情報処理学会論文誌　デジタルコンテンツ　Vol.8　No.1　11–19 (Feb. 2020)

研究論文

擬似乱数系列でつくる二重情報ハイディング

長瀬 智行[1,a)]　佐々木 隆幸[1]

受付日 2019年6月27日, 採録日 2019年9月10日

概要：この論文は，擬似乱数系列を用いて 1 枚の任意の画像の中に 2 枚の情報画像を埋め込む二重の情報ハイディング画像の制作方法と再生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．その 1 つは，任意の擬似乱数系列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 つ目は情報画像を二重に埋め込むため画素空間を 2 層構造にしたことである．これらの考案を多くの画像やイラストで例示し，最後に改ざんに対する特徴を述べる．

キーワード：二重情報ハイディング，擬似乱数系列，直交関数系，量子化，2 層構造，ホログラム，カギ画像

Double Information Hiding Based on Pseudorandom Series

Tomoyuki Nagase[1,a)]　Takayuki Sasaki[1]

Received: June 27, 2019, Accepted: September 10, 2019

Abstract: This paper proposes a method of hiding double digital information in a single private image using pseudorandom series. This proposal has three features. First, the orthonormal system can be reproduced from a pseudorandom series. Second, double hidden images are primarily performed by a quantization process in order to coordinate the images' sizes. Third, two layers structure in pixel space of an image can be constructed in order to hide double information images. The paper also illustrates the images on the composition and reproduction processes, and finally it has the capability to provide robust security against altered pixels.

Keywords: double information hiding, pseudorandom series, orthogonal functions, quantization, two layer structure, hologram, key image

1. はじめに

ディジタル技術の進歩により，サイズの大きな画像や精度が求められる画像が容易に伝達 [1] できるようになってきた．また，Wi-Fi 環境が整備されつつあり，誰でもがネットに簡便にアクセス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ができるようなり，社会的トラブルを生んでいる．このような背景に対応するため，情報画像を秘匿に安全に伝達する方法がいろいろと提案されている [2], [3], [4], [5], [6], [7], [8]．それらの提案の中で採用されている直交関数系の大半は超越関数グループの周期関数やハール関数などである．

しかし，これらの関数だけで秘匿性と安全性を堅持するのは困難になる恐れがある．その理由は，それらの関数の使用方法は定型的であるので，情報ハイディング画像の制作方法が推察されやすくなるからである．したがって，秘匿性と安全性を高めるには，使用できる関数の種類をさらに増やす必要がある．その例として，代数関数グループの直交多項式を活用する方法 [9], [10], [11] も研究されているが，直交多項式の使用方法も定型的であり，直交関数系として採用できる個数は限定的である．

そこで，個数が限定的になる直交関数系から脱皮するために，擬似乱数系列を用いることを考案する．その活用例として，擬似乱数系列による直交関数系を活用した二重情報ハイディングを提案する．それは 2 枚の情報画像を 1 枚

1　弘前大学大学院理工学研究科
Hirosaki University, Hirosaki, Aomori 036–8561, Japan
a)　nagase@hirosaki-u.ac.jp

の任意の画像に埋め込み，再生できる方法である．この方法の長所は，改ざん攻撃に対して耐性を持つことである．改ざんの画素値が大きな数値ならば，改ざん影響がほとんど現れない．しかし短所としては，限られた画素空間に2枚の情報画像を埋め込むため，一重の場合に比べてコンテンツの劣化が抑えにくいという点がある．

2. 擬似乱数系列の直交化と正規化

擬似乱数系列を直交関数系につくり変えるために直交化と正規化の処理を行う．

なお，以降で用いる用語と記号を整理しておく．秘匿に伝達する画像を情報画像，その画像を直交関数系で変換し量子化した画像をホログラム，ホログラムを埋め込む土台となる任意の画像をカギ画像，ホログラムをカギ画像に埋め込めた画像を情報ハイディング画像，そして情報ハイディング画像から再生した画像を再生画像と呼ぶことにする．

また，画像の横，縦の画素数をそれぞれ N 個とする．記号 Z_{ij} は画像画面の最左下位置を1行1列とする i 行 j 列における画素値を表すものとする．展開係数に関する変数が2種類ある．1つは直交関数系で展開したときの展開係数で，もう1つはその展開係数を量子化したときの量子化展開係数である．それらの変数記号の区別のために，量子化展開係数には展開係数の変数に接頭語として q を添える．

2.1 直交化

直交化を次の4つの手順で行う．

①個数 N^2 個の擬似乱数系列を用意する．個々の乱数の値が0〜1の小数であるときは，その値を0.5だけ下げ，正と負の数が混在する擬似乱数系列につくり変える．

②擬似乱数系列を区切り N 行 $\times N$ 列の行列に配置替えする．ここで，各行の横並びの擬似乱数を，点 $j=1,2,\cdots,N$ において定義される関数値と見なす．関数の個数は N 個になる．第 i 行（$i=1,2,\cdots,N$）における関数を $\psi_i(j)$ と書き表す．

③次に，第1行の関数 $\psi_1(j)$ の擬似乱数をすべて値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 $\psi_i(j)$ を順に直交化する．その方法はシュミットの直交化法を用いて行う．直交化した関数 $\phi_i(j)$ は次式のとおり．

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

ただし，$(\phi_i(j),\phi_k(j))=\sum_{j=1}^{N}\phi_i(j)\cdot\phi_k(j)$ とする．

2.2 正規化

直交関数系 $\{\phi_i(j)\}$ の各関数 $\phi_i(j)$ を次式で正規化する．正規化された関数を $\varphi_i(j)$ とする．

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

$\varphi_i(j)$ は次の関係を満たす．

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

以上の処理で，二重情報ハイディング画像に採用できる正規直交関数系 $\{\varphi_i(j)\}$ がつくられる．

3. 二重情報ハイディング画像の制作と再生

3.1 制作方法

二重情報ハイディング画像を制作する過程を図**1**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，カギ画像を1枚用意し，それを F_{ij} とする．

②式(4)を用いて，A_{ij} を正規直交関数系で展開したときの展開係数 a_{mn} を算出する．同様に，B_{ij} の場合の展開係数 b_{mn} を式(5)で算出する．

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

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

カラー画像のときは，赤色，緑色，青色の3つの展開係数を算出する．

③展開係数 a_{mn}，b_{mn} をそれぞれ量子化する．量子化する理由を述べる．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，記録するためには整数値に量子化する必要がある．展開係数 a_{mn} を D_a ビットの画素空間 $\{0,1,\cdots,2^{D_a}-1\}$ の画素値に量子化する．同様に，b_{mn} を D_b ビットの画素空間 $\{0,1,\cdots,2^{D_b}-1\}$ の画素値に量子化する．量子化する画素値をある範囲に制限した理由は，ホログラムをカギ画像に埋め込むとき，その画素値のまま埋め込めるようにしたためである．

展開係数を量子化する方法を述べる．展開係数の範囲を下に示した(i)，(ii)，(iii)の3つの区間に分けて量子化す

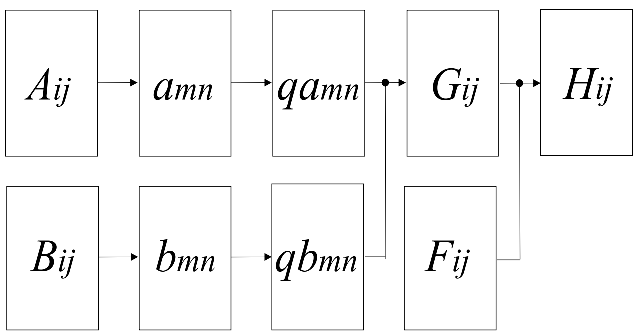


図 1　二重情報ハイディング画像の制作過程
Fig. 1　Composing process of two hidden images.

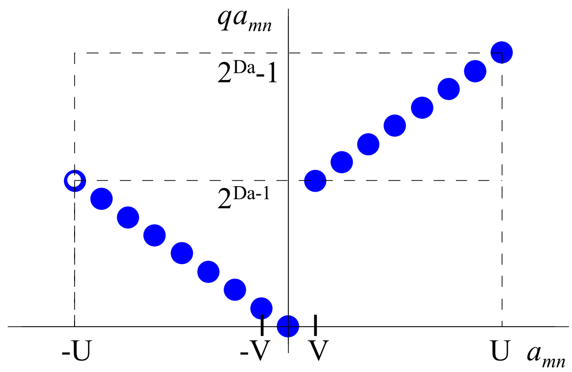


図 **2 (a)**　a_{mn} に関する式 (8)，(9)，(10) のグラフ
Fig. 2 (a)　Graph of Eqs. (8), (9), (10) on a_{mn}.

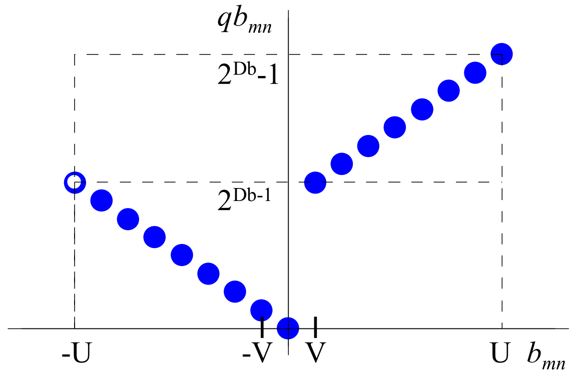


図 **2 (b)**　b_{mn} に関する式 (8)，(9)，(10) のグラフ
Fig. 2 (b)　Graph of Eqs. (8), (9), (10) on b_{mn}.

る．ただし，値 U，V を

$$U=\sum_{j=1}^{N}\left(\sum_{i=1}^{N}255\varphi_1(i)\right)\varphi_1(j) \tag{6}$$

$$V=1/\sqrt{N} \tag{7}$$

とする．U は式 (4)，式 (5) の情報画像 A_{ij}，B_{ij} が最大画素値 255 の場合の値である．V は正規直交関数系 $\{\varphi_i(j)\}$ の関数 $\varphi_1(j)$（$j=1,2,\cdots,N$）の関数値である．

a_{mn} と qa_{mn} の関係および b_{mn} と qb_{mn} の関係をそれぞれの区間ごとに式 (8)，式 (9)，式 (10) とする．それをグラフに表したのが**図 2** (a)，図 2 (b) である．図 2 (a)，図 2 (b) は量子化展開係数の画素値をそれぞれ 16 個で例示したものである．

(i)　$-U<a_{mn},b_{mn}\leq -V$ のとき

$$qa_{mn}=\frac{2^{D_a-1}-1}{\log_{10}U-\log_{10}V}(\log_{10}(-a_{mn})-\log_{10}V)+1$$
$$qb_{mn}=\frac{2^{D_b-1}-1}{\log_{10}U-\log_{10}V}(\log_{10}(-b_{mn})-\log_{10}V)+1 \tag{8}$$

(ii)　$-V<a_{mn},b_{mn}<V$ のとき

$$qa_{mn}=0$$
$$qb_{mn}=0 \tag{9}$$

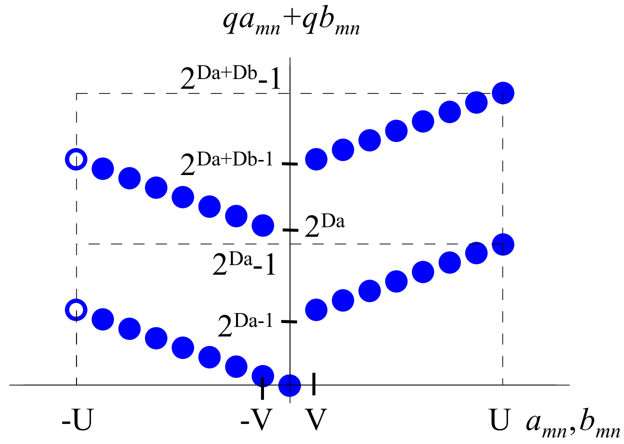


図 **3**　量子化展開係数の 2 層構造
Fig. 3　Two layers of quantized coefficient.

(iii)　$V\leq a_{mn},b_{mn}\leq U$ のとき

$$qa_{mn}=\frac{2^{D_a-1}-1}{\log_{10}U-\log_{10}V}(\log_{10}(+a_{mn})-\log_{10}V)+2^{D_a-1}$$
$$qb_{mn}=\frac{2^{D_b-1}-1}{\log_{10}U-\log_{10}V}(\log_{10}(+b_{mn})-\log_{10}V)+2^{D_b-1} \tag{10}$$

④量子化展開係数 qa_{mn}，qb_{mn} を 1 枚のホログラム G_{ij} に合成する．その合成方法は式 (11) で行う．

$$\{0,1,\cdots,2^{D_a}-1\}+\{0,1,\cdots,2^{D_b}-1\}\times 2^{D_a} \tag{11}$$

つまり，ホログラム G_{ij} は量子化展開係数が $\{0,1,\cdots,2^{D_a}-1\}$ である画素空間と，量子化展開係数が $\{0,1,\cdots,2^{D_b}-1\}$ である画素空間から構成される 2 層構造となる．この 2 層構造が二重情報ハイディング画像の原理である．2 層構造を**図 3** に示す．

⑤最後にホログラム G_{ij} をカギ画像 F_{ij} に式 (12) のように埋め込む．以上で二重情報ハイディング画像 H_{ij} を制作することができる．

$$H_{ij}=G_{ij}+\frac{256-2^{D_a+D_b}}{255}F_{ij} \tag{12}$$

3.2　再生方法

二重情報ハイディング画像を再生する過程を**図 4** に示す．再生方法は原理的には制作方法の逆過程である．

①最初に，二重情報ハイディング画像からカギ画像を差し引く．2 層構造のホログラム G_{ij} が残る．

②2 層構造のホログラムから各層のホログラムを個々に抽出する．1 枚は下層の量子化展開係数 $\{0,1,\cdots,2^{D_a}-1\}$ をそのまま抽出したもので，もう 1 枚はホログラムを 2^{-D_a} 倍して上層の量子化展開係数 $\{0,1,\cdots,2^{D_b}-1\}$ を抽出する．

③それぞれに対して式 (8)，式 (9)，式 (10) の逆演算を

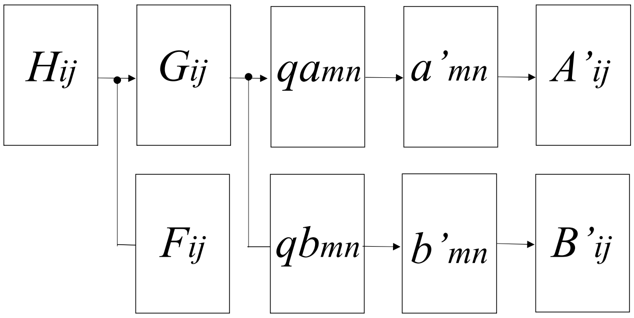


図 4　二重情報ハイディング画像の再生過程
Fig. 4　Reproducing process of two hidden images.

行い，それぞれを a'_{mn}，b'_{mn} とする．

④最後に，それぞれの a'_{mn}, b'_{mn} から再生画像 A'_{ij}, B'_{ij} を再生する．その再生方法は次のとおり．ただし，$max\{X_{ij}\}$, $min\{X_{ij}\}$ はそれぞれ $\{X_{ij}\}$ の最大値, 最小値とする．$\{Y_{ij}\}$ についても同様とする．

$$\begin{cases} X_{ij} = \sum_{n=1}^{N} \left(\sum_{m=1}^{N} a'_{mn}\varphi_m(i) \right) \varphi_n(j) \\ A'_{ij} = \frac{X_{ij}-min\{X_{ij}\}}{max\{X_{ij}\}-min\{X_{ij}\}} \times 255 \end{cases} \tag{13}$$

$$\begin{cases} Y_{ij} = \sum_{n=1}^{N} \left(\sum_{m=1}^{N} b'_{mn}\varphi_m(i) \right) \varphi_n(j) \\ B'_{ij} = \frac{Y_{ij}-min\{Y_{ij}\}}{max\{Y_{ij}\}-min\{Y_{ij}\}} \times 255 \end{cases} \tag{14}$$

4.　制作と再生の実験

1 枚の画像のなかに 2 枚の画像を埋め込む二重情報ハイディングの実験例を示す．一方の画像には 1 ビットの画素空間を，他方の画像には 5 ビットの画素空間を用いて，二重情報ハイディングを行う．なお，画像形式は BMP 形式とし，画像サイズを横 128 画素，縦 128 画素とする．

4.1　擬似乱数系列の乱雑さ確認と正規直交化

実験に採用した擬似乱数系列は「Mathematica」(Wolfram Research 社）が発生したものである．その擬似乱数系列の乱雑さを確認しておく．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 16,384 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 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 5** である．横軸が発生順番，縦軸が擬似乱数の値である．

また，擬似乱数の振幅スペクトル分布を**図 6** に示す．スペ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，擬似乱数系列が乱雑であることを視覚的に理解することができる．

次に，この擬似乱数系列の直交化と正規化を行う．その結果が**図 7**，**図 8** である．図 7 は式 (1) の直交関数系 $\{\phi_i(j)\}$ を表し，図 8 は式 (2) の正規直交関数系 $\{\varphi_i(j)\}$ を表す．

表 1　擬似乱数の出現度数
Table 1　Frequency of the pseudorandom.

0	1	2	3	4
1640	1628	1607	1612	1675

5	6	7	8	9
1611	1642	1596	1683	1690

(上段は出現整数値，下段は 4 桁の度数)

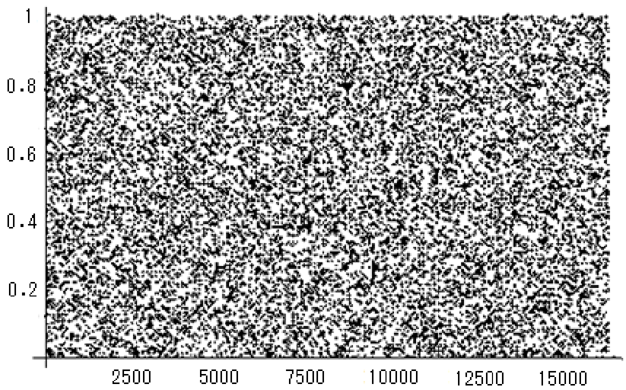


図 5　直線上に並べた擬似乱数
Fig. 5　Pseudorandom series on the line.

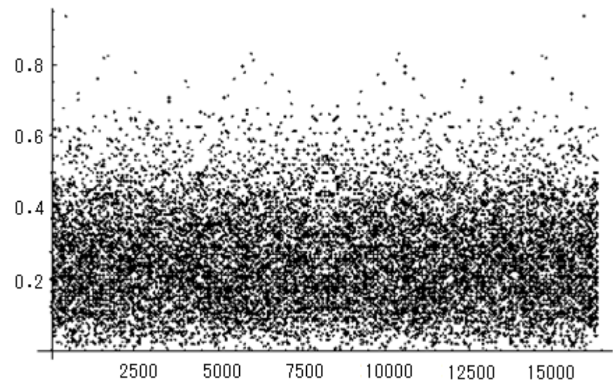


図 6　擬似乱数の振幅スペクトル分布
Fig. 6　Amplitude spectrum of the pseudorandom series.

4.2　二重情報ハイディング画像の制作と再生

実験に用いる 2 層構造を次のように設定する．式 (6) の U は $U = 32640$，式 (7) の V は $V = 0.08839$ である．画素空間の第 1 層のビット数 D_a を $D_a = 1$ とし，最下位ビット（LSB）の 1 ビットを 1 枚目の情報画像に割り当てる．ただし，第 1 層の正領域における量子化展開係数はすべて 0 とする．第 2 層のビット数 D_b を $D_b = 5$ とし，第 1 層の上に 5 ビットの画素空間を 2 枚目の情報画像に割り当てる．以上の様子を**図 9** に示す．

なお，2 層構造の合計ビット数 D を $D = D_a + D_b = 6$ とした理由は，式 (12) の画像 H_{ij} とカギ画像 F_{ij} の相関係

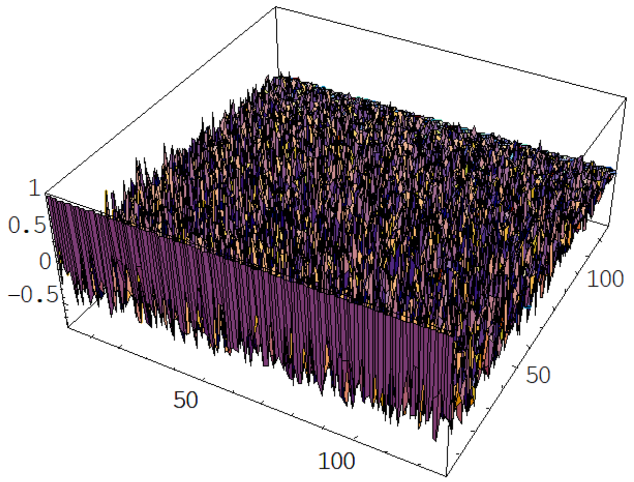


図 7　擬似乱数でつくった直交関数系 $\{\phi_i(j)\}$
Fig. 7　Orthogonal functions $\{\phi_i(j)\}$ made by pseudorandom series.

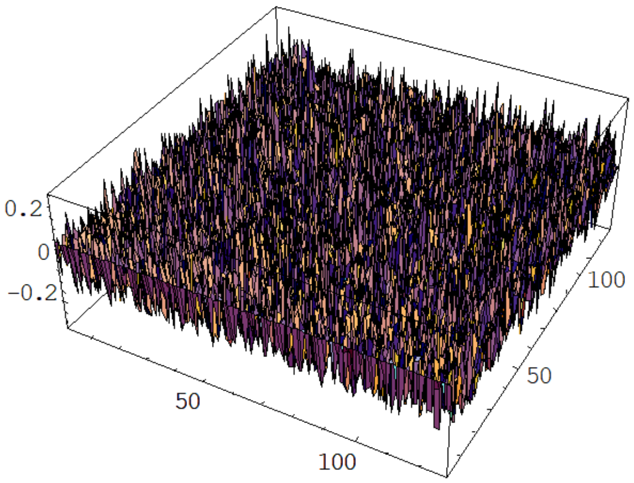


図 8　擬似乱数でつくった正規直交関数系 $\{\varphi_i(j)\}$
Fig. 8　Orthonormal system $\{\varphi_i(j)\}$made by pseudorandom series.

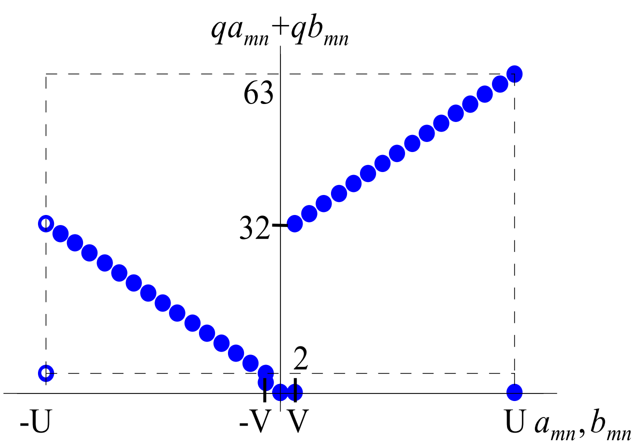


図 9　実験に用いた 2 層構造
Fig. 9　Two layers used in experiment.

数が 0.5 以上となる最大の D を採用したからである．このとき，式 (12) の画像 G_{ij} は画素値が $\{0, 2^D\}$ の 2 値だけで構成される画像で，しかも赤色，緑色，青色ごとに異なる

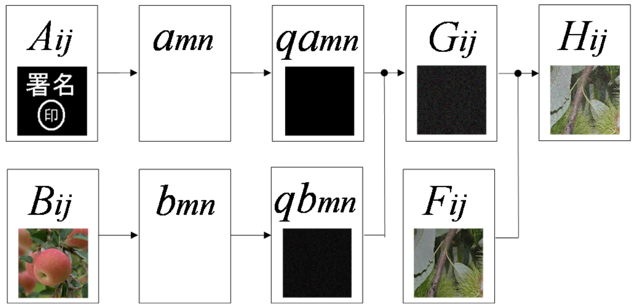


図 10　二重情報ハイディング画像の制作過程（画像挿入）
Fig. 10　Composing process of two hidden images with images.

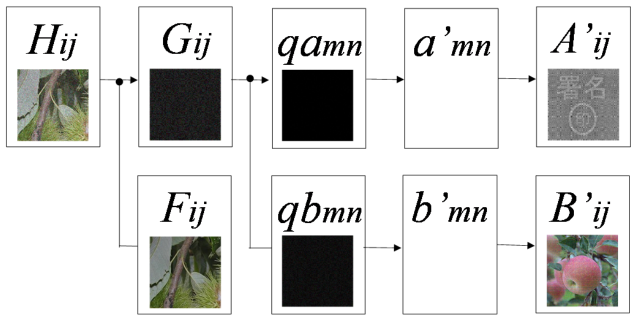


図 11　二重情報ハイディング画像の再生過程（画像挿入）
Fig. 11　Reproducing process of two hidden images with images.

図 12　二重情報ハイディング画像 H_{ij}
Fig. 12　Information hiding image H_{ij}.

図 13　カギ画像 F_{ij}
Fig. 13　Key image F_{ij}.

擬似乱数系列でつくられる画像とする．

(1)　**制作実験**

図 1 の制作過程に制作途中の画像を挿入したのが図 **10** である．

(2)　**再生実験**

図 4 の再生過程に再生途中の画像を挿入したのが図 **11** である．

(3)　**相関係数の測定**

制作した二重情報ハイディング画像 H_{ij}（図 **12**）とカギ画像 F_{ij}（図 **13**）との相関係数を測定する．その結果が表 **2** である．

また，2 枚の情報画像 A_{ij}（図 **14**），B_{ij}（図 **15**）と再

表 2　画像 H_{ij} と画像 F_{ij} の相関係数
Table 2　Coefficient of correlation between H_{ij} and F_{ij}.

	赤色	緑色	青色
H_{ij} と F_{ij} の相関係数	0.933	0.934	0.942

図 14　情報画像 A_{ij}
Fig. 14　Image A_{ij}.

図 15　情報画像 B_{ij}
Fig. 15　Image B_{ij}.

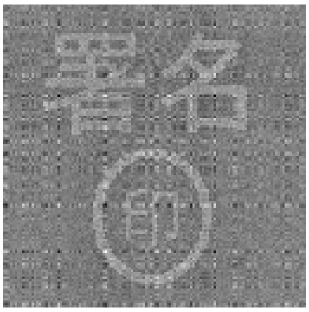


図 16　情報画像 A'_{ij}
Fig. 16　Image A'_{ij}.

図 17　再生画像 B'_{ij}
Fig. 17　Image B'_{ij}.

表 3　A_{ij} と A'_{ij} の相関係数および B_{ij} と B'_{ij} の相関係数
Table 3　Coefficient of correlation between A_{ij} and A'_{ij}, Coefficient of correlation between B_{ij} and B'_{ij}.

	赤色	緑色	青色
A_{ij} と A'_{ij} の相関係数	0.503	0.503	0.503
B_{ij} と B'_{ij} の相関係数	0.970	0.970	0.971

生画像 A'_{ij}（図 **16**），B'_{ij}（図 **17**）のそれぞれの相関係数を測定する．その結果を**表 3** に示す．さらに，図 16 および図 17 に対する評価実験を行う．被験者は学生 21 人である．評価測定は，図 16 では文字を判読できるか否か，図 17 ではコンテンツが不明瞭であるか否かである．測定結果は全員が判読できる，不明瞭であるとはいえないである．なお，図 17 の相関係数が 0.970 以上であるのに対して，図 16 の相関関数が 0.503 になった理由は，図 14 の情報画像の展開係数を量子化するときに使用したビット数を 1 としたこと，さらに正領域における量子化展開係数をすべて 0 としたことによるものと考える．

5.　改ざんにおける特徴

5.1　改ざん痕跡の現れ方

二重情報ハイディング画像が伝達中に改ざんを受けた場合，どのような改ざん痕跡が再生画像に現れるかについて述べる．二重情報ハイディング画像 H_{ij} の位置 i 行 j 列の 1 画素が改ざんを受けて ΔH_{ij} だけ変化すると，ホログラムは位置 i 行 j 列の位置に次式の影響を受ける．

$$\Delta G_{ij} = \Delta H_{ij} \tag{15}$$

これを再生すると，再生画像に改ざん痕跡が現れる．たとえば，m 行 n 列の画素値が改ざんを受け，量子化展開係数に変化 Δqa_{mn} が発生したとする．この変化は式 (8)，式 (9)，式 (10) を介して展開係数に変化 $\Delta a'_{mn}$ を与え，その変化が再生画像に与える変化 $\Delta A'_{ij}$ は式 (13) から

$$\Delta A'_{ij} = \varphi_m(i)\varphi_n(j)\Delta a'_{mn} \tag{16}$$

同様にして，式 (14) から

$$\Delta B'_{ij} = \varphi_m(i)\varphi_n(j)\Delta b'_{mn} \tag{17}$$

となる．

5.2　改ざん実験

制作した二重情報ハイディング画像を用いて，3 種類の改ざん実験を行う．それは，1 画素を改ざんする実験 1，正方形内部を画素値 $(255, 255, 255)$ の白色で塗りつぶす実験 2，そして正方形内部を画素値 $(0, 0, 0)$ の黒色で塗りつぶす実験 3 の 3 種類である．なお，画素値を (赤色, 緑色, 青色) の順で表す．

実験 1　1 画素を改ざんする実験

位置 64 行 64 列の画素を次のように改ざんする場合の改ざん痕跡をみてみる．ただし，その位置での二重情報ハイディング画像，ホログラム，カギ画像の画素値は，それぞれ $H_{64,64} = (59, 88, 55)$，$G_{64,64} = (15, 37, 13)$，$F_{64,64} = (44, 51, 42)$ である．

(1) $H_{64,64}$ を画素値 $(107, 114, 105)$ に改ざんする場合

これはホログラム $G_{64,64} = (15, 37, 13)$ が $(63, 63, 63)$ に変化し，画素値が 2 層構造の画素空間における最大値に改ざんされる場合である．

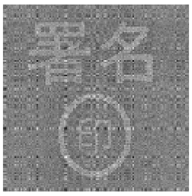
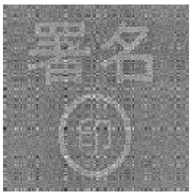
(2) $H_{64,64}$ を画素値 $(108, 115, 106)$ に改ざんする場合

これはホログラム $G_{64,64} = (15, 37, 13)$ が $(64, 64, 64)$ に変化し，2 層構想の画素空間における最大値を $+1$ だけ超えた値に改ざんされる場合である．

それぞれの場合での再生画像と相関係数を**表 4** に併記する．なお，相関係数を色別の組 (赤, 緑, 青) で表す．

表 4　実験 1 の再生画像と相関係数

Table 4　Reproduced images on experiment No.1 and the coefficients of correlation.

実験 1 (1)の場合	
情報画像A_{ij}との相関係数 (0.503,0.503,0.503) 	情報画像B_{ij}との相関係数 (0.128,0.071,0.080) 
実験 1 (2)の場合	
情報画像A_{ij}との相関係数 (0.503,0.503,0.503) 	情報画像B_{ij}との相関係数 (0.970,0.970,0.971) 

実験 2　正方形内部を白色で塗りつぶす実験

塗りつぶす正方形内部のサイズを, (1) 10×10, (2) 40×40, (3) 60 × 60 の場合で実験する．それを再生した画像を**表 5** に示す．

実験 3　正方形内部を黒色で塗りつぶす実験

塗りつぶす正方形のサイズを，(1) 10 × 10，(2) 40 × 40, (3) 60 × 60 の場合で実験する．それを再生した画像を**表 6** に示す．

5.3　改ざん実験の考察

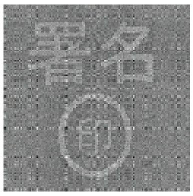
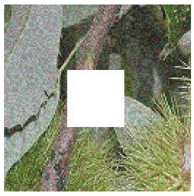
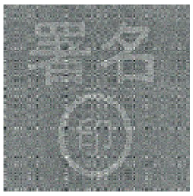
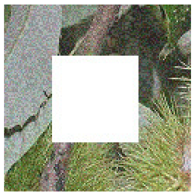
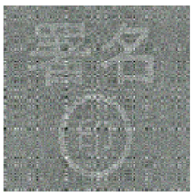
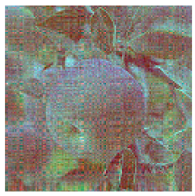
それぞれの実験結果について，その理由を考察する．実験 1 の結果は，改ざん痕跡が顕著に現れるか否かの境界を示している．それは，式 (15) で与えられる変化後のホログラム画素値が 2 層構造の画素空間の範囲内あるか否かに因る．ホログラム画素値が範囲内にあるならば改ざん痕跡は現れ，範囲外であるならば明らかな改ざん痕跡がみられない．実験 1 (1) は，ホログラム画素値が画素空間範囲内にある場合である．実験 1 (2) は範囲外にある場合である．以上を図式化したのが**図 18** である．

実験 2 の結果は，多数の改ざんが図 18 で示される画素空間の範囲外となる場合である．それらの改ざんは再生画像に算入されないまま欠落する．したがって，欠落が少ないうちは再生画像に顕著な改ざん痕跡はみられない．しかし，欠落が多くなるに従い画像が劣化するのが分かる．

実験 3 の結果は，多数の改ざんが式 (11) で示される画素空間の範囲内の場合である．しかし，改ざんによる明白な痕跡はみられない．その理由を第 2 層の場合で示す．

表 5　実験 2 の再生画像と相関係数

Table 5　Reproduced images on experiment No.2 and the coefficients of correlation.

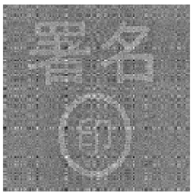
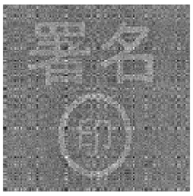
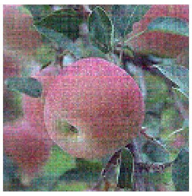
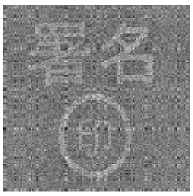
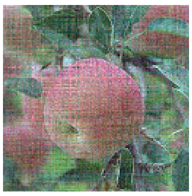
(1)正方形サイズ 10×10（左下位置59行59列）のとき 	
情報画像A_{ij}との相関係数 (0.500,0.500,0.500) 	情報画像B_{ij}との相関係数 (0.967,0.968,0.969) 
(2)正方形サイズ 40×40（左下位置 44行44列）のとき 	
情報画像A_{ij}との相関係数 (0.460,0.458,0.455) 	情報画像B_{ij}との相関係数 (0.937,0.933,0.934) 
(3)正方形サイズ 60×60（左下位置34行34列）のとき 	
情報画像A_{ij}との相関係数 (0.399,0.399,0.400) 	情報画像B_{ij}との相関係数 (0.115,0.885,0.892) 

qb_{mn} のある値がゼロになると，b'_{mn} がゼロになる．すると式 (17) にしたがって画像 $B'_{ij} = \varphi_m(i)\varphi_n(j)b'_{mn}$ がゼロとなる．しかし，それ以外の画像はそのまま再生されるため，明らかな改ざん痕跡は残りにくくなる．

以上で述べたように，この二重情報ハイディング画像

表 6　実験 3 の再生画像と相関係数

Table 6　Reproduced images on experiment No.3 and the coefficients of correlation.

<table>
<tr><td colspan="2">(1)正方形サイズ 10×10（左下位置59行59列）のとき
</td></tr>
<tr><td>情報画像A_{ij}との相関係数
(0.502,0.502,0.502)
</td><td>情報画像B_{ij}との相関係数
(0.967,0.968,0.969)
</td></tr>
<tr><td colspan="2">(2)正方形サイズ 40×40（左下位置44行44列）のとき
</td></tr>
<tr><td>情報画像A_{ij}との相関係数
(0.480,0.480,0.480)
</td><td>情報画像B_{ij}との相関係数
(0.937,0.933,0.934)
</td></tr>
<tr><td colspan="2">(3)正方形サイズ 60×60（左下位置34行34列）のとき
</td></tr>
<tr><td>情報画像A_{ij}との相関係数
(0.450,0.450,0.450)
</td><td>情報画像B_{ij}との相関係数
(0.900,0.885,0.892)
</td></tr>
</table>

は改ざんに対して優れた耐性を有している．比較のため，文献 [10] の場合の改ざん例を示す．文献 [10] は 2 つの異なる直交関数系，Haar 関数系と直交多項式を用いた二重情報ハイディングである．たとえば**図 19** は，情報ハイディング画像 63 行 61 列の画素値 $(52, 78, 40)$ を，画素

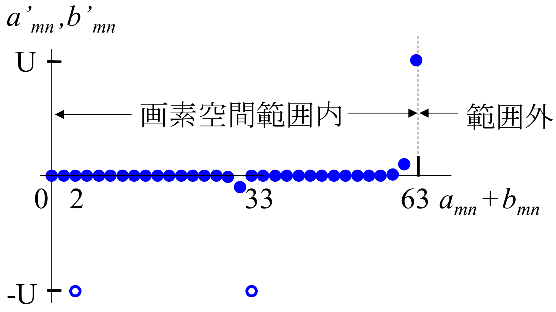


図 18　改ざん痕跡の説明

Fig. 18　Explanation about the trace by altering.

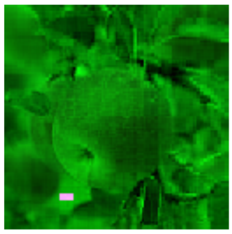
画素値(255,255,255)のとき	画素値(64,64,64)のとき
	

図 19　Haar 関数系二重ハイディング画像の改ざん痕跡

Fig. 19　Trace of alteration on Haar functions.

値 $(200, 200, 200)$ に改ざんした場合の再生画像と，画素値 $(64, 64, 64)$ に改ざんした場合の再生画像である．改ざん痕跡が左下に長方形状にそれぞれ現れている．

6.　まとめ

擬似乱数系列を用いて 1 枚の画像の中に 2 枚の情報画像を埋め込む二重情報ハイディング画像の制作方法と再生方法を述べてきた．その要点は 3 点ある．1 点は，正規直交関数系を擬似乱数系列から構築したことである．そのことによって，多くの情報ハイディング画像で採用されている直交関数系とは異なり，定型的でない直交関数系をつくることができる．2 点目は，その直交関数系による情報画像の展開係数を量子化したことである．そして 3 点目は，量子化展開係数を 2 層構造の画素空間に割り当てたことである．

最後に，伝達途中における秘匿性と安全性について述べる．秘匿性においては，この情報ハイディング画像は高い秘匿性を有する．それは，直交関数系が任意の擬似乱数系列を用いてつくられているので，個人専用の直交関数系と見なすことができ，たとえ盗聴されても第三者が情報画像を再生するのは困難であると考えるからである．安全性においても，この情報ハイディング画像は高い安全性を持つ．なぜならば，ホログラムの中に 1 ビットだけで構成される画素空間を設けてあるからである．この 1 ビット画素空間は改ざんに対して頑健であり，電子透かし画像として利用することも可能である．あるいは，もう一方の情報画像の保証書として活用することもできる．この二重情報ハ

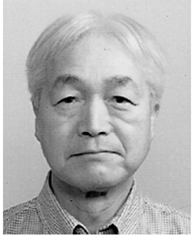
イディング画像が，多くの情報画像を秘匿に安全に伝達できる工法として役立つことを期待する．

参考文献

[1] Mustafa, U., Guzin, U. and Nabiyev, V.: 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，Vol.J85-A, No.3, pp.322–333 (2002).
[5] Celik, M.U., Sharma, G., Tekalp, A.M. and Saber, E.: Lossless generalize-LSB data embedding, *IEEE Trans. Image Processing*, Vol.14, No.2, pp.253–266 (2005).
[6] Thodi, D.M. and Rodriguez, J.J.: Expansion embedding techniques for reversible watermarking, *IEEE Trans. Image Processing*, Vol.16, No.3, pp.723–730 (2007).
[7] 佐々木隆幸：2 枚の電子透かし情報画像を埋め込めた電子透かしの制作と復元，特許庁，特願 2016-217619 (2016).
[8] Alyammahi, S., Taher, F., Al-Ahmad, H. and McGloughlin, T.: A New Multiple Watermarking Scheme for Copyright Protection and Image Authentication, *59th IEEE Inter. Midwest Symposium on Circuits and Systems* (2016).
[9] 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).
[10] Sasaki, T. and Nagase, T.: Constructing Digital Watermark Based on Orthogonal Functions, *5th IEEE Inter. Conference on Cyber Security and Cloud Computing* (*CSCloud*), pp.140–143 (2018).
[11] 佐々木隆幸，長瀬智行：直交多項式でつくる二重電子透かし，情報処理学会研究報告，Vol.2018-DCC-19, No.5 (2018).

長瀬 智行　（正会員）

1994 年東北大学大学院工学研究科博士課程修了．現在，弘前大学大学院理工学研究科准教授．通信ネットワークと情報セキュリティ関する研究．IEICE，IEEE 各会員．



佐々木 隆幸

1971 年弘前大学理学部卒業．1973 年東京農工大学大学院工学研究科修了．1984 年雇用促進事業団青森職業訓練短期大学校教官．2003 年国際協力事業団（日本・パラグアイ職業能力促進センタープロジェクト長期派遣専門家）．2008 年雇用・能力開発機構青森センター嘱託．2013 年高齢・障害・求職者雇用支援機構青森職業能力開発短期大学校非常勤講師，現在に至る．2016 年弘前大学大学院理工学研究科博士後期課程在学．