

瀬川 典久[†] 権藤 広海[†] 中本 泰然^{††} 山根 信二[†] 村山 優子[†] 宮崎 正俊[†]

[†]岩手県立大学 ソフトウェア情報学部

^{††}広島市立大学大学院 情報科学研究科

1 はじめに

一般に手書きにおける筆跡は、個人の情報を残す性質を持っておりために、筆跡鑑定による認証によく用いられる[1][2][3]。しかし、筆跡を操作し、認証を不可能にする手法については現在まで論じられてこなかった。

本稿では、手書きにおける匿名性について提案する。ユーザによって作成された手書きの情報に対して匿名化アルゴリズムを適用することによって、匿名化が可能なることを示す。

2 手書きにおける匿名性

2.1 認証と匿名化

図1に手書きの認証について示す。手書きの認証は、認証に用いるサンプルの手書き（この図の例ではSignature）と、認証したい手書き（Countersignature）との特徴点による照合によって行われる。よく利用される特徴点として、形状、文字列の傾き、筆圧が利用される。

図2に手書きの匿名化について示す。ユーザの書いた筆跡情報を、(1)一方向アルゴリズムで(2)乱数によって変形させる。ただし、変形させた筆跡情報は、人間によって判読可能である。この結果、描画情報における特徴点は、乱数によってその人間によって本来書かれる以外の特徴点が表れる。よって、認証に利用される元の識別情報とは比較が不可能になる。

また、この変形は乱数を用いて行っているので2度と同じ変形は不可能である。つまり、Counter Signatureをこのアルゴリズムで変形させたとしても、その情報は認証には使えない。

2.2 匿名化アルゴリズムの提案

手書きにおける匿名化アルゴリズムを提案する。

今回扱う手書きの筆跡は、ベクター型のデータ(vector drawing)を持つ筆跡である。vector drawingは、ユーザによってかかれた筆跡を、複数の点の集合とそれを直線で結んだ形で処理されている(図3)。

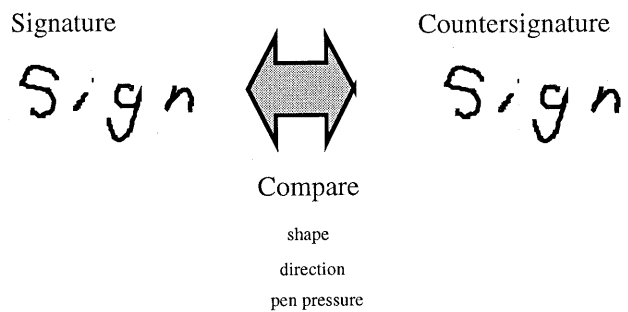


図1 認証

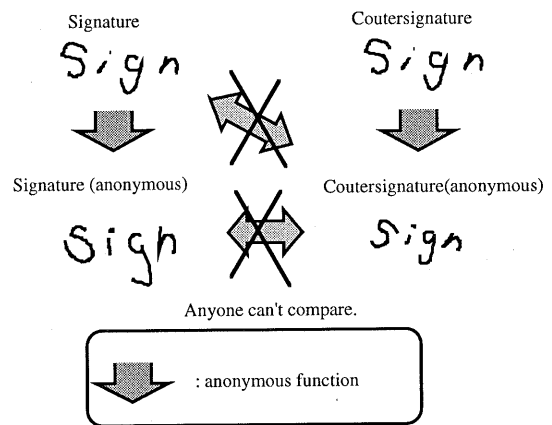


図2 手書きの匿名化

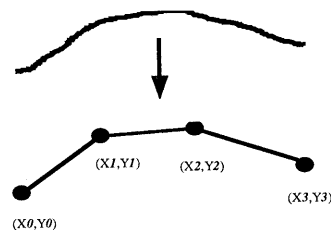


図3 ベクター型データ

Proposal of the anonymous handwriting function
Nori-hisa Segawa[†], Hiromi Gondo[†], Yasunari Nakamoto^{††},
Shinji Yamane[†], Yuko Murayama[†] and Masatoshi
Miyazaki[†]

[†]Faculty of Software and Information Science, Iwate Prefectural University

^{††}Graduate School of Information Sciences, Hiroshima City University

図3のvector drawingに対して、匿名化は、次のように行われる。

手書きによって書かれた点すべてに対して、次の演算を行い、その演算結果に対して点を移動させる。

(1)移動させる点 (X_n, Y_n) に対して、その前後の点 $(X_{n-1}, Y_{n-1}), (X_{n+1}, Y_{n+1})$ の変化量を求める。

(2)変化量に対して、ある時において生成されるユニークな値(nonce)とパラメータPをかけて、点の移動量 dX_n, dY_n を決める。

(3)移動量 dX_n, dY_n だけ点を移動させる。その後、移動した点に対して線を引きなおす。

(4)次の点に対しては、移動させた点を利用し、再計算を行う。

(1)から(4)までの一連の流れを図4に示す。

nonceは、乱数を用いて生成される。パラメータPは、匿名化アルゴリズムにおけるkeyになる変数である。

この匿名化アルゴリズムを用いることによって、人間によって書かれたvector drawingが変形される。その変形は、乱数によって決定され、2度と同じ物は生成されない。よって、人間が手書きを行なう際の特徴点が、消去され匿名化が可能となる。

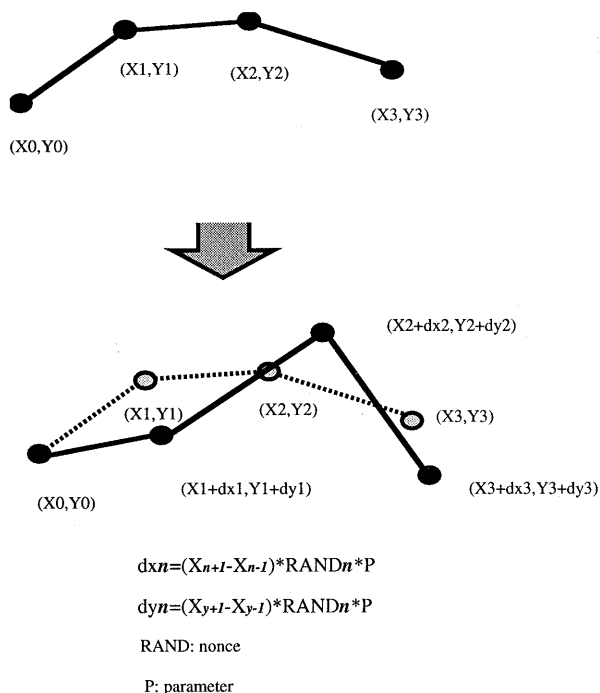


図4 匿名化アルゴリズム

2.3 実装

匿名化アルゴリズムを、Javaを利用して実装した。匿名化アルゴリズムを、手書き描画クラスの一つのメソッドとして実装を行った。

図5の左が匿名化前、図5の右が匿名後の状態である。図5の右を見てもらえばわかるように、点の位置が動くことにより(1)震えたような文字に変化(2)すこし元の形と変化がみられる。

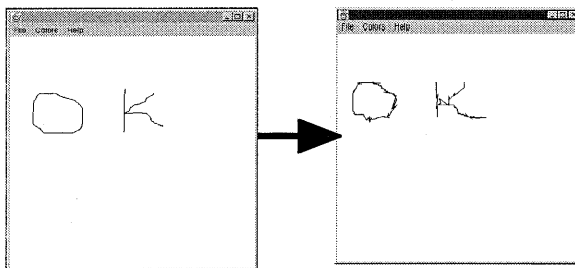


図5 匿名化アルゴリズムの実行例

3 まとめ

手書き情報に匿名化アルゴリズムをかけることによって、特徴点が変わるために従来の手書き認識アルゴリズムでは認証が不可能だと思われる。

匿名化アルゴリズムを適用した手書き情報に、認証アルゴリズムを適用し、認証ができないことを実証している最中である。また、特徴点を細かく調べるアルゴリズムに対しては、有効だと考えるが、全体の癖などを調べるものに対して使えるかどうかの評価も現在行っている。

現在のアルゴリズムでは、ある点に対して、直前、直後の2点のみから計算を行っている。認証アルゴリズムで、特徴点抽出法の場合には問題ないと考えられる。しかし、全体的な文字の癖等に対して、適用できるかどうかを調査している。その場合、ある1点の変化量を求めるのに、現在の直前、直後の2点だけではなく、あらゆる点から求められる手法を提案する予定である。

参考文献

- [1] 山崎, 小松 : バイオメトリック情報を用いた認証・機密保護機能付きテレライティングシステムに関する一検討 : 信学技法, OFS2000-10, pp9-14 (2000)
- [2] Sharath Pankanti Ruud M. Bolle and Anil Jain: Biometrics: The Future of Identification, IEEE COMPUTER, February
- [3] 山中, 浜本, 半谷 : 署名時のペンの傾きによる筆者認証, 2000年暗号と情報セキュリティ・シンポジウム (SCIS2000), SCIS2000-D6, pp1-8, (2000)