

# 擬似乱数でつくる一重と二重の電子透かし画像 Constructing Single and Double Digital Watermark based on Pseudorandom

佐々木隆幸

弘前大学大学院理工学研究科

長瀬智行

弘前大学大学院理工学研究科

**概要**：この発表は、擬似乱数を用いて、1枚の画像の中に1枚の情報画像を埋め込める一重の電子透かし画像と、1枚の画像の中に2枚の情報画像を埋め込める二重の電子透かし画像を制作し再生する方法を提案するものである。

この提案には3つの考案がある。1つ目は擬似乱数を直交関数系につくり変えたことである。2つ目は埋め込む情報画像の画素値を限定された範囲の整数値に量子化したことである。3つ目は二重に埋め込む場合に情報画像1枚あたり3ビットの画素空間を利用する2層構造にしたことである。

ここでは、これらの考案をイラストや画像で例示しながら、擬似乱数による一重と二重の電子透かし画像の制作および再生について発表する。

**キーワード**：電子透かし画像、擬似乱数、直交関数系、量子化、2層構造

## 1. はじめに

デジタル技術の進歩により、医療診断画像のような大きな画像を容易に伝達[1]できるようになってきた。その反面、画像をいとも簡単に盗聴や改ざんをすることができるようになり、社会的トラブルを生んでいる。その対処方法の1つとして、電子透かし技術が盛んに研究されている。その技術に採用される直交関数系の多くは、三角関数やハール関数など超越関数に属する関数[2][3][4]が大半で、代数関数に属する直交多項式で構成される直交関数系が採用されるのは、見当たらない[5][6][7][8]。そして、擬似乱数を採用した電子透かしに関しては、ほぼ皆無である。そこで、擬似乱数を用いた一重および二重の電子透かし画像の制作と再生を試みたので、ここに発表する。

以降で用いる用語を整理しておく。電子透かし情報として埋め込む秘匿情報を情報画像、その画像を直交関数系で変換した画像をホログラム、ホログラムを埋め込むために用いた日常的な画像を土台画像、ホログラムを埋め込んだ土台画像を電子透かし画像または単に電子透かし、電子透かし画像から再生した情報画像を再生画像と呼ぶことにする。

さらに、電子透かし画像の制作・再生における条件を次に設定する。画像形式はすべてBMP形式とする。画素数を $N$ と表し、 $N = 128$ とする。画像サイズはすべて $128 \times 128$ とする。画像の伸長や縮小などのスケール変換はないものとする。なお、記号 $Z_{ij}$ は画像画面の左下から右上に数えて $i$ 行 $j$ 列目の画素値が $Z$ であることを表すものとする。

## 2. 擬似乱数の直交化と正規化

電子透かし画像に取り上げた擬似乱数は、ソフトウェア「Mathematica」(Wolfram Research社)が発生する擬似乱数である。擬似乱数の値は $0 \sim 1$ までの正の小数で、端点の $0$ と $1$ は含まない。この擬似乱数を電子透かし画像に採用できるようにするため、直交化と正規化の手続きを行う。

### (1) 直交化

①16384個の擬似乱数を発生させ、その値を $0.5$ だけ下げた。正と負の乱数が混在する擬似乱数に変える。

②擬似乱数を $128$ 行 $\times$  $128$ 列の行列に並べ替える。各行の擬似乱数を点 $j = 1, 2, \dots, 128$ で定義される関数の値とみなす。第 $i$ 行の関数を $\psi_i(j)$ と書き表すことにする。

③第1行の関数 $\psi_1(j)$ の擬似乱数のすべてを値 $1$ に置き換える。

④その関数 $\psi_1(j)$ を基に、第2行以降の関数 $\psi_i(j)$ を順に直交化していく。その方法は既知なシュミットの直交化を用いる。それは次の数式で表される関数 $\phi_i(j)$ である。

$$\begin{cases} \phi_1(j) = \psi_1(j) \\ \phi_i(j) = \psi_i(j) - \sum_{k=1}^{i-1} \frac{(\phi_k(j), \psi_i(j))}{(\phi_k(j), \phi_k(j))} \phi_k(j) \end{cases} \quad (1)$$

ただし、 $(\phi_i(j), \phi_k(j)) = \sum_{j=1}^{128} \phi_i(j) \cdot \phi_k(j)$ とする。例として、直交化された関数系 $\{\phi_i(j)\}$  ( $i, j = 1, 2, \dots, 128$ )を図1に例示する。

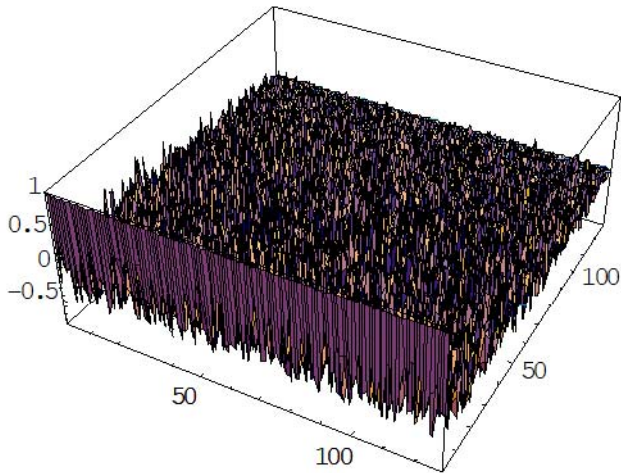


図1 擬似乱数でつくった直交関数系{ $\phi_{ij}$ }

### (2) 正規化

直交化された関数系{ $\phi_i(j)$ }の関数 $\phi_i(j)$  ( $i = 1, 2, \dots, 128$ )の長さを1に正規化する。それを $\varphi_i(j)$ とすると、次式で与えられる。

$$\varphi_i(j) = \frac{\phi_i(j)}{\sqrt{(\phi_i(j), \phi_i(j))}} \quad (2)$$

以上の(1),(2)の手続きで、電子透かし画像に採用できる正規直交関数系{ $\varphi_i(j)$ }を得る。図1の正規直交関数系{ $\varphi_i(j)$ }を図2に例示する。なお、 $\varphi_i(j)$ は次の関係を満たしている。

$$(\varphi_i(j), \varphi_k(j)) = \delta_{ik} \quad (\delta_{ik} \text{はクロネッカーのデルタ}) \quad (3)$$

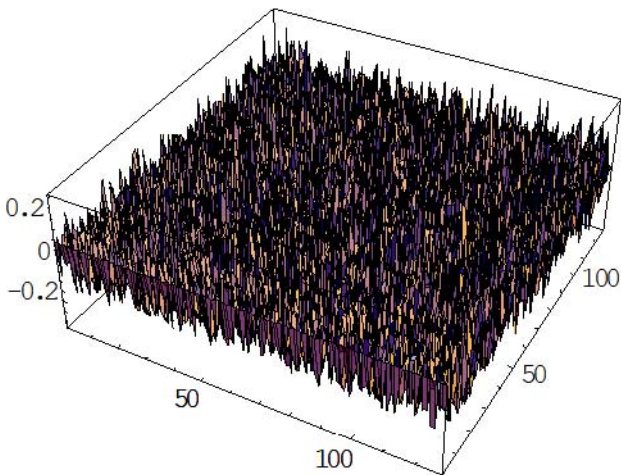


図2 擬似乱数でつくった正規直交関数系{ $\varphi_i(j)$ }

## 3. 電子透かし画像の制作と再生の方法

一重の電子透かし画像の制作方法と再生方法は、二重の電子透かし画像の制作方法と再生方法ほぼ同じ手順である。重複を避けるために、二重電子透かし画像の場合を中心に述べる。必要に応じて、一重の電子透かしの場合を補足する。

### 3.1 制作方法

二重電子透かし画像を制作するときの過程を図3に示す。  
①情報画像を2枚用意する。それらを $A_{ij}, B_{ij}$ とする。さらに、土台画像を1枚用意し、それを $F_{ij}$ とする。

② $A_{ij}$ を正規直交関数系で展開するときの展開係数 $a_{mn}$ を算出する。算出方法は式(3)のとおり。同様に、 $B_{ij}$ を正規直交関数系で展開するときの展開係数 $b_{mn}$ を算出する。

$$a_{mn} = \frac{\sum_{i=1}^N (\sum_{j=1}^N A_{ij} \varphi_m(j)) \varphi_n(i)}{(\sum_{j=1}^N \{\varphi_m(j)\}^2) \cdot (\sum_{i=1}^N \{\varphi_n(i)\}^2)} \quad (4)$$

$$b_{mn} = \frac{\sum_{i=1}^N (\sum_{j=1}^N B_{ij} \varphi_m(j)) \varphi_n(i)}{(\sum_{j=1}^N \{\varphi_m(j)\}^2) \cdot (\sum_{i=1}^N \{\varphi_n(i)\}^2)} \quad (5)$$

この展開係数 $a_{mn}, b_{mn}$ を画素値とする画像がホログラムである。カラー画像のときは、赤色、緑色、青色の3つの展開係数で表現される。

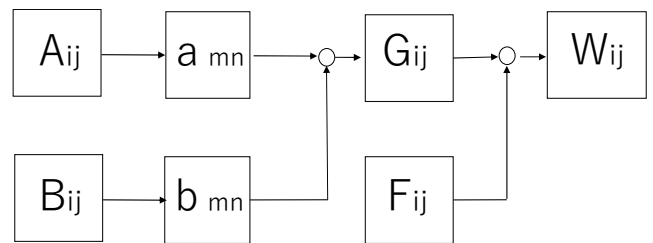


図3 二重電子透かし画像の制作過程

③展開係数 $a_{mn}, b_{mn}$ をそれぞれ量子化する。展開係数 $a_{mn}, b_{mn}$ の数値は広範囲であるのに対して、BMP画像の画素値は限定された正の整数値0~255しかとれない。したがって、展開係数を画像として、記録するためには量子化する必要がある。

展開係数を1つの記号 $p$ に変えて述べる。展開係数 $p$ の範囲を次に示すように3つの区間に分け、画素値 $q$ を0~ $\beta$ の範囲に量子化する。画素値の範囲は0~255ではなく、0~ $\beta$ の範囲に制限してある。その理由は、土台画像に埋め込むとき、そのままの画素値で埋め込むようにしたからである。展開係数 $p$ と画素値 $q$ の関係をグラフに示したのが図4である。なお、画素値 $q$ の個数を8個で例示する。

(i)  $-10^m < p \leq -10^{-n}$ のとき

$$q = \frac{\alpha-1}{m+n} (\log_{10}(-p) + n) + 1 \quad (6)$$

(ii)  $-10^{-n} < p \leq 10^{-n}$ のとき

$$q = 0 \quad (7)$$

(iii)  $10^{-n} < p \leq 10^m$ のとき

$$q = \frac{\beta-\alpha}{m+n} (\log_{10}(+p) + n) + \alpha \quad (8)$$

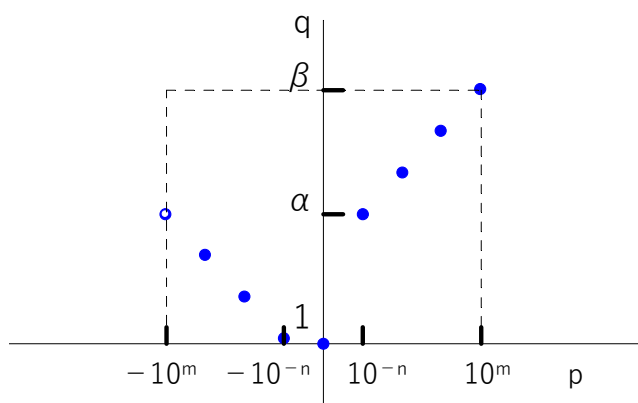


図4 式(6), (7), (8)のグラフ

④次に、量子化した展開係数 $a_{mn}$ ,  $b_{mn}$ を合成し1枚のホログラム $G_{ij}$ にまとめる。そのとき、 $a_{mn}$ ,  $b_{mn}$ のどちらか一方の展開係数を定数 $k$ 倍して合成する。すなわち、1枚にまとめられたホログラムは、画素値が $0, 1 \sim \beta$ の範囲層に量子化された展開係数と、画素値が $0, k \sim k \times \beta$ の範囲層に量子化された展開係数という2層構造で、展開係数を記録している。この2層構造の記録が二重電子透かし画像の要となる。2層構造の量子化を図5に示す。一重電子透かしの場合のホログラムは、1層だけの量子化構造である。

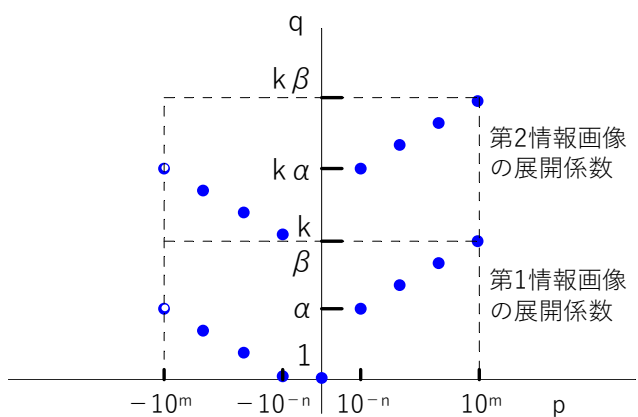


図5 2層構造の量子化

⑤最後に合成ホログラム $G_{ij}$ を土台画像 $F_{ij}$ に埋め込めて、電子透かし画像 $W_{ij}$ を制作する。合成ホログラムに土台画像を埋め込む割合は次のとおり。二重電子透かし画像のときは

$$W_{ij} = G_{ij} + \left(1 - \frac{k\beta}{255}\right) F_{ij} \quad (9)$$

一重の電子透かし画像の場合は

$$W_{ij} = G_{ij} + \left(1 - \frac{\beta}{255}\right) F_{ij} \quad (10)$$

である。

### 3.2 再生方法

電子透かしを再生するときの過程を図6に示す。電子透かし画像の再生方法は、原理的に電子透かし画像の制作方法の逆である。

①最初に、二重電子透かし画像から土台画像を引き算する。

すると、2層構造の合成ホログラム $G_{ij}$ が残る。

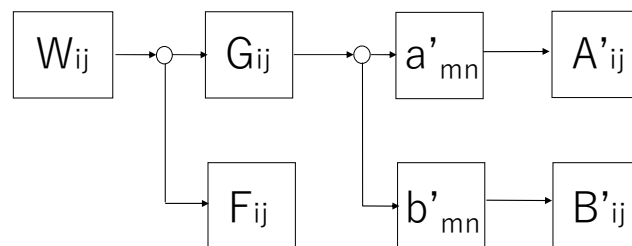


図6 二重電子透かし画像の再生過程

②次に、図5のような2層構造の合成ホログラムを1層構造のホログラム2枚に分ける。その1枚は下層の画素値をそのまま取り出したもので、もう1枚は上層の画素値だけを $1/k$ 倍して取り出したものである。

③それぞれに対して式(6),(7),(8)の逆演算を行い、ホログラム $a'_{ij}$ と $b'_{ij}$ を得る。

④最後に、それぞれのホログラム $a'_{ij}$ ,  $b'_{ij}$ から再生画像を再生する。その算出方法は以下のとおり。

$$A'_{ij} = \sum_{m=1}^{128} \left( \sum_{n=1}^{128} a'_{mn} \varphi_n(i) \right) \varphi_m(j) \quad (11)$$

$$B'_{ij} = \sum_{m=1}^{128} \left( \sum_{n=1}^{128} b'_{mn} \varphi_n(i) \right) \varphi_m(j) \quad (12)$$

## 4. 制作と再生の実験

### 4.1 擬似乱数の乱雑さ確認と正規直交化

最初に、実験に取り上げた擬似乱数の乱雑さを確認する。確認には、カイ二乗検定と、フーリエ変換によるスペクトル分布を用いる。表1は、発生した16384個の擬似乱数をそれぞれ10倍したときの整数値の出現度数を示す。

表1 擬似乱数の出現度数

|     |     |     |     |     |     |     |     |     |     |
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| 0   | 1   | 2   | 3   | 4   | 5   | 6   | 7   | 8   | 9   |
| 164 | 162 | 160 | 161 | 167 | 161 | 164 | 159 | 168 | 169 |
| 0   | 8   | 7   | 2   | 5   | 1   | 2   | 6   | 3   | 0   |

(上段は出現整数値、下段は4桁の度数)

表1のカイ二乗の値は6.3となる。この値は、自由度9で危険率0.01の場合のカイ二乗の値21.7より小さな値になることから、擬似乱数は99%の確率で均等に出現している。発生した擬似乱数を直線上に並べたものが図7である。横軸が発生順番、縦軸が擬似乱数の値である。

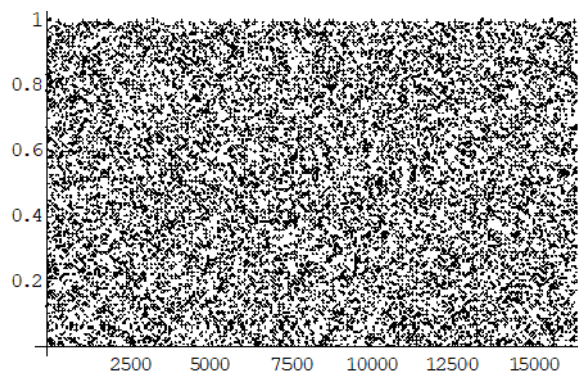


図7 直線上に並べた擬似乱数

また、擬似乱数の振幅スペクトル分布を図8に示す。ス

ベクトルが低周波領域にも高周波領域にもほぼ同程度に分布し、擬似乱数の乱雑さを視覚的に理解することができる。

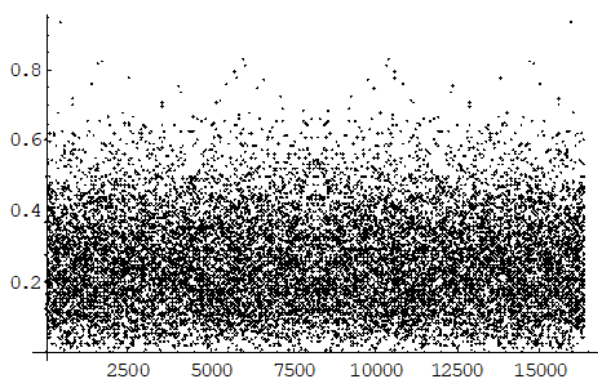


図8 擬似乱数の振幅スペクトル分布

次に、この擬似乱数の直交化と正規化を行う。その結果がそれぞれ図1、図2である。

#### 4.2 一重電子透かし画像の制作と再生

画素値の量子化における $m, n, \alpha, \beta$ をそれぞれ $-2, 6, 24, 47$ とする。

##### (1) 制作実験

制作過程に制作途中の画像を挿入したのが図9である。

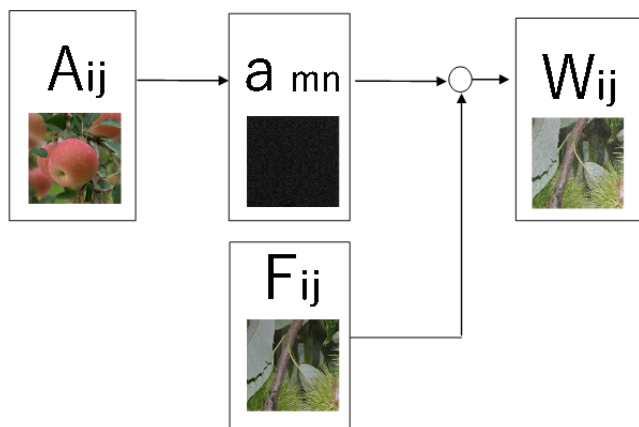


図9 一重電子透かし画像の制作過程(画像挿入)

##### (2) 再生実験

再生過程に再生途中の画像を挿入したのが図10である。

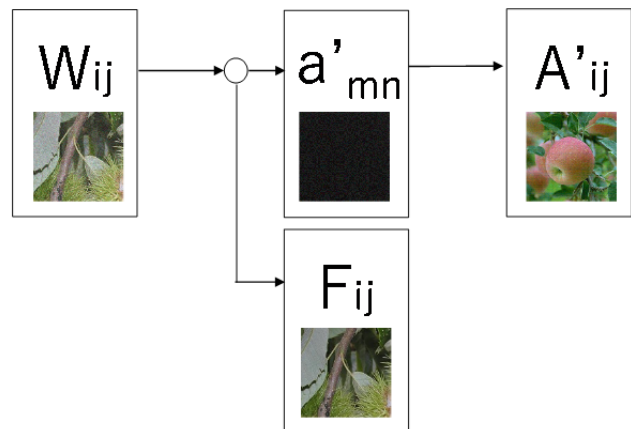


図10 一重電子透かし画像の再生過程(画像挿入)

#### (3) 相関係数の測定

制作した一重電子透かし画像 $W_{ij}$ と土台画像 $F_{ij}$ との相関係数を測定する。その結果を表2に示す。



図11 一重電子透かし画像 $W_{ij}$  図12 土台画像 $F_{ij}$

表2 一重電子透かし画像 $W_{ij}$ と土台画像 $F_{ij}$ の相関係数

|      | 赤色    | 緑色    | 青色    |
|------|-------|-------|-------|
| 相関係数 | 0.965 | 0.966 | 0.970 |

また、情報画像 $A_{ij}$ と再生画像 $A'_{ij}$ の相関係数を測定する。その結果を表3に示す。



図13 情報画像 $A_{ij}$  図14 再生画像 $A'_{ij}$

表3 情報画像 $A_{ij}$ と再生画像 $A'_{ij}$ の相関係数

|      | 赤色    | 緑色    | 青色    |
|------|-------|-------|-------|
| 相関係数 | 0.889 | 0.871 | 0.883 |

#### 4.3 二重電子透かし画像の制作と再生

画素値の量子化における $m, n, \alpha, \beta$ をそれぞれ $-2, 6, 4, 7$ とする。2層構造における定数 $k$ を8と設定する。画素空間8ビットのうち、下位ビットから3ビットと、その上の3ビットの合計6ビットを情報画像に用いる。

##### (1) 制作実験

図3の制作過程に制作途中の画像を挿入したのが図15である。

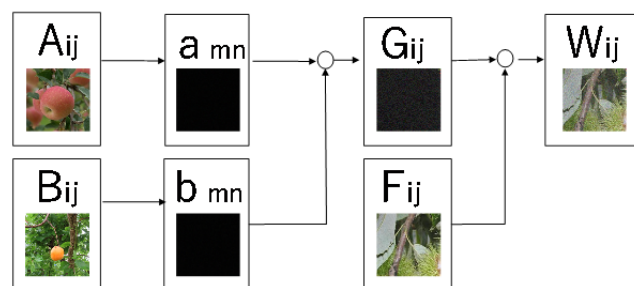


図15 二重電子透かし画像の制作過程(画像挿入)

##### (2) 再生実験

図6の再生過程に再生途中の画像を挿入したのが図16

である。

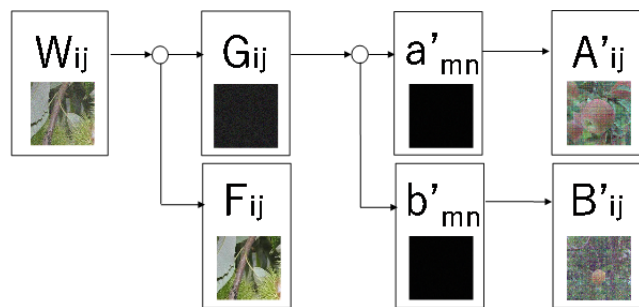


図 16 二重電子透かし画像の再生過程(画像挿入)

### (3) 相関係数の測定

制作した二重電子透かし画像  $W_{ij}$  と土台画像  $F_{ij}$  との相関係数を測定する。その結果が表 4 である。



図 17 二重電子透かし画像  $W_{ij}$  図 18 土台画像  $F_{ij}$

表 4 二重電子透かし画像  $W_{ij}$  と土台画像  $F_{ij}$  の相関係数

|      | 赤色    | 緑色    | 青色    |
|------|-------|-------|-------|
| 相関係数 | 0.959 | 0.958 | 0.964 |

また、2 枚の情報画像  $A_{ij}$ 、 $B_{ij}$  と再生画像  $A'_{ij}$ 、 $B'_{ij}$  のそれぞれの相関係数を測定する。その結果を表 5 に示す。



図 19 情報画像  $A_{ij}$

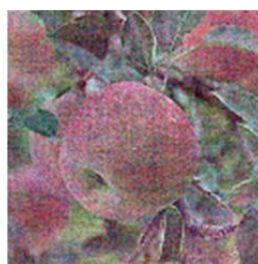


図 20 再生画像  $A'_{ij}$



図 21 情報画像  $B_{ij}$



図 22 再生画像  $B'_{ij}$

表 5 情報画像  $A_{ij}$ 、 $B_{ij}$  と再生画像  $A'_{ij}$ 、 $B'_{ij}$  の相関係数

|                            | 赤色    | 緑色    | 青色    |
|----------------------------|-------|-------|-------|
| $A_{ij}$ と $A'_{ij}$ の相関係数 | 0.699 | 0.796 | 0.760 |
| $B_{ij}$ と $B'_{ij}$ の相関係数 | 0.763 | 0.745 | 0.790 |

## 5. おわりに

擬似乱数を用いて 1 枚の画像の中に 1 枚あるいは 2 枚の情報画像を埋め込む一重電子透かし画像、二重電子透かし画像の制作方法と再生方法を述べてきた。その要点は 3 つある。1 つ目は、擬似乱数でつくった直交関数系を用いたことである。そのことによって、よく知られている直交関数系とは異なり、独自の直交関数系をつくることできる。2 つ目は、擬似乱数で構成した正規直交関数系による展開係数を、限定された BMP 形式画素値に書き換えるため量子化したことである。そして要点の 3 つ目は、二重電子透かし画像をつくる時、2 枚の情報画像に対して、それぞれ画素空間 8 ビットのうち 3 ビットの画素空間を割り当てる 2 層構造にしたことである。

最後に、この一重または二重の電子透かし画像の伝達途中における安全性について述べる。要点の 1 つ目で述べたように、任意の擬似乱数でつくった直交関数系を用いているので、それは唯一な直交関数系であると考えられる。したがって、第三者に盗聴されても安全性を十分に保つことができるものと予想する。

## 参考文献

- [1] U. Mustafa, U. Guzin, V. V. Nabiye, "Medical image security and EPR hiding using Shamir's secret sharing scheme," Journal of Systems and Software, Vol.84, No.3, pp.341-353, 2011.
- [2] 大西淳二, 小野東, 電子透かしを用いた印刷の改ざん検知方法の検討, 電子情報通信学会論文誌 D, Vol. j90-D, No.6, pp.1484-1494, 2007.
- [3] 木野将人, 和田成夫, ビットデータを埋込み可能なウェーブレット画像透かし法, 電子情報通信学会論文誌 A, Vol. J86-A, No.2, pp.160-167, 2003.
- [4] 栗林稔, 田中初一, DCT 係数間の加法特性に基づく電子透かし, 電子情報通信学会論文誌 A, 2002, Vol. J85-A No.3 pp.322-333
- [5] 佐々木隆幸, 2 枚の電子透かし情報画像を埋め込んだ電子透かしの制作と復元, 特許庁, 特願 2016-217619, 2016.
- [6] S. Alyammahi, F. Taher, H. Al-Ahmad, T. McGloughlin, A New Multiple Watermarking Scheme for Copyright Protection and Image Authentication, IEEE 59<sup>th</sup> International Midwest Symposium on Circuits and Systems, 2016.
- [7] 佐々木隆幸, 川守田聡, 直交関数系でつくる電子透かし, 職業能力開発報文誌, Vol.30, No.1, pp.1-12, 2018.
- [8] Takayuki Sasaki and Tomoyuki Nagase, "Constructing Digital Watermark Based on Orthogonal Functions," 5<sup>th</sup> IEEE Inter. Conference on Cyber Security and Cloud Computing (CSCloud), pp.140-143, 2018.