G0906-22
0915-1060/09/¥500/論文/JCLS

なぞり書き認証方式の提案とその認証精度に関する検討

静岡大学
西垣 正勝・梅本 功太・山本 匠

指紋や虹彩などの静的な生体情報は基本的に生涯不変であるため、これらを認証情報として利用する生体認証においては、パスワード認証のように認証情報をユーザの意思によって任意に設定・変更することができない。これに対し、手書き署名などの動的な生体情報を用いた生体認証では、サービスごとに異なる署名テキストを設定することによって任意の認証情報を登録することが可能であり、また、一旦登録した署名テキストを変更することによって認証情報を更新することができる。しかし、利用するサービスが増えるにつれ、異なる複数の署名テキストを記憶・管理することはユーザにとっては大きな負荷となる。また、従来の手書き署名認証においては、正規ユーザの手書き文書が漏洩した際に、そのなりすまし耐性が大きく低下する危険がある。そこで本研究では、認証システムが署名テキストをユーザのディスプレイに表示し、ユーザがその上をスタイラスペンでなぞり書くという「なぞり書き認証方式」を提案する。本方式は、(i) 署名テキストが表示されるため、利用するサービスが多数であっても正規ユーザの記憶負荷はなく、(ii) 一般になぞり書きの際の筆跡は正規ユーザの手書き文書の筆跡とは異なるため、不正者が正規ユーザの手書き文書を入手したとしてもなりすましに利用できない、という特徴を有する。プロトタイプシステムによる認証実験により、提案方式の実現可能性を検証する。

はじめに

生体認証[1]は、各人固有の生体情報を用いた認証であり、パスワードのような記憶の負荷や忘却の恐れがなく、認証トークンのような携帯の煩わしさや紛失の恐れもないという利点を有する。生体認証は、指紋や虹彩などの静的な生体情報を用いるものと手書き署名や歩き方などの動的な生体情報を用いるものに大別される。現在、静的な生体情報を利用した生体認証が広く実用に供されるようになってきた。

しかし、静的な生体情報は基本的に生涯不変であるため、これらを認証情報として利用する生体認証においては、認証情報（生体情報）をユーザの意思によって任意に設定・変更することができないという問題がある。例えば虹彩認証システムを採用しているサービスが複数あった場合、ユーザは右眼または左眼を登録するしかない。これは、プライバシ情報の保護や認証情報漏洩時の被害の最小化の観点から考えると大きなデメリットと言える。例として、一人のユーザが複数のWEBサービスに対して利用登録をするような状況を想定しよう。もし、WEBサービスごとに登録する生体情報を変えることができたとしたら、サービスプロバイダが結託して、登録されている生体情報を使って複数のサービスに登録している同一ユーザを名寄せするというような不正を防ぐことが可能である。WEBサービスを解約する場合にも、登録されている自分の生体情報が確実に廃棄されているかに関して、正規ユーザが気を遣う必要が少なくなる。また、あるWEBサービスに登録されている正規ユーザの生体情報を不正者が盗み出すことに成功したとしても、その生体情報を他のWEBサービスへのなりすましに利用することはできない。

よって、生体認証においても、パスワード認証のように、ユーザが自由に認証情報（生体情報）を設定することが可能であれば、生体認証の利便性も更に向上するものと期待できる。そこで本研究では、動的な生体情報を用いた生体認証の一つである手書き署名認証に注目し、WEBサービスごとに異なる署名テキストをユーザが自由に設定・更新すること

によって、サービスプロバイダ側に登録される認証情報（署名データ）の変更が可能である生体認証に関して検討していく。

ここで、WEBサービスごとに異なる複数の署名テキストを記憶・管理することはユーザにとっては大きな負荷となる。また、従来の手書き署名認証においては、正規ユーザの手書き文書が漏洩した際に、そのなりすまし耐性が大きく低下する危険がある。これらの問題に対処するために、本稿では、認証システムが署名テキストをユーザのディスプレイに表示し、ユーザがその上をスタイラスペンでなぞり書くという「なぞり書き認証方式」を提案する。また、提案方式の精度向上には「本人特徴量を追加するアプローチ」と「他人特徴量を追加するアプローチ」のどちらが有効なのかを実験により検証していく。

生体情報の個別設定に対処した生体認証

キャンセラブル生体認証

生体情報の個別設定に対処するための技術として、キャンセラブル生体認証が研究されている[2),3)]。例えば文献[3)]の方式では、生体情報が乱数によってマスキングされた形でテンプレートとして登録されており、認証時にも生体情報が同じ乱数でマスキングされた上で認証装置に送られテンプレートと比較される。よって、WEBサービスごとに使用する乱数を変更することによって、一つの生体情報から異なるテンプレートを生成して、これを登録することができる。

しかしキャンセラブル生体認証においては、テンプレートを作成した際に用いた乱数が認証時にも必要になる。すなわち、ユーザは利用するWEBサービスの数だけ乱数を管理する必要がある。この乱数は、安全性の観点から人間が記憶できる桁数をはるかに超えるものとなるため、ユーザはこの乱数をICカードなどに記録して携帯することになる。このため、キャンセラブル生体認証においては、記憶の負荷も携帯の煩わしさもないという生体認証のメリットが失われてしまう。

また、キャンセラブル生体認証は、乱数によってマスキングされた後の生体認証の漏洩に対しては十分に機能するが、不正な生体情報のスキャニングなどによって生体情報そのものが漏洩してしまった場合には、その安全性が低下する（生体情報が漏洩した場合は、安全性は乱数のみに依存する）ことになる。

手書き署名認証

認証情報を自由に設定することができる生体認証に対するもう一つの可能性は、動的な生体情報に基づく生体認証[4)-7)]の利用である。動的な生体情報はユーザの動作に応じた情報であるため、ユーザがWEBサービスごとに任意の「パス動作」を登録し、登録されたパス動作に基づいて本人性を確認することができれば、認証情報の個別設定が可能な生体認証を実現することができる[8)]。

動作の変更が容易な動的生体認証として、本稿では、手書き署名認証[9)-14)]に注目する。手書き署名認証では、Fengら[9)]やZhaoら[10)]が提案しているように、ユーザの氏名（クレジットカードでの購入の際などに記すサイン）を署名テキストとするのが一般的である。しかし、ユーザの氏名は通常1つであるため、生体情報の漏洩、再登録という問題の根本的解決にならない。この観点から吉村ら[15)]は、氏名以外の一般的な文書を署名テキストとする方式を提案している。一般的な文書を署名テキストとして使用可能であれば、認証情報（署名テキストや署名データ）を自由に設定することが可能である。

ただし、ここで、署名データを個別に設定する（WEBサービスごとに署名テキストを変える）ことは、正規ユーザに相応の記憶負荷を強いることに留意しなければならない。手書き署名認証においては、署名テキストが漏洩した場合には、当然、その分だけなりすましのリスクが高まることになる。したがって、ユーザは複数の署名テキストを正しく管理する必要がある。すなわち、パスワードと同じように、署名テキストをメモなどに書き留めたり、過去に使用した署名テキストを使い回したりすることは慎まなければならない。このため、WEBサービスごとに署名テキストを変えるような運用をする場合には、署名テキストの忘却などのリスクが高まることが予想される。

ユーザの記憶負荷に対処した手書き署名認証

手書き署名認証における記憶負荷の問題の解決を図るため、山崎ら[13)]は、テキスト提示型筆者照合手法を提案している。この方式では、認証時にシステムが任意のテキストを提示し、ユーザは提示された文字を記入する。システムは、予めユーザの様々な文字に対する筆跡情報を多数取得し、正規ユーザの個人性が強く現れる特徴（「はらい」や「はね」など）を学習しており、認証時に記入され

た文字の中にその特徴が含まれているかどうかによって認証可否を判定する。ユーザはシステムによって認証の都度提示されるテキストを記入すればよいため、記憶負荷の問題はない。

しかし、ユーザ本人が自由に記す文字を使って認証を行っている以上、正規ユーザが書く文字の形状などを不正者が見れば、そこに含まれる「本人らしさ」に関する多くの情報が盗まれることは否めない。このため、山崎らの手法においては、正規ユーザの手書き文書が漏洩した際に、そのなりすまし耐性が低下する可能性がある。そこで本研究では、認証システムが無作為に選択した文字列をディスプレイに表示し、ユーザがスタイラスペンを使って、ディスプレイに表示された署名テキストをなぞり書くという方法を採ることで、この問題の解決を図る。ユーザが提示された文字の上をなぞって書いた場合の筆跡は、同じ文字を自分の思い通りに書いた場合の筆跡とは異なると予想されるため、不正者は正規ユーザの手書き文書から十分な情報を得ることは難しいと期待される。

ここで、今回の認証方式においては、署名テキストがディスプレイに表示されるため、不正者も署名テキストを知ることができるということに注意する必要がある。よって、「ユーザごとに署名テキストが異なる」という点に安全性（の一部）を依拠するような認証システムを構成することは適切とは言えない。すなわち、不正者を含めたすべてのユーザが同じ署名テキストの上をなぞって書いたとしても適正な認証精度が維持されるべきである。このため、なぞり書き認証においては「各ユーザが自分の署名テキストを自由に設定・更新する」という形での運用がもちろん可能であるが、本稿では特に、「認証システムが無作為に選択した文字列を、あるグループに属するすべての正規ユーザに対する署名テキストとして使用する」という運用形態に的を絞った形で、議論を進めることとする。

また、山崎らの手法においては、正規ユーザの筆跡の中から個人性が強く現れる特徴を抽出するために、大量の真筆跡と偽筆跡のサンプルを用いての機械学習が必要であり、登録フェーズが煩雑となるという問題があった。このため本研究では、登録フェーズにおける正規ユーザによる署名データの登録は1回のみとし、これをテンプレートとして認証時の署名データとの比較に用いることによって認証可否を判定するタイプのなぞり書き認証システムを構築していく。

なぞり書き認証方式

提案方式のコンセプト

提案方式では、登録および認証の際に、システムが署名テキストをディスプレイに表示し、ユーザはスタイラスペンを使って、ディスプレイに表示されたテキストの上をなぞり書く。なお本方式では、例えばPDAやタブレットPCのようなタッチパネル機能を有するディスプレイの使用を想定している。また、スタイラスペンの筆跡だけでなく、筆圧も感知可能であるとする。ディスプレイに表示されるテキストが「署名テキスト」、ユーザがその上をなぞり書きした際の筆跡・筆圧データが「署名データ」である。

提案方式による認証システムは、WEBサービスごとに実装される。署名テキストは認証システムが任意に決定する。すなわち、WEBサービスごとに署名テキストは異なる。これによって、サービスプロバイダの結託による生体情報（署名データ）を利用しての名寄せ、あるWEBサービスに登録されている生体情報（署名データ）を盗用しての他のWEBサービスへのなりすましなどの脅威を抑えることが可能である。ユーザに代わって認証システムが署名テキストを決定することは、新しいWEBサービスに登録をする度に使用する署名テキストをあれこれ考えるというユーザの手間を減らすとともに、ユーザがすでにどこか他のWEBサービスで使用した署名テキストを使い回してしまうことを防ぐというメリットも生む。

あるWEBサービスを利用しているすべてのユーザ（その認証システムに登録されているすべてのユーザ）に対する署名テキストは共通である。[*1] 署名テキストは認証時に画面に表示される。これにより、署名テキストに対する正規ユーザの記憶負荷を抑えることができる。署名テキストがディスプレイに表示されるため、不正者も署名テキストを知ることはで

[*1] 前節で述べたように、本稿では、「認証システムが無作為に選択した文字列を、あるグループに属するすべての正規ユーザに対する署名テキストとして使用する」という運用形態に的を絞った形で、議論を進める。ただし、ユーザ数が多い場合には、全ユーザを幾つかのグループに分け、グループ単位で共通の署名テキストを利用するようにしてもよい。

きる。しかし、画面上の文字列のなぞり書きをして得られる署名データは、普段ユーザが紙面等に同じ文字を書く際の署名データとは異なると予想されるため、不正者が署名テキストと正規ユーザの手書き文書を入手できたとしても、なりすまし耐性は保たれると考えられる。

このように提案方式は、「WEBサービスごとの認証情報（署名テキスト、署名データ）の個別設定」を効果的に実現することができると考えられる。しかし、提案方式はどのユーザに対しても同じ署名テキストが使用されるため、そのなぞり書きによって得られる署名データは異なるユーザ間であっても似てしまうと考えられる。よって提案方式においては、既存の手書き署名認証以上に、認証精度を向上させるための方策が必要になると予想される。

一般に、生体認証の認証精度を改善するには、利用する生体情報を追加して本人らしさの評価を強化する「本人特徴量を追加するアプローチ（マルチモーダル化）」[16),17)]と、他人との差異を考慮して本人らしさに加えて他人らしさについても評価を行う「他人特徴量を追加するアプローチ（本人尤度と他人尤度の両者の利用）」[14),18)]が考えられる。ここで、提案方式においては上述のとおり、異なるユーザ間であっても署名データが似てしまうと考えられるため、本人情報を追加するアプローチと比べ、他人特徴量を追加するアプローチの効果は薄いのではないかと予想される。

そこで本稿では、本人の筆跡のみを用いて認証の判定を行う場合（方式1）、本人のみの筆跡と筆圧を利用して認証の判定を行う場合（方式2）、本人の筆跡と（システムに登録されている）他人の筆跡の両方を利用して認証の判定を行う場合（方式3）のそれぞれに対する提案方式の認証精度を実験により比較し、提案方式の実現可能性を確認する。

認証手順

提案方式は登録フェーズと認証フェーズに分かれている。それぞれについて説明する。

【登録フェーズ】

1. 認証システムは署名テキストを決定する。
2. 認証システムは、登録要求を行ったユーザに対し、署名テキストをディスプレイに表示する。
3. ユーザは表示されたテキストの上を、スタイラスペンを用いてなぞり書く。なぞり書きによって得られた署名データ（方式1および方式3においては筆跡の時系列データ、方式2においては筆跡および筆圧の時系列データ）がテンプレートとなる。
4. 認証システムは、テンプレートをユーザ名と合わせて登録する。

【認証フェーズ】

1. 認証者は認証システムにユーザ名を入力する。
2. 認証システムは署名テキストをディスプレイに表示する。
3. 認証者は表示されたテキストの上を、スタイラスペンを用いてなぞり書く。なぞり書きによって得られた署名データ（方式1および方式3においては筆跡の時系列データ、方式2においては筆跡および筆圧の時系列データ）が認証データとなる。
4. 認証システムは、認証データとテンプレートのデータ間の距離（方式1においては筆跡に対する認証データと本人テンプレートデータの距離、方式2においては筆跡および筆圧に対する認証データと本人テンプレートデータの距離、方式3においては筆跡に対する認証データと本人テンプレートデータおよび他人テンプレートデータとの距離）を算出し、認証可否を決定する。

本人認証実験

提案方式の認証精度に関して、「本

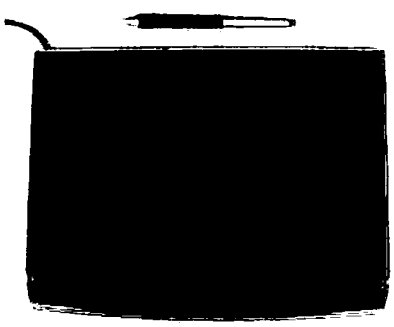

写真1　ペンタブレットの外観

第1表　ペンタブレットの仕様

ペンタブレット		Intuos3 PTZ-630（WACOM社製）
サイズ	タブレット	横345×縦261.5×高さ13mm
	スタイラスペン	長さ175×直径15mm
筆跡検出範囲	横方向	0～1023pixel
	縦方向	0～767pixel
筆圧検出範囲		0～1023レベル
サンプリングレート		100Hz

第2表　解析用PCの仕様

CPU	(Socket AM2) Athlon64 X2 3800+
RAM	1GB
OS	Windows XP Professional

人特徴量を追加するアプローチ」と「他人特徴量を追加するアプローチ」の比較調査を行うための実験を行った。実験環境およびその手順について詳細に述べる。

実験環境

3章で既に述べたように、なぞり書き認証はPDAやタブレットPCのようなタッチパネル機能を有するディスプレイの使用を想定しているが、今回の実験では、ペンタブレットに署名テキストを印刷した紙を敷くことで擬似的にこの入力環境を再現した。

被験者は、ペンタブレット上に敷かれた紙面に印刷された文字の上をスタイラスペンでなぞり書く。なぞり書き中の筆跡（ペン先位置のx座標、y座標）と筆圧の時系列データを取得し、PCにてデータ解析を行った。実験に使用したペンタブレットの外観と仕様、解析に使用したPCの仕様をそれぞれ写真1、第1表、第2表に示す。

データ取得手順

上述の実験環境を用い、数種類の署名テキストに対する被験者の署名データを取得し、認証精度に対する評価実験を行う。被験者は本学学生10人（被験者A～J）であり、今回使用した署名テキストは、「目」、「点」、「辻」という3つの漢字である。

署名テキストのフォントはHG教科書体を使用した。署名テキストは紙に印刷され、ペンタブレット上に敷かれる。ユーザは紙の上から、スタイラスペンによって署名テキストをなぞり書く。印刷された署名テキストは一辺1.5cmの正方形サイズであり、簡単な予備実験を通じてすべての被験者が違和感なくなぞり書きを行うことができたと答えた文字サイズを採用している。実験初日に、全被験者から各署名テキストに対する署名データ（筆跡および筆圧の時系列データ）を1回ずつ取得した。この署名データはテンプレート（登録データ）として扱われる。その後、同日および一週間後に、全被験者から各署名テキストに対する署名データを10回ずつ取得した。今回は、各被験者に『「目」のなぞり書き10回→「点」のなぞり書き10回→「辻」のなぞり書き10回』の順序で、3つの署名テキストのなぞり書きを続けて行ってもらった。ここで得られた各被験者のそれぞれの署名テキストあたり20回分の署名データが認証データとなる。

データの正規化

人間は機械のように完全に同じ動作を繰り返すことは不可能であるため、毎回のなぞり書きにおいて、本人であっても筆跡、筆圧が異なり得る。そこで、筆跡（ペン先位置のx座標、y座標）情報に対しては、なぞり書きの開始から終了までの間のペン先位置の座標の絶対値

$$\left(\sqrt{(x\text{軸の位置座標})^2+(y\text{軸の位置座標})^2}\right)$$

の最大値が1になるように座標データの正規化を行う。筆圧情報に対しても、なぞり書きの開始から終了までの間の筆圧の最大値が1になるように正規化を行う。

データ間距離の算出

データ間距離の算出には以下の3つの方式を用いる。

方式1) 署名データの筆跡情報と本人テンプレートデータの筆跡情報の間の距離を算出する。

方式2) 署名データの筆跡および筆圧情報と本人テンプレートデータの筆跡および筆圧情報の間の距離を算出する。

方式3) 署名データの筆跡情報と本人テンプレートデータおよび（認証システムに登録されている）他人テンプレートの筆跡情報の間の距離を算出する。

方式1は、本人の署名データ中の筆跡情報のみを考慮しており、方式2、方式3との認証精度の比較に用いる。

方式2は、方式1で考慮している本人の筆跡情報に加え、本人の筆圧情報をも考慮する。すなわち、「本人特徴量を追加するアプローチ」の方式である。

方式3は、筆跡情報のみを利用する点は方式1と同じであるが、方式1が本人テンプレートデータとの近さのみを測るのに対し、方式3では他人テンプレートデータとの遠さについても考慮する。すなわち、「他人特徴量を追加するアプローチ」の方式である。

以下では、各方式におけるデータ間距離の算出方法を詳細に述べる。

方式1におけるデータ間距離の算出

データ間距離の算出にはDPマッチングを用いた。DPマッチングはテンプレートマッチングの一種で、時

系列データを非線形伸縮しながらテンプレートデータとの比較を行う手法であり、動的な生体情報を使用した生体認証の多くに使用されている。算出手順は以下のとおりである。ここで、テンプレートデータがT、署名データがSである。

(1) サンプル数Iのデータ Tの、i番サンプルのペン先位置のx座標を$x_T(i)$、y座標を$y_T(i)$とする。同様に、サンプル数Jのデータ Sの、j番サンプルのペン先位置のx座標を$x_S(j)$、y座標を$y_S(j)$とする。

(2) データTのi番サンプルとデータSのj番サンプルの間のユークリッド距離d1(i、j)を次のように定義する。

$$d1(i,j)=\sqrt{d_x^2(i,j)+d_y^2(i,j)}$$
$$d_x(i,j)=x_T(i)-x_S(j)$$
$$d_y(i,j)=y_T(i)-y_S(j)$$

(3) データTとデータSのDPマッチング距離D1(T、S)は次の漸化式で求めることができる。

$$Initialize: g(1,1)=2d1(1,1)$$

$$For\ \ i=1\ to\ I\ \ \ j=1\ to\ J$$

$$g(i,j)=\min\begin{bmatrix} g(i-1,j)+d1(i,j) \\ g(i-1,j-1)+2d1(i,j) \\ g(i,j-1)+d1(i,j) \end{bmatrix}$$

$$D1(T,S)=\frac{g(I,J)}{I+J}$$

(4) 上述の手順で得られたマッチング距離D1(T、S)を、方式1におけるデータ間距離とする。算出されたデータ間距離が小さいほど、データTとデータSは類似していることを表す。

方式2におけるデータ間距離の算出

方式2では、方式1に筆圧情報が加わる。算出手順の詳細を以下に述べる。

(1) サンプル数Iのデータ Tの、i番サンプルのペン先位置のx座標を$x_T(i)$、y座標を$y_T(i)$、筆圧レベルを$p_T(i)$とする。同様に、サンプル数Jのデータ Sの、j番サンプルのペン先位置のx座標を$x_S(j)$、y座標を$y_S(j)$、筆圧レベルを$p_S(j)$とする。

(2) データTのi番サンプルとデータSのj番サンプルの間のユークリッド距離d2(i、j)を次のように定義する。

$$d2(i,j)=\sqrt{d_x^2(i,j)+d_y^2(i,j)+d_p^2(i,j)}$$
$$d_x(i,j)=x_T(i)-x_S(j)$$
$$d_y(i,j)=y_T(i)-y_S(j)$$
$$d_p(i,j)=p_T(i)-p_S(j)$$

(3) データAとデータBのDPマッチング距離D2(T、S)は次の式で求めることができる。

$$Initialize: g(1,1)=2d2(1,1)$$

$$For\ \ i=1\ to\ I\ \ \ j=1\ to\ J$$

$$g(i,j)=\min\begin{bmatrix} g(i-1,j)+d2(i,j) \\ g(i-1,j-1)+2d2(i,j) \\ g(i,j-1)+d2(i,j) \end{bmatrix}$$

$$D2(T,S)=\frac{g(I,J)}{I+J}$$

(4) 上述の手順で得られたマッチング距離D2(T、S)を、方式2におけるデータ間距離とする。算出されたデータ間距離が小さいほど、データTとデータSは類似していることを表す。

方式3におけるデータ間距離の算出

方式3では、筆跡情報における署名データと本人テンプレートデータとの近さを測る方式1をベースに、筆跡情報における署名データと他人テンプレートデータの遠さについても考慮してデータ間距離を算出する。ユーザAの認証を例に挙げ、算出手順の詳細を以下に述べる。

(1) 認証システムに登録されている全ユーザ（今回は10名の被験者A～J）のテンプレートデータTをそれぞれA_T、B_T、・・・、J_Tとする。

(2) ユーザAを名乗る被認証者がなぞり書き認証を実施し、署名データSが得られたとする。

(3) 手順（2）で得られた署名データSと、すべての登録ユーザのテンプレートデータ（A_T、B_T、・・・、J_T）とのデータ間距離D1(A_T、S)、D1(B_T、S)、・・・、D1(J_T、S)を、方式1の手順を用いてそれぞれ算出する。

(4) 手順（3）で得られたデータ間距離から、距離D3(A_T、S)を以下のように求める。

$$D3(A_T,S)=\frac{D1(A_T,S)}{\min(D1(B_T,S),D1(C_T,S),\cdots,D1(J_T,S))}$$

ここで、上式右辺の分子が署名データの本人テンプレートとの近さ（本人特徴量）を、分母が署名データの他人テンプレートとの遠さ（他人特徴量）を表していることに留意されたい。

(5) 上述の手順で算出された距離D3(At、S)を方式3におけるデータ間距離とする。算出されたデータ間距離D3(T、S)が小さいほど、データT（上記の例ではT=AT）とデータSは類似していることを表す。

実験結果

署名テキスト（「目」、「点」、「辻」）

ごとに、各方式（方式1～3）における各被験者（A～J）のEER（等誤り率）を算出した。EERは、FRR（本人拒否率）とFAR（他人受入率）が等しいときのFRR（=FAR）の値であり、値が小さいほど認証精度がよいことを表す。結果を第3表に示す。

考察

本研究では、すべてのユーザに対して同じ署名テキストを使用するという運用形態を想定したため、そのなぞり書きによって得られる署名データは異なるユーザ間であっても似てしまうと考えられる。このため、本人情報を追加するアプローチ（方式2）と比べ、他人特徴量を追加するアプローチ（方式3）の効果は薄いのではないかと予想していた。表3のEERの平均値を見ると、確かに、方式2のEERが総じて一番小さい値となっている。よって、提案方式を今回のような形で運用する際においては、確かに方式2、すなわち「本人特徴量を追加するアプローチ」が適していると考えられる。

しかし、それぞれの署名テキストにおける各被験者のEERを個別に見た場合、方式2のEERと方式3のEERが同程度の値となっているケース、および、方式2のEERよりも方式3のEERが小さい値となっているケースも少なくない。これは、「全ユーザが同じ署名テキストをなぞり書く」という行為の中にも、少なからずユーザごとの個人性が含まれることを示唆する結果であると考えている。また、全ユーザに対して同じ署名テキストを使用する場合は確かに「本人と他人の間の差異」が小さくなるものの、それ以上に「なぞり書きの動作における本人内の分散」が大きいユーザに対しては、ブレが大きい本人情報を追加しても認証精度の向上は期待できず、他人特徴量を追加するアプローチ（方式3）のほうが有効となる傾向にあると言える。

第3表　各署名テキスト・各方式・各被験者のEER（単位[%]）

署名テキスト「目」		被験者										
		A	B	C	D	E	F	G	H	I	J	平均
EER	方式1	21	22	26	40	24	8	37	54	38	9	27.9
	方式2	8	22	5	23	13	13	27	36	28	2	17.7
	方式3	16	6	24	21	25	2	24	41	35	31	22.5

署名テキスト「点」		被験者										
		A	B	C	D	E	F	G	H	I	J	平均
EER	方式1	37	61	16	44	31	24	5	38	30	9	29.5
	方式2	18	48	10	15	19	24	1	28	11	1	17.5
	方式3	33	35	10	45	31	19	5	25	17	5	22.5

署名テキスト「辻」		被験者										
		A	B	C	D	E	F	G	H	I	J	平均
EER	方式1	22	28	20	50	20	14	24	33	31	14	25.6
	方式2	19	14	16	37	10	5	11	20	20	8	16.0
	方式3	22	5	21	30	15	6	20	16	25	24	18.4

おわりに

サービスごとに認証情報（生体情報）を変更することが可能な生体認証の実現を目指し、なぞり書き認証方式を提案した。提案方式では、認証システムが署名テキストをユーザのディスプレイに表示し、ユーザがその上をスタイラスペンでなぞり書くことによって、認証を行う。これによって、ユーザが署名テキストを記憶・管理する負荷を無くすとともに、ユーザの手書き文字がなりすましに利用されるリスクを抑えることが可能となる。

実験を通じて提案方式を評価した結果、「全ユーザが同じ署名テキストをなぞり書く」という提案方式の運用形態においては、基本的には、「本人特徴量を追加するアプローチ」がその精度向上に有効であることが確認された。しかし、すべてのユーザに対して同じ署名テキストを用いる場合であっても、なぞり書きの動作の中にユーザごとの個人性が含まれるケースや、なぞり書きの動作における本人内の分散が大きいケースにおいては「他人特徴量を追加するアプローチ」のほうが有効となるという知見も得られた。

今後は、被験者を増やして実験を繰り返すとともに、署名データにおける筆跡・筆圧以外の情報を利用した場合の提案方式の精度を検証していく予定である。

謝辞　本研究を進めるにあたり、研究に関するご助言を賜りました日立製作所高橋健太様、成蹊大学村松大吾先生に感謝いたします。

参考文献

1) 瀬戸洋一, "バイオメトリックセキュリティ入門", ソフト・リサーチ・センター.
2) N.K.Ratha, J.H.Connell, and R.M.Bolle, "Enhancing security and privacy in biometrics-based authentication system", IBM System Journal, Vol.40, No.3, pp.614-634, 2001.
3) 高橋健太, 比良田真史, "相関不変ランダムフィルタリングを用いたキャンセラブル指紋認証", 暗号と情報セキュリティシンポジウム (SCIS2008), 2008.
4) 石原進, 行方エリキ, 太田雅敬, 水野忠則, "端末自体の動きを用いた携帯端末向け個人認証", 情報処理学会論文誌, Vol.46, No.12, pp.2997-3007, 2005.
5) 佐藤勝規, 佐藤究, 小笠原直人, 布川博士, "握るという動作を用いた個人認証システムの実装", 情報処理学会研究報告, 2006-CSEC-35, pp.7-12, 2006.
6) 樋口岳, 半谷精一郎, "筆記時における指の曲げ角による個人認証", 2004年暗号と情報セキュリティシンポジウム予稿集, pp.683-688, 2004.
7) Davrondzhon Gafurov, Kirsi Helkala, Torkjel Søndrol : Biometric Gait Authentication Using Accelerometer Sensor, JOURNAL OF COMPUTERS, VOL.1, No.7, OCTOBER/NOVEMBER 2006.
8) 梅本功太, 西垣正勝, "人間の動作を用いた認証に関する検討", マルチメディア, 分散, 協調とモバイル (DICOMO 2007) シンポジウム論文集, pp.1338-1346.
9) H.Feng and C.Choong-Wah, "Online signature verification using a new extreme points warping technique", Pattern Recognition Letters, vol.24, No.16, pp.2943-2951, 2003.
10) P.Zhao, A.Higashi and Y.Sato, "On-Line Signature Verification by Adaptively Weighted DP Matching", IEICE Trans. INF. & SYST., Vol.E79-D, No.5, pp.535-541, 1996.
11) M.Parizeau and R.Plamondon, "What types of scripts can be used for personal identity verification?", Computer Recognition and Human production of Handwriting, pp.77-90, 1989.
12) 吉村ミツ, 吉村功, "筆者認識研究の現段階と今後の動向", 信学技報, PRMU96-48, pp.81-90, 1996.
13) Y.Yamazaki and N.Komatsu, "A proposal for a text-indicated writer verification method", IEICE Trans. Fundamentals, Vol.E80-A, No.11, pp.2201-2208, 1997.
14) J.Fierrez-aguilar, J.Ortega-garcia, J.Gonzalez-rodriguez, "Target dependent score normalization techniques and their application to signature verification", IEEE Trans. on Systems, Man and Cybernetics, part C, Vol.35, No.3, pp.418-425, 2005.
15) I.Yoshimura and M.yoshimura, "Off-line writer verification using ordinary characters as the object", Pattern Recognition, Vol.24, No.9, pp.81-90, 1991.
16) 田村哲嗣, 岩野公司, 古井貞熙, "マルチモーダル音声認識のための画像特徴量の改善", 春季音講論, 3-Q-22, pp.195-196, 2003.
17) 上澤泰, 石川雅人, 田村哲嗣, 速水悟, "音声と画像のconfusion networkを用いたマルチモーダル音声認識", 信学技報, SP2007-92, Vol.107, No.356, pp.37-42, 2007.
18) 磯部俊洋, 高橋淳一, "話者照合におけるHMMの局所的音響情報に基づく尤度正規化", 情報処理学会研究報告. SLP, 音声言語情報処理, Vol.98, No.114, pp.69-74, 1998.

【筆者紹介】

西垣 正勝
静岡大学 創造科学技術大学院
准教授
〒432-8011 浜松市中区城北3-5-1
tel:053-478-1467
fax:053-478-1499
E-mail : nisigaki@inf.shizuoka.ac.jp
〈主たる業務暦及び資格〉
1990年静岡大学工学部光電機械工学科卒業。1992年同大学院修士課程修了, 1995年同博士課程修了。日本学術振興会特別研究員 (PD) を経て、1996年静岡大学情報学部助手, 1999年同講師、2001年同助教授。2006年より同創造科学技術大学院助教授。2007年より准教授。博士 (工学)。情報セキュリティ、ニューラルネットワーク、回路シミュレーション等に関する研究に従事。

梅本 功太
静岡大学 大学院 情報学研究科
〈主たる業務暦及び資格〉
2007年静岡大学情報学部情報科学科卒業。2009年同大学院修士課程修了。現在、日本アイ・ビー・エム株式会社に勤務。在学中、情報セキュリティに関する研究に従事。

山本 匠
静岡大学 創造科学技術大学院
〈主たる業務暦及び資格〉
2006年静岡大学情報学部情報科学科卒業。2007年10月同大学院修士課程修了。現在、同創造科学技術大学院博士課程。日本学術振興会特別研究員 (DC1)。情報セキュリティに関する研究に従事。