コンピュータセキュリティ 13－3
（２００１．５．２５）

２次元への投影モデルにおける手書きステガノグラフィの提案

瀬川 典久 村山 優子 宮崎 正俊
岩手県立大学

概要

近年、ネットワークが発達するに従って、さまざまなところでコミュニケーションシステムが利用されている。そのコミュニケーションシステムで、手書きによるコミュニケーションが行われるようになってきている。また、手書きは認証のためにもよく利用されている。しかし、コミュニケーションシステムには認証以外にも、匿名化、情報隠蔽等の実現が要求される。

本稿では、２次元への投影モデルにおける手書きステガノグラフィの提案を行う。手書きによって生成された筆跡情報の中に、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。そのサブリミナルチャネルを、空間上のある手書きからの２次元への投影として扱う手法を提案する。

キーワード：筆跡・サブリミナルチャネル・認証

The proposal of the handwriting steganography in a 2-dimension projection model

Norihisa Segawa　Yuko Murayama　Masatoshi Miyazaki
Faculty of Software and Information Science, Iwate Prefectural University

The computer network, as has typically been utilized in an e-mail system and WWW, can only cover a limited range of human communication. We use all kinds of communication system. Some communication system deals with handwriting information used in identification. When communication system supports various communication style, communication system has to treat not only identification but also anonymity and information hiding.

We have tried and developed to make a subliminal channel in the handwriting information. Subliminal channel is one of the way for specified person communication on a public space.

In this paper, the steganography in a 2-dimension projection model is proposed. A subliminal channel is built by inserting the data which cannot be recognized only among specific users into the hand information generated by handwriting. The technique of treating the subliminal channel as projection to 2 dimensions from a certain handwriting on space is proposed.

Keyword: hadwriting, Subliminal Channel, authentication

1 はじめに

ネットワークの普及・拡大と個人利用の増加にともない，コンピュータネットワークはコミュニケーションのためのシステムとして利用されるようになってきている．

また、コミュニケーションシステムで扱う情報は、文字だけではなく、図、絵等さまざまな種類を扱うようになってきている。特に、コミュニケーションシステムの一つの応用例として挙げられるグループウェアにおいては、動画、手書きによる筆跡の交換などが

利用されている[1]。特に、手書きによる筆跡は、(1)短い文章を素早く書ける(2)文字だけではなく図等も扱うことが出来る(3)キーボード入力に比べ初心者の利用が行いやすい等の特徴がある[2]。

一方、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、コミュニケーションシステムにおいては、認証だけでは不十分で、匿名化、情報隠ぺい等の他の概念を実現する必要がある。それは、利用者が行いたいコミュニケーションの性質に対して利用される物である。

匿名化、情報隠蔽を行うために利用するための筆跡情報を用いたサブリミナルチャネルについて提案を行ってきた[7]。これは、誰でも見れる筆跡情報に、特定の利用者のみにしかわからない情報を付加することである。例えば、共有型ホワイトボードシステムのようなコミュニケーションにおいて、全ての参加者が、筆跡情報が見える状況下で、特定の参加者だけで、情報が交換できるシステムを構築するのに利用できる。

この、サブリミナルチャネルを実現するには、(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。

現在までに、手書きによるサブリミナルチャネルを構築し、そのサブリミナルチャネルの考察を行ってきた[7]。

本稿では、２次元への投影モデルにおける手書きステガノグラフィの提案を行う。本稿では、普通２次元上で行われる手書きを、3次元から２次元への投影としてとらえ、その仕組みを利用してステガノグラフィを行うことを提案する。

以下、2章で、手書きの筆跡情報に、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。3章で、3次元の手書きを利用して２次元に投影してステガノグラフィを実現する手法について述べる。4章で、まとめと今後の課題について述べる。

2筆跡情報における情報隠蔽

2.1概要

筆跡情報を用いた、サブリミナルチャネルを構築するには、(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。

そのために、本研究では次の手法を考えた。

(1)手書きの筆跡を、vector drawingとしてとらえ、符号化を行う。

(2)符号化された情報に対して、第3者には気づかれないような情報を付加する。

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することである。

2.2 vector drawing

今回扱う筆跡情報は一般にvector drawaingと呼ばれる点と直線の集合として管理されている.

利用者の手書きによって作られた筆跡に対して、一定時間毎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。

本研究では、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（図1）。

写真などの画像を格納するのによく利用されるbitmapデータより、vector drawingの方がデータ量が小さくなる事が多い。しかし、手書きのような自由曲線を扱うのには、サンプリングする点の数を多くしないと、不自然な筆跡になる。

例えば、図2に示す２００画の情報には、約１７００個の点の情報が含まれている。この筆跡情報は、16232byteから構成されている。

2.3 情報の埋込

図3に、誰もが読める筆跡情報に、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、$\alpha \times \beta$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(bit)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。

埋め込める情報の最大量は、次のように計算できる。

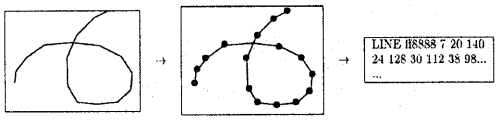

図1 描画情報（符号化）

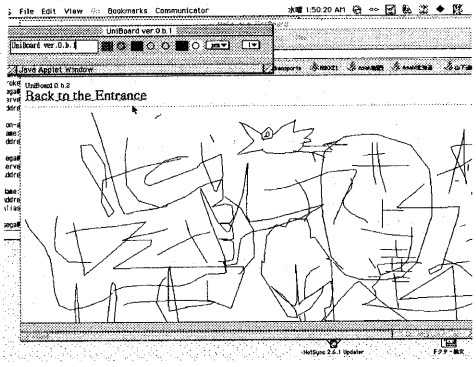

図2 200画の筆跡情報

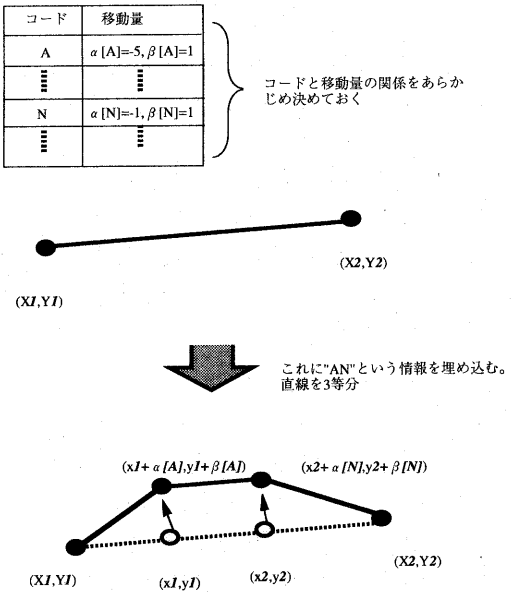

図3 情報の埋込手法

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2の手書きに情報を埋め込む場合、約9600×(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。

2.4 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4)。

(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)筆跡情報から、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。

(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。

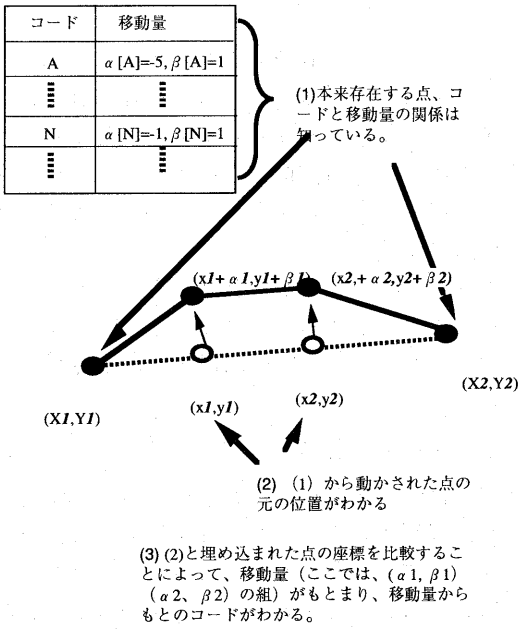

図4 情報の復元手法

2.5 埋込の実現例

2.3で述べた情報の埋込手法を用い、実際の筆跡情報に、情報を埋め込んでみた。

図5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5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。

実行結果は、図5の下になる。

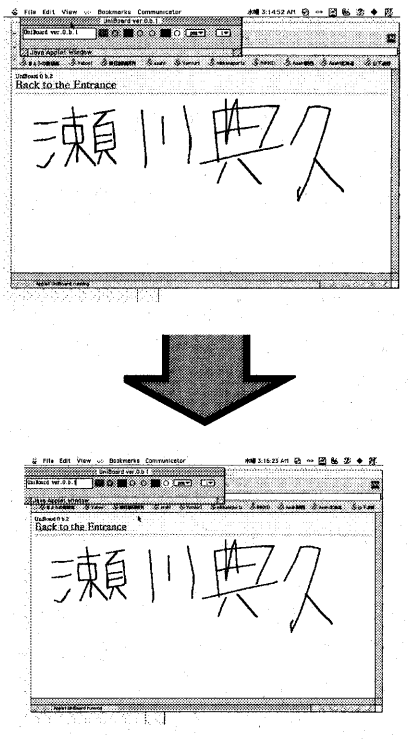

図5 実現例

3　2次元への投影モデルにおける手書きサブリミナルチャネル

3.1 概要

2章でとりあげたサブリミナルチャネルは、筆跡をvector drawingとして符号化した後、その符号化を利用して情報を埋め込む手法である。

しかし、この手法は、手書きの癖を読みとられると、サブリミナルチャネルの存在に気づいてしまう。一般に、人間の筆跡は癖を持っている。その癖は、その筆跡をよく知っている人なら気づきやすい。本来かかれる筆跡を崩して、サブリミナルチャネルを実現しているので、その筆跡の崩れを第3者が気づけば、その段階でサブリミナルチャネルは破られる。

上記のことを解決するために、人が書く筆跡を、人工的に崩し、それにサブリミナルチャネルを加えると、人工的に崩した段階で、人の癖が消去されているので、第3者には破られにくくなる。

人工的に筆跡を崩す手法は、筆跡の匿名化[8]によって行われている。しかし、匿名性に着目して筆跡を人工的に崩しており（図6)、この手法を用いた筆跡にサブリミナルチャネルに適用すると、第3者がその筆跡を見た場合、明らかにその筆跡に何か処理をしていると疑う。

そこで、今回は、3次元空間に手書きを行い、その空間から2次元への投影モデルを与えることによって、2次元の筆跡を与える手法を考える。その2次元の座標にサブリミナルチャネルを構築する。

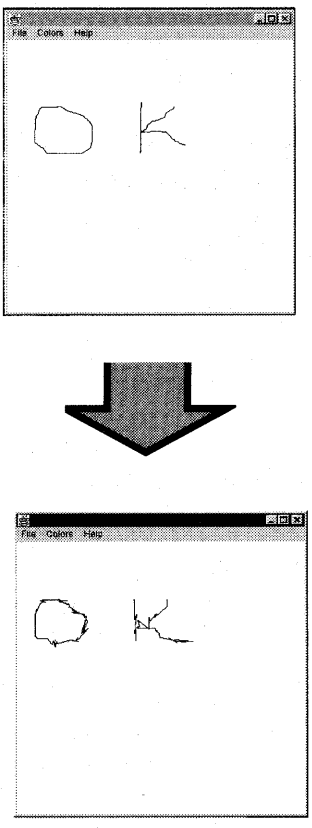

図6 筆跡の匿名化

3.2 投影モデル

従来の手書きは、平面上に行ってきたが、今回のモデルでは空間上に手書きを行う。図7は、完全に3次元空間で手書きを行い、2次元に投影するモデルである。ユーザが、空間上に手書きの筆跡をとる。そして、光源から空間上の筆跡に光を当

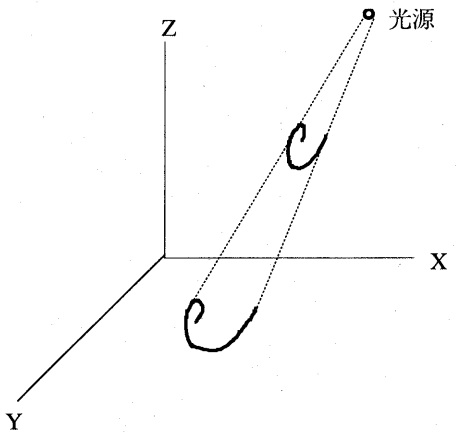

図7 3次元空間での筆跡とその投影

て、その投影した物をXY平面に写す。写された物が、投影された筆跡である。この投影された筆跡に、２章の情報隠蔽を行う。

この手法では、情報を埋め込む前の段階で筆跡の癖が変更されている。なおかつ、匿名性の手法のような、筆跡の座標をジグザグに変更するのではなく、滑らかに筆跡を変更する。よって、この筆跡にサブリミナルチャネルを適用しても、第3者への存在は気づかれにくい。また、ユーザが筆跡に対しての光源の位置を変更することによって、癖の変化を与えることができる。

しかし、図7のモデルを利用して人間が筆跡を利用するには、(1)空間と投影される平面の関係を常に認識する必要がある(2)3次元空間に自由に手書きをするためのツールが少ないといった問題が発生する。

そこで、図8のような、空間上にある平面を定義して、その平面から投影する平面を決定する手法を提案する。この手法は、空間上におかれたある平面上に、ユーザが手書きを行う。その時に生成された、筆跡を光源から投影し、XY平面に写す。この手法は、光源と平面の傾きをいろいろ変えることで、筆跡の癖を変化させることができる。また、ユーザが平面上に手書きを行うので、図７のような手書きの難しさという問題は発生しない。

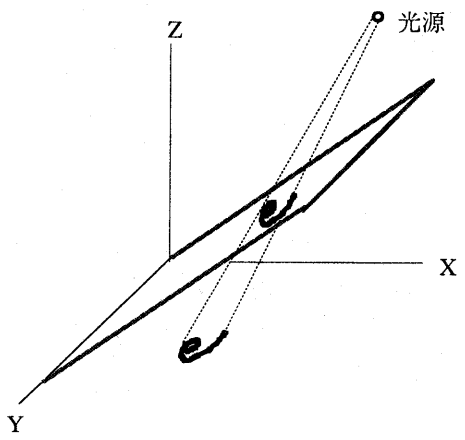

図8 3次元空間の平面からの投影

4 まとめ

本稿では、筆跡情報に対するサブリミナルチャネルを示し、その筆跡情報を3次元空間から２次元平面への投影として与える手法についてのべた。

今後、空気ペン[9]のような入力装置の開発、及びこの手法の評価などを行っていく。さらに、空間そのものの座標に対してのサブリミナルチャネルの構築も行う予定である。

参考文献

[1]J. Rekimoto:A multiple device approach for supporting whiteboard-based interactions,Proc.Conference proceedings on Human factors in computing systems(CHI ヨ98), pp.344-351, (1998)

[2]瀬川 典久, 村山 優子, 権藤 広海 , 中本 泰然, 宮崎正俊: WWW上の戸口伝言板における手書きの評価,第60回情報処理学会全国大会講演CD-ROM, 4W-02 (2000)

[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 晋爾, 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]瀬川 典久, 権藤 広海, 中本 泰然,村山 優子, 宮崎 正俊: 筆跡情報を用いたサブリミナルチャネルの構築,情報処理学会コンピュータセキリティシンポジウム2000論文集,pp331-336(2000)

[8]]瀬川 典久, 権藤 広海, 中本 泰然,山根 信二, 村山 優子 宮崎 正俊 :戸口伝言板における匿名性の提案,電子情報通信学会 技術報告 ISEC2000-25,pp17-22,(2000)

[9]椎尾一郎, 山本吉伸, "コミュニケーションツールのための簡易型AR システム"インタラクティブシステムとソフトウェアVIII（日本ソフトウェア科学会 WISS2000）pp. 117-124 (2000)