筆跡情報を利用したステガノグラフィの構築

瀬川典久[†,☆] 村山優子[†]
宮崎正俊[††] 根元義章[†††]

近年 IT 技術の急速な進歩により PDA やタブレット PC 等の手書きデバイスが注目されており，それらはペンの位置だけでなく，筆圧，傾き等の情報の処理も可能である．さらに最近，これらの情報を利用したサービス（手書き E-mail，手書きメモ等）も利用され始めている．本論文では，我々は手書きデバイス情報隠蔽の手法を開発した．これは筆跡情報の中に特定のユーザだけが解読できる情報を埋め込むというもので，具体的には筆跡からペンの座標，筆圧，傾きを読み取り，それらを瞬時に標本化し，伝えたい情報をステゴ鍵を利用して，筆跡情報の中に埋め込むという手法である．これによって，第三者が気付かない情報隠蔽を行うことが可能になる．本論文ではプロトタイプシステムを作成し複数の被験者によるステガノグラフィの評価から，その有効性を明確にする．

Construction of a Steganography with Handwriting Information

Norihisa Segawa,[†,☆] Yuko Murayama,[†] Masatoshi Miyazaki[††]
and Yoshiaki Nemoto[†††]

With the quick advance of information technology, handwriting device, such as PDA and Tablet PC, is getting high attention from all over the world recently. Additionally, a lot of services (handwriting e-mail, memorandum, etc.) are utilized effectively. In this paper, we developed a technique of information hiding for the handwriting devices. This is to embed data in handwriting information that could be understood by specific users. To be more specific, these information such as pen's coordinates and pressure, slant, are sampled in an eye blink, and information to tell is embedded into handwriting information which use the stego key. It becomes possible to perform information hiding at the level which other person does not notice, by this technique. In this paper we implemented a prototype system and evaluated steganography with some testers. We clarify the effectiveness of our technique by showing experimental results.

1. はじめに

近年，パーソナルコンピュータ（PC）の機能の高度化，低価格化の影響で，様々な人が様々な状況でコンピュータを利用している．また，コンピュータに関係する人だけではなく，芸術家，作家等コンピュータと直接関係しない人々が，コンピュータを利用し，様々なマルチメディアコンテンツを作成している．また，様々な分野で作成されたコンテンツは，インターネット等を利用して，様々な人の間で交換され，流通している．

近年，その交換されるコンテンツの中に，特定の人だけが理解できる情報を隠す情報隠蔽（インフォメーションハインディング）の研究が行われている．インフォメーションハインディングの主な研究対象として，電子透かし[1)]と本論文で対象とするステガノグラフィ[12),13)]がある．電子透かしとは，交換されるコンテンツに，その情報の著作者，作成した日付，利用目的等をそのコンテンツの中に，第三者が気づかないように埋め込むことである．第三者が無断でそのコンテンツを悪用した場合，コンテンツの作成者が，その電子透かしを証拠とすることで，不正利用を証明することができる[1)]．一方，ステガノグラフィとは，特定の人だけが分かる情報を，普通の情報の中に第三者には気づかれないように隠し，情報を交換することである．

本論文では，筆跡情報を利用したステガノグラフィ

† 岩手県立大学
Iwate Prefectural University
†† 情報技術総合研究所
Digitally Advanced Integrated Solutions Laboratories Ltd.
††† 東北大学大学院情報科学研究科
Graduate School of Information Science, Tohoku 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

の手法について提案する．従来のステガノグラフィの研究では，情報が埋め込まれるコンテンツとして，写真等の画素情報，音声情報を対象にしてきた．本論文では，人間が書く手書きによる筆跡を情報が埋め込まれるコンテンツとして取り上げる．手書きは，携帯型端末（PDA），液晶タブレットを用いた PC 等で利用されている．手書きは，(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できる，(3) キーボード入力に比べ初心者が利用しやすい等の特徴がある[2),3)]．また，手書きの特性を利用したアプリケーションの構築が行われており，ユーザが手書きを行って文字入力を行うシステム，グループウェアにおいて手書きメッセージを交換するシステム等が開発され利用されている[4)]．

本論文で対象とする筆跡情報は，従来の手書きアプリケーションで対象にしていた座標情報だけではなく，今後普及が見込まれるペンタブレット等を用いて入力される筆圧，ペンの傾き等の情報も対象にしている．たとえば，今後普及が予想される Windows XP Tablet PC Edition（Tablet PC）[5),6)] では，手書き機能が OS の機能として実装されている．Tablet PC では，筆跡の座標だけを扱うのではなく，タブレットから入力されるすべての情報を処理するライブラリが提供されている．Tablet PC では，タブレットから入力されるすべての情報を活用したメールソフト，ワープロソフト等が利用可能になっており，今後もペン入力の特性を生かした様々なアプリケーションが開発される予定である．今後ペン入力を利用したアプリケーションが様々なところで利用され，またそれらのアプリケーションによって手書きのドキュメントが作られ，様々な人の間で交換されることが予想される．本論文では，このように今後利用が予想されるペンタブレット等を利用した筆跡情報にステガノグラフィを構築する手法を示し，その有効性を示す．本論文での手法が，今後開発される手書きアプリケーションのコンテンツを利用したステガノグラフィとして利用できる．

以下，2 章ではユーザが書く筆跡を符号化するための筆跡情報について述べる．3 章では，筆跡情報を利用した情報隠蔽について述べ，4 章では，3 章で示した情報隠蔽が実現できることを，プロトタイプシステムの実現により示す．5 章で，関連研究との比較を行い，6 章でまとめを行う．

2. 筆跡情報

2.1 筆跡入力と筆跡情報の取得

筆跡をステガノグラフィのデータとして利用するために，筆跡の符号化を行う[7)]．システムが取り出すデータの種類には，座標 (X, Y)，筆圧，ペンの傾き等がある．

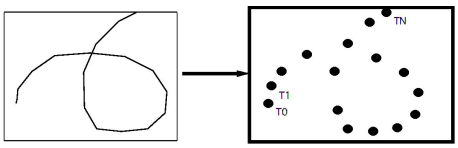

図 1 筆跡のサンプリング
Fig. 1 A sampling of handwriting information.

ユーザが書く 1 つの筆跡を極小時間 T_s ごとに，時刻 T_0 から T_E までとらえたとする（**図 1**）．

そのとき，以下の定義が成り立つ．

標本化されるデータの種類を $a_1, a_2..a_m$

時刻 T におけるデータを

$$(D_{a_1}(T), D_{a_2}(T), \cdots D_{a_m}(T))$$

標本化して得られたデータの個数 $N = \frac{T_E - T_0}{T_s} + 1$

時刻 $T_n (0 \leq n \leq N, T_0 \leq T_n \leq T_E, T_s = T_n - T_{n-1})$ としたとき，

時刻 T_n において標本化して得られたデータは，

$$(D_{a_1}(T_n), D_{a_2}(T_n), \cdots D_{a_m}(T_n))$$

とする筆点座標として定義される．

筆跡情報 **H** は，ある時刻 T_n において，標本化して得られたデータを利用して，次のように定義される．

$$\mathbf{H} = \{(D_{a_1}(T_n), D_{a_2}(T_n), \cdots D_{a_m}(T_n)) \mid (n = 0, 1, 2, \cdots, N)\}$$

筆跡情報は，時刻 T_n における m 次元の筆点座標列として表される．

D_{a_m} は，それぞれ $S(a_m)$ ビットで符号化する．よって，筆跡情報 **H** は，

$$(N+1)\sum_{k=1}^{m} S(a_k)$$

ビットの情報を持つ．

2.2 筆跡情報から筆跡の復元

筆跡情報 **H** は，筆跡を離散化した筆点座標列として符号化したものである．筆跡情報を復号化しただけでは，離散化した筆跡の座標点しか表すことができない．

筆跡を復元するには，符号化された筆点座標列を復号化し，その復号化された座標点を連続した線で補間する必要がある．

2.1 節で定義した筆跡情報 **H** を復号化し，復号化によって得られた筆点座標を連続した線で補間したものが，**図 2** である．

座標点を補間する手法には，直線補間，B スプライン補間が用いられる[8)]．また，標本化して得られた

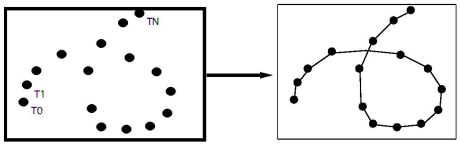

図 2 筆跡の復元
Fig. 2 Redraw handwriting.

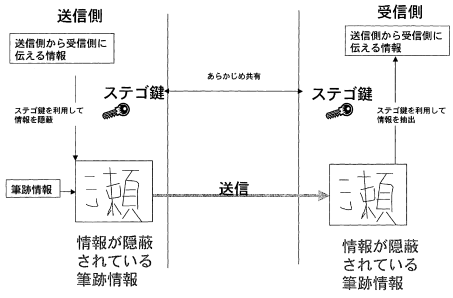

図 3 筆跡情報を利用したステガノグラフィ
Fig. 3 Steganography with a handwriting information.

データの個数 N が少ない場合，復元される筆跡ともとの筆跡との誤差が大きくなってしまう．

3. 筆跡情報を用いた情報隠蔽

3.1 ステゴデータの構築

送信者は，ステゴ鍵を決定し，送信するデータをカバーデータとなる筆跡情報に埋め込む．データが埋め込まれた筆跡情報は，ステゴデータとして，受信者に送信される（**図 3**）．ステゴデータは，もとのカバーデータと同様に筆跡情報であるが，情報が埋め込まれている分，もとの筆跡情報から変化している．

(1) 送信者は，送信するデータ長が q ビットとしたとき，$q = p \cdot k (1 \leq k \leq N-1,\ k$ は自然数) となる p と k の組を選ぶ．送信者は，p ビットのコードと筆跡情報の変化量の 1：1 の対応表を作成し，それをコードブックとする．送信者は，p ビットのコード $C_j (1 \leq j \leq 2^p)$ と埋め込み終了を表す 'STOP' コード C_{2^p+1} に対して，筆跡情報のデータの種類の変化量 $\mathbf{c_j} (1 \leq j \leq 2^p + 1)$ の対応表を作成する．**図 4** は，1 ビットのコードと筆圧の変化で定義されたコードブックである．p ビットのコードを符号化するためのコードブックを作成するには，$2^p + 1$ だけのコードと筆跡情報の変化量の組合せを用意する必要がある．

(2) 送信側は，送信するデータをコードブックに従って符号化を行う．送信側は，送信する q ビットのデータを，先頭から p ビットごとに分ける．

埋め込むコード(bit)	筆圧
1	1
0	0
STOP	-1

図 4 コードブックの例
Fig. 4 An example of a code book.

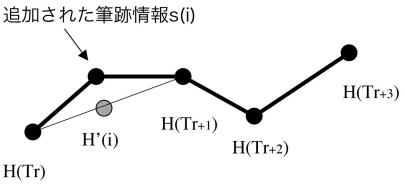

図 5 送信するデータの埋め込み手法
Fig. 5 Embedded technique of sending data.

送信する q ビットのデータは，p ビットのデータ $E_i (1 \leq i \leq k,\ i$ は自然数) に分割される．E_{k+1} は，'STOP' とする．送信するデータ E_i は，コードブックにしたがって $\mathbf{e_i} (1 \leq i \leq k+1)$ と符号化される．つまり，k 個の p ビットの送信するデータと埋め込み終了を表す 'STOP' が，筆跡情報の変化量として符号化される．

(3) 送信者は，$\mathbf{e_i} (1 \leq i \leq k+1)$ をカバーデータに埋め込む．送信者は，$\mathbf{e_i} (1 \leq i \leq k+1)$ をカバーデータに埋め込むためのアルゴリズムを決める．

アルゴリズムは，送信者が筆跡情報の任意の 2 点 $\mathbf{H}(T_r)$，$\mathbf{H}(T_{r+1})$，$(0 \leq r \leq N-1,\ r$ は自然数) を $k+1$ 組取り出し，その 2 点の中点 $\mathbf{H}'(i)$ を求める．

$$\mathbf{H}'(i) = \frac{\mathbf{H}(T_r) + \mathbf{H}(T_{r+1})}{2}$$

その後，$\mathbf{H}'(i)$ を $\mathbf{e_i}$ の変化量に従い移動させ，$\mathbf{H}(T_r)$，$\mathbf{H}(T_{r+1})$ の間に筆跡情報 $\mathbf{s}(i)$ として追加する（**図 5**）．追加した筆跡情報が，ステゴデータになる．追加した筆跡情報 $\mathbf{s}(i)$ を筆跡情報 $\mathbf{H}$ に追加しても，筆跡がほとんど変化しない場合には，第三者は，情報を埋め込んだことに気づかない．また，受信者が，$\mathbf{H}'(i)$ を取得し，$\mathbf{H}'(i)$ からの $\mathbf{s}(i)$ の変化量を求めることができれば，コードブックから埋め込まれたデータを復号できる．

以下では，筆跡情報の w 点おきに $\mathbf{e_i}$ を埋め込むアルゴリズムについて説明する．

筆跡情報 $\mathbf{H}(T_{w \cdot i-1})$ と $\mathbf{H}(T_{w \cdot i})$ の間に，情報を埋め込むための点 $\mathbf{H}'(i)$ をとる．

$$\mathbf{H}'(i) = \frac{\mathbf{H}(T_{w\cdot i-1}) + \mathbf{H}(T_{w\cdot i})}{2}$$
$$(1 \le i \le k+1, 1 \le w\cdot i \le N)$$

$\mathbf{H}'(i)$ を，符号化された座標の変化量 $\mathbf{e_i}$ に従い変化させる．$\mathbf{s}(i) = \mathbf{H}'(i) + \mathbf{e_i}$ となる

ステゴデータ $\mathbf{S}(\mathbf{z})(0 \le z \le N+k+1)$ は，次のアルゴリズムで生成される．

(a) a に 0 を代入する．
(b) b に 1 を代入する．
(c) j に 0 を代入する．
(d) j が $w\cdot b-1$ に等しくなければ，(k) に移る．
(e) $\mathbf{S}(j+a)$ に，$\mathbf{H}(\mathbf{T_j})$ を代入する．
(f) a に 1 加える．
(g) $\mathbf{S}(j+a)$ に，$\mathbf{s}(b)$ を代入する．
(h) b が $k+1$ と等しい場合には，(n) に移る．
(i) b に 1 加える．
(j) j に 1 加える．
(k) $\mathbf{S}(j+a)$ に，$\mathbf{H}(\mathbf{T_j})$ を代入する．
(l) j に 1 加える．
(m) (d) に移る．
(n) $\mathbf{S}(j+a)$ に，$\mathbf{H}(T_j)$ を代入する．
(o) j が N に等しい場合，動作を止める．
(p) j に 1 加える．
(q) (n) に移る．

ステゴデータ $\mathbf{S}(z)$ は，m 次元の筆点座標列である．筆跡情報 $\mathbf{H}(T_n)$ を復号化して補間して生成される筆跡と，ステゴデータ $\mathbf{S}(z)$ を復号化して補間して生成される筆跡を比較して，第三者が同じ人が書いた筆跡だと判断すれば，第三者は送信するデータの存在に気づかない．

また，受信者にあらかじめ伝えておくステゴ鍵は，符号化に利用したコードブック，情報を埋め込むのに利用した点の情報，ステゴデータを生成するアルゴリズムである．

3.2 受信側のデータの抽出

受信側は，送信側から安全な手法でステゴ鍵をあらかじめ入手しておく．受信者はステゴ鍵の情報から，ステゴデータの中から情報が埋め込まれているステゴデータを取り出すことができる．

受信者は，c 個の筆点座標からなるステゴデータ $\mathbf{S}(l)(1 \le l \le c,\ l,\ c$ ともに自然数) を入手する．受信者は，送信者から送られてきたステゴ鍵を利用し，ステゴデータ $S(l)$ から送信者が情報を埋め込むのに利用した筆跡情報 $\mathbf{S}(r-1)$，$\mathbf{S}(r+1)$ と，情報が埋め込まれている筆跡情報 $\mathbf{S}(r)$ を取り出す．受信者は，$\mathbf{S}(r-1)$，$\mathbf{S}(r+1)$ の中点を求める．

$$\mathbf{S_{r-1,r+1}}' = \frac{\mathbf{S}(r-1) + \mathbf{S}(r+1)}{2}$$

受信者は，情報が埋め込まれている点 $\mathbf{S}(\mathbf{r})$ から中点 $\mathbf{S_{r-1,r+1}}'$ の座標の差 $\mathbf{s_r}'$ を求める．

$$\mathbf{s_r}' = \mathbf{S}(\mathbf{r}) - \mathbf{S_{r-1,r+1}}'$$

$\mathbf{s_r}'$ は，送信者が情報を埋め込むために，筆点情報を移動した座標になる．その座標をコードブックにあてはめ，コード C を取得する．

以下は，送信者が 3.1 節の例に従って，w 点おきに情報を埋め込んだステゴデータ $\mathbf{S}(l)$ に対して，次のアルゴリズムを適用して，送信者が埋め込んだデータの座標情報を取り出し，埋め込んだデータを復号化する．

(1) j に 1 を代入する．
(2) $\mathbf{h} = \frac{S(w\cdot j) + S(w\cdot j+2)}{2}$ を求める．
(3) $\mathbf{e_j} = \mathbf{h} - \mathbf{S}(w\cdot j+1)$ を求める．
(4) $\mathbf{e_j}$ の座標を，コードブックにあてはめてコード $\mathbf{E_j}$ を取得する．コード $\mathbf{E_j}$ が'STOP' の場合，(6) に行く．
(5) j に 1 を加えて (2) に戻る．
(6) コード $E_i(1 \le i \le j-1)$ を先頭からつないだコード $E_0E_1\cdots E_{j-1}$ が，送信者が埋め込んだコードになる．

4. 筆跡情報を利用したステガノグラフィの実現

3 章の考え方を実証するために，プロトタイプシステムを実装し，筆跡情報を用いたステガノグラフィを実現する．

4.1 プロトタイプシステムの概要

プロトタイプシステムは，ユーザがペンタブレットに書いた筆跡を筆跡情報として符号化し，その符号化した情報に，ステゴ鍵を利用して，ステガノグラフィを作成する．

ユーザは，ペンタブレット（**図 6**）を利用してペン入力を行い，筆跡情報を取得する．プロトタイプシステムで用いる筆跡入力装置は，Wacom Tablet Intuos I-600 である．Wacom Tablet IntuosI-600 の仕様は，**図 7** である．プロトタイプシステムでは，ペンタブレットから (a) ペンの X 座標（16 ビット），(b) ペンの Y 座標（16 ビット），(c) ペンの筆圧（16 ビット）の情報を取得する．よって，1 つの筆点座標において 48 ビットの筆跡情報が生成される．

図 6 筆跡入力システム（Pen Tablet）
Fig. 6 Handwriting input system (Pen Tablet).

読み取り可能範囲	8×6inch（203.2×152.4mm）
読み取り分解能	0.0004inch (0．01mm)
読み取り精度	0.0098inch (±0.25mm)
読み取り速度	200ポイント/秒
筆圧レベル	1024レベル

図 7 Intuious-600 の仕様
Fig. 7 Features of Intuios-600.

埋め込むコード	埋め込む点のX方向の移動量(ピクセル)	埋め込む点のY方向の移動量(ピクセル)
000	1	1
001	1	0
010	1	−1
011	0	1
100	0	0
101	0	−1
110	−1	1
111	−1	0
STOP	−1	−1

図 8 コードブック (A)
Fig. 8 Code book (A).

埋め込むコード	埋め込む点のペンの太さの変化量（ピクセル）
00	2
01	1
10	0
11	−1
STOP	−2

図 9 コードブック (B)
Fig. 9 Code book (B).

プロトタイプシステムは，ペンタブレットによって得られた筆跡情報を横 225 mm の長さに 640 ピクセル，縦 140 mm の長さに 400 ピクセルとして出力する．出力は，600 dpi のモノクロレーザプリンタによって行った．線の太さは，ペンの筆圧に比例し，最大 10 ピクセル（3.5 mm）として表示する．隣り合う 2 つの筆点は，直線によって補完される．

本実験で利用したステゴ鍵は，2 種類のコードブックおよび 3.1 節で示したアルゴリズムである．2 種類のコードブックは，コードブック (A)（**図 8**）およびコードブック (B)（**図 9**）である．コードブック (A) は，コードをペンの座標 (X,Y) の変化に対応させている．コードブック (B) は，コードをペンの太さの変化に対応させている．

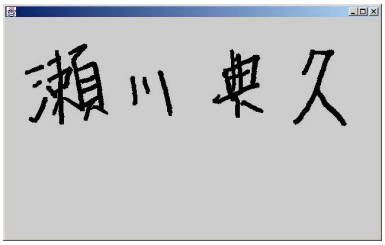

図 10 カバーデータ (A)
Fig. 10 Cover data (A).

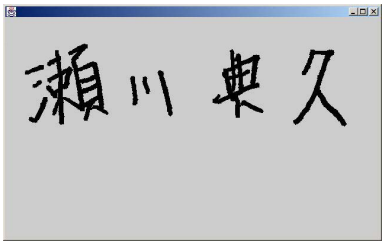

図 11 ステゴデータ (A)（コードブック (A) を用いた場合）
Fig. 11 Stego data (A) (in case of using code book (A)).

プロトタイプシステムは，Java によって実装され，情報を埋め込むためのステゴ鍵は，Java プログラムのアルゴリズムとして記述され実現される．

4.2 筆跡情報の取得と情報の埋め込み

図 10 は，ユーザがタブレットを用いカバーデータ (A) を取得し，カバーデータ (A) を復号化し筆跡として復元した図である．サンプリングによって得られた筆点座標は，865 点存在し，筆跡情報のデータ長は，248,064 ビットである．

ユーザは，カバーデータ (A) に対し，コードブック (A) を用いデータを埋め込みステゴデータ (A) を生成し，そのステゴデータから筆跡を復元した．埋め込むデータは，乱数で生成された 150 ビットの情報である．このデータを，カバーデータ (A) の筆跡 10 点おきに情報を埋め込んだ．ステゴデータ (A) を復号化し復元された筆跡は，**図 11** である．埋め込みにより，筆跡情報は 5%増加している．埋め込みによって筆跡は，平均 0.05 ピクセル長水平方向に移動している．また，カバーデータ (A) に対する埋め込むデータのビット長の比率は，0.06%である．

図 12 は，図 10 と同様に，ユーザがタブレットを用いカバーデータ (B) を取得し，カバーデータ (B) を復号化し筆跡として復元した図である．サンプリングによって得られた筆点座標は，729 である．筆跡情報のビット長は，279,936 ビットである．

ユーザは，カバーデータ (B) に対し，コードブック (B) を用いデータを埋め込みステゴデータ (B) を生成

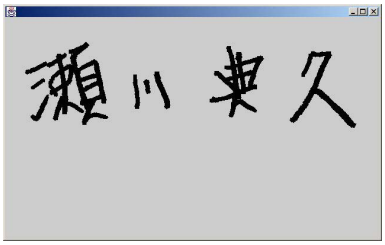

図 12 カバーデータ (B)
Fig. 12 Cover data (B).

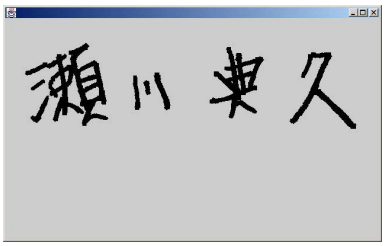

図 13 ステゴデータ (B)（コードブック (B) を用いた場合）
Fig. 13 Stego data (B) (in case of using code book (B)).

し，そのステゴデータから筆跡を復元した．埋め込むデータは，乱数で生成された 100 ビットの情報である．このデータを，カバーデータ (B) の筆跡 10 点おきに情報を埋め込んだ．ステゴデータ (B) を復号化し復元された筆跡は，**図 13** である．埋め込みにより，筆跡情報は 6%増加している．埋め込みによって筆跡は，平均 0.07 ピクセルペンの太さが増減している．また，埋め込むデータとカバーデータ (B) のビット長の比率は，0.03%である．

4.3 第三者による主観的評価

本実験のステゴデータを評価するために，岩手県立大学ソフトウェア情報学部の 10 人の学生に，情報が埋め込まれる前の筆跡と情報が埋め込まれた筆跡を比較し，その結果を考察した．

評価手法として，MOS（Mean Opinion Score）法を利用した．MOS 法とは，被験者が実験を行い，**図 14** の評価基準を利用し実験の主観的評価を行う評価手法である．複数の被験者から得られた点数を集計し，その平均を MOS（平均オピニオン値）として評価する．

被験者は最初に，情報が埋め込まれる前の筆跡（カバーデータ (A) 図 10）と情報が埋め込まれた筆跡（ステゴデータ (A) 図 11）を同時に 30 秒見る．その 2 つを比較し，図 14 から一番近い値を選んでもらう．同様に，カバーデータ (B) とステゴデータ (B) も行う．

評定者数を n，k 番目の評価者の評価値を a_k とするとき，MOS は次式で表される．

評価値	評価尺度
1	筆跡に変化はない
2	わずかな変形がわかる
3	筆跡の変形がわかる
4	読むのが難しいほど変形している
5	読めない

図 14 評価指標
Fig. 14 Evaluation index.

		比較した筆跡	
		カバーデータ(A) ステゴデータ(A)	カバーデータ(B) ステゴデータ(B)
被験者	A	2	2
	B	1	1
	C	1	1
	D	1	2
	E	1	1
	F	1	1
	G	1	1
	H	1	1
	I	1	1
	J	1	1

図 15 実験結果
Fig. 15 Results of experiment.

$$MOS = \frac{1}{n} \cdot \sum_{k=1}^{n} a_k$$

MOS が低いほど，第三者は情報が埋め込まれる前の筆跡と情報が埋め込まれた後の筆跡が変化していないと考えており，情報が埋め込まれた事実に気づきにくいと考えることができる．

4.3.1 実 験 結 果

実験結果は，**図 15** に示す．MOS は，カバーデータ (A) とステゴデータ (A) の比較で 1.1，カバーデータ (B) とステゴデータ (B) の比較で 1.2 になった．筆跡の変化に気づいた 2 人にインタビューを行った．2 人は，「筆跡の先端部分の微妙な変化はなんとなく分かった」，「筆跡における縦棒の太さの変化に気づいた」「太さの変化によって，筆跡の線分の間隔の微妙な変化に気づいた」という意見を述べてくれた．

また，気づいた 2 人に，埋め込んだ後の筆跡だけを見て，筆跡の変化が分かるかどうかを尋ねた．その結果 2 人とも比較しないと筆跡の変化は気づかないと答えた．

本手法において，送信者と受信者の間でカバーデータになる筆跡を共有する必要はない．よって，本実験の結果からは，本手法によって，筆跡情報にステガノグラフィを構築できることが可能であるといえる．しかし，万が一，もとのカバーデータが流出した場合，本手法におけるステガノグラフィが第三者に気づかれる恐れがあることが分かった．

5. 考　　察

本章では，3 章で示した筆跡情報におけるステガノグラフィについて考察を行う．

5.1 筆跡情報と埋め込めるデータの情報量の関係

筆跡情報のデータ長に対して，埋め込めるデータ量の割合について考察する．

2.1 節で示したように，筆跡情報 **H** は，ユーザが書く 1 つの筆跡を極小時間 T_s ごとに，時刻 T_0 から T_E までサンプリングした時の筆点座標列として表される．

よって，標本化してえられた筆点座標の数 N は，

$$N = \frac{T_E - T_0}{T_s} + 1$$

となる．

本手法における情報の埋め込み手法は，3 章で示したとおり送信者が筆跡情報の任意の隣り合う 2 点の中点を求め，その中点を埋め込む情報に対して移動させ，もとの筆跡情報に追加することである．コードブックによって 1 つの中点に対し p ビットの情報が埋め込め，なおかつ任意の隣り合う 2 点 $k(k \leq N-1)$ 組を取り出す．1 点は，埋め込み終了を表す情報を埋め込むのに利用されるので，情報を埋め込むのに利用できる隣り合う 2 点の組の総数は，$k-1$ になる．

よって，筆跡情報 **H** に埋め込める情報量は次式で表される．

$$p \cdot (k-1) \text{ [bit]}$$

また，情報を埋め込むことによって筆跡情報は，$\frac{k+N}{N}$ 倍増加する．

筆跡情報におけるすべての隣り合う 2 点を情報の埋め込みに利用するとき，埋め込む情報量は最大になる．筆跡情報 **H** において，筆点座標の数が N のとき，隣り合う 2 点の組の総数は，$N-1$ である．よって，情報を埋め込むのに利用できる隣り合う 2 点の組の総数は，$N-2$ になる．このことから最大埋め込み情報量は次式で表される．

$$p \cdot (N-2) \text{ [bit]}$$

また，このときの筆跡情報は，$\frac{2N-1}{N}$ 倍増加する．

埋め込み可能最大情報量を増やすためには，筆跡情報における筆点座標列を増やすもしくはコードブックにおける埋め込むコードと筆跡情報の変化の対応表を大きくする 2 つの手法がある．

筆点座標を増やすには，筆跡を長くする，もしくは T_s をできる限り短くすることである．ただし，情報を埋め込むのに利用する筆跡情報が多くなると，カバーデータの筆跡情報対して，筆跡の細かい変化が多くの場所で見られるようになり，第三者が人為的に筆跡を操作したことに気づき，ステゴデータの存在を発見する恐れがある．

また，コードブックにおいて，p ビットのコードを座標の変化量に対応させるためには $2^p + 1$ のコードと座標の変化量の組を用意する必要がある．ただし，p が増えるに従って，コードと座標の変化量の組を増やす必要があり，それにともない，埋め込みに利用する筆点の移動量が増加する．よって，情報を埋め込む際に筆点の移動量が増加し，第三者が人為的に筆跡を操作したことに気づき，ステゴデータの存在を発見する恐れがある．そこで，コードブックにおける，p ビットのコードと座標の変化量について考察をする．埋め込みに使用するコード C_j が，確率を P_{C_j} で利用されるとしたとする．情報を埋め込むために筆跡情報に追加した中点が，埋め込みに使用するコード C_j に応じて座標が変化するときの移動量の期待値 $\mathbf{c_E}$ は，

$$\mathbf{c_E} = \sum_{j=1}^{2^p+1} P_{C_j} \cdot |\mathbf{c_j}|$$

で表される．

コードブックを作成するとき，あらかじめ送信データが決定している場合は，c_E を計算できるので，c_E を最小にするようにコードブックを作成する．送信データの内容は決定されていない場合，$P_{C_1} = P_{C_2} \cdots = P_{C_{2^p}} = \frac{1}{2^p}$，$P_{C_{2^p+1}} = \frac{1}{k}$ と考え，c_E を最小にするようにコードブックを作成する．今後この結果を利用し，コードブックを作成するアルゴリズムを設計する予定である．

5.2 バイオメトリクス認証を用いたステガノグラフィの検出

ステゴデータを人為的に操作した筆跡であるとアルゴリズム的に解析する手法の 1 つに，バイオメトリクス認証を利用する手法がある．バイオメトリクス認証とは，身体的特徴を利用して，認証を行う仕組みである．身体的特徴として利用されるのは，指紋，声紋，筆跡等[9)~11)] である．筆跡を利用した認証システムでは，複数人の筆跡の性質をシステムに登録しておき，認証する筆跡をシステムに与えて登録していた筆跡から誰が書いた筆跡かを特定するシステムである．たとえば，認証システムに A さんの筆跡が登録されていると仮定する．送信者は，A さんの筆跡に情報を埋め込みステゴデータを作成する．生成されたステゴデータから復元された筆跡は，A さんの筆跡から情報が埋め込まれている部分が変化している．生成された筆跡を認証アルゴリズムに与えた場合，認証アルゴリズム

は，変化している部分が存在するために A さんの筆跡と判定しない可能性がある．

認証アルゴリズムが，筆跡を書く速度の傾向を調べるアルゴリズムを利用している場合，本手法のステガノグラフィを検出する可能性がある．筆跡情報に情報を埋め込むために，特定の 2 点間に筆点座標を付加する必要がある．筆点座標は，ペンの動きを一定時間でサンプリングしたデータであるので，特定の 2 点間に筆点座標を付加することは，その 2 点間だけペンの動作速度が減少したことと同じことになる．認証アルゴリズムが，2 つの筆跡の書く速度の傾向を分析するアルゴリズムを持っていた場合，認証システムは同一人物が書いた筆跡と判定しない可能性があり，本手法におけるステガノグラフィを検出する可能性がある．

今後，認証アルゴリズムに，カバーデータとなる筆跡情報とその筆跡情報から本手法で生成したステゴデータの筆跡情報を与えて，同一人物が書いた筆跡と判断される，ステゴ鍵の開発を行うことが今後の課題である．

5.3 ステゴデータに対する攻撃

第三者が，ステゴデータを変化させ，埋め込まれたデータを破壊する手法について考察する．本手法は，受信者が埋め込まれている情報を復号化するのに，基になるカバーデータの筆跡情報を必要としない．筆跡情報が変更された場合には，埋め込まれたデータを抽出することができない．よって，第三者がステゴデータを変更すると埋め込まれたデータが壊れる可能性がある．また，第三者がステゴデータの一部を破壊したとしても筆跡が人間の目に変化を感じなければ，ステゴデータが破壊されたことを検出するのは困難である．

破壊されたかどうかを検出するには，送信するデータに対してパリティ情報等を付加し送られたデータが正しいかどうかを検証する必要がある．

今後，第三者がステゴデータを変更しても，システムがその変更点を発見し修正できるステゴデータの構築方法を開発することが課題の 1 つである．

6. 関 連 研 究

ステガノグラフィは，インフォメーションハインディングの 1 つであり，情報の存在を秘匿することを目的とする[13),14)]．近年，インフォメーションハインディングの技術の 1 つで，ステガノグラフィの類似技術として，電子透かしがあげられる．電子透かしは，デジタルコンテンツの著作権を明らかにするための手法として，幅広く用いられている[1),14)]．また電子透かしは，デジタルコンテンツの一部の無断引用等を検出するためにも用いられる．特に，静止画，動画，音声に対する電子透かしの研究は幅広く行われている．電子透かしは，第三者に電子透かしが埋まっていることが知られてもかまわないが，画像を改変しても電子透かしを取得できることが重要である．一方，ステガノグラフィは，情報が隠蔽されていること自体が第三者に知られてはいけない．また，秘匿通信等に利用されるので，できる限り多量のデータを隠蔽することが重要である．

筆跡を利用したステガノグラフィの類似研究として，ベクトルデータを利用した電子透かしがあげられる．ベクトルデータを利用した電子透かしの代表的なものとしては，地図情報を利用した電子透かしがある[15),16)]．

従来のベクトルデータは，複数の座標点とその座標点をつなぐ図形（直線，曲線）を表す情報を符号化したものである．たとえば地図情報は，地形情報，建物等の情報が，座標および座標をつなぐ直線，曲線等を表す 2 次元ベクトルの集合として表される．ベクトルデータは，一般的に利用されている画素データと異なり，拡大，縮小，回転をしてももとの図形情報が壊れることはない．一方本論文で提案する筆跡情報は，筆跡を複数の座標点とそれをつなぐ線を表す情報を符号化する点では同一であるが，座標点の情報は，2.1 節で述べたように，従来の座標情報だけではなく，筆圧やペンの傾き等ペンタブレットから入力される 2 次元以上のベクトル情報である．この情報を利用することによって，従来の手法では難しかった，習字のような筆圧，ペンの傾きが書く筆跡に影響を与えるアプリケーションのコンテンツに本論文で提案したステガノグラフィが適用できる．

従来のベクトルデータにおける情報隠蔽は，埋め込む情報の内容とベクトルの変更の仕方（ベクトルの移動，分割等）をあらかじめ決めておき，埋め込む情報をもとのベクトル情報が崩れないようにベクトルを変更することによって実現する．電子透かしの抽出は，電子透かしを埋め込んだ情報ともとのベクトル情報を比較し，変更があったベクトル情報を抽出し，その抽出されたベクトル情報から埋め込まれた情報を抽出する．しかし，たとえば地図情報の電子透かしのように，もし基となる地形情報が存在し，第三者がその地形情報を入手した場合，電子透かしの解析が可能になる．一方，筆跡を用いたステガノグラフィは，地図のように唯一の原本が存在せず，筆跡情報は，筆跡を書いた人のそのときの唯一のもので，完全に同一の筆跡を第三者が手書きによって生成することはできない．また，

送信者が情報を埋め込むために利用した筆跡を破棄しても，受信者に情報を伝えることができる．従来のベクトル型電子透かしに見られる，もとのデータと埋め込んだ後のデータの比較による埋め込みの検出という手法が使えず，筆跡情報を用いたステガノグラフィは，従来のベクトル型電子透かしより安全に運用できると考えられる．

7. おわりに

本論文では，ユーザが書く筆跡に対してステガノグラフィを構築する手法を提案し，プロトタイプシステムを用いて筆跡に対してステガノグラフィが構築できることを示した．本手法は，まず，ユーザが書く手書きの筆跡を，極小時間で標本化を行い，複数の筆点座標に符号化する筆跡情報を取得する．情報の送信者が，情報を埋め込むためのステゴ鍵を利用して，カバーデータとなる筆跡情報に送信する情報を埋め込む．ステゴ鍵は，送信する情報を筆跡の変化量に符号化するコードブックと，カバーデータの筆跡情報の任意の 2 点の中点に埋め込む情報を符号化した変化量に応じてその中点を移動させ，移動した中点をカバーデータに追加するアルゴリズムである．

また，本手法の実現性を示すために，プロトタイプシステムを作成し，筆跡のステガノグラフィを実現した．本手法によって実現したステガノグラフィを，第三者が評価し，情報隠蔽が実現していることを確認した．その結果から，本手法を用いて，特定の利用者が，第三者に対して秘匿通信ができる可能性があることを示した．

今後の研究課題は，効率的な情報の埋め込みを実現するステゴ鍵の開発，認証アルゴリズムに対する対策，本手法におけるステゴデータの攻撃に対する対策である．

5.1 節で示したように埋め込むデータ量は，ステゴ鍵の作り方に依存する．コードブックにおけるコードと埋め込みに利用する点の移動量の関係，埋め込むのに利用する点の個数について，様々なカバーデータから考察を行い，効率が良く多量のデータを埋め込め，なおかつ第三者に発見されないステガノグラフィの実現のためのステゴ鍵の開発を行う．

また，様々な機関で開発されている認証アルゴリズムを入手し，本手法で開発したステガノグラフィをそれらのアルゴリズムに適用し，それらのアルゴリズムがステガノグラフィの発見に利用できるか見極め，本手法のステガノグラフィの評価をする予定である．

謝辞 本研究にあたり様々なご協力をいただいた岩手県立大学ソフト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．特に，研究に対して貴重なご意見をいただいた富田哲也氏に感謝いたします．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みなさまおよび東京農工大学中川研究室のみなさまにつつしんで感謝いたします．

本研究は，文部科学省科学研究費補助金基盤研究（C）「ネットワーク上における戸口通信に関する研究」（課題番号 13680486）および若手研究（B）「筆跡情報を利用したステガノグラフィに関する研究」（課題番号 1570067）の支援を受けて行われました．

参考文献

1) 松井甲子雄：電子透かしの基礎，森北出版 (1998).
2) Segawa, N., Murayama, Y. and Miyazaki, M.: Information Hiding with a Handwritten Message in Vector-drawing Codes, *Proc. 35th Hawaii International Conference on System Sciences 2002*, CD-ROM Proceedings (2002).
3) 中川正樹：ペン入力インタフェースとオンライン手書き文字認識，新版情報処理ハンドブック，第 10 編ヒューマンインタフェース，4 章，4.5 節，pp.1171–1174, オーム社 (1995).
4) 権藤広海，村山優子：ネットワーク上の戸口通信のための戸口伝言板に関する研究，岩手県立大学 2002 年度博士前期課程（ソフトウェア情報学）論文 (2003).
5) Microsoft Tablet PC Home Page. http://www.microsoft.com/windowsxp/tabletpc/（2002 年 12 月現在）
6) タブレット PC 総合情報サイト. http://tabletpc.jp/
7) 藤原　良，神保雄一：符号と暗号の数理，情報数学講座 第 11 巻，共立出版 (1993).
8) 内藤敦士，中川正樹：デジタルインクの一圧縮・復元方式，情報処理学会研究報告，DD，デジタルドキュメント，Vol.96, No.94, pp.9–16 (1996).
9) 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).
10) 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).
11) 孫，大町，加藤，阿曽：特徴量の要素の相関を考慮した高速・高精度な識別関数と文字認識への応用，電子情報通信学会誌 D-II，Vol.J81-D-II, No.9, pp.2027–2034 (1998).

12) Simmons, G.J.: The Prisones' Problem and the Subliminal Channel, *Advances in Cryptology, Proc. CRYPTO '83*, pp.51–67 (1983).
13) Fabien, S.K. and Petitcolas, A.P.: *INFORMATION HIDING, techniques for steganography and digital watermarking*, Artech House Publishers (2000).
14) 情報処理振興事業協会（IPA）：インフォメーションハイディング技術の研究. http://www.ipa.go.jp/security/fy10/contents/crypto/report/Information-Hiding.htm（2002 年 12 月現在）
15) 植田寛郎，大渕竜太郎，遠藤　州：ベクトル型地図データへの電子透かし埋め込み手法，情報処理学会論文誌，Vol.43, No.8, pp.2478–2488 (2002).
16) 栗原　誠，柳井　紳，小松尚久，有田，秀昶：ベクトル表記されたデータに対する電子透かし，情報処理学会研究報告，CSEC，コンピュータセキュリティ，Vol.2000, No.36, pp.1–5 (2000).

(平成 14 年 12 月 10 日受付)
(平成 15 年 6 月 3 日採録)

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．平成 9 年 4 月より東北大学大学院情報科学研究科在籍．工学修士．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，特にペンコンピューティングに関わるセキュリティの研究に従事．電子情報通信学会，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．平成 14 年 4 月より教授．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，情報知識学会各会員．

宮崎　正俊（正会員）

昭和 13 年生．昭和 37 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，同大学院情報科学研究科教授を経て，平成 10 年 4 月岩手県立大学ソフトウェア情報学部教授・学部長（初代，平成 14 年 3 月まで）．平成 15 年 3 月同大学定年退職．平成 15 年 5 月有限会社情報技術総合研究所を設立，代表取締役に就任，現在に至る．昭和 47 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）．東北大学名誉教授．工学博士．専門は基本ソフトウェア，情報システム，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，セキュリティ，情報教育，地域情報化等にも関心を持つ．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，日本ロジスティックスシステム学会，日本都市学会．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．

根元　義章（正会員）

昭和 43 年東北大学工学部通信工学科卒業．昭和 48 年同大学大学院博士課程修了．同年同大学助手，昭和 59 年同大学電気通信研究所助教授，平成 3 年同大学大型計算機センター教授，平成 7 年同大学大学院情報科学研究科教授，平成 10 年より同大学大型計算機センター長併任．工学博士．マイクロ波伝送路回路，衛星利用ネットワーク，情報伝送システム，画像処理，文字認識等の研究に従事．昭和 56 年 IEEE・MTT・Micro Wave Prize 受賞．IEEE 会員．