推薦論文

戸口伝言板における匿名化の提案

瀬川典久[†,☆] 村山優子[†] 権藤広海[††]
山根信二[†] 宮崎正俊[†]

WWW（World Wide Web）上で動作するコミュニケーションシステムの 1 つである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たちに利用されている．これらのシステムの多くは，文字情報の交換を基本としている．そのため，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意する必要があり，さらに，図などを用いることができない．本研究では，文字コードによらないエンターテイメントコミュニケーションのための手書き伝言板システム「戸口伝言板」をWWW 上に実装した．戸口伝言板とは，学生寮などで個人の部屋の扉に設置した伝言板のことである．実装したプロトタイプシステムでは，ユーザがマウスなどを用いて手書きでメッセージを作成する．このようなシステムでは自由で活発なコミュニケーションのために匿名性が必要となる．従来の電子掲示板のメッセージは，利用者自身が明らかにしない場合，匿名性が保証される．戸口伝言板では，利用者が手書きのメッセージを伝言板に残すため，筆跡から書き手を特定される恐れがある．本論文では，戸口伝言板のような手書きのメディアにおけるメッセージの匿名化について報告する．筆跡から書き手を特定できないようにするためには，書き手の筆跡の癖をその筆跡から取り除くことが必要であるが，同時に筆跡を取り除いた後のメッセージは読める形でなければならない．本論文では，筆跡における匿名化アルゴリズムを提案し，実装した．ユーザによる利用実験により匿名化アルゴリズムの評価を行い，その有効性を確認した．

Proposal of the Anonymous Handwriting Function of an “On-Door” Communication System

Norihisa Segawa,[†,☆] Yuko Murayama,[†] Hiromi Gondo,[††]
Shinji Yamane[†] and Masatoshi Miyazaki[†]

Message board systems are used extensively over the world wide web (WWW). Most of the systems provide users with communications using character codes, hence, they need to agree on what codes to be used. Figures cannot be used as well. We have tried and developed a whiteboard-type message board on the network and developed a message board system on WWW for entertainment communications, 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. Anonymity was one of the factors for the success of such a system. In this paper we report an anonymity of message on a handwriting media. Handwritten messages need to be readable even if we remove any specific individual characteristics from them. We propose such an algorithm and report our implementation. The evaluation of the algorithm is presented as well in terms of user’s viewpoints.

1. はじめに

近年インターネット上で動作する様々なコミュニケーションシステムが開発されている．それらの 1 つである，WWW（World Wide Web）を用いた電子掲示

† 岩手県立大学ソフトウェア情報学部
Faculty of Software and Information Science, Iwate Prefectural University
†† 岩手県立大学大学院ソフトウェア情報学研究科
Graduate School of Software and Information Science, Iwate Prefectural University
☆ 現在，東北大学大学院情報科学研究科
Presently with Graduate School of Information Science, Tohoku University

本論文の内容は 2000 年 7 月のコンピュータセキュリティ研究会にて報告され，CSEC 研究会主査により情報処理学会論文誌への掲載が推薦された論文である．

板システムは，幅広い人たちに利用されている．これらの電子掲示板システムは，文字情報の交換を基本としているため，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意する必要がある．さらにそれらのシステムでは，図などを用いることができない．

本研究では WWW 上に戸口伝言板という手書きの伝言板システムを設計および実装した[1)~3)]．プロトタイプシステムでは，ユーザはマウスなどを用いて手書きでメッセージを作成し，他のユーザとコミュニケーションを行う．

戸口伝言板とは学生寮などの個人の部屋の戸口にとりつけた伝言板で，それを通して匿名の複数の受信者および発信者で行うコミュニケーションが実現する．実際の戸口伝言板は，ロンドン大学大学院生のための寮において筆者の 1 人の部屋の扉に設置した．寮は約 500 人ほどの学生や研究者を収容し，当該筆者の部屋はエレベータ前に位置していた．本来，戸口伝言板のメッセージはその戸口の部屋の住民に宛てられるはずであった．しかし，実際の運用では，戸口の部屋の住人に関係のないメッセージの交換に利用されるようになった．書き手は匿名で「ドラキュラ」などと実際と異なる名前で出現し，ゲーム感覚のやりとりを繰り広げ，不特定多数の読み手の興味を誘い，さらに参加者が増えることとなった．

学生寮における運用では，書き手の匿名性を尊重するために，部屋の住民が自分の部屋を出るときには，外部の書き手に注意を促すために部屋の中からわざわざノックをすることとなった．書き手と読み手の間に通信される内容は，本来の住民相手のメッセージというよりも，他人を楽しませるための新しいマスメディアとして展開し，多対多のエンタテイメントコミュニケーションのためのメディアの要素が強くなった．このようなメディアを WWW 上に構築することが戸口伝言板の研究目的である．本論文では，戸口伝言板などの手書きメディアにおける匿名性について報告する．

一般にメッセージの匿名化については，送信者はその内容により，暴力を受けたり，社会的地位を失ったりするなどの危険を冒さずに情報を発信できるといわれている[4)]．たとえば，新聞の投稿において匿名にするものもある．匿名性は，送信者の社会的背景（性別，年齢，身分など）に左右されずにコミュニケーションを行うためにも利用される．現在利用されている匿名を利用できる電子会議システムでは，ユーザが身分などによる発言力の差を意識せずに，コミュニケーションを行える．匿名化をしないシステムでは，参加者はそれぞれの社会的に応じたコミュニケーションを行うために，発言内容に制限が加わる．

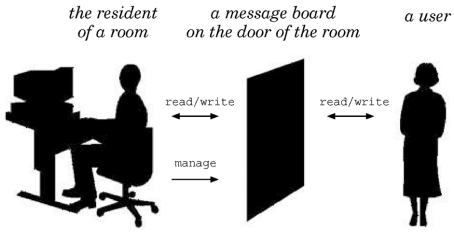

図 1 戸口伝言板のモデル
Fig. 1 On-Door Communication model.

WWW で利用されている文字情報を利用した電子掲示板では，利用者自身が明らかにしない場合，メッセージの送信者の匿名性が保証される．掲示板システムが送信者の個人情報を第三者に公表しない限り，匿名性は保証される[5)]．ところが，戸口伝言板では，手書きのメッセージの筆跡の癖から書き手を特定される恐れがある．匿名化のためには，書き手の筆跡の癖をそのメッセージから取り除くとともに元のメッセージの内容は読めなければならない．本論文では筆跡の匿名化アルゴリズムを提案し実装した．ユーザによる利用実験を行い，アルゴリズムの有効性を検証する．

以下，2 章で，戸口伝言板システムを紹介し，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 章では，本論文の匿名化の手法についての評価について述べる，5 章で関連研究について述べ，6 章でまとめを行う．

2. 戸口伝言板システム

2.1 戸口伝言板の概要

戸口伝言板では，部屋の前を通った人たちは，誰でも伝言板上のメッセージ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（**図 1**）．

戸口伝言板は，利用者が手書きで短いメッセージを伝言板に残すためのものである．伝言板を利用できる誰もが，上書きや落書きのように既存のメッセージへ付け足して書いていくが，伝言板の所有者だけが，書かれたメッセージを消すことができる．戸口伝言板は，伝言板を利用する人の間での，メッセージの書き手，読み手の匿名性は保証される．つまり，伝言板には，メッセージそのものしか表示されず，そのメッセージを誰がいつ見たかという情報も残されない．

2.2 WWW 上の戸口伝言板システム

WWW 上に戸口伝言板のプロトタイプシステムを

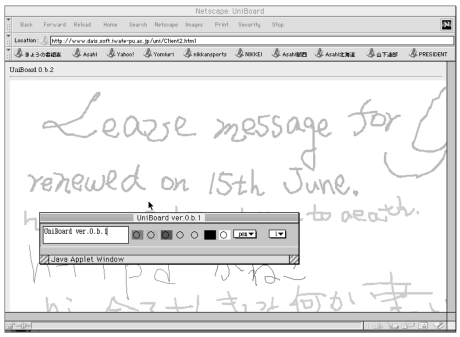

図 2 戸口伝言板のプロトタイプシステム
Fig. 2 Prototype system of On-Door Communication.

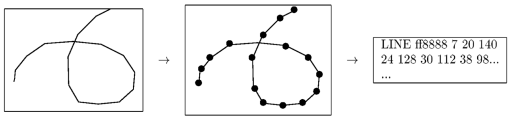

図 3 描画情報（符号化）
Fig. 3 Information drawing (encoding).

クライアントサーバ型で実装した（**図 2**）．本システムは，WWW 上に用意された伝言板に，ユーザがマウス・タブレットを用いて，手書きのメッセージを残す．

クライアントは，ユーザにメッセージの表示・書き込みなどの機能を提供する．サーバはユーザが手書きの情報を管理する．サーバは，Java アプリケーション，クライアントは Java Applet として実装した．ユーザでは，WWW ブラウザを通して自動的にクライアントプログラムをダウンロードし，実行する．

メッセージは，直線の集合として符号化される（**図 3**）．手書きにおける 1 画すなわちペンをおろして書いたものが，1 行の筆跡情報として表される．利用者の手書きによって作られた筆跡に対して，一定時間ごとにサンプリングを行い，(1) 複数の座標点と，(2) その複数の座標点をつなぐ図形を取り出す．その複数の座標点と，座標点をつなぐ図形情報が符号化される．符号化されたデータが，本研究で扱う筆跡情報になる．1 行の筆跡情報は，(A) データの形式，(B) 色，(C) 線の太さ，(D) 点の座標情報（X，Y 座標の集合）が含まれている．

3. 手書きにおける匿名性

3.1 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（Counter Signature）との特徴点による照合によって行われる．利用される特徴点として，形状[6]，文字列の傾き，筆圧[7]

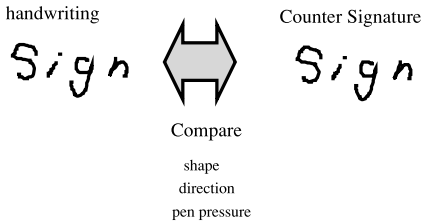

図 4 認証
Fig. 4 Authentication.

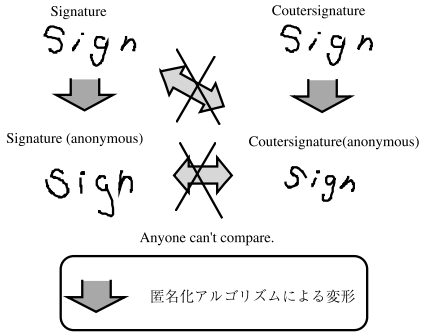

図 5 手書きの匿名化
Fig. 5 Anonymity of information drawing.

があげられる．手書きのメッセージからは，形状，傾きの筆跡情報を得ることができる．

筆跡を匿名化するためには，筆跡から書き手を特定する特徴点を消し，なおかつ第三者がそのメッセージを判読することが可能である必要がある．このことを解決するために，筆跡を一方向アルゴリズムと乱数より変形を行う（**図 5**）．一方向アルゴリズムは，変形した筆跡から，元の筆跡を復元できないようにするために必要である．また，この変形は乱数を用いて行うので 2 度と同じ変形は不可能である．つまり，Signature とこのアルゴリズムで変形させた Counter Signature は，異なる形になり，Counter Signature を認証に利用することができなくなる．

3.2 匿名化アルゴリズムの提案

戸口伝言板では，図 3 で示すように，手書きの筆跡に vector drawing 型の符号化を行っている．手書き情報は複数の点とそれらを直線で結んだ形で符号化されている．戸口伝言板上のメッセージの匿名化アルゴリズムを以下に提案する．

描画情報に対して，3.1 節で記したように，一方向アルゴリズムと乱数により変形させる．

アルゴリズムは以下のとおりである．

手書きによって書かれた点に対して，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

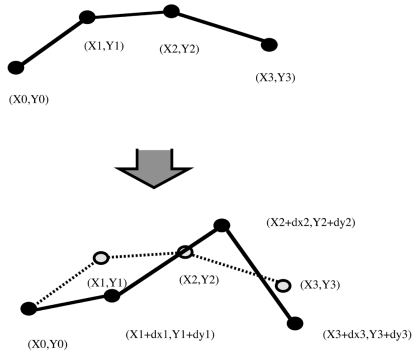

図 6 匿名化アルゴリズム
Fig. 6 Algorithm of anonymity.

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，あるときにおいて生成されるユニークな値 $nonce$ $(0 \leq nonce \leq 1)$ とパラメータ P $(0 \leq P)$ 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 6** 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鍵になる変数である．パラメータ P の値については，4.1 節で解説する．

移動量の絶対値は，$0 \leq |dX_n| \leq (X_{n+1} - X_{n-1}) \cdot P \cdot nonce$，$0 \leq |dY_n| \leq (Y_{n+1} - Y_{n-1}) \cdot P \cdot nonce$ となる．nonce の値は，$(0 \leq \text{nonce} \leq 1)$ なので，移動量の絶対値の最大値は $(|dX_n|, |dY_n|) = (|(X_{n+1} - X_{n-1}) * P|, |(Y_{n+1} - Y_{n-1}) * P|)$ となる．よって，移動量の絶対値の大きさは，前後の点の間隔とパラメータ P の値の積に影響する．前後の点の間隔が大きくなりすぎると，書いた文字などが読めなくなってしまい，0 に近づくと筆跡は変化しない．前後の点の間隔は，ユーザによって異なるので，書いたメッセージが第三者にも読めるように，ユーザはパラメータ P の値を決定する．

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 度と同じものは生成されない．人間が手書きを行う際の特徴点が，消去され匿名化が可能となる．

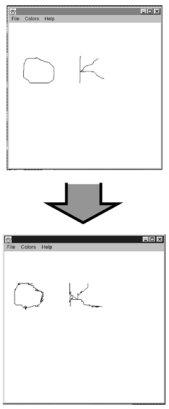

図 7 匿名化アルゴリズムの Java による実装
Fig. 7 Sample implement of algorithm of anonymity by Java.

```
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 8 匿名化アルゴリズムの Java のソースコード（一部）
Fig. 8 A part of source code of algorithm of anonymity by Java.

3.3 実　　装

匿名化アルゴリズムを，Java により，手書き描画クラスの 1 つのメソッドとして実装を行った．

図 7 の上が匿名化前，図 7 の下が匿名後の状態である．図 7 の下を見てもらえば分かるように，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) 元の形と少し変化している．

図 8 は，図 7 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 1 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，本来書かれた点から変化量 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．乱数

は最小値 0，最大値 1 の 64 bit 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()（この筆跡の書き手の場合は，1.3）を掛けて変化量を決定している．P.get は，パラメータ値 P を取り出すメソッドである．

4. 匿名化アルゴリズムの評価

匿名化アルゴリズムの有効性を示すには，書き手が送信するメッセージの匿名化が可能と認識し，なおかつ第三者がそのメッセージの書き手を特定できないことを示す必要がある．匿名化アルゴリズムを利用した戸口伝言板を用いて，書き手および読み手それぞれの観点からユーザによる評価実験を行った．今回の実験では，コンピュータのマウスの操作の慣れ，不慣れの影響が，実験結果に反映されないようにするために，岩手県立大学ソフトウェア情報学部の学生を被験者とした．マウスの操作に慣れていない場合，操作の誤りの影響が筆跡に加わり，匿名化アルゴリズムの評価が正しく行えないからである．

4.1 書き手の評価実験

書き手の評価実験は，21 人の被験者に，戸口伝言板を利用して，伝言板に描かれているメッセージが匿名化されているかどうかを判定してもらった．

被験者に対しては次のような実験を行った．

(1) 実験者は，匿名化アルゴリズムを利用した匿名機能つき戸口伝言板を用意する．その際に，匿名化アルゴリズムにおけるパラメータ P を，0.1 から 2 まで 0.1 間隔で可変にしておく．
(2) 被験者が，戸口伝言板に「永」という文字を書く.「永」という字は，縦線横線，斜めの線をすべて含んでおり，筆跡の変化を考察するのに適していると考えた．
(3) 文字を書き終わった後，被験者が普段書く字と比べて，文字が判別できて，なおかつ自分の筆跡ではないかどうかを判定してもらう．
(4) (2)，(3) について，パラメータ P を 0.1 から 2 まで変化させて実験を行う．

被験者が，文字が判別できて，自分の筆跡とは見えないと判別した場合，戸口伝言板における匿名化機能がうまく働いたと考えることができる．被験者が，文字を読めなかった場合，また，読めたとしても被験者自身の筆跡と判断した場合には，匿名化機能が働かなかったと考える．

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，変化量が大きすぎ，元の文字，図形が判別できなくなり，実用性が失われる（**図 9**）．つまりパラメータ P の値を変えることは，筆跡の変化の度合いを変化させることである．利用者によって，筆跡の変化と匿名化の関係がどのようになるかを調べる．

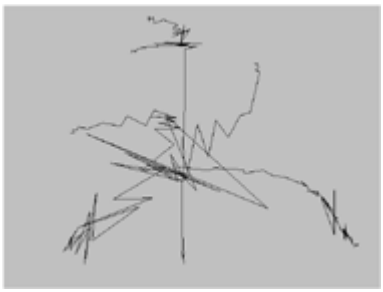

図 9 ある被験者において，匿名化アルゴリズムにおけるパラメータ P の値を 2 にした場合
Fig. 9 In case of parameter P = 2.

以下に結果および考察を述べる．

図 10 は，被験者 21 人に対する実験結果である．被験者 21 人中，1 人だけ（被験者 E）は匿名化が行われなかったと判断した．本論文で示したアルゴリズムで，匿名化が行われたと判断した人数は，約 95%である．このことから本アルゴリズムは，有効な手法と考えられる．

被験者のうち 1 人が，どのパラメータ P の値でも匿名化が行われなかった．匿名化アルゴリズムによって計算される点の移動量は，(1) 移動する前後の点の座標値の差，(2) nonce ($0 \leq nonce \leq 1$)，(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，移動量は，(1) 移動する前後の点の座標値の差と (3) パラメータ P の値の関係によって決まってくる．

パラメータ P をどのように変化させても筆跡が変化しないことは，移動する点の前後の点の座標値の差が生じないときに起きる．つまり，当該被験者はほかのユーザに比べて極端に手書きの動作が遅かったと考えられる．戸口伝言板の現在のプロトタイプシステムでは，極端に遅く手書きをすることによって，サンプリング点の間隔がほぼ 0 に近くなり，移動量が 0 に近くなるため，匿名化が行われない．この点は，今後の課題である．

また，パラメータ P が 1.7 および 1.8 のとき，13 人（65%）が匿名化が行われたと判断した．また，被験者 E の 1 人を除いた 20 人すべてが，パラメータ P の値が 1.4〜1.9 の中に 1 つは匿名化が行われると判

被験者	パラメータP 0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0	1.1	1.2	1.3	1.4	1.5	1.6	1.7	1.8	1.9	2.0	計
A																			○		1
B																○	○	○	○		4
C																	○				1
D																		○	○		2
E																					0
F															○	○	○	○			4
G																○	○	○			3
H																		○	○		2
I																	○	○			2
J													○	○	○	○	○				5
K															○	○	○				3
L													○	○	○						3
M														○	○						2
N																	○	○			2
O																	○	○			2
P														○	○	○	○	○	○		6
Q																		○	○		2
R														○	○	○	○	○	○		6
S	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	20
T	○	○	○	○	○	○	○	○	○	○	○	○	○	○							14
U														○	○	○	○	○	○	○	7
合計延べ人数	2	2	2	2	2	2	2	2	2	2	2	2	4	8	9	9	13	13	9	2	

○:被験者が匿名化したと判断した物

被験者が匿名化したと判断した筆跡の数の平均= 4.3
標準偏差= 4.67

全被験者によるパラメータPの加重平均= 1.39
標準偏差= 0.692358

図 10 書き手の評価実験の結果
Fig. 10 The result of an evaluation experiment of writers.

書き手		A	B	C	D	E	F	G	H	I	J	K	L	M	N
匿名化された筆跡		No.1	No.2	No.3	No.4	No.5	No.6	No.7	No.8	No.9	No.10	No.11	No.12	No.13	No.14
被験者	A		●	●	○	●	●	●	●	●	●	●	●	●	●
	B	●		○	●	●	●	●	●	●	●	●	●	●	○
	C	●	●		●	●	●	●	●	●	●	●	●	●	●
	D	●	●	●		●	●	○	●	●	●	●	●	●	○
	E	●	●	●	●		●	●	○	●	●	●	●	●	●
	F	●	●	●	●	○		●	○	●	○	●	●	●	○
	G	○	●	●	●	●	●		●	●	●	●	●	●	●
	H	●	●	●	○	○	●	●		●	○	○	●	●	●
	I	○	●	●	●	●	●	●	●		●	●	●	●	○
	J	●	●	●	●	●	○	●	●	●		●	○	●	●
	K	●	●	●	●	●	●	●	○	●	●		●	○	●
	L	●	●	●	●	○	●	●	●	●	●	●		○	●
	M	○	●	●	○	●	●	●	●	●	●	●	●		●
	N	○	●	○	●	●	●	●	○	●	●	●	○	●	
筆跡に対する認識率 (%)		30.77	0	15.38	23.08	23.08	7.692	7.692	30.77	0	15.38	7.692	15.38	15.38	30.77
パラメータP		1.1	1.7	1.8	1.4	2	1.8	1.7	1.4	1.9	1.6	1.6	1.8	1.7	1.6

○:書き手が特定可能
●:書き手が特定不可能

筆跡に対する認識率の平均値(%): 15.93406593 標準偏差 10.65

図 11 読み手の評価実験の結果
Fig. 11 The result of an evaluation experiment of readers.

断した．したがって，このアルゴリズムでほぼ大多数の人の匿名化が可能であり，しかも筆跡の変化の度合いを利用者ごとにそれぞれ用意する必要がないことが分かった．

4.2 読み手による認証実験による評価

読み手の評価実験は，14 人の被験者による戸口伝言板を利用して書かれたメッセージの読み手の被人認証である．

被験者に対しては次のような実験を行った．

(1) 実験者は，匿名化アルゴリズムを利用した匿名機能つき戸口伝言板を用意する．

(2) 被験者が，戸口伝言板に「永」という文字を書く．パラメータ P の値は，書き手が匿名化可能と考える P の値の中で最大値を利用する．

(3) 匿名化前の筆跡と，匿名化後の筆跡を紙に印刷する．

(4) 被験者すべての元の筆跡と匿名化後の筆跡をそれぞれ順不同並べ，同じ書き手が書いたと思われる匿名化前の筆跡と匿名化後の筆跡の組合せを答えてもらう．ただし，被験者本人によって書

全筆跡のパラメータPの平均値	1.65
認識率が，全体の平均値より高い筆跡におけるパラメータPの平均値	1.5
認識率が，全体の平均値より低い筆跡におけるパラメータPの平均値	1.73
認識率が，被験者が一切筆跡を見ずに書き手を特定する場合の認識率の値より高い筆跡におけるパラメータPの平均値	1.6
認識率が，被験者が一切筆跡を見ずに書き手を特定する場合の認識率の値より低い筆跡におけるパラメータPの平均値	1.74

図 12 認識率とパラメータ P の関係
Fig. 12 Relation between the rate of recognition and parameter P.

かれた筆跡とその匿名化したものは，実験データから除外する．被験者が，記憶を利用して筆跡とその匿名化したものの関係を答えられるからである．

もし匿名化が行われていれば，被験者は書き手を特定できない．14 の匿名化された筆跡が，13 人の認証によって，どの程度書き手が特定されないのかを評価する．

以下に，結果および考察を述べる．

図 11 は，14 の筆跡に対する実験結果である．ここでいう認識とは，認証によって書き手が特定されたことをいう．認識率は，(書き手を特定することができた人数)/(認証した人数) × 100 と定義する．14 の筆跡に対して，認識率は平均約 15.9%である．被験者が，いっさい筆跡を見ずに書き手を特定する期待値は 1 人☆であり，この場合の認識率は，8%である．この値は，匿名化アルゴリズムの手法で行った認識率とほぼ近い．この結果から，匿名化アルゴリズムは有効であることが分かる．

図 12 は，筆跡の認識率とパラメータ P の値の関係の関係を示したものである．認識率が平均より低い筆跡におけるパラメータ P の平均値を見ると，高いものに比べて 0.2 高くなっている．また同様に，認識率が，被験者がいっさい筆跡を見ずに書き手を特定する場合の認識率の値より低い筆跡における，パラメータ P の平均値を見ると，高いものに比べて 0.14 高くなっている．パラメータ P の値は，筆跡の変化の大きさを決めるパラメータである．よって，筆跡の変化が大きいほど，元の筆跡を特定することが困難になり，書き手の特定が困難であると考えられる．

4.3 実験による匿名化アルゴリズムの評価

2 つの実験から，ユーザレベルでは，提案する匿名化アルゴリズムにより，書き手はメッセージの匿名化が可能であると認識でき，第三者は書き手の特定が困難であると考えられる．したがって，この匿名化アルゴリズムは，戸口伝言板での利用が十分可能であると判断できる．

4.4 他の手法との比較

手書きによる筆跡を匿名化する手段として，文字認識[11] を利用した手法がある．

文字認識を用いた手法とは，手書きの筆跡から文字認識を行い，その結果を利用して文字コードに変換する手法である．この手法の利点は，文字に変換されるために文字認識が正しく行われれば，確実に匿名化が可能である．この手法には，文字認識と言語の次のような問題がある．

書き手が，画面上の自由な領域に文字の手書きを行い，その手書きを文字認識させる場合，認識率は約 85〜95%である．文字と記号を混在させた場合，その認識はさらに難しくなる（たとえば，0 と O と○の区別）[12]．システムが誤認識したとき，ユーザは再度筆跡を入力する必要がある．また，文字認識を行わせるためには，文字認識を行うプログラムを組み込む必要がある．

手書きの筆跡から文字認識を行うと，その結果を利用して文字コードに変換する必要がある．しかし，利用するシステムに文字コードが存在しない場合には，この手法は利用できない．世界には，約 6000[10] もの言語が存在し，そのほとんどには文字コードが割り当てられていない．これらすべての言語に対して，文字コードを用意することは現実的ではない．

戸口伝言板は，世界中の人々が WWW ブラウザと Java だけを利用して言語コードの変換なしにメッセージを交換できるシステムである．この特徴のために，インターネットさえつながれば，世界中のどのような言語メッセージでも交換することができる．

したがって，言語コードに依存する文字認識の手法は，戸口伝言板には適さない．

このことから，戸口伝言板においては，文字認識の手法を採用せずに，本論文での手法を採用する方が適している．

4.5 匿名化アルゴリズムを用いた伝言板の運用に関する問題

匿名を利用してメッセージを送信できる伝言板では，匿名性を悪用し，第三者への中傷などの攻撃や，いたずら書きなどが可能である[4]．

匿名化前の筆跡をサーバに保持しておけば，筆跡を頼りに書き手を特定することも可能である．また，匿名化前の筆跡を一般には公開しないがサーバに保持していることを，ユーザに告知しておけば，いたずら書きに対しての抑止力になると考えられる．

☆ この値は，完全順列を利用した解法で得られる．導出は付録に記述した．

5. 関連研究

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[6)~8)]．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[9)]．

暗号の技法には数千年の歴史がある[13)]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う本論文と類似した研究として，digital pseudonym [14)] や anonymous message broadcast [15)] についての研究がある．digtal pseudonym とは，電子的なコミュニケーション環境における，仮名を利用した匿名化手法の 1 つである．anonymous message broadcast とは，ネットワーク通信において送信者と受信者がトレースできない通信手法の 1 つである．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，筆跡に対して個人を特定する情報は保護できないためである．

本論文に近いもう 1 つの研究として，会話の暗号化についての研究があげられる．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[16)]．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，本研究のように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ではない．

6. まとめ

本論文では，戸口伝言板における手書きの匿名性の提案を行った．手書きの描画情報が，匿名化アルゴリズムによって変形され，筆跡の特徴点での筆跡の比較が困難になることを示した．また，このアルゴリズムを Java で実装した．また，このアルゴリズムの利用者による評価実験を行い，このアルゴリズムの有効性を示した．

今後の課題は，筆跡の傾向を利用した匿名化アルゴリズムと認証アルゴリズムを利用した匿名化アルゴリズムの評価である．

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．このアルゴリズムの欠点としては，標本加速度に近くゆっくりと手書きを行う場合匿名化が行われにくくなる．そのために，対象となる元の点の前後の 2 点についてだけではなく，より広い範囲の点を利用して匿名化を行うアルゴリズムの開発が必要である．

また，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する．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行いたい．

謝辞 戸口伝言板の利用にあたり様々なご協力をいただいた広島市立大学の中本泰然氏に感謝いたします．評価実験をお手伝いいただいた岩手県立大学ソフトウェア情報学部コミュニケーション学講座の学生諸君に感謝いたします．また，本研究を進めるにあたり様々なご助言をいただいた情報処理学会コンピュータセキュリティ研究会の皆様につつしんで感謝いたします．

参考文献

1) 村山，中本：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) Segawa, N., Murayama, Y., Nakamoto, Y., Gondo, H. and Miyazaki, M.: A Message Board on WWW for On-Door Communication, *Proceedings of ACM Multimedia '99* (part 2), pp.187–190 (1999).
3) Murayama, Y., Gondo, H., Nakamoto, Y., Segawa, N. and Miyazaki, M.: Vusualization of Time in a Message Board System on WWW for On-Door Communication, *Hawaii International Conference on System Sciences (HICSS-34)*, p.20 (CD-ROM of Full paper), IEEE Computer Society (2001).
4) 川浦：匿名社会と人間関係，こころの科学，Vol.58, pp.2–6 (1994).
http://revir.cc.yokohama-cu.ac.jp/work/anonym/ANONYM.html
5) 2 ちゃんねる．http://www.2ch.net/
6) 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, pp.9–14 (2000).
7) Pankanti, S., Bolle, R.M. and Jain, A.: Biometrics: The Future of Identification, *IEEE Computer*, February 2000 (2000).
8) 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, pp.1–8 (2000).
9) Signature Verification, Cyber SIGN Inc..
http://www.cybersign.co.jp/tech/syogo.html
（2001 年 10 月を参照）
10) 津曲：言語の危機と 21 世紀言語学の課題，日本言語学会第 122 回大会シンポジウム講演 (2001).

http://www.osaka-gu.ac.jp/php/miyaoka/elpr/essay/tsumagari.htm
11) Rèjean, P. and Srihari, S.N.: On-Line and Off-Line Handwriting Recognition: A Comprehensive Survey, *IEEE Trans. Pattern Analysis and Machine Intelligence*, Vol.22, No.1, pp.63-84 (2000).
12) 豊原，佐賀：ファジイスプライン曲線の分割処理に基づく書描弁別法の提案，日本ソフトウェア科学会 WISS2000 CD-ROM (2000).
13) Chaum, D.: Security without identification: Transaction systems to make Big Brother obsolete, *CACM*, Vol.28, No.10, pp.1030–1044, (1985).
14) Kahn, D.: *The Codebreakers: The Story of Secret Writing*, Revised ed., Scribner, New York (1996). Originally published in 1967.
15) Schneier, B.: *Applied Cryptography*, 2nd ed., John Wiley and Sons (1996).
16) Diffie, W. and Landau, S.: *Privacy on the Line: The Politics of Wiretapping and Encryption*, ch.3 and ch.9, MIT Press (1998).
17) 馬場：確率論，放送大学教材，pp.36–43 (1997).

付録　完全順列を利用した解法

この問題は，13 個の匿名化した筆跡とその書き手の組合せをランダムに決めた場合の正解した数の期待値を求める問題と同意である．この問題は，完全順列の概念を利用して解くことができる[17]．

n 個の匿名化した筆跡とその書き手の組合せが k 個正解する筆跡と書き手の組合せを $g(n,k)$ $(0 < n, 0 \leq k \leq n)$ とするとき，$g(n,k)$ は，次式で定義される．

$$g(n,n) = 1 \tag{1}$$
$$g(n,n-1) = 0 \tag{2}$$
$$g(1,0) = 0 \tag{3}$$
$$g(2,0) = 1 \tag{4}$$
$$g(n,0) = (n-1)\cdot\{g(n-1,0) + g(n-2,0)\} \quad (3 \leq n) \tag{5}$$
$$g(n,k) = {}_nC_k \cdot g(n-k,0) \quad (1 \leq k \leq n-2) \tag{6}$$

式 (1) は，筆跡と書き手の組合せがすべて正解の場合で，それは 1 通りしかない．

式 (2) は，$n-1$ 個正解ならば，残りの 1 個も正しいので，この組合せは存在しない．

式 (3) は，1 個の筆跡と書き手の組合せは，必ず正解するので，この組合せは存在しない．

式 (4) は，2 個の筆跡と書き手の組合せは，全部で 2 通りあり，一方は正解で，もう一方は不正解なので，1 になる．

式 (5) は，n 個の筆跡の書き手をすべて間違える場合である．$(n-1)\cdot g(n-1,0)$ と $(n-1)\cdot g(n-2,0)$ の和になる．

式 (6) は，n の筆跡の書き手を，k だけ正解する場合である．任意の k が正解する組合せ ${}_nC_k$ に対して，残りすべてが不正解 $g(n-k,0)$ である組合せの積になる．

n の筆跡に対し，n 人の書き手を決める組合せの総数は $n!$ である．

よって，13 の匿名化した筆跡に対し，k 個正解する確率 $p(k)$ は

$$p(k) = \frac{g(13,k)}{13!} = \frac{1}{k!}\sum_{m=0}^{13-k}(-1)^m\frac{1}{m!} \tag{7}$$

となる．

ある 1 つの筆跡が，1 人の被験者によって正解される確率 P は，式 (7) を利用して求められる．

$$\begin{aligned} P &= \sum_{k=1}^{13}\frac{k}{13}\cdot p(k) \\ &= \sum_{k=1}^{13}\frac{k}{13}\cdot\frac{1}{k!}\sum_{m=0}^{13-k}(-1)^m\frac{1}{m!} \\ &= \frac{1}{13} \end{aligned} \tag{8}$$

この値は，被験者独立なので，ある 1 つの筆跡が，被験者 13 人によって正解される期待値 E は，

$$E = P\cdot 13 = \frac{1}{13}\cdot 13 = 1 \tag{9}$$

になる．

(平成 13 年 4 月 6 日受付)
(平成 13 年 12 月 18 日採録)

推　薦　文

手書き署名の匿名性を，戸口伝言板の電子化の際の課題としてとりあげている．これまで検討されている電子情報の匿名性では，電子マネーなど手書きでないデジタルデータが対象であり，本研究では，従来にない応用課題を扱っている．単なる方式提案だけの理論研究ではなく，実際に試作システムのレポートもある．（電子）手書き文書が認証手段として利用される今日，こうした情報の匿名性も新たな応用が期待される．CSEC としてぜひ論文に推薦したい研究である．

（CSEC 研究会主査　佐々木 良一）

瀬川　典久（正会員）

昭和 46 年生．平成 9 年 3 月奈良先端科学技術大学院大学情報科学研究科修了．同年 4 月より東北大学大学院情報科学研究科在籍．修士（工学）．平成 10 年 4 月より岩手県立大学助手．現在に至る．ユーザインタフェース，およびユーザインタフェースに関わるセキュリティの研究に従事．IEEE，ACM 各会員．

村山　優子（正会員）

津田塾大学学芸学部数学科卒業．三菱銀行および横河ヒューレット・パッカード社に勤務．昭和 59 年 University College London 大学院理学部計算機科学科修士課程修了．平成 2 年同大学院博士課程修了．Ph.D.（ロンドン大学）慶應義塾大学環境情報学部非常勤講師を経て，平成 6 年 4 月より広島市立大学情報科学部情報工学科講師，平成 10 年 4 月より岩手県立大学ソフトウェア情報学部助教授，現在に至る．インターネット，ネットワークセキュリティの研究に従事．IEEE，ACM，電子情報通信学会，映像情報メディア学会，日本 OR 学会，情報知識学会会員．

権藤　広海（学生会員）

昭和 51 年生．平成 13 年岩手県立大学ソフトウェア情報学部中途退学．同年同大学大学院ソフトウェア情報学研究科博士前期課程入学，現在に至る．インターネットにおけるコミュニケーションの研究に従事．ACM 学生会員．

山根　信二（正会員）

昭和 44 年生．国際基督教大学教養学部卒業．CSK に勤務．平成 8 年東北大学大学院情報科学研究科博士前期課程修了．平成 12 年同大学大学院情報科学研究科博士後期課程中退．修士（情報科学）．平成 12 年から岩手県立大学ソフトウェア情報学部コミュニケーション学研究室助手，現在に至る．コンピュータのリスクおよびネットワークセキュリティの研究に従事．共著書に Duncan Langford（Ed.）*Internet Ethics*（Macmillan Press, 2000），東浩紀「不過視なものの世界」（朝日新聞社, 2000）がある．CPSR，ACM，IEEE Computer Society 会員．

宮崎　正俊（正会員）

1938 年生．1962 年東北大学工学部電気工学科卒業．東北大学大型計算機センター講師，助教授，同教養部情報科学科教授，同大学大学院情報科学科教授を経て，1998 年 4 月より岩手県立大学ソフトウェア情報学部長（初代），現在に至る．1972 年マサチューセッツ工科大学客員研究員（文部省在外研究員，1 年間）．工学博士．東北大学名誉教授．専門は基本ソフトウェア，分散システム，システム評価，データベースシステム等．ユーザインタフェース，コミュニケーションモデル，セキュリティ，情報教育等にも関心を持つ．所属学会は，電子情報通信学会，日本エム・イー学会，ACM，IEEE，日本教育工学会，教育システム情報学会，日本テレワーク学会等．主な著書に，「UNIX 使い方入門」（日刊工業新聞社），「コンピュータ概説」（共著，共立出版）等．