K08	0	0	0	0	0	0	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
K09	0	0	0	0	0	0	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
k0a	51	51	50	49	46	41	21.25%	21.25%	20.84%	20.42%	19.17%	17.09%
k0b	21	21	17	11	7	5	8.75%	8.75%	7.09%	4.59%	2.92%	2.09%
計	76	76	70	62	55	47	4.56%	4.56%	4.20%	3.72%	3.30%	2.82%

偽筆認証率

TH	0.4	0.5	0.6	0.7	0.8	0.9	0.4	0.5	0.6	0.7	0.8	0.9
K05	17	17	17	16	14	8	31.49%	31.49%	31.49%	29.63%	25.93%	14.82%
K06	16	16	16	12	10	7	29.63%	29.63%	29.63%	22.23%	18.52%	12.97%
K07	19	19	18	18	16	14	35.19%	35.19%	33.34%	33.34%	29.63%	25.93%
K08	35	35	34	32	30	26	64.82%	64.82%	62.97%	59.26%	55.56%	48.15%
K09	22	22	22	21	19	14	42.31%	42.31%	42.31%	40.39%	36.54%	26.93%
k0a	22	22	18	17	14	14	40.75%	40.75%	33.34%	31.49%	25.93%	25.93%
k0b	30	30	29	29	28	25	58.83%	58.83%	56.87%	56.87%	54.91%	49.02%
計	161	161	154	145	131	108	43.16%	43.16%	41.29%	38.87%	35.12%	28.95%

7.3 考察

今回の実験では、抑制データの作成法として他人の登録データから作成する場合と、本人の登録データから得られた正規乱数から作成する場合の二種類を用いた。実験結果から見ると、認証精度は正規乱数を用いた方が、若干ではあるが上であると思われる。しかしながら、前項で述べたが誤認証率が高くなってしまい、これでは極端な話、誰の署名でも本人と判定してしまうといったことになってしまう。また、偽筆に対する誤認証も、しきい値を一番大きくしても 30%近くの値を示した。実験結果で表示された二つの表の偽筆認証では、どちらも本人と誤って認証した偽筆は、ほぼ同じ人物であった。たとえば、どちらの表においても学生 k05 の偽筆認証率の結果では、k09 から採取した偽筆 9 回のほとんど全てに対して本人と判断している。

現在の NN への入力データの作成手法として、筆記データの時間軸方向を、50 個にしているため、時間情報が消失している。また、筆圧軸方向は、データ自身の最大値で除算することにより正規化を行なっているため、筆圧の強弱情報が失われている。以上の処理のため、入力データの持つ情報や個人差が少なくなっている。

偽筆署名データと本人の署名データを筆圧波形で比べてみると、同じ氏名を書いたものなので当然波形は似たものとなる。しかしながら、筆記の開始から終了までの時間は大幅に違い、文字を書くリズムも違うことがわかる。本人の署名データをいくつか比較してみたところ、筆記の時間・リズム・筆圧は若干の違いはあるもののほぼ同じであった。また、波形の形自体は似ていても、筆圧の強弱までは似せることができていない。

実験を通して、時間情報と筆圧情報は他人と本人との識別をするために重要な情報であると考えられる。これからの筆記による個人認証システムにおける NN への入力データ作成手法では、採取された筆記データの個人的特徴となる情報を失わせないようにすることが必要であると考えられる。合わせて、抑制データも有効な学習が行なえるような手法を検討することが望まれる。

8　まとめ

本論文では、筆記という動的な生体情報を用いることに着目し、学習にニューロテンプレートマッチング識別手法を用いた個人認証システムの研究を行なってきた。また、学習における抑制データの新しい作成手法として、本人の登録署名データから正規乱数を発生させ、それをもとに抑制データを生成することを提案した。実験では、シミュレーションにより従来手法と提案手法とで個人認証性能の比較を行ない、提案手法の有効性を確認した。しかしながら、他人が登録者を模倣した偽筆データについての誤認が非常に多いといった問題も残っている。今後、現在の本人認証率、誤認率を保つとともに、偽筆による誤認証率を低下させることを目的とし、抑制データ生成手法,ニューラルネットワークへの入力筆記データの作成法を検討する必要がある。

9　謝辞

一年に渡りご指導いただきました竹田史章教授に深く感謝いたします。本研究を進めるにあたり、研究用資料の提供および貴重な助言を賜りました日本システム株式会社仁木章人様ならびに、実験データ採取に協力していただいた、高知工科大学情報システム工学科竹田研究室所属の学生一同に感謝いたします。

10　参考文献

(1) 瀬戸洋一, “ バイオメトリクスを用いた本人認証技術 ”, 計測と制御, 第 37 巻, 第 6 号, pp.395-401, 1998
(2) 内田　薫, “ バイオメトリクスによる個人認証技術とその応用 ”, 電学誌, 120 巻, 第 7 号, pp.407, 2000
(3) 西陰紀洋, 竹田史章, 吉田与志一, 仁木章人、“ 小規模ニューラルネットワークによる筆記者認証装置 ”, 電子情報通信学会論文誌　D-Ⅱ 投稿中
(4) 猿田和樹, 加藤　寧, 安倍正人, 根元義章, “ 排他的学習ネット（ELNET）を用いた手書き文字認識の細分類手法 ”, 電子情報通信学会論文誌　D-Ⅱ　Vol.J79-D-Ⅱ　No.5　pp.851-859　1996 年
(5) 松井和子, “ HMM による話者認識 ”, 信学技報, SP95-111, 1996
(6) 津雲　淳, “ 方向パターンマッチング法の改良と手書き漢字認識への応用 ”, 信学技報, PRU90-20, 1990
(7) 孫　寧, 田原　透, 阿曽弘具, 木村正行, “ 方向線素特徴量を用いた高精度文字認識 ”, 信学論（D-Ⅱ）, Vol.J74-D-Ⅱ, No.3, pp.330-339, 1991
(8) 猿田和樹, 孫　寧, 安倍正人, 根元義章, “ 係数変化型学習法とその手書き文字認識への応用 ”, 信学論, (D-Ⅱ), Vol.J78-D-Ⅱ, No.6, pp.973-981, 1995
(9) S.Nagata, M.Sekiguchi& K.Asakawa, “ Mobile Robot Control by a Structured Hierarchical Neural Network“ , IEEE, Control System Magazine, Ap69, 1990
(9) 竹田史章, 西陰紀洋, “ 紙幣用ニューロテンプレートマッチング識別手法の開発 ”, 電学論C, 121 巻 1 号, 平成 13 年