

# 筆画のクラスタリングを考慮した署名認証手法

西郷里 拓<sup>†1</sup> 川本 淳平 櫻井 幸一<sup>†2</sup>

**概要:** スマートフォンにおける個人情報保護手法の一つとして署名認証の研究が行われている。スマートフォン署名認証では、端末の大きさなどの制約により認証精度が課題の一つである。本研究では、漢字圏の利用者を対象に、永字八法という書道における考え方を取り入れた署名認証手法を提案する。永字八法とは漢字に必要な8つの技法が永という字に含まれていることを表した言葉である。認証を行う人は事前に永の字からいくつかのクラスタを作成し、テンプレートの署名が一画ごとにどのクラスタに属するかを決めておく。認証の際には一画ごとにどのクラスタに入るかを判定し事前に決めたものと一致するかという要素と従来のデータ間距離を判定に用いる。

**キーワード:** 署名認証, 筆画, バイオメトリクス, クラスタリング, DTW

## Signature authentication method that takes into account the clustering of stroke

Taku Nishigori<sup>†1</sup> Junpei Kawamoto Kouichi Sakurai<sup>†</sup>

**Abstract:** A study of the signature authentication in the smartphone is studied. By the signature authentication of the smartphone, authentication precision is one of the problems. In this study, the users of the Chinese characters, we propose a method that incorporates Eight Principles of Yong. The Eight Principles of Yong a term, which indicates that the eight techniques needed for kanji, is included in the character of permanent. Certifier creates some cluster from the character Ei. Moreover, we cluster each one section of the template. Consider whether the match in a cluster at the time of authentication

**Keywords:** Signature Authentication, Strokes, Biometrics, Clustering, Dynamic Time Warping,

### 1. はじめに

スマートフォンやタブレットといったモバイル端末は近年ますます普及してきており、日常生活でも欠かせないものとなってきている。そういった情報化社会において個人情報を保護するためのセキュリティの一つに個人認証がある。スマートフォンにおける個人認証は4桁の数字によるパスワード認証や、9つの点をつなぐパターンロックによる認証といった簡単なものが主流である。このような簡単な認証の持つ問題として入力の様子を見られてしまうと簡単にパスワードを知られてしまうということがあげられる。こういった攻撃は覗き見攻撃と呼ばれ覗き見攻撃に対する認証も多く研究されている[1]。そういった研究で提案されている手法は入力する情報を増やしたり入力方法を複雑にしたりするといったユーザーの負担を増やすものが多い。覗き見攻撃に耐性がありユーザーの負担が少ない認証として特に近年研究がすすめられている個人認証の手法にバイオメトリクスがある。

バイオメトリクスには指紋や目の虹彩といった身体的特徴を使うものと、歩き方や文字の書く時の癖といった行

動的特徴を使うものがある。身体的特徴を利用する認証の場合指紋や眼などをセンサにかざすだけで認証が出来るという利点がある。しかし、指紋は犯罪捜査でも使われているイメージが強く、登録の際に心理的な抵抗感があると言える。本研究では行動的特徴を利用したバイオメトリクスの一種である署名認証に着目する。署名認証はクレジットカードを使用するときにも署名を行っているように社会的に受け入れられておりデータの取得に対する抵抗感が少ないことや、意思決定を伴う認証であるということなどの利点があり様々な研究がなされている[2]。また、指紋などの身体的特徴を使ったバイオメトリクスにない特徴として、登録情報が漏えいしてしまった際に登録署名を変更することでその被害を減らすことが容易であるという利点もある。本研究では漢字を書く際の特徴を表す永字八法という考え方をデータ間の距離を計算する際に利用した署名認証の手法を提案する。

### 2. 署名認証

署名認証とは行動的特徴を使ったバイオメトリクスの一つである。署名認証は大きく分けてオフライン署名認証とオンライン署名認証の二つがある。オフライン署名認証とは得られた署名の形状のみを認証に用いる手法である。オンライン署名認証は筆記された署名の座標データ、筆圧、筆記速度やペンの角度などの署名を書く際の動作の特徴を

<sup>†1</sup>九州大学大学院システム情報科学府  
Kyushu University

<sup>†2</sup>九州大学大学院システム情報科学府研究院  
Kyushu University

用いた認証でオフライン認証よりも取得できるデータの種類が多いため署名認証の研究ではオンライン署名認証が数多くなされている。署名認証では署名の登録者が初めにテンプレートと呼ばれる署名を登録する。登録者の署名の癖がある程度分かるように一定数以上の署名を登録してテンプレートを選択しなくてはならない。このテンプレート選択に必要な署名数が少ないとユーザーの負担が少ないことにつながる。認証の際には決めておいたテンプレートと入力された署名のデータを比較しどれくらい似ているのかを計算しその値があらかじめ決めておいた閾値を超えるかどうかで本人かどうかを判断する。この閾値が低すぎると他人受入率が高くなり、高すぎると本人拒否率が高くなるというトレードオフの関係にあり、閾値の設定にも課題が残されている。

署名の比較に使うアルゴリズムに Dynamic Time Warping(DTW)というものがある[3]。これは二つの時系列データの間の距離を比較する際に使われるアルゴリズムであり、片方を動的に伸縮することでデータ長の違うデータに対してよく使われているアルゴリズムであり、署名認証においてもよく利用されているアルゴリズムである。

本研究では永字八法という永という漢字を書くときの特徴を8つに分類する考え方を利用してオンライン署名認証の認証精度を上げるために署名を一画ごとにクラスタリングし、その結果をデータ間距離の計算にも影響させるという手法を提案する。

### 3. 既存研究

本論文で提案する署名認証の手法において参考にした既存研究を紹介する。

#### 3.1 Kinwrite[4]

KinwriteはMicrosoft社から発売されたKinectというモーションキャプチャができるデバイスを用いて認証を行う手法である。その認証手法はKinectの前に立ち指先で空中に文字を描くことによって三次元の時系列データを取得し認証を行う手法である。この手法では時系列データを比較する際にDynamic Time Warpingを利用している。本研究ではこの研究で用いられているテンプレートの選び方を参考にしてテンプレートを選択している。

この手法では、登録者の入力を事前に知っている場合や全く知らない場合など様々な攻撃パターンを含めたときの実験の結果として、他人受入率を0%にしたときに本人拒否率が23%になるという結果が出た。また攻撃者が何の情報も持たずに攻撃した場合には他人受入率0%のときも本人拒否率は0%になった。

#### 3.2 永字八法に基づく手書き文字認識用辞書の動的構成法[5]

手書き文字認識とはタブレット端末などで指やペンを用いて文字を書いた際にそれが何という文字なのかを判別す

るための技術であり、特に漢字はアルファベットと違い種類が非常に多く、またよく似た文字も多いため漢字圏ではこの研究はとても重要なものである。

この研究では入力された漢字に含まれる個人の特徴を永字八法の考え方に基づきクラスタリングすることで文字認識の精度を上げることに成功している。

永字八法とは漢字を書く際の特徴を、点・横画・縦画・はね・右上がり横画・左払い・短い左払い・右払いの8つに分類したものでこの研究ではそのうち縦横画と左右の払いに個人の特徴が大きく出るとして利用している。

本研究は署名認証の研究であり手書き文字認識とは違う研究ではあるが人が書いた文字の個人的特徴に着目しているという点で永字八法に従う属性付けの方法を参考にして

## 4. Dynamic Time Warping

Dynamic Time Warping(DTW)は二つの時系列データのデータ間の距離を算出する際に使用するアルゴリズムである。これはDynamic Programming(DP)マッチングとも呼ばれており、1970年代に作られたものである。理論的に明快でありアルゴリズムの実装も容易で計算量が非常に少ないという特徴を持つ。よって時系列パターン認識においては基本的なアルゴリズムとして知られている。

ここではDTWの計算過程を説明する。DTWでは2つの時系列データ(シーケンス)

$$S = [s_1, s_2, \dots, s_i, \dots, s_I] \text{と}$$

$$T = [t_1, t_2, \dots, t_j, \dots, t_J] \text{との間の弾性マッチングを考える。}$$

ここで $s_i$ と $t_j$ は特徴ベクトルとする。弾性マッチングをするというのは、シーケンスSのi番目の特徴ベクトルである $s_i$ と、シーケンスTの $u_i$ 番目の特徴ベクトル $t_{u_i}$ との対応付けを最適化する問題である。これ以降は $s_i$ に $t_{u_i}$ を対応付けることを $u_i = j (i \in [1, I])$ と書く。この対応付け $u_i = j$ のコスト(局所距離)を $d_i(u_i) = \|s_i - t_{u_i}\|_2$ とすると、対応付けの最適化問題は次のように定式化することができる。

$$\text{minimize} \quad F = \sum_{i=1}^I d_i(u_i)$$

$$\text{w.r.t} \quad u_1, \dots, u_I$$

$$\text{subject to} \quad 0 \leq u_i - u_{i-1} \leq 1, u_1 = 1, u_I = J$$

局所距離は任意の距離を用いることができるが、署名認証においては、取り扱うデータが署名データのX,Y座標と圧力の3次元のベクトルからなる時系列データであり、ユークリッド距離が妥当であると考えられるため2ノルムを用いることが普通である。

最適化の結果として得られるものは、二つのシーケンス間の距離(DTW距離)  $\min F$  と対応関係 $u_1, \dots, u_I$ の二つである。

本研究ではスマートフォンのタッチ位置のX座標、Y座標、圧力Pからなる三次元のベクトルのシーケンスを考える。あらかじめ登録しておいたテンプレートを上の系列の

T とすると認証時の入力データを S として DTW 距離を計算する。ここでテンプレートのデータ長 J は入力データのデータ長 I と等しくなることは少ないが DTW の特徴により許容できる。得られた DTW 距離が閾値以下であれば入力者はテンプレートの登録者本人であると判断し認証成功としている。

## 5. 提案手法

### 5.1 概要

本研究では署名認証の際にテンプレートと入力する署名データを一面ごとに分割しそれぞれに永字八法を参考にした属性を割り当てていく。その後テンプレートと入力データを一面ごとに DTW 距離を計算していき、属性が同じであれば DTW 距離にボーナスを与えるという手法を提案する。

本人の署名であれば一面ごとに分割して属性を割り当てていくと個人的な特徴から同じ属性に割り当てられやすくなると考えられ、入力したのが他人であればその人の特徴から同じ画でも違う属性に割り当てられやすくなり個人の特徴を抽出できるのではないかと考えた。

### 5.2 属性割り当て

本手法では署名データを一面ごとに分割してそれぞれに属性を割り当てていくがここではどのように属性を割り当てていくかを説明する。

まず署名のテンプレートを登録する登録者が登録する署名とは別に属性割り当て用の文字を入力しておく。その文字のデータを属性割り当て用の時系列データとする。ここでは仮に割り当てる属性を A,B,C,D の 4 つとしておく。A,B,C,D はそれぞれ X,Y 座標と圧力 P の 3 次元の時系列データである。次に登録者はテンプレートを登録する。ここで仮に登録する文字を総画数 5 画の文字とするとテンプレートの署名データを  $T=[T_1, T_2, T_3, T_4, T_5]$  とおける。この署名データの  $T_k(k=1\sim 5)$  はそれぞれテンプレートの 1 画目から 5 画目の時系列データであり 3 次元の時系列データである。この  $T_k(k=1\sim 5)$  にそれぞれ A,B,C,D の属性のいずれかを割り当てる。1 画目の  $T_1$  と時系列データ A,B,C,D それぞれの DTW 距離を計算し、最も小さい値をとった属性を割り当てていく。同様に 5 画目までをそれぞれ割り当てることでテンプレートの属性のリスト  $L_T$  (ここでは長さ 5 とする) が完成する。

### 5.3 認証

認証の際には入力された署名データにもテンプレートの時と同様に一面ごとに分割したのちそれぞれに属性を割り当てていく。このとき属性を割り当てる際に使うのは先ほどテンプレートで使った属性の時系列データ (上の例では A,B,C,D) である。

認証の際にはまず入力された文字の画数がテンプレートの画数と等しいかどうかを確認し、違っていればその時点

で認証失敗とする。次に入力署名データ  $S=[S_1, S_2, S_3, S_4, S_5]$  にテンプレートと同様に属性を割り当て  $L_S$  を作る。

先ほど割り当てた属性のリスト  $L_T$  と  $L_S$  を仮に  $L_T=[A,B,C,D,A]$   $L_S=[A,B,C,D,B]$  とおく。入力署名データの属性割り当て後にデータ間の距離を計算する。テンプレートの 1 画目と入力署名データの 1 画目の間の DTW 距離  $F_1$  を計算する。その際にそれぞれの属性のリストの 1 画目が同じ属性であれば得られた DTW 距離  $F_1$  にあるパラメータ  $\phi$  をかける。  $\phi$  はテンプレートと同じ属性が割り当てられていた際にどの程度ボーナスを与えるかという数であり外部から与えられる。その計算をすべての画で行い、得られた DTW 距離の合計  $F$  を算出する。今回の例では 5 画目だけが属性が異なっているので

$$F = F_1 \times \phi + F_2 \times \phi + F_3 \times \phi + F_4 \times \phi + F_5$$

を結果として得る。この  $F$  が閾値を下回っていれば登録者本人であるとして認証は成功となり、閾値を上回っていれば他人であるとして認証失敗となる。

一般的にすると、テンプレートと入力署名データに割り当てる属性のリストをそれぞれ  $L_T, L_S$  とすれば、それぞれの  $i$  画目の属性は  $L_{T_i}, L_{S_i}$  となる。テンプレートの  $i$  画目と入力署名の  $i$  画目の間の DTW 距離を  $F_i$  とする。  $\phi$  はその画の属性が一致していれば DTW 距離にかけるので、一致していない場合は 1 をかけるのに等しくなる。署名の画数を I とすると、テンプレートと入力署名の間の非類似度は次のように立式できる。

$$F = \sum_{i=1}^I F_i \times \lambda \quad \begin{cases} \lambda = \phi (L_{T_i} = L_{S_i}) \\ \lambda = 1 (L_{T_i} \neq L_{S_i}) \end{cases}$$

## 6. 実験

### 6.1 実験準備

今回の実験では第一著者がテンプレートの登録者となり実験を行った。実験に使う漢字の署名には画数が短く単純な名前として「山本」という署名と、画数が多いものとして「高橋」という二つの署名を実験に用いた。これらは日本人の苗字の中でも子の苗字である人が多い苗字のうちの二つである。

登録者はスマートフォンを机の上に置き外部からの振動などが極力入らない状態で署名を入力した。また、実験の協力者 10 名に同様の署名を同じ条件で入力してもらいそれらを攻撃者の署名とした。

また今回割り当てる属性として 12 個の属性を用意した。その内訳は、永字八法の分類である点・横画・縦画・はね・右上がり横画・左払い・短い左払い・右払いに加えて逆方向のはね・横画から縦画・アルファベットの J のようなそり・縦画から横画から縦画の 4 個の属性を追加した 12 個である。

実験で用いる署名データ S と T はそれぞれ X 座標, Y 座

標、圧力 P の 3 つの要素を持っているので

$$S = [(s_{x_1}, s_{y_1}, s_{p_1})^T, \dots, (s_{x_i}, s_{y_i}, s_{p_i})^T, \dots, (s_{x_l}, s_{y_l}, s_{p_l})^T]$$

$$T = [(t_{x_1}, t_{y_1}, t_{p_1})^T, \dots, (t_{x_j}, t_{y_j}, t_{p_j})^T, \dots, (t_{x_l}, t_{y_l}, t_{p_l})^T]$$

と表すことができる。ここでの添え字 T は転置を表す。これらは 0~1 の間の値で正規化している。X 座標と Y 座標の正規化に関しては入力機器のスマートフォンのタッチパネルの縦横比が違うのでその比に合わせて正規化している。属性割り当て用の時系列データも同様に正規化している。

今回の実験は割り当てる属性の数を 4 個、8 個、12 個の 3 種類にして 3 つの実験を行った。

テンプレートの決定は Kinwrite の研究に従って、登録者が入力した署名全てをそれぞれ DTW 距離を計算し、その合計が最も小さいものをテンプレートに設定した。

## 6.2 実験 1 4 属性割り当て

署名の画それぞれに割り当てる属性を縦画・横画・右払い・左払いの 4 つにして実験を行った。

属性があっていた際のボーナスとして DTW 距離にかける  $\phi$  を 0.1~1.0 で変化させてどの値が最も適切かどうかを調べた。 $\phi = 1.0$  とは何の補正もかけなかった場合となる。

実験の結果を調べる指標として今回は ROC カーブを用いた。ROC カーブは分類器の性能を測るときに用いるもので、横軸に他人受入率、縦軸に本人受入率としてプロットしていき、線の下側の面積 (AUC) が大きいものほど性能が良く、最良のもので 1.0 となる。

「山本」と「高橋」の二つの署名において  $\phi$  を 0~1.0 で変化させたときの AUC のグラフを図 1, 図 2 に示す。

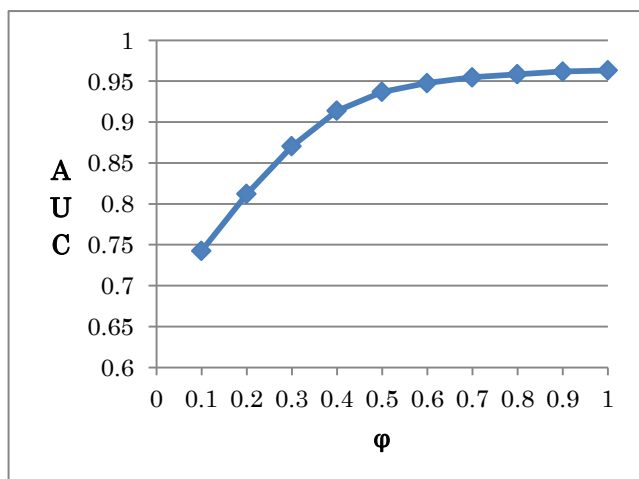


図 1 4 属性の AUC (山本)

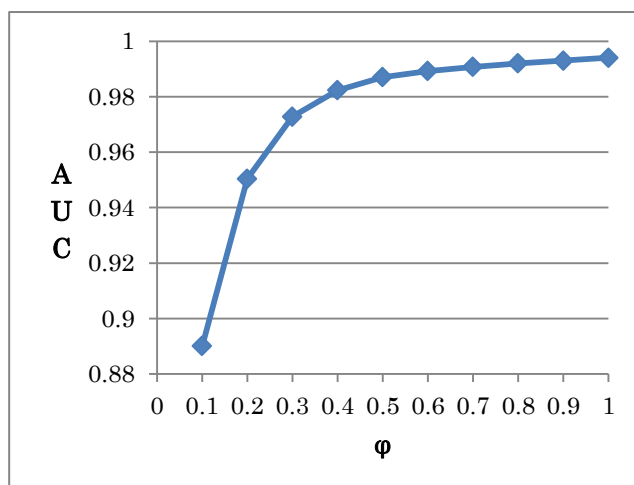


図 2 4 属性の AUC (高橋)

図 1 から、「山本」という署名において  $\phi = 1.0$  の時が最大であるため割り当てる属性が 4 属性の場合は補正をかけない方がよいという結果になった。図 2 から「高橋」という署名でも  $\phi = 1.0$  の時が AUC が最大となり同様の結果が得られた。

## 6.3 実験 2 8 属性割り当て

署名の画それぞれに割り当てる属性を点・横画・縦画・はね・右上がり横画・左払い・短い左払い・右払いの 8 つにして実験を行った。

これも 4 属性の時と同様に  $\phi$  を 0.1~1.0 まで変化させて ROC カーブを描き AUC を算出した。実験 1 と同様に結果を図 3, 図 4 に示す。

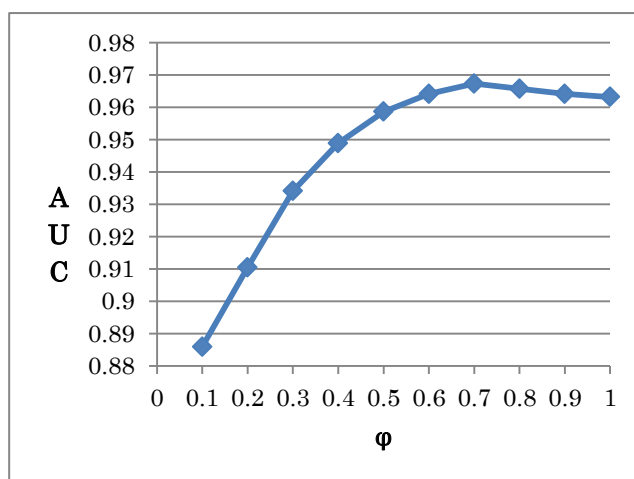


図 3 8 属性の AUC (山本)

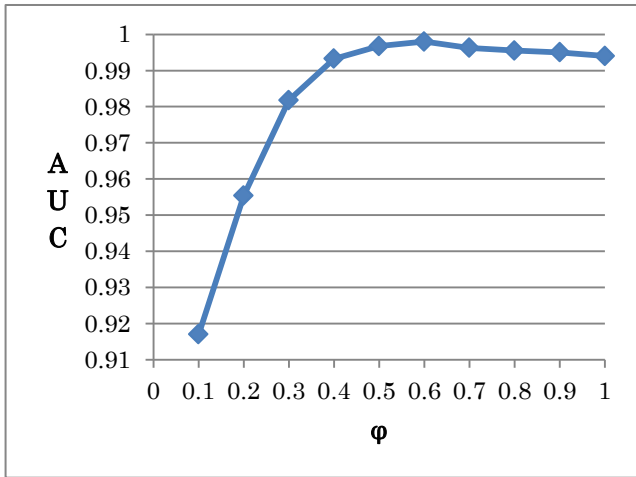


図4 8属性のAUC (高橋)

図3を見ると、「山本」という署名の場合  $\phi=0.7$  のときがAUCが最大になっているのが分かる。 $\phi=1.0$ つまり補正をかけなかった場合のAUCは0.96318であり $\phi=0.7$ のときのAUCは0.96727となり0.00409増加したことになる。

図4から「高橋」という署名の場合 $\phi=0.6$ の時にAUCが最大になっていることが分かる。 $\phi=1.0$ のときと比べると

AUCが0.99401から0.99800になっていることが分かった。増加値は0.00399となった。

これらの結果から「山本」という署名での8属性のAUCが最も増加したときの本人拒否率と他人受入率を閾値を変えてグラフ化したものと補正しなかったときのグラフを図5、図6に示す。

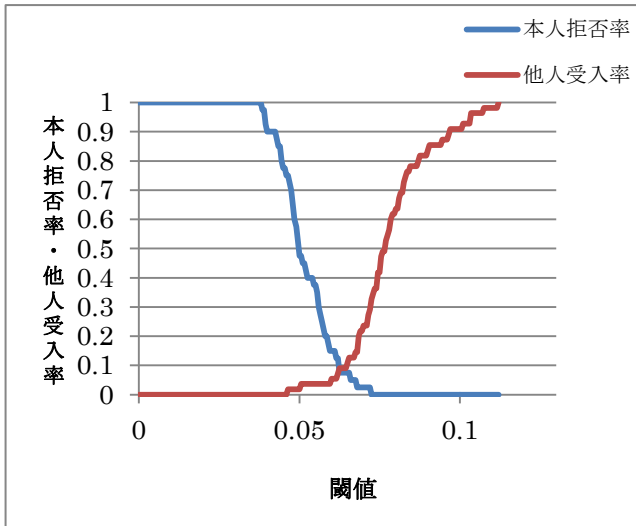


図5 8属性補正なし時のエラー率 (山本)

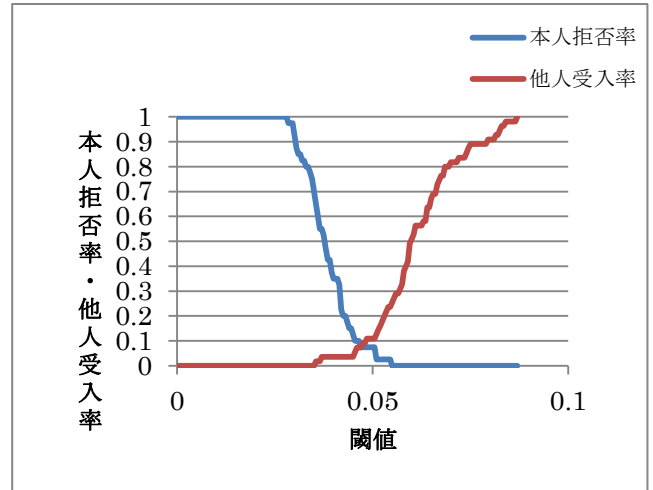


図6 8属性 $\phi=0.7$ の時のエラー率 (山本)

このような図から分類器の性能を知るための指標として等価エラー率というものがある。等価エラー率は上の図において本人拒否率と他人受入率が交わっているときのエラー率をいい、この値が小さいほど良い分類器であると言える。図5と図6では等価エラー率がわかりにくいので拡大したものを図7、図8に示す。図7から「山本」という署名で8属性に割り当てたときの補正なしの等価エラー率は約8.5%、 $\phi=0.7$ の時の等価エラー率は約7.5%であることが分かった。

次に「高橋」という署名においても同様に補正なしの時と $\phi=0.6$ の時の等価エラー率を調べるグラフを作成し図9、図10に示す。同様に拡大したものを図11、図12に示す。図11から「高橋」という署名で8属性に割り当てたときの補正なしの等価エラー率は約5.9%、図12から $\phi=0.6$ の時の等価エラー率は約2.3%であることが分かった。

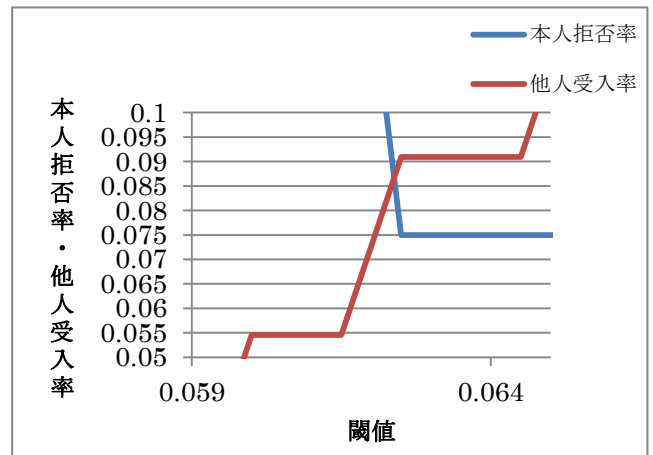


図7 図5の拡大

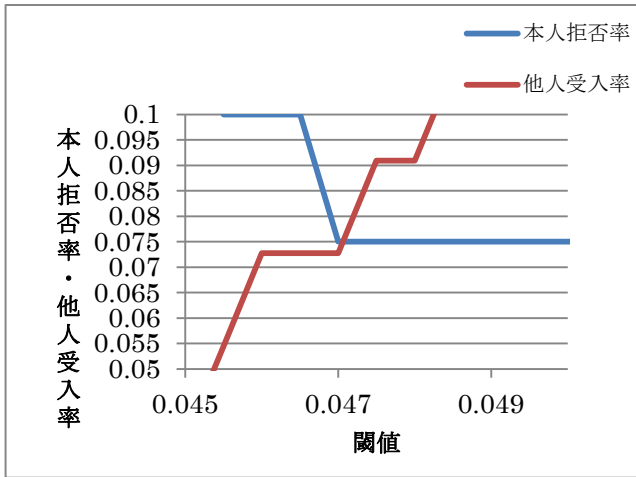


図8 図6の拡大

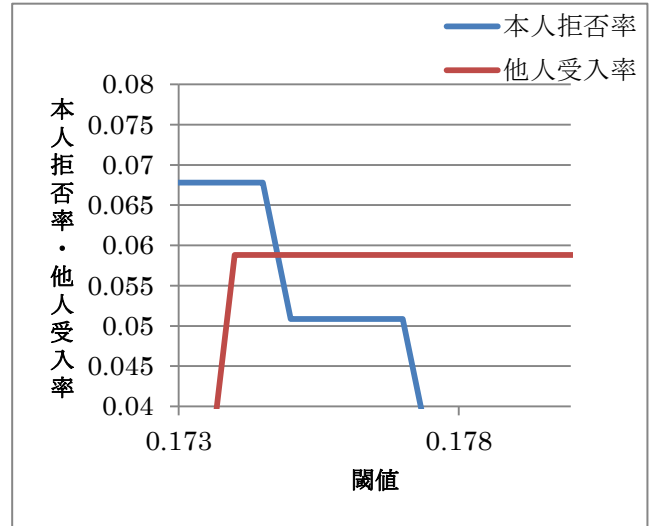


図11 図9の拡大

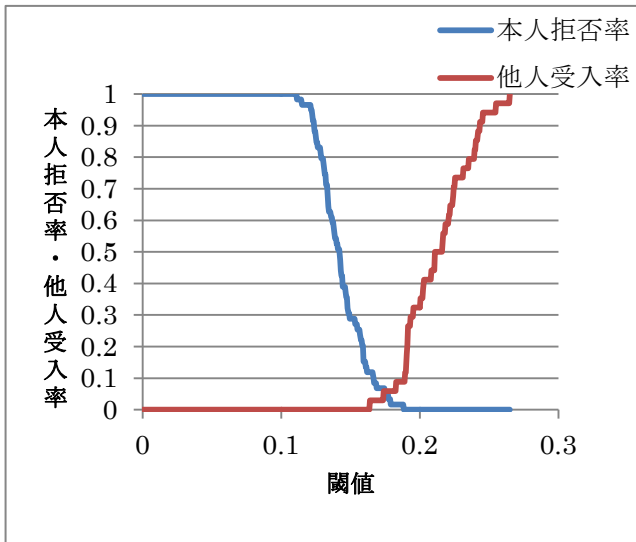


図9 8属性補正なしの時のエラー率 (高橋)

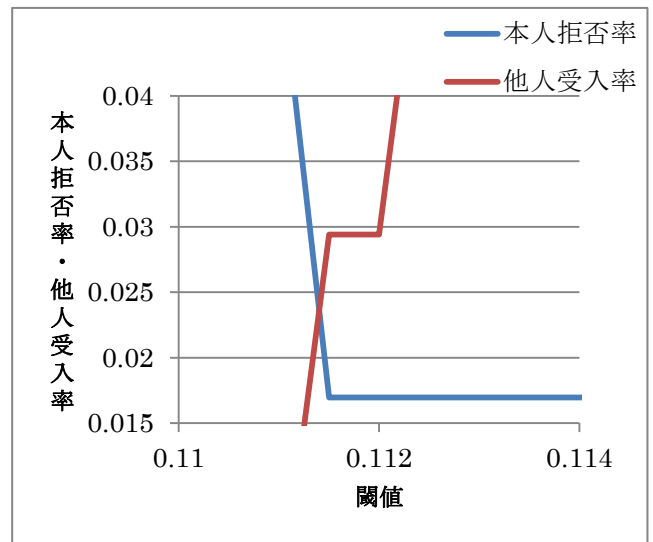


図12 図10の拡大

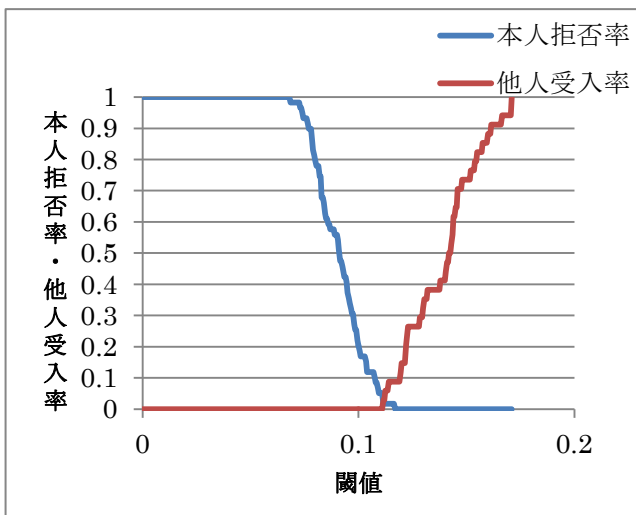


図10 8属性  $\phi=0.6$  の時のエラー率 (高橋)

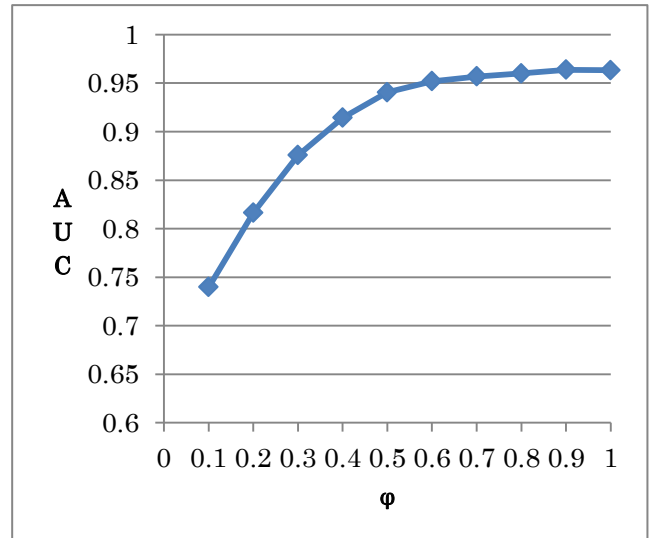


図13 12属性のAUC (山本)

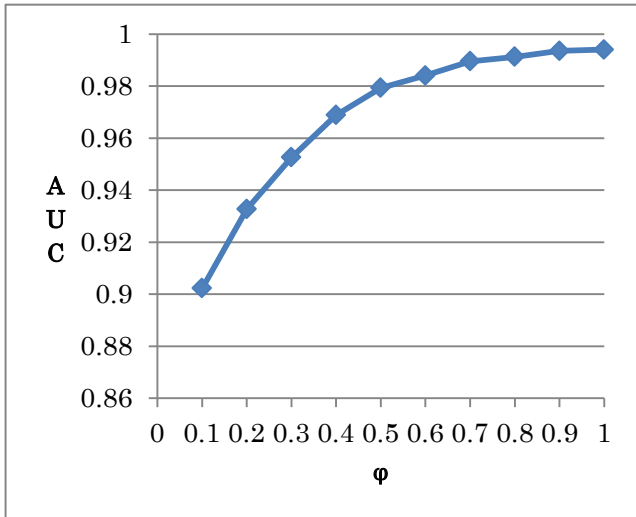


図 14 12属性のAUC (高橋)

### 6.4 実験3 12属性割り当て

次に、実験2の8つの属性に加えて逆方向のはね・横画から縦画・アルファベットのJのようなそり・縦画から横画から縦画の4つの属性をさらに追加して同様の実験を行った。

実験2の時と同様にφを0.1~1.0まで変化させたときのROCカーブを描き、AUCを算出したグラフを図13、図14に示す。図13から、「山本」の署名の場合ほんの少しではあるがφ=0.9の時に補正なしの時よりAUCが増加している。補正なしの時はAUCが0.96318であり、φ=0.9の時のAUCは0.96363となった。増加値は0.00045となった。

図14から、「高橋」の署名の場合は補正なしのときのAUCが最大となり補正しないのが最良の結果となった。

「山本」の署名の場合のみ補正なしの時とφ=0.9の時の等価エラー率を調べるグラフを作成し図15、図16に示す。これも等価エラー率が分かるように拡大したものを図17、図18に示す。図17から「山本」という署名において12属性で補正なしの時の等価エラー率は約8.7%となり、

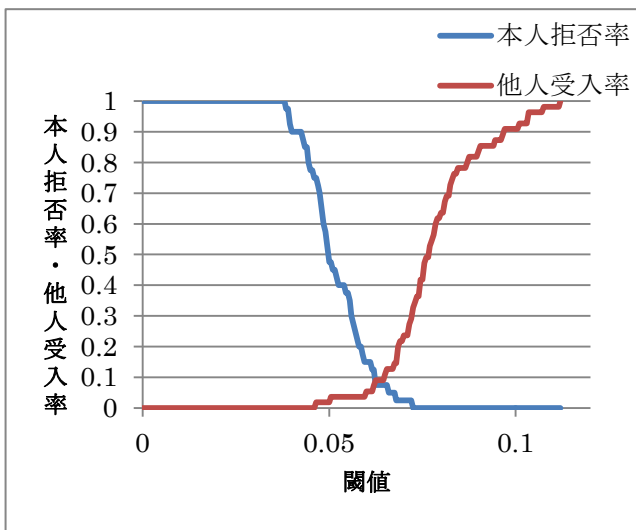


図 15 12属性補正なし時のエラー率 (山本)

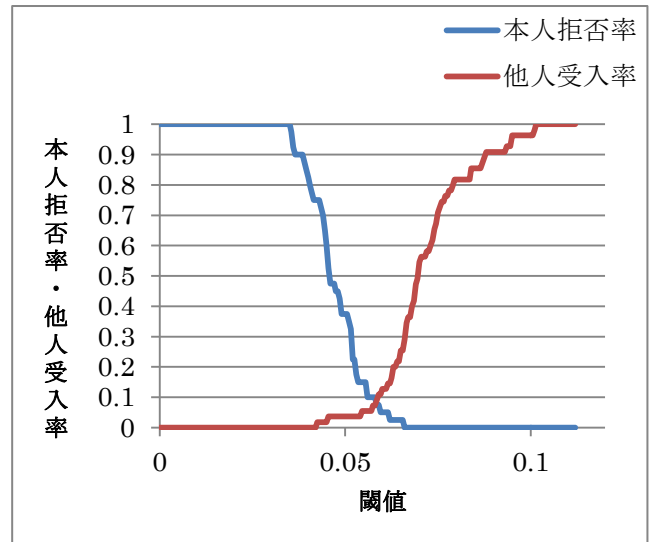


図 16 12属性φ=0.9の時のエラー率 (山本)

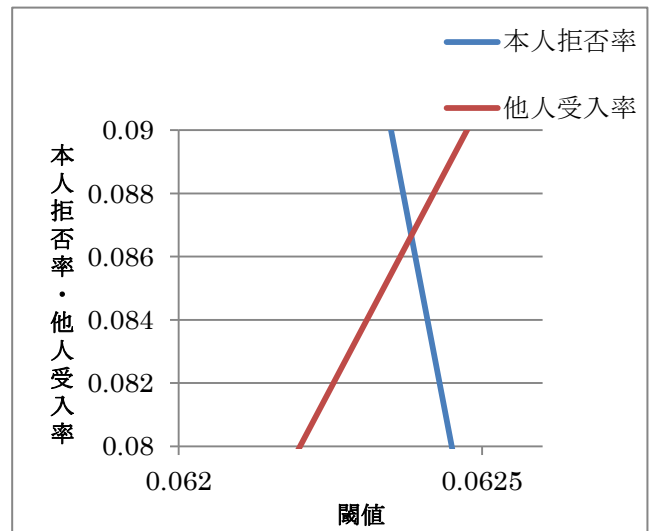


図 17 図 15 の拡大

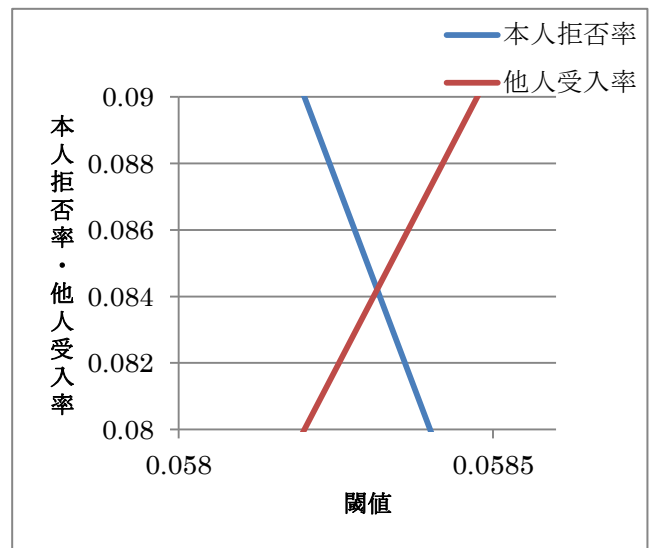


図 18 図 16 の拡大

図 18 から φ=0.9 の時の等価エラー率は約 8.4% になること

が分かった。

## 7. 考察

実験の結果をまとめる。属性の割り当てを4属性にした場合は補正しない方がよい結果になるという結果になった。8属性に割り当てた場合、署名が「山本」の時、補正なしの時の等価エラー率約8.5%が、 $\phi = 0.7$ の時の等価エラー率は約7.5%になり、署名が「高橋」の時、補正なしの時の等価エラー率が約5.9%から $\phi = 0.6$ の時約2.3%になった。属性を12個にした場合、「高橋」の署名については補正しない方がよい結果になったが、「山本」の署名では補正なしの時の等価エラー率約8.7%が $\phi = 0.9$ の時約8.4%になった。

この結果から、割り当てる属性の数とボーナスの $\phi$ の値が適切であれば署名認証の精度を向上させることができた。しかし、割り当てる属性の数や $\phi$ を正しく設定していないと逆に認証精度が下がってしまうことも分かった。

今後は割り当てる属性の種類を変えてみたり属性の外れ方でボーナスを変えてみたりして、より精度の向上が見込めるように改良していくことができると考えている。

## 8. まとめ

近年注目されている覗き見攻撃に耐性のある認証に行動的特徴を用いたバイオメトリクスの署名認証がある。本研究では署名データを一画ごとに分割し、あらかじめ決めておいた複数の属性データから最も近い属性を割り当てていく。認証の際にはテンプレートと入力署名データを一画ごとにDTW距離を算出していき割り当てた属性が一致したときにボーナスとして $\phi$ をかけて補正をする。

今回の実験では署名の種類は「山本」、「高橋」の2種類、割り当てる属性の数を4, 8, 12の3種類で実験を行った。実験の結果、4属性の割り当ての時は「山本」と「高橋」のどちらの場合でも補正をしない方がよいという結果になり、12属性で「高橋」の署名の時も同様に補正しない方がよいという結果になった。8属性の割り当てで「山本」の署名では補正なしの等価エラー率8.5%を7.5%まで減らすことができた。8属性の割り当てで「高橋」の署名では等価エラー率5.9%を2.3%に減らすことができた。12属性で「山本」の署名の時は、幅は小さいが等価エラー率を8.7%から8.4%に減らすことができた。

このように割り当てる属性の数と $\phi$ の値を適切に設定することで認証精度を向上させることができた。しかし、きちんと設定できないと逆に認証精度が下がってしまうこともあり、今後は適切な属性の種類と数を調査していく必要がある。

## 参考文献

[1] 池田匡視, 菅井文郎, and 岡崎直宣. "アイコンとタッチパネル液晶を用いた覗き見耐性を持つ認証方式についての一検討." *宮崎大学工学部紀要* 41 (2012): 241-245.

[2] Plamondon, Rejean, and Guy Lorette. "Automatic signature verification and writer identification—the state of the art." *Pattern recognition* 22.2 (1989): 107-131.

[3] 内田誠一. "DP マッチング概説: 基本と様々な拡張 (テーマセッション (2), パターン認識・メディア理解のための学習理論とその応用)." *電子情報通信学会技術研究報告. PRMU, パターン認識・メディア理解* 106.428 (2006): 31-36.

[4] Tian, Jing, et al. "KinWrite: Handwriting-Based Authentication Using Kinect." *NDSS*. 2013.

[5] 鈴木雅人, et al. "D-12-58 永字八法に基づく手書き文字認識用辞書の動的構成法 (D-12. パターン認識・メディア理解, 一般セッション)." *電子情報通信学会総合大会講演論文集* 2011.2 (2011): 161.