コンピュータセキュリティ 10－3
(2000. 7. 25)

戸口伝言板における匿名性の提案

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

[†††]東北大学大学院情報科学研究科

概要

戸口伝言板とは学生寮などで個人の部屋の前に置いてある伝言板のことで、本研究ではWWW上に戸口伝言板システムを設計し、プロトタイプUni Boardを開発した.

Uni BoardではWWWのブラウザーを通し,ユーザがマウス等を用いて手書きでメッセージを作成し,その情報を利用者間で交換することによってコミュニケーションを行なう.本システムの評価のためには,手書きの評価を行うことが必要となる.

本稿では、戸口伝言板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、匿名化が可能なことを示す。

Proposal of the anonymous handwriting function of an "on-door" communication system

Norihisa Segawa[†,†††] Hiromi Gondo[†] Yasunari Nakamoto[††]

Shinji Yamane[†] Yuko Murayama[†] Masatoshi Miyazaki[†]

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

[††]Graduate School of Information Science, Hiroshima City University

[†††]Graduate School of Information Science, Tohoku University

Abstract

We have tried and developed a whiteboard-type message board on the network and developed a message board system on WWW for asynchronous communication, which provides users with simple tools for drawing. On this board, any message can be written by hand, making use of mouse and tablets. Letters are coded as a collection of lines. We call this type of system an "on-door" communication system, and implemented a prototype based on our experience of the operation of such a board on the door of a room in a graduate student hall of residence.

In this paper we propose a function to make one's writng anonymous. Anonymity was one of the factors for the success of the message board in the real world.

1 はじめに

近年のインターネット技術の発達により、インターネット上で動作するコミュニケーションシステムが開発されている。特に、電子メール、WWW（World Wide Web）を用いた電子掲示板システムは、様々なシステムに搭載され幅広い人達に利用されている。

これらの電子掲示板システムは、基本的に文字情報を扱うシステムなので、情報の受け手と送り手とであらかじめ使用する文字コードについて合せる必要がある。また、文字だけではなく、図等を用いたコミュニケーションを行ないたい場合がある。

そこで、中本等によってWWWを利用した戸口伝言板システムUni Boardが開発された[1][2]。

本研究における戸口伝言板とは、学生寮等部屋のドアに設置された伝言板を指す。利用者は、伝言板の持ち主に対してメッセージを書き込めるが、部屋の持ち主だけではなく通りすがりの他の人もメッセージを読むことが出来る。

本稿では、戸口伝言板における匿名性について報告する。戸口伝言板でのメッセージは、匿名であることが重要である。部屋の前にかけてある伝言板のメッセージは、一見しただけでは誰が書いたのかはわからない。その性質を利用者がわかっているから、誰でも自由に使える戸口伝言板という使い方が成立する。WWW上で実現する際も、この特性を保証する必要がある。

以下、2章で、戸口伝言板について報告する。3章で、戸口伝言板で用いられる手書き情報の匿名化について報告する。4章で、関連研究について述べ、5章でまとめを行う。

2 戸口伝言板とは

2.1 戸口伝言板の概要

戸口伝言板とは、1章で述べたとおりに、学生寮等部屋のドアに設置された伝言板を指す。部屋の前を通った人達は、誰でも戸口伝言板を見ることが可能で、また書き込むことも可能である。伝言板を通して、伝言板の所有者、および伝言板の利用者間でコミュニケーションを行うことが可能となっている。

以下に、戸口伝言板の特徴を示す。

(1)メッセージは短く,手書きである.

(2)上書きやらくがきのように既存のメッセージへ付け足して書いて行く.

(3)一度書かれたメッセージを消すのは、掲示板の持ち主だけに限定する

(4)非同期のコミュニケーションである.

(5)誰でも読み書き可能である.

(6)読み手・書き手の匿名性が保証されている

2.2 戸口伝言板のモデル

概要を踏まえ、図1に戸口伝言板のモデルを示した。戸口伝言板においてモデルを構成する要素は、コミュニケーションの媒体となる「伝言板」と、読み書きを行う「利用者」、および伝言の受けてであり管理者でもある「部屋の住民」の3つである。

(1)伝言板 (message board)

伝言板は、利用者が書き込んだ情報を蓄積および表示する媒体であり、住民の部屋の戸口に設置される。利用者からの書き込みの他、部屋の住民からの返事なども伝言板に記録される。また、伝言板にはすべての利用者が自由に読み書きを行うことが出来る。

(2)利用者 (user)

利用者は、住民へのメッセージを持つ人の他、通りがかりの人も含んでいる。利用者は自由に伝言板をみたり、書き込むことが出来るが、書かれている情報を消すことは出来ない。利用者の匿名性は、自分で名乗らない限り保証される。

(3)部屋の住民 (resident)

部屋の住民とは伝言板の管理者であり、特別な利用者である。他の利用者は、基本的には、この住民にあてたメッセージを書き込むことになる。部屋の住民も利用者と同じく伝言板の読み書きを行うが、書き込まれた内容の消去など、管理者としての役割を持っている点が、他の利用者と異なる。

2.3 WWW上の戸口伝言板システム Uni Board

2.2章で示した戸口伝言板を、WWW上に実現した物がUni Boardである（図2）。Uni Boardは、WWW上に用意された伝言板に、利用者がマウス・タブレットを用いて、図等の手書きのメッセージを残せるシステムである。

Uni Boardはクライアントサーバ方式による実装である。クライアントは、各利用者にメッセージの表示・書き込み等の機能を与える。サーバは各利用者が手書きによって書き込んだ描画情報を管理する（図3）。これらのシステムは、Javaによって実装され、クライアントはWWWブラウザを用いることに

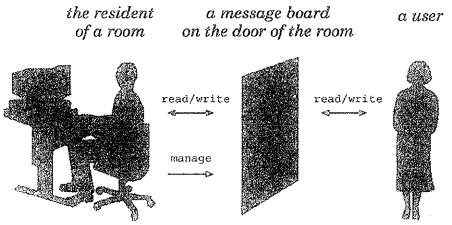


図1 戸口伝言板のモデル

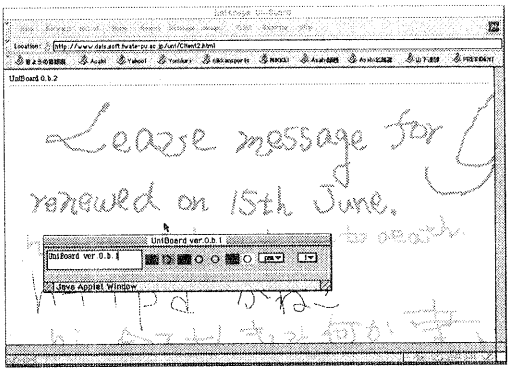


図2 Uni Board

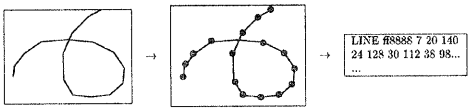


図3 描画情報（符号化）

よって実現している。各利用者は、Javaで書かれたクライアントプログラムをダウンロード、実行することによって手書きのメッセージが交換可能となっている。

手書きの線を扱うことで、1章であげた文字情報の取り扱いの問題の回避、絵の利用によるコミュニケーションの実現を可能とする。また、WWWとJavaを用いることによって、特別なソフトを利用者が用意する必要がなくなる。

3 手書きにおける匿名性

3.1 概要

現実社会における戸口伝言板において、誰が書いたのかを調べるには、筆跡鑑定を行うのに専用の知識が必要であり、一般の人が筆跡情報から誰が書いたのかを特定することは困難である。しかし、WWW上の戸口伝言板は、誰が書いたのかを調べるのに、一般人が筆跡情報をプログラム的に解析を行い誰が書いたのかを特定することが可能である。

このような状況では、WWWの戸口伝言板で自由なコミュニケーションを行うことが難しくなる。Uni Boardに手書きの匿名化機能を付加することによって、自由なコミュニケーションを行うことを保証する。

3.2 認証と匿名化

図4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[3]、文字列の傾き、筆圧[4]が利用される。戸口伝言板では、形状、傾きが筆跡情報として利用できる。

図5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。

3.3 匿名化アルゴリズムの提案

戸口伝言板における匿名化アルゴリズムを提案する。戸口伝言板では、２章の図3で示すように、手書きの筆跡をvector drawingとして処理をしている。この、vector drawingに対して匿名化アルゴリズムを適用する。

vector drawingなので、手書き情報は図6のように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6の描画情報に対して、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(Xn,Yn)に対して、その前後の点(Xn-1,Yn-1),(Xn+1,Yn+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dXn,dYnを決める。

(3)移動量dXn,dYn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7に示す。

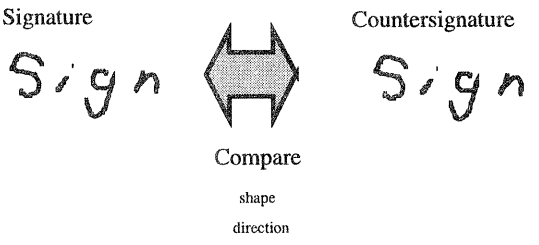


図4 認証

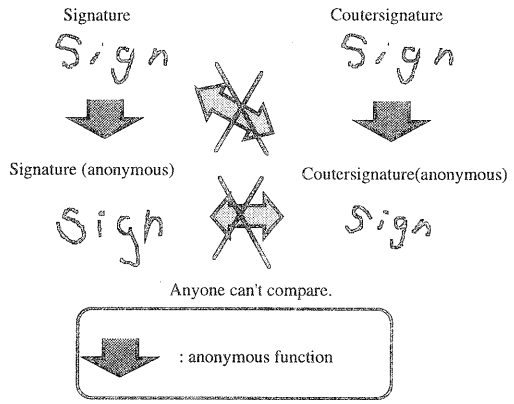


図5 手書きの匿名化

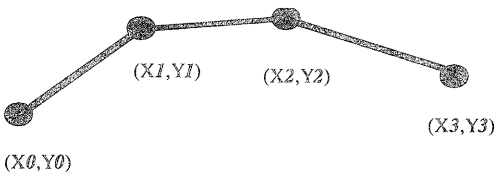
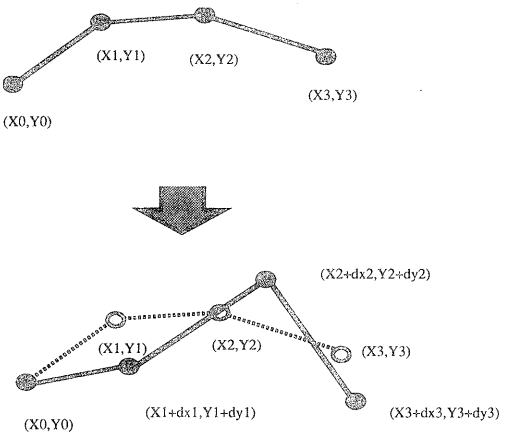


図6 vector drawingの手書き情報



$dx_n=(X_{n+1}-X_{n-1})*RAND_n*P$

$dy_n=(X_{y+1}-X_{y-1})*RAND_n*P$

RAND: nonce

P: parameter

図7 匿名化アルゴリズム

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。

3.4 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8の上が匿名化前、図8の下が匿名後の状態である。図14の下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している。

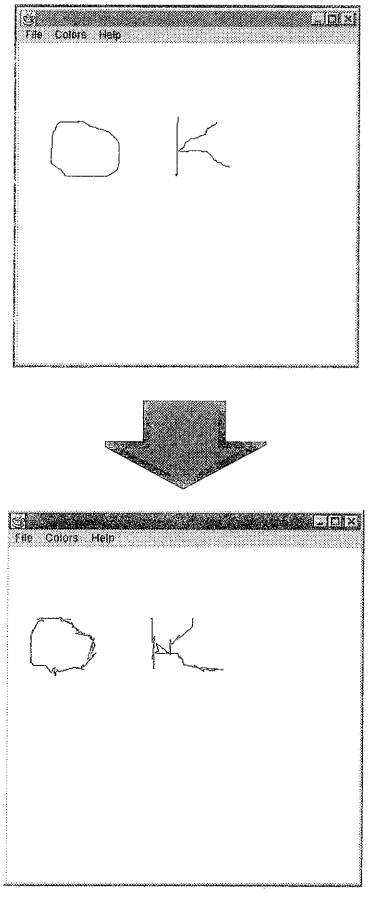


図8 匿名化アルゴリズムのJavaによる実装

図9は、図8を実現した実際のプログラムのコード（一部）である。x,yは、現在の点、nextx,nextyは現在の点より1つ先の点を表す。previousx,previousyは一つ前の点を表す。

匿名化アルゴリズムを施すことによって、本来かかれる点から変化量Xr,Yrだけずれたところに点が描画される。

また、この変化量は乱数によって決定される。Javaの乱数は最小値0、最大値1の64bitの浮動小数点で生成される。得られた乱数の値に、適当なパラメータP.get() (この場合は1.3)を掛けて変化量を決定している。

```
double xr = 0;
double yr = 0;
Parameter P;

xr =  nextx+ ((nextx - previousx) *Math.random()
*P.get());
yr =  nexty + ((nexty - priviousy)* Math.random()
*P.get());
x = (int) xr;
y = (int) yr;

g.drawLine(priviousx,priviousy,x,y);
```

図9 匿名化アルゴリズムのJavaのソースコード（一部）

3.5考察

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、特徴点が変化す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。

また、このアルゴリズムの今後の改良点として次のことを上げている。

(1)パラメータPの設定

匿名化アルゴリズムは、パラメータPの値をどのように決定するかが重要である。なぜなら、パラメータPの値が0に近づくと、変化量が0になり、匿名化が行われない。大きすぎる場合には、変化量がおおきすぎ、元の文字、図形が判別できなくなり、実用性が失われる（図10）

匿名化アルゴリズムは、(1)点と点の間隔(2)nonce（0-1の値）(3)パラメータPの積で求められる。よって、nonceはたかだか1とした場合、(1)点と点の間隔と(3)パラメータPの値の関係によって決まってくる。

ある人が、手書きを行う際に点と点の間隔が極端に長い人（手書きの動作が早い人）は、パラメータの値を大きくしすぎると、変化量が大きくなりすぎ読めなくなってしまう。逆に、間隔が極端に短い人（手書きの動作が遅い人）は、変化量が小さくなり

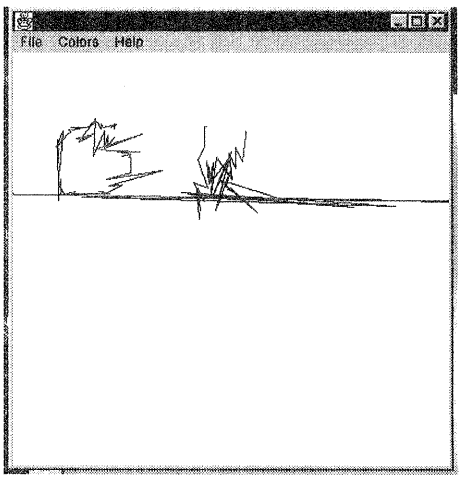


図10 パラメータPの値を2にした場合

すぎ匿名化がほとんど行われなくなってしまう。

現在、筆跡情報からパラメータPを生成するアルゴリズムを考案中である。

(2)全体的なデータの処理方法

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。

4他の研究との比較

その筆跡の癖を認証に利用することは、biometricsの分野で幅広く研究されている[3][4][5]。

この手書きを利用した認証は、認証精度が非常に高いことが実証されており、securityの分野で幅広く使われつつある[6]。

しかし、暗号の技法には数千年の歴史がある[7]が、手書きにおける匿名性はこれまで研究の対象として議論されていない。

匿名性を保ちつつコミュニケーションを行なう本稿と類似した研究として、digital pseudonym[8] やanonymous message broadcast[9]についての研究がある。しかし、それらの手法では手書きにおける匿名性を保証することはできない。traffic analysis に対して個人を特定する情報を保護できるが、手書きにおいて個人を特定する情報は保護できないためである。

本稿に近いもう一つの研究として、会話の暗号化についての研究が挙げられる。音声情報を暗号化する voice scrambler については20世紀初頭から研究が進められてきた[10]。しかしながら、それらの研究は通信内容の機密保持のための暗号化/復号化を目的としたものであり、匿名性を保ちつつ多数の人間とコミュニケーションを行うための研究は考慮されてこなかった。

このように本論は従来の研究に対してユニークなアプローチをとっている。

5まとめ

本稿では、戸口伝言板における手書きの匿名性の提案を行った。手書きの描画情報を、匿名化アルゴリズムを用いて処理を行うと、認証アルゴリズムにかけることが、困難であるということを示した。また、このアルゴリズムをJavaで実装した。

今後は、匿名化アルゴリズムの改良、および、匿名化の定量的な評価手法の提案を行っていきたい。

参考文献

[1]村山 優子, 中本 泰然:WWW上の戸口伝言板の実現, 情報処理学会DICOMO'99論文集,pp.339-344(1999)

[2]村山 優子, 中本 泰然, 瀬川 典久, 権藤 広海, 宮崎正俊: WWWを用いた戸口伝言板システムUni Boardの概要,第59回情報処理学会全国大会論文集CD-ROM,3ZB-3,(1999)

[3] 山崎 恭,小松 尚久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)

[4]Sharath Pankanti Ruud M. Bolle and Anil Jain: Biometrics: The Future of Identification, IEEE COMPUTER, February

[5] 山中 , 浜本 隆之, 半谷 精一郎: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)

[6]Signature Verification, Cyber SIGN Incorporated: http://www.cybersign.com/techoverview_what.htm#signatureverification

[7] Chaum, D. Security without identification: Transaction systems to make Big Brother obsolete. CACM Vol. 28, No. 10 pp 1030-1044,(Oct. 1985

[8] Diffie, W., and Landau, S. Privacy on the Line: The Politics of Wiretapping and Encryption. MIT Press, 1998, ch. 3 & 9.

[9] Kahn, D. The Codebreakers: The Story of Secret Writing, Revised ed. Scribner, New York, 1996. Originally published in 1967.

[10] Schneier, B. Applied Cryptography, 2nd ed. John Wiley & Sons, (1996).