コンピュータセキュリティ 11－1
（2000．9．8）

WWW上の戸口伝言板におけるサブリミナルチャネルの提案

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

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.

本稿では、戸口伝言板におけるサブリミナルチャネルについて提案する。手書き情報の中に、特定の利用者の間でしか認識が不可能なデータの挿入を行なうことで、サブリミナルチャネルを構築する。

Proposal of the subliminal channel on "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

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 a subliminal channel on "on-door" communication . Subliminal channel is one of the way for specified person communication on a public space.

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サブリミナルチャネルについて提案する。戸口伝言板は、すべての利用者に対して、メッセージの交換を行える。戸口伝言板において、特定の利用者間でのメッセージの交換を行なうには、(1)特定の利用者間でしかわからないメッセージの交換、なおかつ(2)一般の利用者には、特定の利用者間でのメッセージの交換の事実を気づかれない事が重要である。

以下、2章で、戸口伝言板について報告する。3章で、戸口伝言板で利用される手書き情報に、特定の人だけが理解できる情報を埋め込む手法について述べる。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。

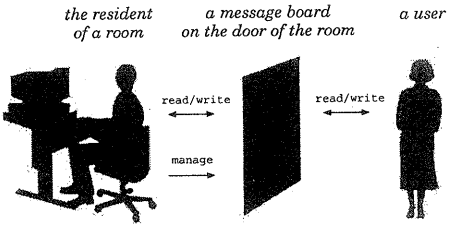

図1 戸口伝言板のモデル

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。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。

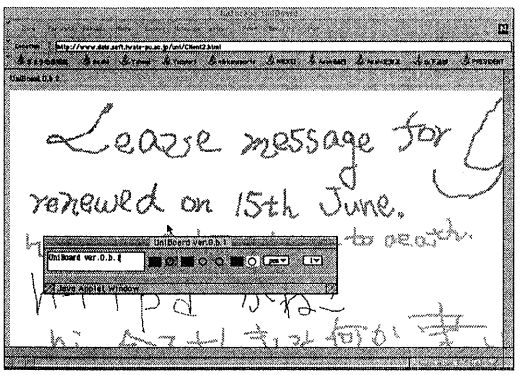

図2 Uni Board

3手書き情報における情報隠蔽

3.1概要

戸口伝言板は、２章で示したとおりに不特定多数の利用者間でのコミュニケーションを支援するものである。この戸口伝言板を、特定の利用者のコミュニケーションに利用するためには、(1)特定の利用者間でしかわからないメッセージの交換、なおかつ(2)一般の利用者には、特定の利用者間でのメッセージの交換の事実を気づかれない事が重要である。つまり、特定の利用者間のみに理解でき、なおかつ一般の利用者には普通の手書きと見えるような特殊な手書き情報の交換を行えるように戸口伝言板を拡張する。

3.2 筆跡情報

戸口伝言板では、筆跡情報は一般にvector drawaingと呼ばれる点と直線の集合として管理されている（図3）. 手書きにおける一画が、1行の筆跡情報として表される。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の組みの集合）が含まれている。

２００画（図4）の情報には、約１７００個の点の情報が含まれている。

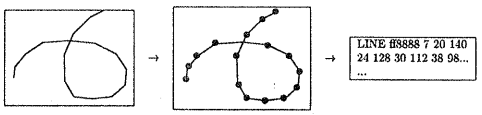

図3 描画情報（符号化）

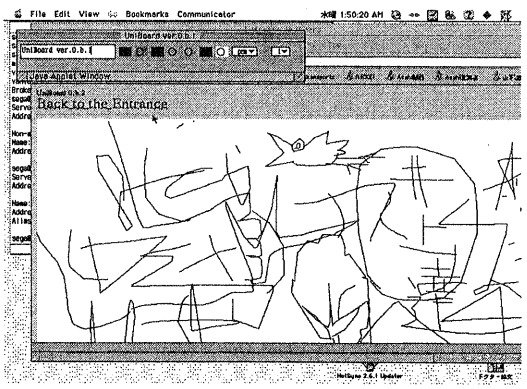

図4 200画の描画情報

3.3 情報の埋込

図5に、誰もが読める手書き情報に、特定の利用者間のみで共有される情報を埋め込む手法を示す。基本的な考え方は、本来かかれる線分に複数の点をとり、その複数の点を、埋め込む情報にしたがって移動させ、線を引き直すということである。その際に、元の図形と著しく異ならないようにする事が重要なことである。

まず、送信者が手書きを行ない、筆跡情報を生成する。生成された筆跡情報は、複数の点と線からなる。点(X0,Y0),点(X1,Y1)が本来の点である。

(1)点A,点Bをn等分する。（この例では3等分）

(2)ある点に対して移動させる量の最大値を決定する。移動する量の最大値を、x軸はα、y軸はβとすると、この点の移動させる組み合わせは、$\alpha \times \beta$になる。

(3)この組み合わせに対して、コード（例えばアルファベット）との1対1対応を決めておく。よって、$\alpha \times \beta$/256が、一つの点の移動量に対して組み込める情報量の大きさ(byte)である。

(4)埋め込む情報から、各点の移動量を決定し、点を移動させる。そして、移動した点に対して、線を引き直す。

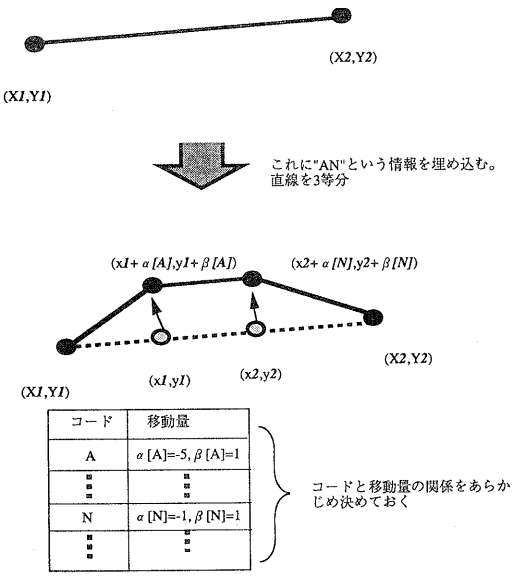

図5 情報の埋込手法

埋め込める情報の最大量は、次のように計算できる。

埋込に利用する線分の数 A

一つの線分を分割する数、N

一つの点の移動量 X軸: α Y軸: β

埋め込める情報の最大量Z = A×(N-1)× α × β/256 (byte)になる。例えば、図4の手書きに情報を埋め込む場合、1200×(N-1)× α × β (byte)だけ情報を埋め込むことが可能となる。

ただし、分割数N,移動量α、βが大きくなってしまうと、本来かかれるはずの情報からおおきくはみ出てしまい、第3者に情報が埋め込まれていることがわかってしまう恐れがあるので、N,α,βを調整することによって回避する。

3.4 情報の復元

埋め込まれた情報を取り出すためには、次のことを行なう(図6)。

(1)情報を埋め込んだ人から、次の情報を鍵として安全な手法を用いあらかじめ受け取っておく。

(A)埋込に利用する線分の集合

(B)線分の分割数

(C)点の移動量とコードの対応表

(2)手書き情報から、情報が埋め込まれた点、本来ある点に分類する。(A),(B)の情報を利用して、分類を行なう。

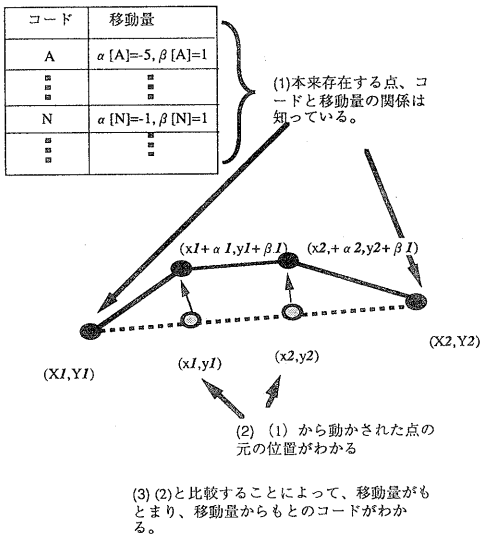

図6 情報の復元手法

(3) 情報が埋め込まれた点を使い、埋め込まれた情報を取り出す。取り出しかたは、埋め込むときと逆になり、本来ある点に引かれた線分からの変化量が、埋め込まれた情報に対応する。

3.5 第3者による検出

第3者が、埋め込まれた情報を検出するには、（A）情報が埋め込まれたことを認識し（B）手書き情報から、埋め込まれた情報を正しく取り出す事が必要である。

（A）は、第3者が手書きの形をみて、情報が埋め込まれていることを認識する必要がある。手書き情報その物は、特別なデータが埋め込まれているわけではないので、手書き情報その物から埋め込まれた情報を取り出したり、情報が埋め込まれていることを認識したりすることは不可能である。

情報が埋め込まれているかどうかを判別するには、人為的に作られた筆跡ではないことを調べる手段が必要である。これは、筆跡鑑定などの手段が必要である[3]。

（B）は、すべての線分から、情報が埋め込まれている点を見つける必要がある。まず、線分の数がNとする。情報が埋め込まれていると考えられる線分は、$O(N^2)$だけ存在する。分割数を、nとすると、組み込まれている点の数は、$O(N^2 \times (n-1))$になる。よって、線分の数が大きくなると計算量が大きくなり、検出は非常に困難になるといえる。

3.6 情報の埋込の実現

3章で述べた情報の埋込手法を用い、実際の手書き情報に、情報を埋め込んでみた。

図7の上は、情報を埋め込む際の元になった手書きである。画数は、３１画で、１９０の点と１５９本の直線で構成されている。

図7の上に、"NORIHISA SEGAWA"というアルファベット文字列を埋め込んでみた。

次の手法で行なっている。

(1)情報を埋め込む位置、埋め込む情報とコードの関係を決める。

(A)利用する線分：各画における一番目の線分

(B)分割数：2

(C)移動量とコードの関係：アルファベットに順番に番号をつけておき、その番号を16で割ったときの商から８引いた値をx軸、余りから８引いた値をy軸の移動量とした。

(2) (1) の情報に従い、情報を埋め込んでいく。まず、各画における1番目の点と2番目の点の中間点を求める。その中間点に対して、アルファベットに対応した移動量だけその中間点を移動する。

(3)1番目の点から、移動された中間点経由して、2番目の点に線を引き直す。

実行結果は、図7の下になる。

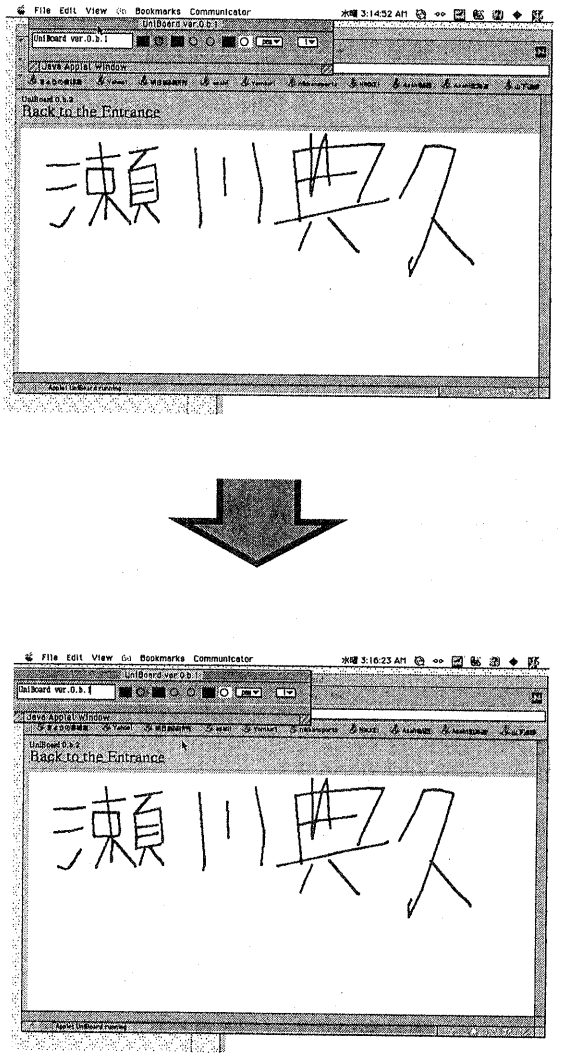

図7 実際の情報の埋込

3.7考察

図7の結果からわかるように、情報を埋め込む前、埋め込んだ後で、第3者にその事が気づかれることはまずないと考えられる。この図形を、第3者に見せて比較してもらったが、どこが違うかを発見することは不可能であった。これは、点の移動量が余り大きくなかったので、元の直線と比較することが困難であったからである。この事で、第3者に対しての情報隠蔽はうまくいっていると考えられる。

もし、見つかったとしてもどの点に情報が埋め込まれているかを調べるのは難しいと考えられる。それは、（1）まずどの点が情報が埋め込まれた点かを調べることが必要（2）なおかつ、移動量とアルファベットの組みを調べる必要がある。

この事から、この手法によって手書き情報の中に、(1)特定の利用者間でしかわからないメッセージの交換、なおかつ(2)一般の利用者には、特定の利用者間でのメッセージの交換の事実を気づかれない事が可能であると言える。

4関連研究

図形情報に、特定の人だけが読める情報を埋め込む手法として、電子透かしがあげられる[4][5]。電子透かしは、図形の画素情報に、特殊な変換を施し、情報を離散的に埋め込む手法である。

電子透かしは、(1)情報を埋め込む位置の決定手法(2)元の図形との変化をいかに少なくするかが、評価の対象となる。

今回の手法と比較すると、埋め込んだ情報の取り扱いが異なる。電子透かしは、元になる図形から出来る限り変化がないようにしなければならない。そうしないと、埋め込んだ後の図形の利用価値が下がってしまう。今回の手法は、伝言板における特定利用者間の情報の埋込なので、埋め込む前と埋め込んだ後で、情報が埋め込んだことが第3者に気づかれなければ、変化が多少あっても良い。よって、埋め込む際の自由度が電子すかしに比べて高くなる。

また、ネットワークを利用した、情報隠蔽としては、[6]があげられる。[6]は、WWWブラウザーで利用されるクッキーに情報を埋め込む手法である。一つのクッキーは、この手法の手書き情報に比べてデータ量が小さくなっているので、埋め込まれている情報を調べるのが容易である。そこで、複数のクッキーを組み合わせて情報埋込をすることによって問題を回避している。

5 まとめ

本稿において、戸口伝言板におけるサブリミナルチャネルを提案した。これは、戸口伝言板で利用される、誰もが読める手書き情報の中に、(1)特定の利用者間でしかわからないメッセージの交換、なおかつ(2)一般の利用者には、特定の利用者間でのメッセージの交換の事実を気づかれない事を実現するものである。

今後、この手法がどの程度有効なのか、また第3者に気づかれないことを、定量的に保証する手法の開発について現在研究を行っている。

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

[4] 山田孝行, 松井甲子雄:周波数変換係数比をを用いたのうたん画像への可変表示型電子透かし,情報処理学会コンピュータセキュレィティシンポジウム論文集,pp197-pp202(1999)

[5]村上健自, 上野義人:特徴空間のクラスタリングにより埋め込み位置選択を行う電子透かし,電子情報通信学会技術報告,ISEC2000-27,pp27-32,(2000)

[6]松本 勉, 池田 竜朗, 牧野 京子, 佐藤 明男, 村瀬 一郎:クッキーを用いた情報ハイディング方式とその実装,情報処理学会コンピュータセキュレィティシンポジウム論文集,pp243-248,(1999)