

ランダム中点変位法によるフラクタル画像へのデータハイディング

林 幸彦[†] 田 中 清^{††} 杉 村 立 夫^{††}

本論文では、コンピュータグラフィックスなどで用いられるフラクタル画像を対象とする、新しいデータハイディングの一手法を提案している。我々は、フラクタル画像生成におけるランダム性に注目し、それをデータハイディングに利用する。画像生成にランダム中点変位法を用い、内挿点のランダム加算値として付加情報のビット系列を分解して埋め込み、逐次粗い解像度から詳細な解像度へと画像表面を生成していく。その結果、従来のランダム中点変位法と比較して、生成画像のフラクタル性をほとんど損わず、十分に自然な形状を呈する地形データを生成することができる。また、257×257画素、256階調の生成画像中に、フラクタル次元に依存しておよそ9～32kバイトに及ぶ情報を埋め込み、内蔵できることを示す。

Data Hiding under Fractal Image Generation via Random Midpoint Displacement Method

YUKIHIKO HAYASHI,[†] KIYOSHI TANAKA^{††} and TATSUO SUGIMURA^{††}

This paper presents a new data hiding scheme under fractal image generation for Computer Graphics (CG) applications. We focus on the randomness in fractal image generation and use it for data hiding. We generate an image surface from coarse to fine resolution via random midpoint displacement method while controlling the additive random variable of interpolating points by bits of additional information to be embedded. As the result, our scheme generates a terrain surface which gives us natural impression without loss of fractalness analogous to conventional scheme. Moreover, about 9 ~ 32 kbytes of additional information can be embedded in a generated 257×257 image with 256 gray levels depending on fractal dimension.

1. ま え が き

近年、高性能コンピュータの普及とネットワークの整備により、ネットワークを利用したマルチメディア情報の流通がさかんである。そこでは、静止画像、映像、音声やテキストなどデジタル化された様々な情報が利用されている。しかし、これらのデジタルコンテンツは取扱いが容易な反面、以下のような課題を含んでいる。

(i) コンピュータを使用すれば第三者がコンテンツを容易に複製・編集したり、配布したりできるので、著作権所有者の著作権を保護する必要があること。

(ii) 大量に取り扱われる各種メディアを効率良く統合し、蓄積・管理する必要があること。

これらの問題に対応しうる有力な方法としてデータ

ハイディングがある¹⁾。このアプローチは画像深層暗号²⁾とも呼ばれ、これまで主として画像データを対象に研究されてきたが、最近では音声を対象とする試みも報告されている³⁾。(i)に目的を絞った方法は電子透かし⁴⁾と呼ばれ、あらかじめ画像データに著作権所有者の署名情報(ID情報やロゴ・マークなど)を密かに埋め込んでおき、第三者の不正利用の抑制を図るとともに、認証に用いようとするものである⁴⁾。この場合、比較的少ない情報量の署名データ⁵⁾を画像内に分散隠蔽し、秘匿度を高めることに重点が置かれている。一方、(ii)の目的では、画像に付随するキャプションなどの付加情報を画像中に埋め込んで一元管理しておき、必要に応じて両者をインタラクティブに表示する。また同時に、埋め込んだ情報の軽易な秘匿効果も期待できる⁶⁾。この場合、画像データを補足するための埋め込み可能な情報量は多い方が望ましい。

従来のデータハイディングの手法は、その大部分が与えられた画像データを何らかの形で処理して情報を埋め込むホール¹⁾を見出し、画質劣化の許される(視

[†] 株式会社日立西部ソフトウェア

Hitachi Western Software Corporation

^{††} 信州大学工学部

Faculty of Engineering, Shinshu University

覚的に識別できない) 範囲で情報を埋め込むものである。一方、コンピュータグラフィックス(CG)などにおける画像生成を対象とするデータハイディングの方法は、これまでに検討されていないようである。

このような観点から、本論文ではコンピュータグラフィックスなどで用いられるフラクタル画像(地形データ)に付加情報を埋め込む新しいデータハイディングの一手法を提案する。海岸線や雲、地形データなどの多くの自然のシーンは、統計的にランダムなフラクタルでよく記述できることが知られている⁷⁾。我々は、フラクタル画像生成⁸⁾におけるランダム性に注目し、それをデータハイディングに利用する。画像生成にランダム中点変位法⁸⁾を用い、内挿点のランダム加算値として付加情報のビット系列を分解して埋め込み、逐次粗い解像度から高い解像度へと画像表面を生成していく。その結果、従来の中点変位法と比較して、生成画像のフラクタル性をほとんど損なわず、十分に自然な形状を呈する地形データを生成することができる。また、257×257画素、256階調の生成画像中にフラクタル次元に依存して、およそ9~32kバイトの容量に及ぶ情報を埋め込み、内蔵できることを示す。本手法は、埋め込む情報をもとに画像を生成するので、従来の与えられた画像データを処理するデータハイディングと比較してより大量の情報を埋め込むことができる。また、本手法の概念は地形データの生成にとどまらず、ランダムフラクタルで生成する様々なオブジェクトに容易に適用できる特徴がある。

以下、2章では準備としてランダムフラクタルに情報を内蔵できることを示唆し、画像生成モデルとして非整数ブラウン運動(fBm)について示す。3章ではfBmを近似しフラクタル画像を生成するランダム中点変位法について示す。4章ではこの方法を修正したデータハイディングをともなうランダム中点変位法を提案し、その具体的な方法を示す。5章ではいくつかの実験結果を示し、考察する。最後に、6章で本論文をまとめ、今後の課題について言及する。

2. 準備

2.1 幾何学的フラクタル

まず、フラクタルを直感的に理解するために、図1に示す3分割コッホ曲線を用いて説明する。コッホ曲線の作り方は、まず、第0世代として図1(a)に示す長さ1の線分を用意する。この線分はイニシエータと呼ばれる。次に、第1世代としてこのイニシエータを図1(b)のような長さ1/3の線分4個で構成される曲線に置き換える。この第1世代の形はジェネレータと

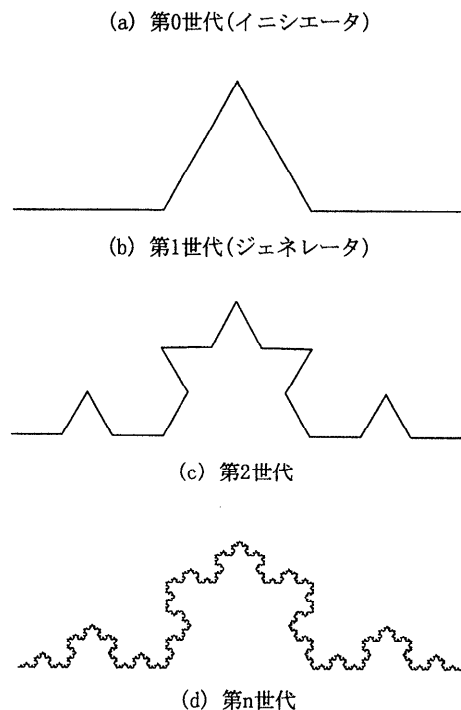


図1 3分割コッホ曲線
Fig. 1 Triadic Koch curve.

呼ばれる。さらに第2世代は、図1(c)に示すように第1世代の構成線分をそれぞれ縮小したジェネレータで置き換えることで得られる。第2世代は、長さ1/9の線分16個で構成される。このように、各世代の構成線分をそれぞれ縮小したジェネレータで置き換え、世代を更新していくと図1(d)のようなコッホ曲線が生成される。この図から明らかなように、コッホ曲線は全体と部分がいたるところで相似な自己相似構造になっており、幾何学的フラクタルと呼ばれる。また曲線の複雑さの度合いはフラクタル次元で特徴づけられ、オブジェクトの構成線分の長さを δ 、構成線分の個数を $N(\delta)$ とすると

$$D = -\frac{\log N(\delta)}{\log \delta} \quad (1)$$

で与えられる⁷⁾。したがって、コッホ曲線のフラクタル次元は、第 n 世代における構成線分の長さが $\delta = 3^{-n}$ で、その個数は $N(\delta) = 4^n$ であるから、これらを式(1)に代入すると

$$D = -\frac{\log 4^n}{\log 3^{-n}} = \log_3 4 \simeq 1.2618$$

となる。

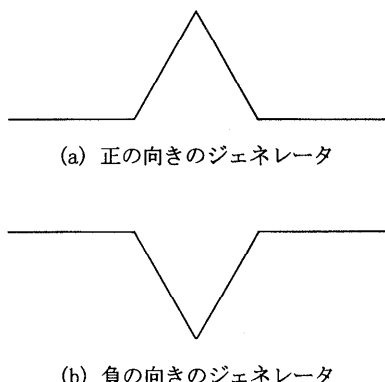


図2 ランダムコッホ曲線のジェネレータ
Fig. 2 Generators of random Koch curve.

2.2 ランダムフラクタル

これに対して、ランダムフラクタルは全体と部分が統計的な意味で自己相似な構造になっており、自然界でしばしば見出される⁷⁾。その典型例として、リアス式海岸のような入り組んだ海岸線があげられる。自然によって形成された海岸線は入り組んだ複雑な形状をしているが、大域的に眺めても、縮尺を変えて局所的に見ても同様に入り組んでおり、その複雑さの度合いはスケールに依存しない特徴がある。

ここで、2.1節で示した3分割コッホ曲線の生成過程において、ランダム性を導入してみよう。すなわち、まず図2に示すように第1世代で得られるジェネレータの向きとして正(+)/負(-)の2パターンを準備する。そして、このジェネレータの向きをランダムに変化させながら第1世代以降の手順を繰り返すと、図3に示すようなランダムコッホ曲線ができあがる。この曲線の形状は、図1(d)に示した本来のコッホ曲線と比べて、複雑さの度合いは同じであるが($D \simeq 1.2618$)、海岸線に似たより自然な印象を与えている。このとき、図2のジェネレータの正(+)/負(-)の向きを1ビットの“1”/“0”符号に見立ててみよう。すると第1世代で1ビット、第2世代で4ビット(合計5ビット)、…、第 n 世代で 4^{n-1} ビット(合計 $(4^n - 1)/3$ ビット)、解像度に制限がなければ無限の情報をランダムコッホ曲線の中に埋め込み、内蔵できることが分かる(図3の例では、系列“10010…”が内蔵されている)。

このように、ランダムさを含むようなフラクタルは自然な印象を与える形状を表現するのに適しているばかりでなく、その形状の中に情報を内蔵できる可能性があることに我々は注目する。

2.3 非整数ブラウン運動

ランダムフラクタルを記述する数学モデルとして、

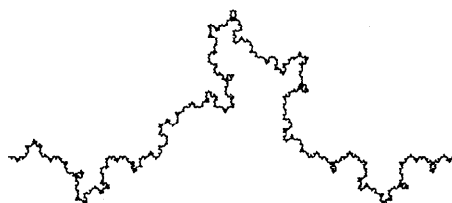


図3 ランダムコッホ曲線
Fig. 3 Random Koch curve.

ブラウン運動と呼ばれる気体中の微粒子の不規則な運動を拡張した非整数ブラウン運動(fractional Brownian motion; 以下fBmと略す)が定義されている^{7),8)}。簡単のために1次元(1変数)の場合を考え、動き回る粒子の時刻 t での位置を $X(t)$ とする。 $X(t)$ の増分が平均0のガウス分布に従い、その分散について

$$\text{var}(X(t_2) - X(t_1)) \propto |t_2 - t_1|^{2H} \quad (0 < H < 1) \quad (2)$$

の関係が成り立つとき、 $X(t)$ はfBmである。ただし、 $\text{var}(\cdot)$ は分散を示す。パラメータ H はハースト指数と呼ばれ、 $X(t)$ の軌跡の複雑さを左右する。すなわち、 $X(t)$ の軌跡は H が0に近いときにはギザギザになり、 H が1に近づくとき滑らかになる。このときフラクタル次元は $2 - H$ で表される。なお、 $H = 1/2$ の場合、式(2)は通常のブラウン運動に帰着する。

この1変数のfBmは、最も単純なランダムフラクタルを構成し、容易に高次元へと拡張できる。一般に、多次元のランダム過程 $X(t_1, t_2, \dots, t_n)$ が以下に示す性質を満たすならば、 $X(t_1, t_2, \dots, t_n)$ は n 次元のfBmである。

(i) 増分 $X(t_1, t_2, \dots, t_n) - X(s_1, s_2, \dots, s_n)$ が平均0のガウス分布に従う。

(ii) 増分 $X(t_1, t_2, \dots, t_n) - X(s_1, s_2, \dots, s_n)$ の分散が、距離

$$\left(\sum_{i=1}^n (t_i - s_i)^2 \right)^{1/2}$$

のみに依存し、距離の $2H$ 乗に比例する。すなわち

$$\begin{aligned} &\text{var}(X(t_1, t_2, \dots, t_n) - X(s_1, s_2, \dots, s_n)) \\ &\propto \left(\sum_{i=1}^n (t_i - s_i)^2 \right)^H \quad (0 < H < 1). \quad (3) \end{aligned}$$

このとき、 $X(t_1, t_2, \dots, t_n)$ の軌跡のフラクタル次元は $n + 1 - H$ となる。

以下、本論文では画像生成の目的から、とくに2次元fBmについて記述する。

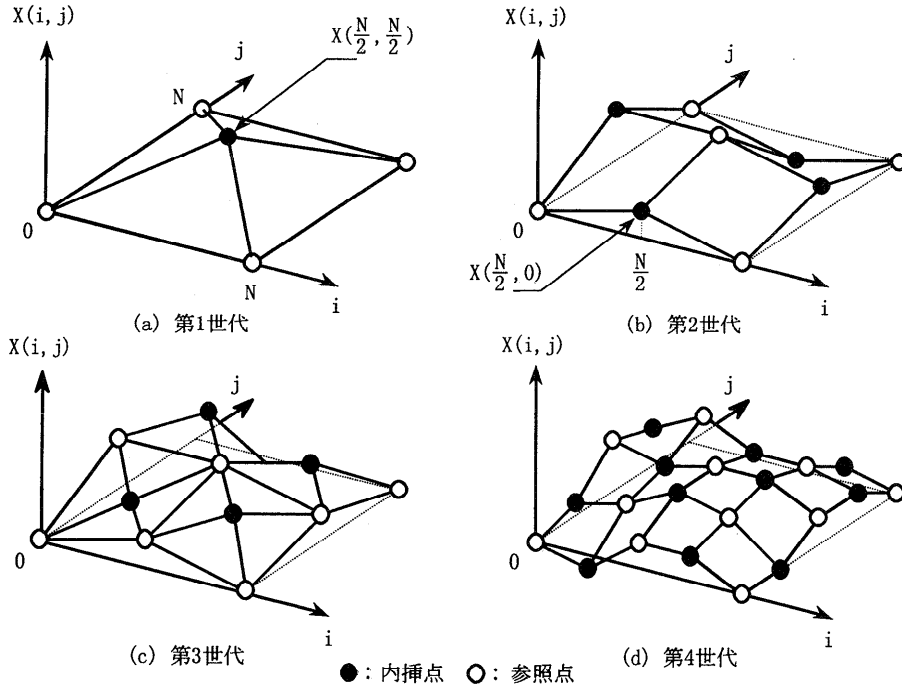


図4 ランダム中点変位法による2次元fBmの生成過程
Fig. 4 2D-fBm generation via random midpoint displacement method.

3. ランダム中点変位法による2次元fBmの生成

fBmを近似する方法として、本論文では単純な規則で効率良くfBmを近似するランダム中点変位法⁸⁾を用いる。ここでは、離散的な2次元平方格子 $[0, N] \times [0, N]$ 上に2次元fBmを生成し、それを $(N+1) \times (N+1)$ 画素の画像として出力する。ただし、 N は2のべき乗の整数である。まず、格子上的4隅の点 $X(0, 0)$, $X(0, N)$, $X(N, 0)$ および $X(N, N)$ を0に設定する。そして、これら4点を参照点とし、中央に位置する点 $X(N/2, N/2)$ を

$$X\left(\frac{N}{2}, \frac{N}{2}\right) = \frac{1}{4}(X(0, 0) + X(0, N) + X(N, 0) + X(N, N)) + D_1 \quad (4)$$

によって内挿する(第1世代; 図4(a)参照)。ここで、 D_1 は平均0のガウス分布に従うランダム加算値で、その分散は $\sigma_0^2(N/\sqrt{2})^{2H}$ である。ただし、 $\sigma_0^2 = N$ とする。次に、新たに4点 $X(N/2, 0)$, $X(0, N/2)$, $X(N, N/2)$ および $X(N/2, N)$ を

$$\left. \begin{aligned} X\left(\frac{N}{2}, 0\right) &= \frac{1}{3}(X(0, 0) + X(N, 0) + X\left(\frac{N}{2}, \frac{N}{2}\right)) + D_2^{(1)} \\ X\left(0, \frac{N}{2}\right) &= \frac{1}{3}(X(0, 0) + X(0, N) + X\left(\frac{N}{2}, \frac{N}{2}\right)) + D_2^{(2)} \\ X\left(N, \frac{N}{2}\right) &= \frac{1}{3}(X(N, 0) + X(N, N) + X\left(\frac{N}{2}, \frac{N}{2}\right)) + D_2^{(3)} \\ X\left(\frac{N}{2}, N\right) &= \frac{1}{3}(X(0, N) + X(N, N) + X\left(\frac{N}{2}, \frac{N}{2}\right)) + D_2^{(4)} \end{aligned} \right\} \quad (5)$$

によって内挿する(第2世代; 図4(b)参照)。ここで、 $D_2^{(1)} \sim D_2^{(4)}$ は同様に平均0のガウス分布に従うランダム加算値で、その分散は $\sigma_0^2(N/2)^{2H}$ である。さらに、式(4), (5)と同様な処理を $[0, N/2-1] \times [0, N/2-1]$, $[N/2, N] \times [0, N/2-1]$, $[0, N/2-1] \times [N/2, N]$ および $[N/2, N] \times [N/2, N]$ の4つの部分正方領域について行う(第3~4世代; 図4(c)~(d)参照)。以下、再帰的にさらに小さな部分正方領域に同様な処理を適用し、所望の解像度におけるすべての振幅値 $X(i, j)$ ($i, j = 0, 1, \dots, N$) が内挿されるまで繰り返す。第 n 世代における平均0のガウス分布に従うランダム加算値 D_n の分散は、一般に

$$\sigma_n^2 = \sigma_0^2 (2^{-\frac{n}{2}} N)^{2H} \quad (6)$$

で与えられる．また，第 n 世代における内挿点の数 p_n ($n = 1, 2, \dots, n_f$) は

$$p_n = \begin{cases} 2^{n-1} & (n = \text{奇数}) \\ 2^{n-1} + 2^{\frac{n}{2}} & (n = \text{偶数}) \end{cases} \quad (7)$$

で与えられる．ここで， n_f は最終世代番号を示す．たとえば， $N = 256$ のとき $n_f = 16$ となり，全世代にわたる内挿点の数は $(N+1)^2 - 4 = 66,045$ 個である．

得られた $X(i, j)$ は実数値であるので，表示装置で表現可能なグレイレベルなどを考慮して適当に線形変換した後，

$$X'(i, j) = \lfloor sX(i, j) + t \rfloor \quad (8)$$

によって整数化する．ただし， $\lfloor \cdot \rfloor$ は小数点以下切り捨て処理を示す．

4. データハイディングをともしうランダム中点変位法

4.1 シングルビット埋め込み

4.1.1 情報の埋め込み

従来のランダム中点変位法では，内挿点のランダム加算値 D_n に関して，平均と分散以外に制約がない．そこで，2.2 節で示したランダムコッホ曲線の考え方を思い出すと，加算値 D_n の符号は正 (+) でも負 (-) でもかまわない．この点に注目して， D_n の符号 (正負) を別の情報源 (付加情報) から抽出した 1 ビットの符号 (“1” あるいは “0”) に対応させ，振幅の決定を試みる．以下，このような内挿点の振幅の決定操作を埋め込みと呼ぶことにする．ただし，自然な形状を生成する必要性から，埋め込むビット系列はシフトレジスタ⁹⁾などを用いてあらかじめランダムな系列 $B = b_k \in \{0, 1\}$ ($k = 1, 2, \dots$) として準備しておく．

まず，3 章と同様に $[0, N] \times [0, N]$ の離散的な 2 次元格子を用意する．そして，格子上の四隅の点 $X(0, 0)$ ， $X(0, N)$ ， $X(N, 0)$ および $X(N, N)$ の値を 0 とする．内挿の第 1 世代では，図 4(a) と同様に四隅の点を参照点とし， $X(N/2, N/2)$ の値を

$$X\left(\frac{N}{2}, \frac{N}{2}\right) = \frac{1}{4}(X(0, 0) + X(0, N) + X(N, 0) + X(N, N)) \pm |D_1| \quad (9)$$

として決定する．ここで，式 (9) の右辺第 2 項の符号は，埋め込む系列 B から抽出した 1 ビットの値に

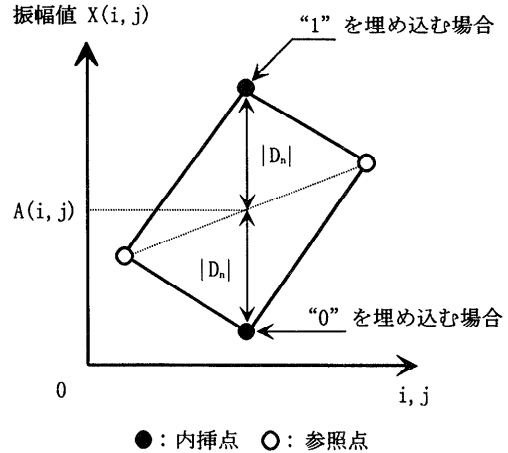


図 5 シングルビット埋め込みによる振幅値の決定

Fig. 5 Determination of amplitude value by single-bit embedding.

依存して決定する．たとえば， $b_1 = 1$ のとき，4 つの参照点の平均値に $|D_1|$ を加算し， $b_1 = 0$ のとき， $-|D_1|$ を加算する（もちろん，この規則は反対でもかまわない）．ただし，復号時に埋め込まれたビットを誤りなく識別するために，ここでは $D_n \neq 0$ とする．内挿の第 2 世代では，図 4(b) と同様に， $X(N/2, 0)$ ， $X(0, N/2)$ ， $X(N, N/2)$ および $X(N/2, N)$ の値を決定する．これらの値は次式によって決定される．

$$\left. \begin{aligned} X\left(\frac{N}{2}, 0\right) &= \frac{1}{3}(X(0, 0) + X(N, 0) + X\left(\frac{N}{2}, \frac{N}{2}\right)) \pm |D_2^{(1)}| \\ X\left(0, \frac{N}{2}\right) &= \frac{1}{3}(X(0, 0) + X(0, N) + X\left(\frac{N}{2}, \frac{N}{2}\right)) \pm |D_2^{(2)}| \\ X\left(N, \frac{N}{2}\right) &= \frac{1}{3}(X(N, 0) + X(N, N) + X\left(\frac{N}{2}, \frac{N}{2}\right)) \pm |D_2^{(3)}| \\ X\left(\frac{N}{2}, N\right) &= \frac{1}{3}(X(0, N) + X(N, N) + X\left(\frac{N}{2}, \frac{N}{2}\right)) \pm |D_2^{(4)}| \end{aligned} \right\} \quad (10)$$

ここでも，第 1 世代と同様に右辺第 2 項の符号は，埋め込むビット $b_2 \sim b_5$ の値に依存して決定する．

このように，埋め込む情報 B から抽出した 1 ビットの値 b_k ($k = 1, 2, \dots$) を用い，オリジナルの中点変位法と同様に各世代の内挿点の値を順次決定していく．一般に，第 n 世代の内挿点の値 $X(i, j)$ は，参照点の平均値を $A(i, j)$ とすると，

$$X(i, j) = A(i, j) \begin{cases} +|D_n| & (b_k = 1) \\ -|D_n| & (b_k = 0) \end{cases} \quad (11)$$

と表される．この様子を図 5 に示す．この方法では，参照点の平均値に対する加算値の正負の符号を埋め込

む1ビットの値に対応させているので、各内挿点に1ビットの情報が含まれている。したがって、画素数が $(N+1) \times (N+1)$ の画像を生成するとき、埋め込み可能なビット数の合計 T_b は

$$T_b = (N+1)^2 - 4 \quad (12)$$

である。すべての内挿作業が終了した後に、すべての内挿点の値は式(8)によって $X'(i, j)$ に整数化される。ただし、整数化は内挿点の決定と同様な順序で行い、復号時に埋め込まれた情報を後述の式(13)によって正しく抽出できるように、 b_k と $A'(i, j)$ の値を参照し、必要に応じて $X'(i, j)$ の値を微小に補正する。ここで、 $A'(i, j)$ はすでに整数化された参照画素の平均値を示す。

4.1.2 埋め込まれた情報の復号

次に、整数化された $X'(i, j)$ の系列、すなわち生成画像から埋め込まれた情報を復号する方法を示す。埋め込まれた1ビットの値 b_k ($k = 1, 2, \dots$) は、参照点の平均値と内挿値の大小関係を調べればよいので、

$$\left. \begin{aligned} b_k &= 1 & (X'(i, j) > A'(i, j)) \\ b_k &= 0 & (X'(i, j) < A'(i, j)) \end{aligned} \right\} \quad (13)$$

として容易に復号できる。ここで、 $A'(i, j)$ は参照画素の平均値であり、前述の補正処理により $X'(i, j) = A'(i, j)$ となることはない。ただし、この作業は画像生成時と同じ順序で各世代の内挿点に対して順次行い、最終的に復号したビットを系列 B として再構成する。

4.2 マルチビット埋め込み

シングルビット埋め込みでは、各内挿点に埋め込み可能な情報量は1ビットだけであった。そこでこの節では、埋め込み可能な情報量を増加させるために、1つの内挿点に複数のビットを埋め込むことを試みる。

4.2.1 情報の埋め込み

まず、内挿点のランダム加算値 D_n に関するガウス分布の条件をランダムな一様分布に緩和する。そして、式(6)より、第 n 世代の $|D_n|$ の最大値 r_n を

$$r_n = \sigma_n \quad (n = 1, 2, \dots, n_f) \quad (14)$$

とする。ここで、 r_n はハースト指数 H に依存することに注意する。ランダム中点変位法にこのような修正を加えても、ガウス分布を用いる従来法との差は少なくとも生成画像を見る限り識別できない。文献8)では、ガウス分布を他の分布に置き換えることで、むしろより地形らしい形状を生成できる可能性を示唆している。 D_n のとりうる範囲を係数 s でスケールした区間幅は

$$R_n = [2r_n s] \quad (15)$$

となる。係数 s の算出法については4.2.3項で述べ

る。ランダム中点変位法による加算値として、この区間 R_n 内の任意の整数値を選ぶことができるので、 R_n には

$$b_n = \lfloor \log_2 R_n \rfloor \text{ (bits)} \quad (16)$$

の情報を埋め込むことができる。したがって、全世代にわたり埋め込み可能なビット数の合計 T_b は、式(7)の p_n と b_n を用いて

$$T_b = \sum_{n=1}^{n_f} p_n b_n \text{ (bits)} \quad (17)$$

となる。

以下、3章と同様の順序で $[0, N] \times [0, N]$ の平方格子内の各内挿点に系列 B から取り出した複数のビットを埋め込みつつ、内挿を行う。ここでは、最初に決定する四隅の参照点 $X(0, 0)$, $X(0, N)$, $X(N, 0)$ および $X(N, N)$ の値を α とする。この α は、すべての内挿点の値を正の整数とするためのオフセット値であり、この算出方法についても4.2.3項で後述する。

第1世代では、 B から b_1 ビットの埋め込み情報 I_1 (b_1 ビットのデータを整数値としたもの)を抽出し、これを使用して内挿値 $X(N/2, N/2)$ を

$$\begin{aligned} X\left(\frac{N}{2}, \frac{N}{2}\right) &= \left\lfloor \frac{1}{4}(X(0, 0) + X(0, N) + X(N, 0) \right. \\ &\quad \left. + X(N, N)) - \frac{R_1}{2} + I_1 \frac{R_1}{2^{b_1} - 1} \right\rfloor \end{aligned} \quad (18)$$

により決定する。ここで、 b_1 と R_1 は式(14)～(16)によって算出される。

第2世代では、系列 B から引き続く4個の b_2 ビットの埋め込み情報 $I_2 \sim I_5$ を抽出し、図4(b)と同様に次式を用いて内挿する。

$$\left. \begin{aligned} X\left(\frac{N}{2}, 0\right) &= \left\lfloor \frac{1}{3}(X(0, 0) + X(N, 0) \right. \\ &\quad \left. + X\left(\frac{N}{2}, \frac{N}{2}\right)) - \frac{R_2}{2} + I_2 \frac{R_2}{2^{b_2} - 1} \right\rfloor \\ X\left(0, \frac{N}{2}\right) &= \left\lfloor \frac{1}{3}(X(0, 0) + X(0, N) \right. \\ &\quad \left. + X\left(\frac{N}{2}, \frac{N}{2}\right)) - \frac{R_2}{2} + I_3 \frac{R_2}{2^{b_2} - 1} \right\rfloor \\ X\left(N, \frac{N}{2}\right) &= \left\lfloor \frac{1}{3}(X(N, 0) + X(N, N) \right. \\ &\quad \left. + X\left(\frac{N}{2}, \frac{N}{2}\right)) - \frac{R_2}{2} + I_4 \frac{R_2}{2^{b_2} - 1} \right\rfloor \\ X\left(\frac{N}{2}, N\right) &= \left\lfloor \frac{1}{3}(X(0, N) + X(N, N) \right. \\ &\quad \left. + X\left(\frac{N}{2}, \frac{N}{2}\right)) - \frac{R_2}{2} + I_5 \frac{R_2}{2^{b_2} - 1} \right\rfloor \end{aligned} \right\} \quad (19)$$

以下、同様の内挿作業を再帰的に繰り返していくが、一般に k 番目に内挿される $X(i, j)$ の値は

$$\begin{aligned} X(i, j) &= \left\lfloor A(i, j) - \frac{R_l}{2} + I_k \frac{R_l}{2^{b_l} - 1} \right\rfloor \\ &\quad (k = 1, 2, \dots, (N+1)^2 - 4) \end{aligned} \quad (20)$$

によって決定される。ただし、 l は k 番目の内挿点に

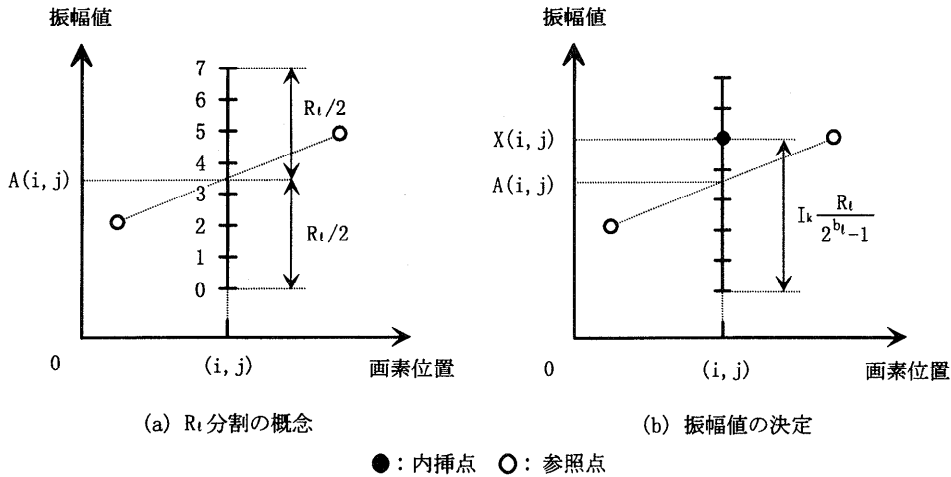


図6 マルチビット埋め込みによる振幅値の決定

Fig. 6 Determination of amplitude value by multi-bits embedding ($b_l = 3$).

対応する世代番号を示し, l と k は

$$\sum_{n=1}^l p_{n-1} < k \leq \sum_{n=1}^l p_n \quad (l = 1, 2, \dots, n_f) \quad (21)$$

の関係にある。ここで, $p_0 = 0$ である。また, $A(i, j)$ は $X(i, j)$ を決定するのに必要な周辺の4 (または3) 個の参照画素の平均値, I_k は k 番目の内挿点に埋め込まれる系列 B から抽出した b_l ビットの整数値である。この埋め込みの様子を便宜上1次元的に図6に示す。つまり, 内挿値のとりうる範囲 R_l を 2^{b_l} 個に分割し, 埋め込む b_l ビットの情報 I_k ($0 \leq I_k < 2^{b_l}$) に対応する位置を内挿値とする。すべての内挿点は, 3章で示したとおり各世代ごとに粗い解像度から精細な解像度へ, 左上の部分正方領域から右下の部分正方領域へ決定されていく。ただし, マルチビット埋め込みでは, 式(20)により直接整数化された $X(i, j)$ が生成される。

4.2.2 埋め込まれた情報の復号

生成された画像から埋め込まれたデータ I_k ($k = 1, 2, \dots$) を復号する方法を示す。まず, 画像生成に使用したハースト指数 H を準備し, H と式(6), 式(14)~(16)を用い, 各世代の埋め込みビット数 b_n と加算値のとりうる範囲 R_n を算出する。そして, 生成された画像データを埋め込み操作(内挿)と同様に各世代ごと粗い解像度から精細な解像度へ, また左上の部分正方領域から右下の部分正方領域へ順次走査し, 逐次埋め込まれた情報を復号する。すなわち, 第1世代の内挿点に埋め込まれた I_1 は, 式(18)を変形して

$$I_1 = \left[\left(X\left(\frac{N}{2}, \frac{N}{2}\right) - \frac{1}{4} \left(X(0, 0) + X(0, N) + X(N, 0) + X(N, N) \right) + \frac{R_1}{2} \right) \frac{2^{b_1} - 1}{R_1} \right] \quad (22)$$

から求める。同様に, 第2世代の内挿点に埋め込まれた情報, たとえば, I_2 は

$$I_2 = \left[\left(X\left(\frac{N}{2}, 0\right) - \frac{1}{3} \left(X(0, 0) + X(0, N) + X\left(\frac{N}{2}, \frac{N}{2}\right) \right) + \frac{R_2}{2} \right) \frac{2^{b_2} - 1}{R_2} \right] \quad (23)$$

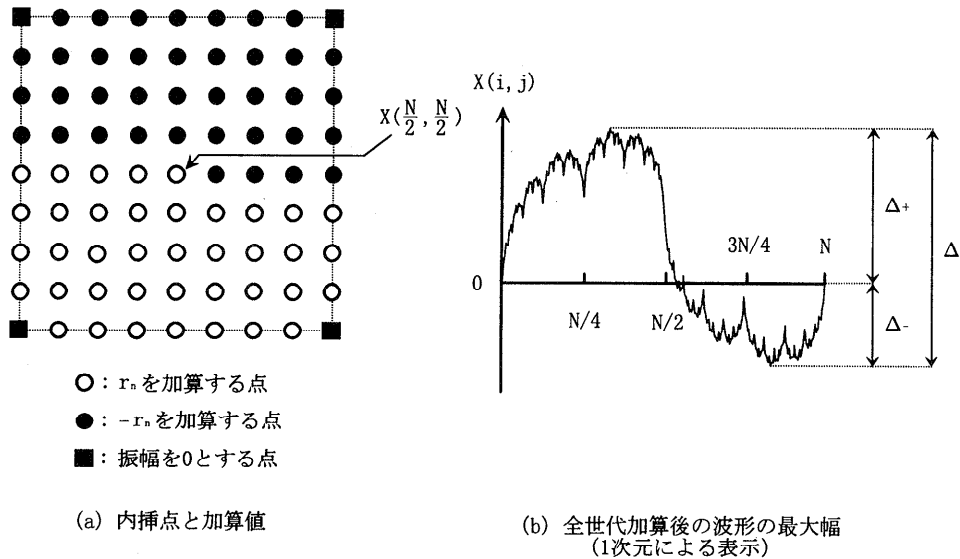
により得られる。一般に, k 番目に内挿された情報 I_k は

$$I_k = \left[\left(X(i, j) - A(i, j) + \frac{R_l}{2} \right) \frac{2^{b_l} - 1}{R_l} \right] \quad (k = 1, 2, \dots, (N+1)^2 - 4) \quad (24)$$

によって容易に復号することができる。ただし, $\lceil \cdot \rceil$ は小数点以下の切上げによる整数化処理を示す。各内挿点から復号された I_k は, 最終的に系列 B として再構成される。

4.2.3 係数 s の算出

マルチビット埋め込み方式では, 埋め込み可能なビット数 b_n が使用できるグレイレベルに依存して変化するため, 内挿を行う前にあらかじめ係数 s を算出しておく必要がある。そこで, 式(14)の r_n を用い, 生成される $X(i, j)$ がとりうる最大幅 Δ を求める。まず, $X(0, 0)$, $X(0, N)$, $X(N, 0)$ および $X(N, N)$ を0とおき, 式(4)による内挿の第1世代の加算値 D_1 を r_1 として $X(N/2, N/2)$ を決定する。続く第2世代では,

図7 最大幅 Δ の算出Fig. 7 Calculation of maximum amplitude width Δ .

$X(0, N/2)$, $X(N/2, 0)$ については $D_2 = r_2$ とし, $X(N/2, N)$, $X(N, N/2)$ には $D_2 = -r_2$ を用いる. このような手順で図7(a)に示すように, $X(N/2, N/2)$ を境とする2つの領域において, 一方には r_n を加算し, 他方には $-r_n$ を加算することを反復して, $X(i, j)$ がとりうる最大幅 Δ を事前に求める (図7(b)参照). 得られた Δ と表示可能なグレイレベル L を

$$s = \frac{L}{\Delta} \quad (25)$$

に代入し, 係数 s を求める. 次に, 2次元格子 $[0, N] \times [0, N]$ 上の四隅の値として最初に設定する α の算出方法を示す. オフセット α を用いる理由は, 生成される $X(i, j)$ の値をすべて正の値にするためである. α は算出された s を用い, 第1世代の内挿で用いられる埋め込みデータ I_1 に依存して,

$$\alpha = \begin{cases} \lfloor s\Delta_- \rfloor & (I_1 > \frac{2^{b_1}-1}{2}) \\ \lfloor s\Delta_+ \rfloor & (I_1 < \frac{2^{b_1}-1}{2}) \end{cases} \quad (26)$$

として設定する.

5. 実験結果と考察

シミュレーション実験では, 生成画像の仕様を $N = 256$ すなわち 257×257 画素, グレイレベルを $L = 256$ に設定した. まず, この条件におけるマルチビット埋め込みによって画像全体に埋め込み可能なビット数 T_b を表1に示す. シングルビット埋め込みではフラクタル次元にかかわらず一律に $T_b = 66,045$ ビット

表1 埋め込み可能な情報量

Table 1 The amount of embedable bits/bytes.

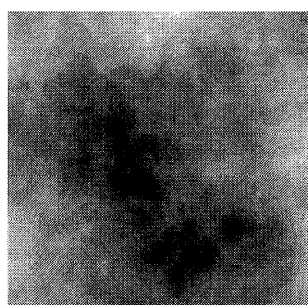
フラクタル次元	T_b (bits / bytes)
$D = 2.9$ ($H = 0.1$)	264,321 / 33,040
$D = 2.7$ ($H = 0.3$)	214,913 / 26,864
$D = 2.5$ ($H = 0.5$)	167,370 / 20,921
$D = 2.3$ ($H = 0.7$)	103,915 / 12,989
$D = 2.1$ ($H = 0.9$)	75,831 / 9,478

(8,255 バイト)であったが, マルチビット埋め込みにより, その情報量が増加していることが分かる. このとき, フラクタル次元 D が3に近づく (H が0に近づく) ほど, つまり生成画像の起伏が激しいほど, 埋め込み可能な情報量が増加する. なお, 参考のためにマルチビット埋め込みによって各内挿点に埋め込まれたビット数とその頻度 (画素数) を計測した結果を表2に示しておく.

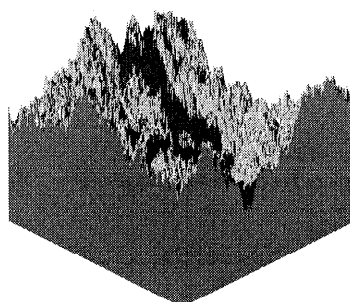
次に, 生成された画像データの例をグレイレベル表示および鳥瞰図として図8, 図9および図10に示す. 図8はシングルビット埋め込みによる生成画像, 図9はマルチビット埋め込みによる生成画像であり, 参考のために図10に従来の中点変位法による出力画像を示す. ただし, すべての生成画像のフラクタル次元は $D = 2.3$ ($H = 0.7$) であり, 振幅の最大幅 Δ が等しくなるようにスケーリングしてある. 図8, 図9の情報埋め込まれた画像は, ランダム中点変位法における内挿点のランダム加算値の正 (+)/負 (-) の符号や振幅値をランダムなビット系列 B によって制御・決

表2 画素あたりの埋め込みビット数とその頻度
Table 2 Embedable bits per pixel and their frequencies.

フラクタル次元	埋め込みビット数と頻度						
	7	6	5	4	3	2	1
$D = 2.1 (H = 0.9)$	1	20	56	208	800	7,232	57,728
$D = 2.3 (H = 0.7)$	1	8	68	464	3,680	28,800	33,024
$D = 2.5 (H = 0.5)$	—	9	132	1,968	30,912	33,024	—
$D = 2.7 (H = 0.3)$	—	—	141	16,496	49,408	—	—
$D = 2.9 (H = 0.1)$	—	—	141	65,904	—	—	—

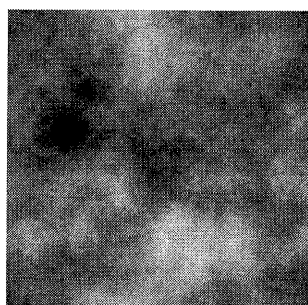


(a) グレイレベル表示

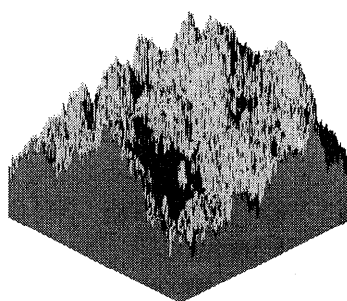


(b) 鳥瞰図

図8 シングルビット埋め込みによる生成画像

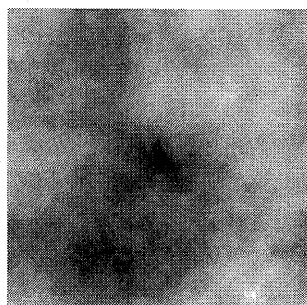
Fig. 8 Generated image by single-bit embedding ($D = 2.3$).

(a) グレイレベル表示

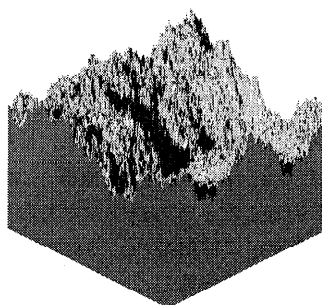


(b) 鳥瞰図

図9 マルチビット埋め込みによる生成画像

Fig. 9 Generated image by multi-bits embedding ($D = 2.3$).

(a) グレイレベル表示



(b) 鳥瞰図

図10 従来法による生成画像

Fig. 10 Generated image by conventional scheme ($D = 2.3$).

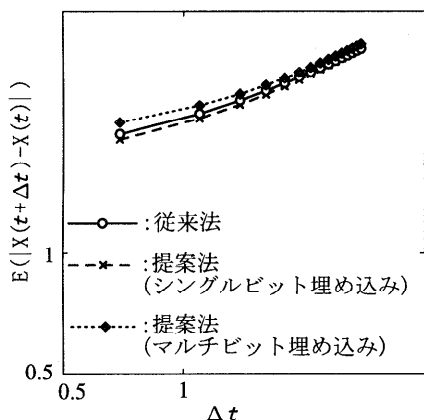


図 11 生成画像のフラクタル性

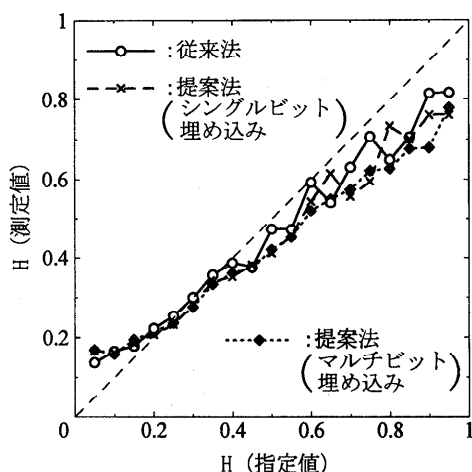
Fig. 11 Fractal plots for generated images ($D = 2.3$).

図 12 生成前後のハースト指数の対応関係

Fig. 12 Relationship between Hurst exponents before and after image generation.

定しているにもかかわらず、図 10 で示した本来の中間変位法と変わらない自然な印象を与える地表面データが生成されていることが分かる。

次に、生成画像のフラクタル性について調べてみた。文献 10) にない、図 8～図 10 の生成画像について $\log E|X(t+\Delta t) - X(t)|$ と $\log \Delta t$ をプロットしたものを図 11 に示す。ただし、 t は画像上の座標、 Δt は変位、 $E(\cdot)$ は Δt を固定したときの期待値である。これよりプロットの線形性がほぼ保たれ、またフラクタル次元を示す直線の傾きもほぼ等しく、情報の埋め込みにより生成画像のフラクタル性は従来法に比べてほとんど損なわれていないことが分かる。

さらに、画像生成前に指定したハースト指数 H が生成後の画像にどの程度正確に反映されているか調べ

てみた。その結果を図 12 に示す。これより、提案法も従来の中間変位法と同様に $H = 0.2 \sim 0.3$ 付近で正確な波形生成が可能である。それ以外の値では、指定したハースト指数からややずれた複雑さの波形が生成されているが、このグラフに基づく対応表をあらかじめ作成しておくことで、所望の複雑さの波形を得ることが可能である。

6. む す び

本論文では、コンピュータグラフィックスなどで用いられるフラクタル画像を対象とする、中間変位法に基づく新しいデータハイディングの一手法を提案した。まず、シングルビット埋め込みでは、中間変位法における内挿点のガウス分布に従うランダム加算値の正 (+)/負 (-) の符号を埋め込むランダムなビット系列で制御した。その結果、フラクタル次元にかかわらず各内挿点に 1 ビットずつ、 $(N+1) \times (N+1)$ 画素からなる生成画像中に $(N+1)^2 - 4$ ビットの情報を埋め込むことができた。次に、埋め込み可能な情報量をさらに増加させる観点から、マルチビット埋め込みでは、中間変位法における内挿点のランダム加算値に関する枠組みをガウス分布からランダムな一様分布に緩和した。そして、各内挿点でとりうる振幅の範囲を分割し、振幅値を埋め込むランダムなビット系列の値に応じて決定した。その結果、 257×257 画素、256 階調の生成画像に、フラクタル次元に依存して 9 ～ 32 k バイトの情報を埋め込むことができた。さらに、本手法で生成したフラクタル画像は、従来の中間変位法と同様にほとんどフラクタル性を損なわず、十分に自然な印象を与える形状をしており、実際の CG 画像として十分利用できるとされる。また、本手法の概念は地形データの生成にとどまらず、ランダムフラクタルで生成できる様々なオブジェクトに容易に適用可能である。さらに、埋め込む情報をもとに画像を生成するという本手法の特徴は、情報を画像に見せかけたステガノグラフィックな秘匿通信手段¹¹⁾としての応用も考えられる。

今後の課題として、実用上の観点から本手法の応用場面を特定し、それに適応するシステムを構築することがあげられる。たとえば、コンピュータによる仮想現実世界でフラクタルオブジェクトの描写が必要とされる場面では、その形状データの蓄積方法について考慮する必要がある。本手法で生成される形状データに一般的有歪データ圧縮を加えると、埋め込まれた情報に欠損が生じ、同時に形状データのフラクタル性も失われてしまう。データの欠損については埋め込む情

報にあらかじめ誤り訂正符号¹²⁾を施しておくことが考えられる。また、生成データのフラクタル性を失わず、できるだけ埋め込まれた情報に損傷を与えないデータ圧縮に関する検討も必要と思われる。

謝辞 本研究の推進にあたり、その基礎を築きながら不慮の事故で他界した故水野幸崇君に深謝するとともに、本論文を捧げ、心からのご冥福を祈念いたします。

参 考 文 献

- 1) Bender, W., Gruhl, D. and Morimoto, N.: *Techniques for Data Hiding*, MIT Media Laboratory (1997).
- 2) 松井甲子雄: 画像深層暗号, 森北出版 (1993).
- 3) 岩切宗利, 松井甲子雄: 適応差分 PCM 符号化における音声符号へのテキスト情報の埋込み, 情報処理学会論文誌, Vol.38, No.10, pp.2053-2061 (1997).
- 4) 高橋史忠: 電子透かしがマルチメディアを守る, 日経エレクトロニクス, No.683, pp.99-124 (1997).
- 5) 森本典繁, 清水周一, 沼尾雅之: デジタルメディアへのデータハイディング, 第 53 回情報処理学会全国大会論文集, 第 2 分冊, pp.259-260 (1996).
- 6) 片岡利幸, 田中 清, 中村康弘, 松井甲子雄: 適応型離散コサイン変換符号化におけるカラー画像への記述情報の埋込み, 電子情報通信学会論文誌 (B-I), Vol.J72-B-I, No.12, pp.1210-1216 (1989).
- 7) Mandelbrot, B.B.: *The Fractal Geometry of Nature*, Freeman, New York (1983).
- 8) Peitgen, H.-O. and Saupe, D. (Ed.): *The Science of Fractal Images*, Springer-Verlag, New York (1988).
- 9) 柏木 潤: M 系列とその応用, 昭晃堂 (1996).
- 10) 横矢直和, 山本和彦, 舟久保登: フラクタルによる 3 次元自然形状の解析とその地形モデル作成への応用, 電子情報通信学会論文誌 (D), Vol.J70-D, No.12, pp.2605-2614 (1987).
- 11) Johnson, N.F. and Jajodia, S.: Exploring Steganography: Seeing the Unseen, *IEEE Computer*, Vol.31, No.2, pp.26-34 (1998).
- 12) Peterson, W.W. and Weldon, Jr. E.J.: *Error-Correcting Codes*, MIT Press (1996).

(平成 10 年 3 月 17 日受付)

(平成 10 年 10 月 2 日採録)

林 幸彦

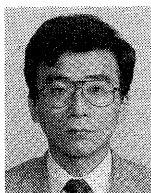


昭和 49 年生。平成 8 年信州大学工学部電気電子工学科卒業。平成 10 年同大大学院博士前期課程修了。同年 (株) 日立西部ソフトウェア入社。在学中はフラクタル画像生成に関する研究に従事。電子情報通信学会会員。

田中 清



昭和 36 年生。昭和 59 年防衛大学校電気工学科卒業。平成元年同大学理工学研究科オペレーションズリサーチ専攻修了。平成 4 年同大学情報工学科助手。平成 7 年信州大学工学部電気電子工学科助教授。現在に至る。画像処理、フラクタル工学、情報セキュリティ等に関する研究に従事。工学博士。IEEE, 電子情報通信学会, 画像電子学会等会員。



杉村 立夫 (正会員)

昭和 27 年生。昭和 51 年大阪大学工学部通信工学科卒業。昭和 57 年同大大学院博士後期課程修了。工学博士。同年松下電器産業 (株) 入社。昭和 60 年福岡工業大学助教授。平成 3 年信州大学工学部電気電子工学科助教授。現在に至る。誤り訂正符号の構成およびその応用, 有限体理論, 情報セキュリティに関する研究に従事。IEEE, 電子情報通信学会, 情報理論とその応用学会各会員。