

電子認証におけるサインの識別

Discrimination of the Sign in Electronic Certification

○ 高木 博基*, 坂野 進**

○ Hiroki Takagi*, Susumu Sakano**

*日本大学大学院工学研究科, **日本大学工学部

*,**Nihon University, College of Engineering

キーワード : 電子認証(electronic certification), MTS 法(Mahalanobis Taguchi system)
マハラノビスの距離(Mahalanobis distance), 直交表(orthogonal array)
ユークリッドの距離(Euclid distance), 最大エントロピー法(maximum entropy method)

連絡先: 〒963-1165 郡山市田村町徳定字中河原1番地

日本大学 工学部 機械工学科 メカトロニクス研究室

坂野 進, Tel.: (024)956-8774, Fax.: (024)956-8860, E-mail: sakano@mech.ce.nihon-u.ac.jp

1. はじめに

我々は、身分証明書、暗証番号、パスワード、鍵など個人が所有するセキュリティアイテムは現在たくさんある。しかし、これらは紛失したり、忘れたり、また個人に偽造・変造・コピーされてしまう危険性が常につきまとっている現状がある。

近年、電子商取引を実現するため、オープンネットワーク化や法整備が現在急速に進められている。オープンネットワークでは、電子申請や電子決済等の手続きを電子機器などにより簡単に実施できる一方で、送受するデータはすべて公開されてしまうため、個人情報セキュリティに関する問題をかかえている。バイオメトリクス(Biometrics)はセキュリティ問題を解決する技術として注目されている。バイオメトリクスとは、人それぞれに固有な生体情報を用いた認証法である。利用されるのは生体情報であるので、他人による偽造・変造・コピーは非常に困難である。また、もともと個人の身体

に備わっている物であるので、忘れたり紛失したりすることはない。

そこで本研究では、個人がサインするときに得られる筆圧からその人特有の身体的特徴を抽出し、多次元情報分析法であるMTS法を用いて解析を行い評価した。

2. MTS法の概要

2.1 MTS法

MTS法は多次元の情報を総合し、マハラノビスの距離に対する誤差の評価によって、システムの有効性を総合判定することが可能である。MTS法では、人間が分類したデータを学習データ(基準空間)として多次元空間における基準点と単位量を定義する。そしてこのデータ群に内在する特徴量間の相関と密度(勾配)を考慮し、人間の持つ識別能力を反映した仮想的な参照パターンである。

マハラノビスの距離は真の分布が既知ですべてのカテゴリで同じ正規分布であるとき最適な識別関数である。しかし、マハラノビスの距離をパターン認識に適用する場合、真の分布が既知であることはほとんどなく、パターンの分布を表す情報は学習データから推定される。

2.2 マハラノビスの距離

マハラノビスの距離 $D^2(x)$ は未知パターン特徴ベクトルを x 、あるクラスの平均ベクトルを μ 、共分散行列を Σ とすると

$$D^2(x) = (x - \mu)' \Sigma^{-1} (x - \mu) \dots \dots (1)$$

と表される。ここで共分散行列の固有値を λ_k ($\lambda_1 \geq \dots \geq \lambda_d$)、それに対応する固有ベクトルを φ_k 、次元数を d とすると

$$D^2(x) = \sum_{k=1}^d \frac{1}{\lambda_k} (\varphi_k \cdot (x - \mu))^2 \dots \dots (2)$$

と表される。しかしながら、学習データが少量の場合には次元数分の固有値、固有ベクトルを求めることが出来ない。そのために実際には、求まる固有値、固有ベクトルを M として

$$\tilde{D}^2(x) = \sum_{k=1}^M \frac{1}{\lambda_k} (\varphi_k \cdot (x - \mu))^2 \dots \dots (3)$$

を用いて識別を行うことになる。学習データ数を N とすると固有値、固有ベクトル数 M は $M \leq \min\{d, N-1\}$ で与えられる。

データ間に相関がある場合はマハラノビスの基準空間、マハラノビスの距離となる。しかし、相関のない場合にはユークリッドの基準空間、ユークリッドの距離となる。

以上から得られた基準空間と評価対象の距離と

を、ある範囲でしきい値を設けることで二つのグループを判別するものである。そのモデルを Fig.1 に示す。

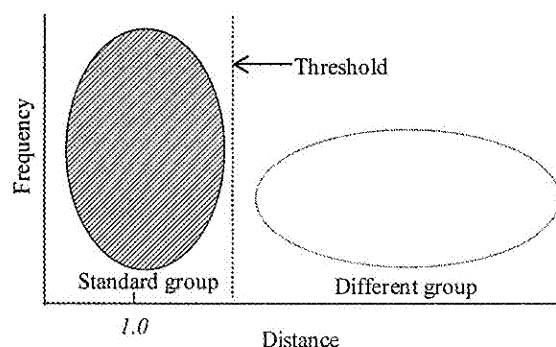


Fig.1 Concept of MTS

3 筆圧測定システムの原理

触覚センサを利用した電子認証用筆圧測定システムの基本原理は、有限長の振動棒を任意の対象物体に接触させた場合に、棒の固有振動数が対象物体の音響負荷(密度や伝播速度)の有無によって変化することを利用した物である。

基本構成は、市販のボールペン軸にジルコンチタン酸鉛の圧電セラミック素子(PZT)をセンサ部にして振動させたときの振動モードの変化を利用している。システムの概要を Fig.2 に示す。

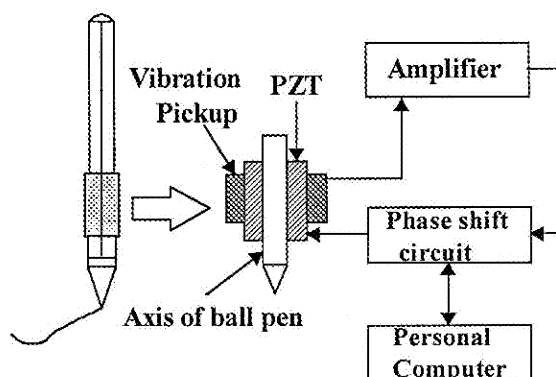


Fig.2 Summary of system

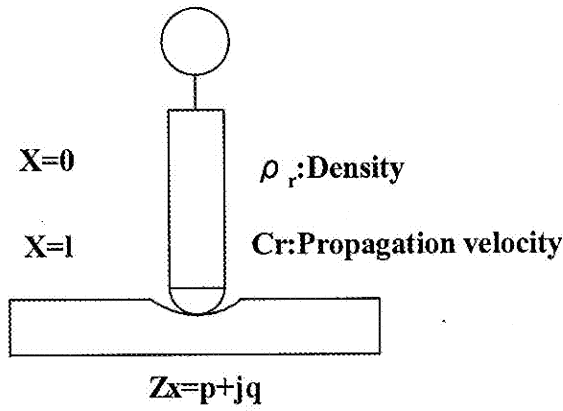


Fig.3 Action specific

このシステムの動作特性を Fig.3 に示す。図はボールペン軸が紙などの表面に接触してサインするときの様子をモデル的に示した物で、共振状態にある長さ $x=l$ の有限長の棒の先端に、未知の音響インピーダンスを持つ物質を接触させた場合、棒の長さ方向に平面波が伝搬する時の波動方程式は

$$\frac{\delta^2 \phi}{\delta t^2} = C_r^2 \frac{\delta^2 \phi}{\delta x^2} \dots (1)$$

ϕ : Velocity potential

C_r : Pole sonic

t : Time

x : Distance

となる。(1)式から物質が接触している状態の共振周波数は、変数分離法を用いて境界条件の導入により、(2)式ようになる。

$$f_x = \frac{nC_r}{2l} \left(1 - \frac{qx}{n\pi\rho_r C_r} \right) \dots (2)$$

n : Degree

ρ_r : Density of pole

また、振動棒が物質に接触していない自由共振状態での棒の共振周波数は(3)式になる。

$$f_0 = \frac{nC_r}{2l} \dots (3)$$

従って、(2)、(3)式により周波数変化量は(4)式で表される。

$$\begin{aligned} \Delta f &= f_x - f_0 \\ &= \frac{nC_r}{2l} \left(1 - \frac{qx}{n\pi\rho_r C_r} \right) - \frac{nC_r}{2l} \\ &= -\frac{C_r q x}{2n\pi l Z_r} \dots (4) \end{aligned}$$

Z : Echo impedance of pole

Fig.4 に性能曲線(理論値)を示す。低筆圧時における感度が高い特性を持つ。

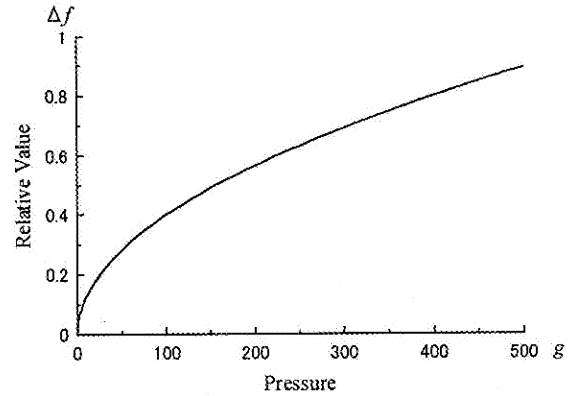


Fig.4 Performance characteristic

4 実験

4.1 実験方法

- (1) 用紙に5回サインをする。
- (2) 得られた時系列データを周波数スペクトルに変換し、平均パワー値を直交表に割り付け基準空間を設定する。(データベースの作成)
- (3) 本人や他人のデータを採取する。
- (4) 得られたデータに対して評価を行う。

4.2 基準空間の設定

MTS 法においては、基準空間を設定するデータの収集が重要な課題である。個人の文字データをデータベース化するには膨大なデータが必要となる。しかしながらサンプルデータを採取する際に何度もサインをしてもらうことは大変なことである。そのために少ないサンプル数から十分な学習データを与えなければならない。その手法として直交

表を用いて仮想データを発生させる。この手法を用いると相関が0になるので、基準空間は前述したようにユークリッドの基準空間となり、距離はユークリッドの距離となる。

4.2.1 直交表

直交表(Orthogonal array)はラテン方格を発展させた物である。例として Table.1 に2水準直交表 $L_8(2^7)$ を示す。表は第1水準と第2水準からなり、任意の2列をとったとき、数字の並びは(1,1)(1,2)(2,1)(2,2)の4通りがありこの4通りの並びがどの2列をとってもかならず同数回現れるという特徴を持つ。直交表を用いて、得られたデータのある範囲においてノイズを与えてそれらを割り付けることにより、求めるべき多くの要因効果を少ないサンプルから再現性よく求めることが可能になる。また、こうして得られた学習データは相関のない安定した物となり識別・評価精度の向上にもつながる。

Table.1 Orthogonal array experiment $L_8(2^7)$

No.	Parameters						
	1	2	3	4	5	6	7
1	1	1	1	1	1	1	1
2	1	1	1	2	2	2	2
3	1	2	2	1	1	2	2
4	1	2	2	2	2	1	1
5	2	1	2	1	2	1	2
6	2	1	2	2	1	2	1
7	2	2	1	1	2	2	1
8	2	2	1	2	1	1	2

4.3 周波数解析

周波数解析を行う際に、FFT(Fast Fourier Transform)は最も一般的な手法である。FFT は定常性と線形性を仮定しているので、非定常で非線形データ解析には他の解析法が適している場合もある。そこで本研究ではFFTとMEM(Maximum

Entropy Method)による解析を行い比較した。結果を Fig.5 に示す。

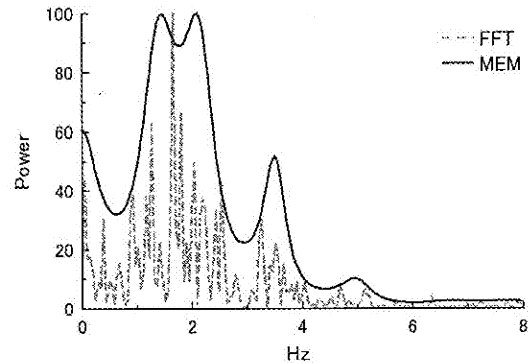
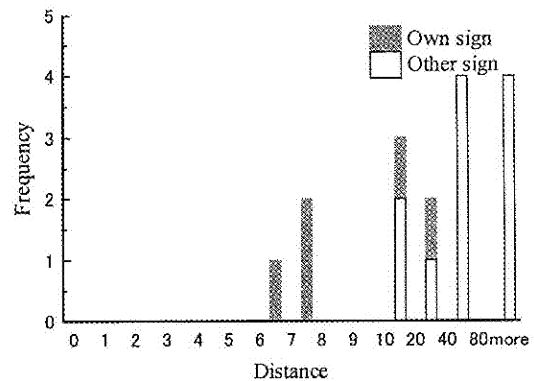
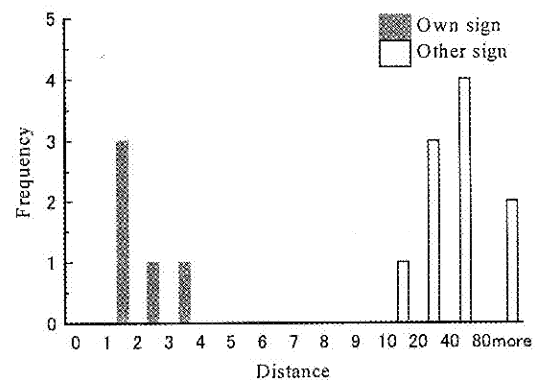


Fig.5 Result of a comparison between FFT and MEM

FFTはノイズが目立つのに対して、MEMは波形が安定していて分解能が高い。MEMはスペクトルの分解能が高くノイズに強い特徴を持つ。これらの解析法から評価を行った結果を Fig.6 に示す。



(a) Distribution of distance (FFT)



(b) Distribution of distance (MEM)

Fig.6 Comparison between FFT and MEM(斉藤)

FFT において、本人の文字は広い範囲に分布しており、また一部に誤識別されるサインが見られるのに対して MEM では誤識別がなく、また本人の文字は狭い範囲に分布を示している。

以上の結果から、周波数解析には MEM を採用した。

5 実験結果

漢字と英字のサインについて認証を行った結果を以下に示す。15人に2回ずつ同じ文字を書いてもらい、それに対する本人の文字とのユークリッドの距離を比較した。

5.1 漢字の識別

鈴木 一郎 鈴木 一郎

(a) (b)

Fig.7 Own sign

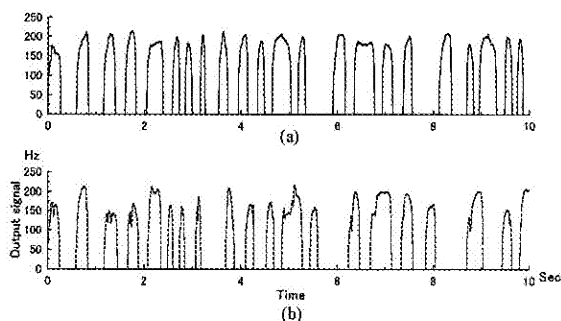


Fig.8 Output signal of own sign

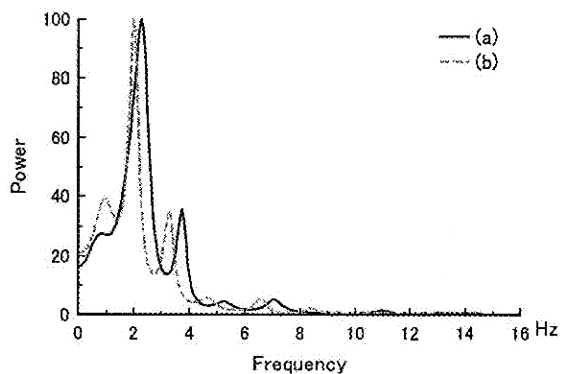


Fig.9 Analysis of MEM

鈴木 一郎 鈴木 一郎

(a) (b)

Fig.10 Other sign

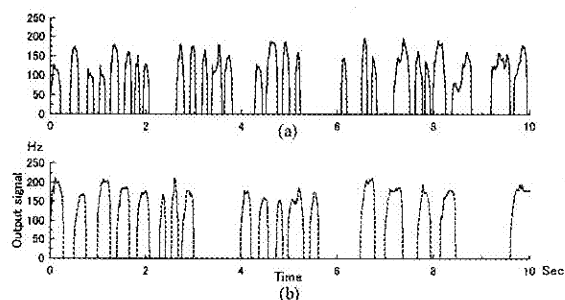


Fig.11 Output signal of other sign

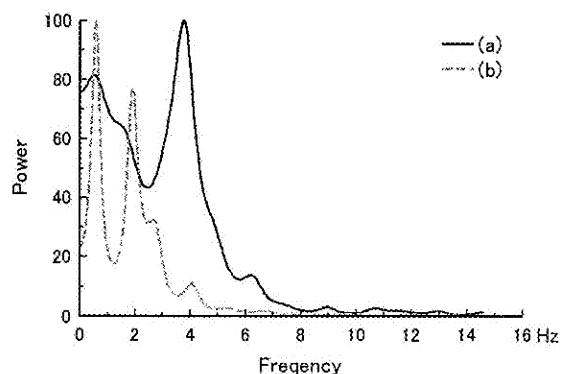


Fig.12 Analysis of MEM

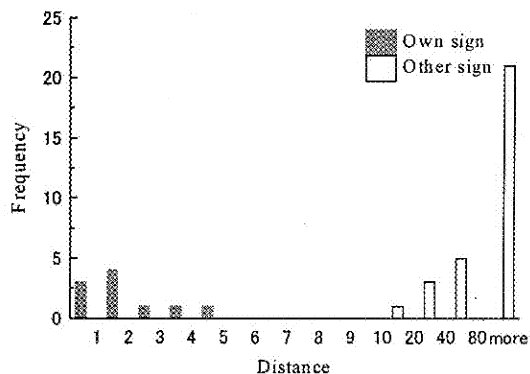


Fig.13 Distribution of distance (Japanese writing)

5.2 英語の識別

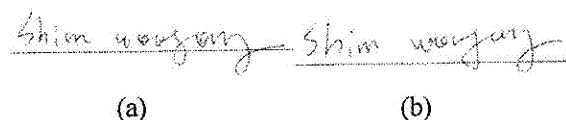


Fig.14 Own sign

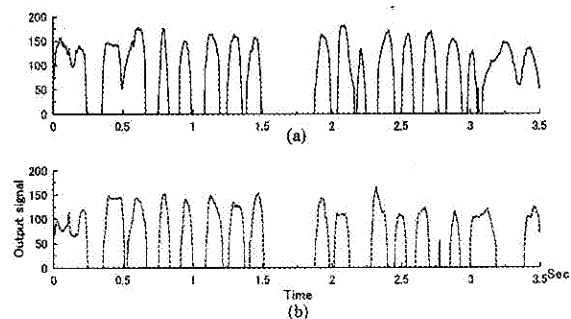


Fig.15 Output signal of own sign

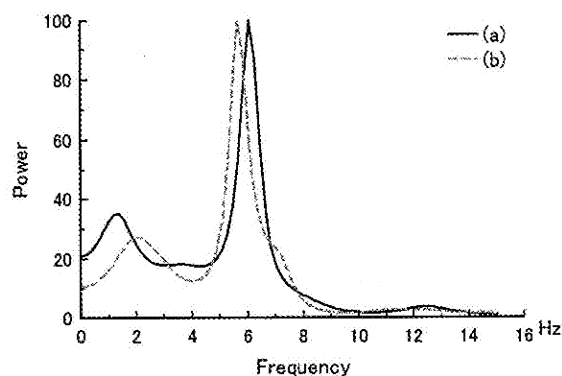


Fig.16 Analysis of MEM

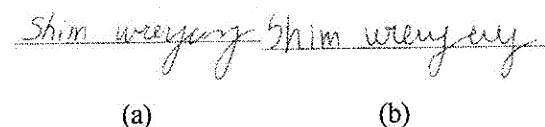


Fig.17 Other sign

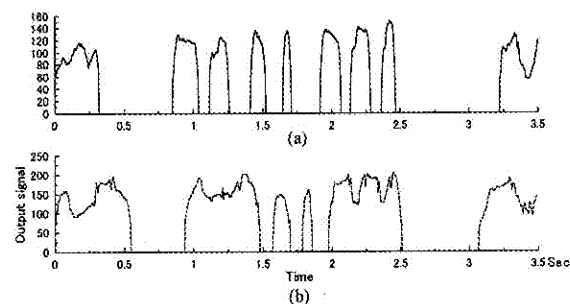


Fig.18 Output signal of other sign

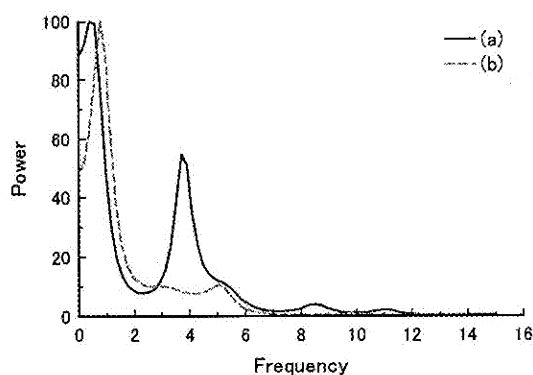


Fig.19 Analysis of MEM

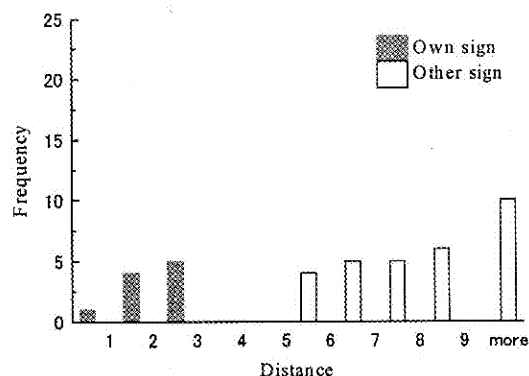


Fig.20 Distribution of distance (Alphabet)

漢字、英字ともに本人のサインと他人のサインとのユークリッドの距離の違いは明らかである。英字のサイン識別において、結果から見ると本人と他人とのユークリッドの距離の差は小さいが、英字におけるサインの筆圧は漢字のサインに比べてばらつきが小さく再現性良くデータが得られる傾向にある。よってユークリッドの距離も狭い範囲に分布していた。以上のことから識別には問題ないと考えられる。

得られる本人の筆圧データは毎回、完全な一致をしない。しかしながら MEM 解析したデータを直交表に割り付けて評価を行うと、柔軟な識別を行うことができた。

6 まとめ

本研究において、MTS法をもとにしたサインの認識を行い漢字及び英字のサインにおいてユークリッドの距離の大小で評価、識別する事を行った。この評価法でサインが本人のものであるかを簡単に評価することができた。

直交表を用いて基準空間を作成することにより、少ないデータから均一な相関が低い(実際は0)仮想基準データ群を作成することができ、安定した評価ができるようになる。

参考文献

- 1) 田口玄一:品質設計のための実験計画法,57/63,日本規格協会(1988)
- 2) 竹下鉄夫,木村文隆,三宅康二:マハラノビス距離の推定誤差に関する考察,電子情報通信学会誌,Vol.J70-D,No.3,567/573(1987)
- 3) 南茂夫:科学計測のための波形データ処理,166/174,CQ 出版(1988)
- 4) J.S.Bendat,A.G.Piersol,得丸英勝 他訳:ランダムデータの統計的処理, 299/313, 倍風館(1976)
- 5) 平成11年度コンソーシアム研究開発事業「ベンチャー企業支援型地域コンソーシアム研究開発」,21/24,(2001)