

二重情報ハイディング画像に関する研究

(A Study on Double Information Hiding Images)

2021年3月18日

佐々木 隆幸

二重情報ハイディング画像に関する研究

(A Study on Double Information Hiding Images)

弘前大学大学院理工学研究科

博士後期課程

博士論文

2021年3月18日

佐々木 隆幸

目次

(二重情報ハイディング画像に関する研究)

序章 要約	1
第1章 目的と意義	
1.1 目的	2
1.2 意義	5
第2章 情報ハイディングとは	
2.1 情報ハイディングの分類と用語	6
2.2 バーナム暗号	9
2.3 DES 暗号	10
2.4 RSA 暗号	15
2.5 楕円曲線暗号	18
2.6 ステガノグラフィ	23
2.7 電子透かし	30
第3章 秘匿化のために	
3.1 正規直交関数系とそのグラフ	34
3.2 正規直交関数系による秘匿化	40
3.3 展開係数分布図の平坦性	42
3.4 強制的な平坦化	44
3.5 展開係数の量子化	46
第4章 多重化のために	
4.1 偶関数と奇関数を活用する二重化	50
4.2 画素平面の2分割	53
4.3 画素空間の2分割	54
4.4 画像の三重化方法	55
4.5 ステガノグラフィと電子透かしによる二重化	56
第5章 安全のために	
5.1 改ざん範囲の集約化	57
5.2 情報ハイディング画像の高画質化	59

第 6 章 アルゴリズムと実験	
6.1 制作アルゴリズム	61
6.2 再生アルゴリズム	65
6.3 制作実験	66
6.4 再生実験	73
第 7 章 測定と評価	
7.1 制作・再生実験の測定と評価	74
7.2 改ざん実験の測定と評価	77
7.3 ビットプレーン転置効果の検証	86
第 8 章 結論	97
参考論文	99
研究報告	99
参考講義	99
参考文献	100

序章 要約

この論文は個人情報を秘匿に大量に安全に伝達することを目的に研究した論文である。ここに想定している個人情報は画像と文書の2種類である。

論文の独創的な着眼点は3つある。1つは画像を暗号化するための正規直交関数系を擬似乱数系列で構築した点である。数多くの文献で採用される正規直交関数系は超越関数グループに属する三角関数やハール関数などである。しかし、ここでは秘匿性を高めるために擬似乱数系列で構築した正規直交関数系を採用する。

2点目は1枚の画像の中に大量の個人情報を埋め込むために1枚の画像と1枚の文書の埋め込みを可能にした点である。1枚の画像の中に二重に埋め込むことによって、種類の異なる個人情報を大量に伝達することができる。

3点目は伝達途中における改ざんや傍受に対する安全対策の強化のために、画像のビットプレーンを転置した点である。ビットプレーン転置は改ざん領域の集約化が可能となる利点、しかも伝達する画像の高画質化が可能となる利点がある。したがって、伝達途中の安全性向上が期待できる。

3つの独創的な着眼点を中心にアルゴリズムの制作、実験、そして評価を多くの画像とイラストを用いて具体的に記述する。

第 1 章 目的と意義

1.1 目的

この論文の目的は個人情報を秘匿に大量に安全に伝達することである。想定している個人情報は画像と文書の 2 種類である。論文の目的をもう少し明確にするために、個人情報が画像の場合を例として伝達の周辺を俯瞰する[α],[1].

(1) 画像をそのまま伝達する場合

この場合には、画像が伝達途中で第三者に傍受されると、その画像は容易に閲覧されてしまう。また、第三者が画像を改ざんすると、受信者は改ざんされた画像を送信者が送信した画像であると誤解して、そのまま受信してしまう恐れがある。したがって、この伝達方法では秘匿性や安全性の確保は困難である。これを図 1.1 に例示する。

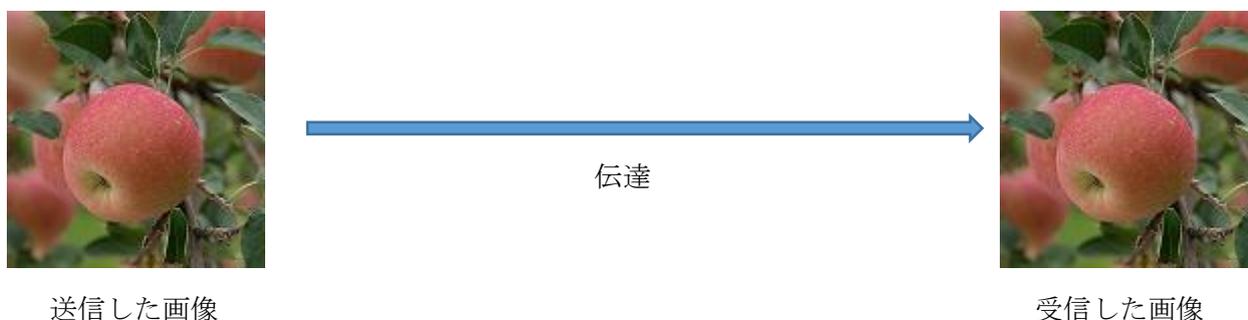


図 1.1 画像をそのまま伝達する場合

(2) 画像を暗号に変換して伝達する場合

画像が第三者に容易に閲覧されないようにするために、画像を暗号に変換し、暗号に変換した画像を伝達する場合である。これを図 1.2 に例示する。この場合は画像が第三者に傍受されても、第三者は画像を容易に閲覧することはできない。閲覧できるようになるまでは多少の解読時間が必要である。したがって、解読している時間中は秘匿性を保つことができる。

しかし、意味不明な画像が伝達されていることは明らかである。意味不明なこの画像の中に何かは隠されていると第三者に興味を惹起させる可能性が高い。また、そのような興味をもつ第三者の人数が増える恐れもある。したがって、第三者による改ざんも高まることが予想される。このような伝達にも安全性に不安が残る。

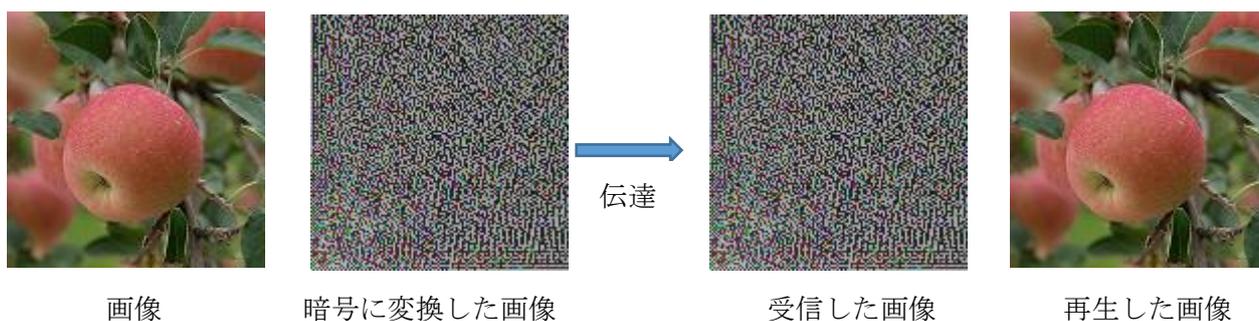


図 1.2 画像を暗号に変換して伝達する場合

(3) 暗号に変換した画像を日常的な画像に埋め込んで伝達する場合

画像を暗号に変換し、その変換した画像を日常的な画像の中に埋め込んで伝達する場合である。その日常的な画像を第三者が閲覧しても、その画像の中の暗号に気づくのは困難であろう。したがって第三者に傍受される可能性が低くなり、秘匿性を高めることができる。たとえ日常的な画像の中に暗号に変換した画像が隠されていることを知られたとしても、それを解読するためには多くの解読時間がかかる。その解読時間は前例(2)の場合よりも長くなる。なぜならば、第三者は伝達に使用した日常的な画像を所有していないからである。

しかし、この伝達方法を可能にするためには送信者と受信者が日常的な画像を共有しなければならない。しかし、(1)と(2)の場合より安全性の高い伝達方法である。この例を図 1.3 に例示する。

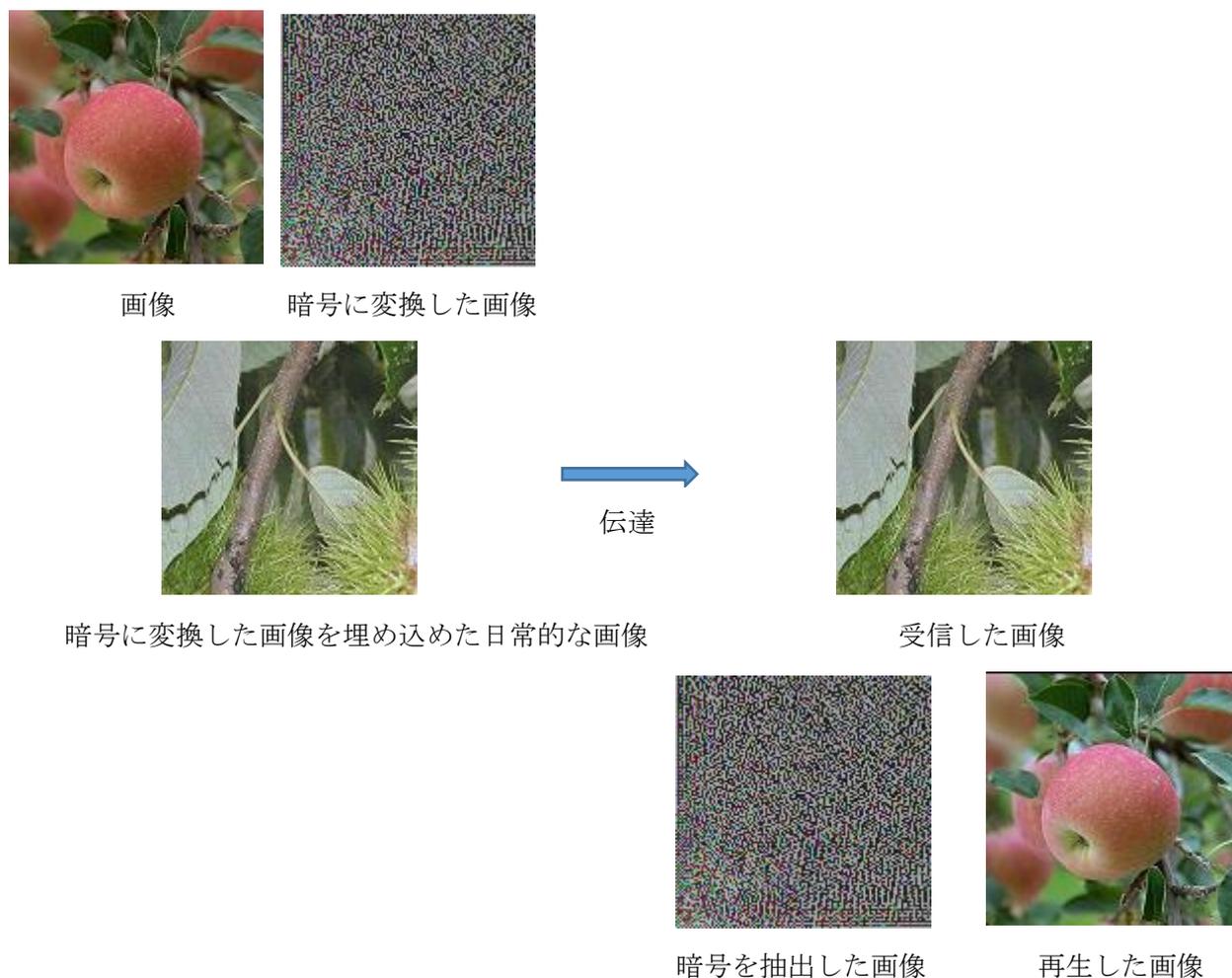


図 1.3 暗号に変換した画像を日常的な画像に埋め込んで伝達する場合

(4) 複数枚の画像を伝達する場合

暗号に変換した画像を 1 枚だけではなく複数枚の画像を日常的な画像の中に埋めることができれば、画像をその枚数だけ大量に伝達することができる。2 枚の画像を伝達する場合の例を図 1.4 に示す。



第 1 の画像



第 1 の画像を暗号に変換した画像



第 2 の画像



第 2 の画像を暗号に変換した画像



伝達



暗号に変換した第 1, 第 2 の画像を埋め込めた日常的な画像

受信した画像



第 1 の暗号を抽出した画像



再生した第 1 の画像



第 2 の暗号を抽出した画像



再生した第 2 の画像

図 1.4 暗号に変換した画像 2 枚を日常的な画像に埋め込んで伝達する場合

1.2 意義

デジタル技術の進歩により、画素数の大きな画像や精度よい医療画像などを容易に伝達できるようになってきた。一方、Wi-Fi 環境が整備され、誰でもが通信ネットワークに簡単にアクセスできるようになり、画像をいとも簡単に傍受や改ざんすることができるようになってきた。したがって、プライバシー保護の観点からは伝達途中における個人情報の安全性を確実に高めなければならない。その要請に応えるための方法として、情報ハイディングがいろいろと提案されている。

この論文は画像と文書、たとえば図 1.5 のような医療画像と図 1.6 のような患者カルテなどの個人情報を、秘匿に、大量に、安全に、伝達することを目的とする論文である。



図 1.5 医療画像

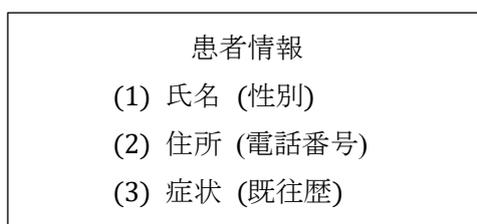


図 1.6 患者カルテ

第2章 情報ハイディングとは

2.1 情報ハイディングの分類と用語

情報ハイディングは、暗号(cryptography)、ステガノグラフィ(steganography)、そして電子透かし(watermark)の3つに大別できる[2],[3],[4].

さらに、暗号は共通キー暗号と公開キー暗号の2つに分類できる。共通キー暗号にはバーナム暗号(Vernam)とDES暗号(Data Encryption Standardの略)がある。公開キー暗号にはRSA暗号(開発者 Ron L. Rivest, Leonard Adleman, Adi Shamirの頭文字)と楕円曲線暗号(Elliptic curve)がある。以上を一覧にまとめたのが図2.1である。

この章では、バーナム暗号、DES暗号、RSA暗号、楕円曲線暗号、ステガノグラフィ、そして電子透かしについて、その原理と模擬実験例および長所や短所を簡潔に述べる。

バーナム暗号、DES暗号、RSA暗号、そして楕円曲線暗号は、節1.1(2)で述べた画像を暗号に変換して伝達する場合に類似する伝達方法である。それに対して、ステガノグラフィおよび電子透かしは節1.1(3)に対応する伝達方法である。

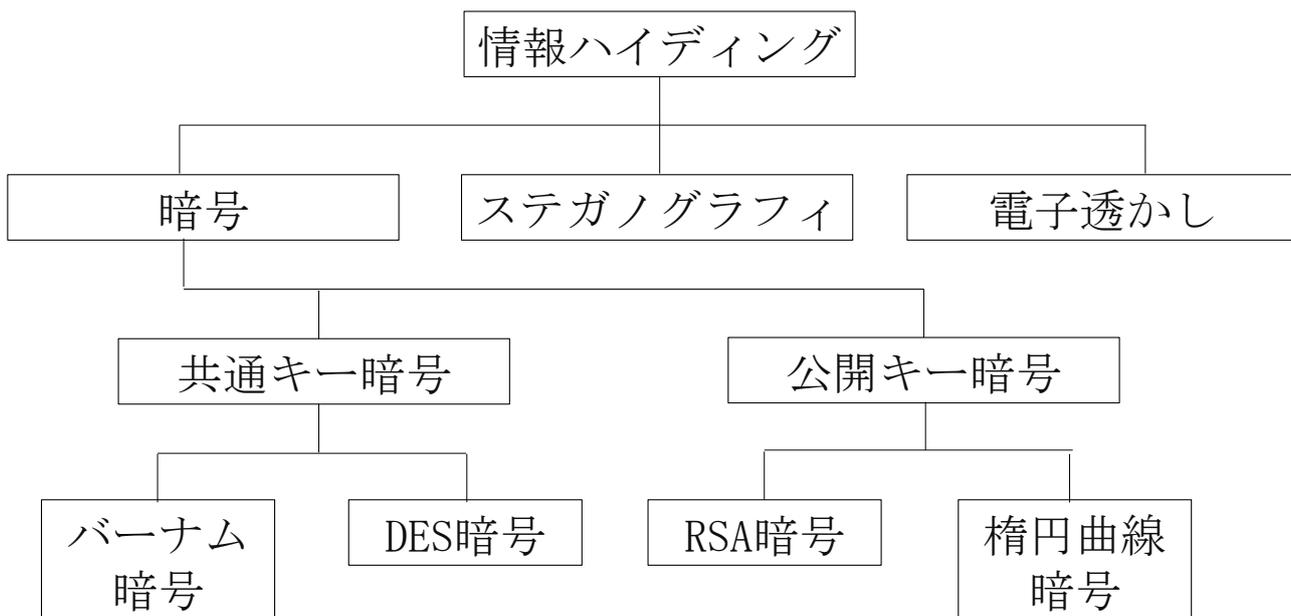


図2.1 情報ハイディングの分類

以降で用いる用語と記号を次のように整理しておく。理解のために図 2.2 (a), (b)に用語を付与する。

- (1) 平文：いかなる加工も施していない通常の文
- (2) 暗号化：平文を暗号に変換すること
- (3) 暗号：暗号化された文
- (4) 復号：正規の受信者が正規の手順で暗号を平文に戻すこと
- (5) 傍受：送信者が受信者に伝達中の暗号を第三者が盗み見や盗み取りこと
- (6) 解読：第三者が傍受した暗号から平文を推察すること
- (7) キー：暗号化または復号のために必要な情報
- (8) 共通キー：平文を暗号化するキーと暗号を復号するキーが共通である場合のキー
- (9) 公開キー：平文を暗号化するキーと暗号を復号するキーが異なる場合のキーで暗号化するキー
- (10) 秘密キー：平文を暗号化するキーと暗号を復号するキーが異なる場合のキーで復号するキー
- (11) DES：Data Encryption Standard の省略形
- (12) RSA：開発者 R. L. Rivest, A. Shamir, L. Adleman の 3 人の頭文字

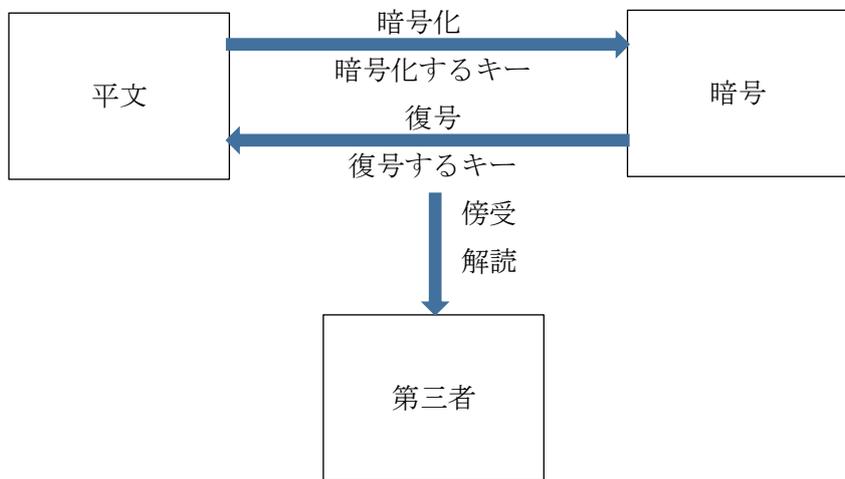


図 2.2 (a) 暗号関連用語の図例

- (13) 秘匿文書：秘匿に伝達する文書
- (14) 秘匿画像：秘匿に伝達する画像
- (15) 展開係数：画像を正規直交関数系で展開した直後の実数値の展開係数
- (16) 展開係数分布図：展開係数の分布図
- (17) 量子化係数：展開係数を整数値に量子化した係数
 なお量子化係数には展開係数の記号に接頭語 q を添える
- (18) 量子化特性：横軸を展開係数，縦軸を量子化係数とするグラフ
- (19) ビットプレーン：画像を2進数に分解したとき，同一ビットにおける2値画像
- (20) 量子化画像：ビットプレーン転置前の量子化係数の画像
- (21) 転置後量子化画像：ビットプレーン転置後の量子化係数の画像
- (22) サイファ画像：秘匿な文書を埋め込めた画像
- (23) ホログラム画像：転置後量子化画像とサイファ画像を合成した画像
- (24) カギ画像：ホログラム画像を埋め込む土台となる任意の日常的な画像
- (25) 情報ハイディング画像：ホログラム画像をスカラー倍のカギ画像に埋め込めた画像
- (26) 再生画像：情報ハイディング画像から再生した画像
- (27) 再生文書：情報ハイディング画像から再生した文書
- (28) ステガノグラフィ：秘匿情報を画像データに置き換えて秘匿情報の存在を隠す技術
- (29) 電子透かし：秘匿情報を画像データに埋め込めて秘匿情報の存在を隠す技術
- (30) 記号 Z_{ij} ：画像画面の最左下位置を1行1列とする行列 i 行 j 列における画素値
- (31) 記号 N ：画像の画素数
- (32) PSNR：ピーク信号対雑音比(Peak Signal to Noise Ratio) (単位[dB])

$$PSNR[dB] = 10 \log_{10} \frac{MAX^2}{\frac{1}{N^2} \sum_{i=1}^N (\sum_{j=1}^N (A_{ij} - B_{ij})^2)} \quad (A, B \text{ は画像}, N \text{ は画素数})$$

- (33) 相関係数 r ：類似性を表す尺度

$$r = \frac{\sum_{i=1}^N (\sum_{j=1}^N (A_{ij} - \bar{A})(B_{ij} - \bar{B}))}{\sqrt{\sum_{i=1}^N (\sum_{j=1}^N (A_{ij} - \bar{A})^2)} \cdot \sqrt{\sum_{i=1}^N (\sum_{j=1}^N (B_{ij} - \bar{B})^2)}} \quad (A, B \text{ は画像}, \bar{A}, \bar{B} \text{ は平均値}, N \text{ は画素数})$$

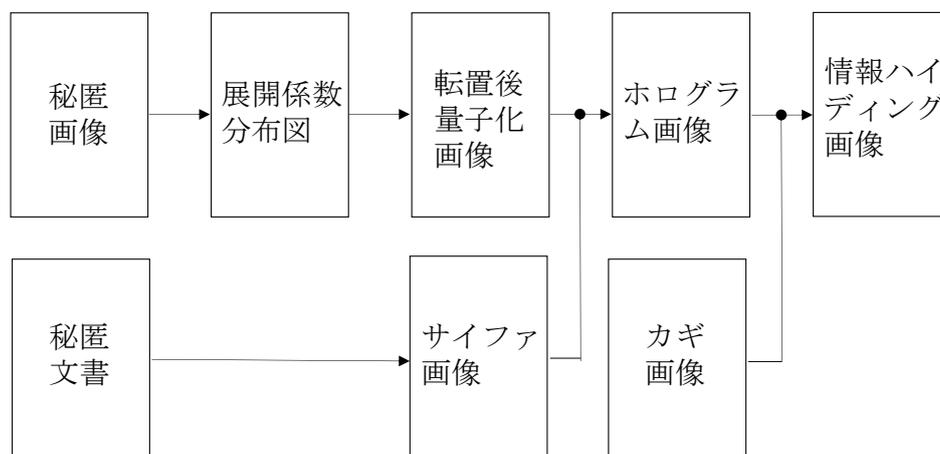


図 2.2 (b) ステガノグラフィおよび電子透かし関連用語の図例

2.2 バーナム暗号

(1) 原理

バーナム暗号はギルバート・バーナム(Vernam)が考案した暗号である。平文 M を、平文と同じ長さの共通キー K を用いて暗号化した暗号 C は式(2.1)で与えられる。ただし、記号 \oplus はビットの排他的論理和(Exclusive OR)を表すものとする。

$$C = M \oplus K \quad (2.1)$$

暗号 c を復号するには式(2.2)を用いる

$$M = C \oplus K \quad (2.2)$$

復号できる理由は

$$M = (M \oplus K) \oplus K \quad (2.3)$$

が成り立つからである。

なお、このような暗号方法は平文を 1 ビットずつ暗号化することからストリーム暗号[5],[6]とも呼ばれる。

(2) 模擬実験例

8 ビットの例で実験してみる。平文 $M = 10011010$ 、共通キー $K = 10101010$ とする。

暗号 c は

$$C = 10011010 \oplus 10101010 = 00110000 \quad (2.4)$$

になる。この暗号 C を共通キー K で復号すると

$$00110000 \oplus 10101010 = 10011010 \quad (2.5)$$

結果は元の平文と一致する。

(3) 長所

① この暗号の長所は理論的に解読不可能な点である。完璧な秘匿性をもつ点である。このことがシャノン[7]によって 1949 年に数学的に証明されている[8]。その概略を述べる。傍受した暗号に総当たりで排他的論理和計算を実行すると、その中には平文と一致するものが必ず存在する。しかし第三者はそれが正しい平文か否かを判定するための情報を所有してないので、暗号を解読することはできない。つまり、平文、共通キー、暗号という 3 つの情報のうちの暗号 1 つを傍受するだけでは、他の 2 つを解読することはできない。

② もう 1 つの長所は、暗号化計算においても復号計算においても、ビットごとに mod 2 で足し算[9]するだけであるので演算処理が高速である。

(4) 短所

① この暗号の短所は平文と同じ長さの共通キーを用意しなければならない点である。安全性を確保するには、暗号通信を行うごとに新しい共通キーを共有する必要がある。

② 安全のために暗号を伝達する都度に新しい共通キーを共有するならば、その共通キーを事前に配送しなければならないという不便さがある。

2.3 DES 暗号

(1) 原理

DES 暗号 (Data Encryption Standard) はアメリカ国立標準局が定めた標準規格となる暗号アルゴリズムである。DES 暗号の基本原理[10],[11],[12]を述べる。

最初に、0 と 1 に符号化された平文を英数字 8 文字分に相当する 64 ビットのブロックごとに分割する。その 64 ビットをさらに 32 ビットの左半分 L_1 、残り 32 ビットの右半分 R_1 に分割する。ここから第 1 段階の暗号化を開始し、第 16 段階まで続ける。各段階における暗号化は同じ手順であるので、第 n 段階における暗号化について述べる。

図 2.3 は第 n 段階における暗号化を示したものである。第 n 段階の右半分 R_n がそのまま第 $n+1$ 段階の左半分の入力 L_{n+1} として出力される。

他方、第 n 段階の左半分の L_n は次のように暗号化されて第 $n+1$ 段階の入力 R_{n+1} として出力される。初めに第 n 段階の右半分 R_n と鍵長さが 32 ビットの第 n 段階の共通キー K_n を関数 F に引数として渡し、32 ビットの関数值 f_n が戻る。次に f_n と L_n の排他的論理和をとる。その結果が第 $n+1$ 段階の右半分の入力 R_{n+1} として出力される。

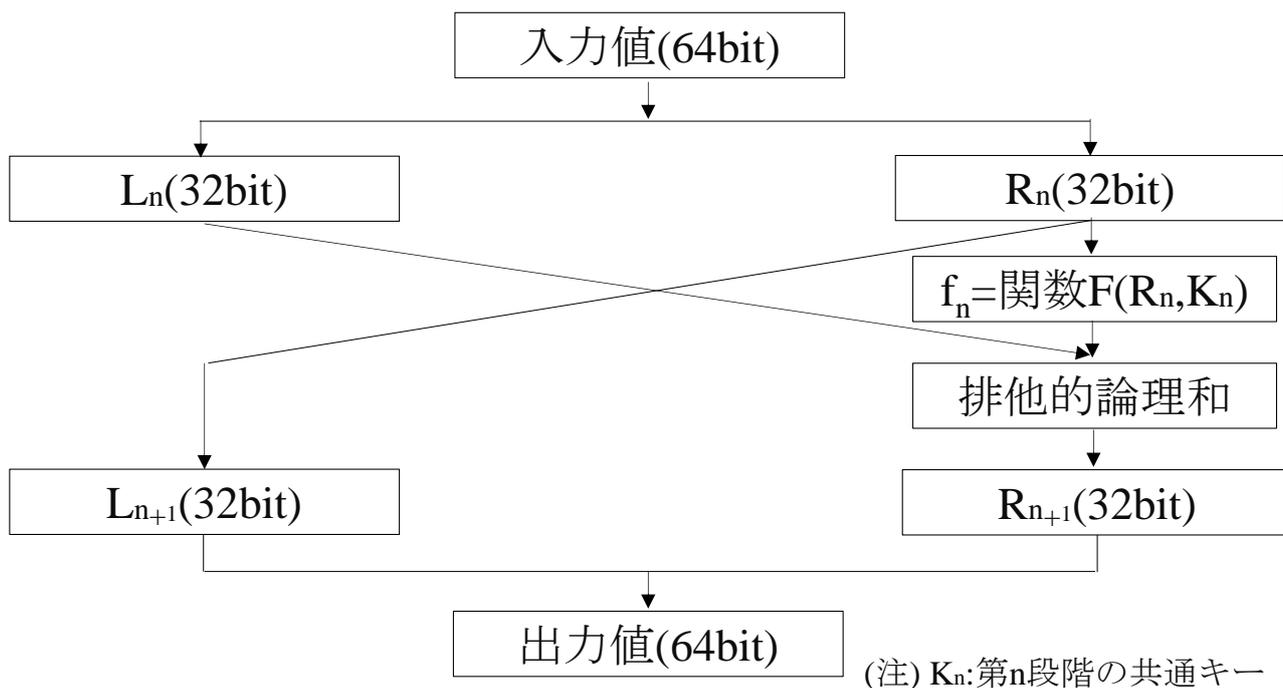


図 2.3 第 n 段階における DES 暗号化

(2) 模擬実験例

DES 暗号の実験を簡単なモデルで行う。それはビット長が 8 ビットで、段階数が 2 段階のモデル[13]である。共通キーを表 2.1 と設定する。関数 $F(R_n, K_n) = F(R_n) \oplus K_n$ とし、その関数値を f_n とする。関数 $F(R_n)$ における対応表を表 2.2 と設定する。

表 2.1 共通キーの設定

段階番号	共通キー
第 1 段階	1100
第 2 段階	0010

表 2.2 関数の対応表 (段階 $n=1,2$ のとき)

R_n	$F(R_n)$
0000	1001
0001	1011
0010	1101
0011	1111
0100	1000
0101	1010
0110	1100
0111	1110
1000	0111
1001	0101
1010	0011
1011	0001
1100	0110
1101	0100
1110	0010
1111	0000

① 暗号化するとき

平文「ア」を暗号化する。「ア」のJISコード「10110001」をそのまま平文 $M = 10110001$ とする。その後の暗号化過程を表 2.3 に示す。

表 2.3

	$M = 10110001$	
	第 1 段階($n=1$)のとき	
$L_1 = 1011$	4 ビットずつ左右に分割する	$R_1 = 0001$
$L_2 = R_1 = 0001$	右半分を左半分に移す $L_{n+1} = R_n$	
	関数処理 $f_n = F(R_n, K_n) = F(R_n) \oplus K_n$	対応表から $R_1 = 0001$ のとき $F(R_1) = 1011$ 共通キーとの排他的論理和 $f_1 = F(R_1) \oplus K_1$ $= 1011 \oplus 1100 = 0111$
	排他的論理和 $R_{n+1} = L_n \oplus f_n$	左半分との排他的論理和 $R_2 = L_1 \oplus f_1$ $= 1011 \oplus 0111 = 1100$
$L_2 = 0001$	結果を次段に出力	$R_2 = 1100$
	第 2 段階($n=2$)のとき	
$L_2 = 0001$	前段の出力	$R_2 = 1100$
$L_3 = R_2 = 1100$	右半分を左半分に移す $L_{n+1} = R_n$	
	関数処理 $f_n = F(R_n, K_n) = F(R_n) \oplus K_n$	対応表から $R_2 = 1100$ のとき $F(R_2) = 0110$ 共通キーとの排他的論理和 $f_2 = F(R_2) \oplus K_2$ $= 0110 \oplus 0010 = 0100$
	排他的論理和 $R_{n+1} = L_n \oplus f_n$	左半分との排他的論理和 $R_3 = L_2 \oplus f_2$ $= 0001 \oplus 0100 = 0101$
$L_3 = 1100$	左右の出力	$R_3 = 0101$
	以上から暗号 C を得る $C = 11000101$	

② 復号するとき

表 2.3 で得た暗号 $C=11000101$ を平文 $M = 10110001$ に戻す。復号過程は暗号化の逆過程である。それを表 2.4 に示す。

表 2.4

	$C = 11000101$	
	第 2 段階($n=2$)のとき	
$L_3 = 1100$	4 ビットずつ左右に分割する	$R_3 = 0101$
	左半分を右半分に移す $R_n = L_{n+1}$	$R_2 = L_3 = 1100$
対応表から $R_2 = 1100$ のとき $F(R_2) = 0110$ 共通キーとの排他的論理和 $f_2 = F(R_2) \oplus K_2$ $= 0110 \oplus 0010 = 0100$	関数処理 $f_n = F(R_n, K_n) = F(R_n) \oplus K_n$	
右半分との排他的論理和 $L_2 = R_3 \oplus f_2$ $= 0101 \oplus 0100 = 0001$	排他的論理和 $L_n = R_{n+1} \oplus f_n$	
$L_2 = 0001$	結果を次段に出力	$R_2 = 1100$
	第 1 段階($n=1$)のとき	
$L_2 = 0001$	前段の出力	$R_2 = 1100$
	左半分を右半分に移す $R_n = L_{n+1}$	$R_1 = L_2 = 0001$
対応表から $R_1 = 0001$ のとき $F(R_1) = 1011$ 共通キーとの排他的論理和 $f_1 = F(R_1) \oplus K_1$ $= 1011 \oplus 1100 = 0111$	関数処理 $f_n = F(R_n, K_n) = F(R_n) \oplus K_n$	
右半分との排他的論理和 $L_1 = R_2 \oplus f_1$ $= 1100 \oplus 0111 = 1011$	排他的論理和 $L_n = R_{n+1} \oplus f_n$	
$L_1 = 1011$	左右の出力	$R_1 = 0001$
	以上から平文 M を復号できる $M = 10110001$	

(3) 長所

- ① DES 暗号アルゴリズムは 1977 年に米国連邦政府情報処理規格 FIPS(Federal Information Processing Standard) [14], [15]として制定され公開される。共通キーさえ秘密に管理すれば、当時のコンピュータの計算能力では解読に長い時間を要することから安全性が高い。
- ② 暗号化処理と復号処理はブロック長の半分ずつの排他的論理和と関数の対応表を主体としているので、ハードウェアが小型実装でよい。
- ③ 暗号化および復号の処理速度が公開キー暗号法よりも高速である[16]。

(4) 短所

- ① コンピュータ性能の向上によって解読される危険性が増大してきた。たとえば RSA Security 社が主催の 1999 年 DES 解読コンテストで、非営利団体 EFF(Electronic Frontier Foundation)が総当たり探索の方法で DES の共通キーが 22 時間 15 分で解読されたという報告がある。そのため、より高速でより安全な暗号法として、AES 暗号(Advanced Encryption Standard)が米国連邦政府情報処理規格[17]に制定される。
- ② 共通キーを配送する必要がある、配送中に盗まれる危険性がある。
- ③ 送信者 1 人と受信者 1 人だけで暗号を伝達し合う場合には共通キーは 1 種類あればよい。しかし、 N 人が相互に伝達し合うためでは、共通キーの種類は $N(N - 1)/2$ となり、共通キーが盗まれないように管理することが困難になる。

2.4 RSA 暗号

(1) 原理

RSA 暗号は 1977 年に R. L. Rivest, A. Shamir, L. Adleman の 3 人が開発した暗号[18]で, RSA は 3 人の頭文字である. この暗号法は公開キーによる暗号法[19],[20],[21]の代表例である. この暗号法の安全性は大きな素数の積の素因数分解が困難である[22],[23]ことに基づいている. RSA 暗号の原理を下に述べる.

- ① 大きな素数を 2 つ用意する. それらを p, q とする.
- ② $n = p \cdot q, \varphi = (p - 1)(q - 1)$ とおく.
- ③ 式 $k \cdot \varphi + 1 = e \cdot d$ を満たす e, d を決める. ただし, k は自然数, e, d は素数とする.
- ④ e と n の組を暗号の送信者に事前に公開キーとして公開する. 受信者は d と n の組を秘密キーとして秘密にしておく.
- ⑤ 暗号の送信者はその公開キーを用いて, 平文 M を次式で暗号化する. その暗号 C を公開キーの発行者である受信者に送る.

$$C \equiv M^e \pmod{n} \quad (2.6)$$

- ⑥ 受信者は自分の秘密キー d と n の組を用いて復号する. 次式で復号できる.

$$M \equiv C^d \pmod{n} \quad (2.7)$$

RSA 暗号法の特徴は, 平文を暗号化する公開キー e と n の組と, 暗号を復号する秘密キー d と n の組が異なる点である.

次に復号できる理由を述べる.

式(2.6)の C から

$$C^d \equiv (M^e)^d \equiv (M^{ed}) \pmod{n} \quad (2.8)$$

そして, ③から

$$ed = k\varphi + 1 = k(p - 1)(q - 1) + 1 \quad (2.9)$$

したがって, オイラーの定理から

$$(M^{ed}) \equiv M^{k(p-1)(q-1)+1} \equiv M \pmod{n} \quad (2.10)$$

となる.

(2) 模擬実験例

50音のひらがなといくつかの記号に適切な2桁の数値を対応づける。たとえば表2.5のように対応づける。送信したい平文「おはようございます。」を数値に変換すると次のようになる。

「 05 26 40 03 55 56 02 31 13 70 」

そして、これらの数値の区切り方を、2桁ではなく、異なる桁ごとに区切るのが一般的である。その理由は統計的な規則性が暗号の中に出現するのを避けるためである。ここでは簡便さのため3桁ごとに区切りにする。すると

「 052 640 035 556 023 113 700 」

となる。なお、最後の数値は2桁になるので、0の1桁を追加して3桁に揃えてある。

表 2.5 ひらがなと記号に対応づけられた数値

あ	01	い	02	う	03	え	04	お	05
か	06	き	07	く	08	け	09	こ	10
さ	11	し	12	す	13	せ	14	そ	15
た	16	ち	17	つ	18	て	19	と	20
な	21	に	22	ぬ	23	ね	24	の	25
は	26	ひ	27	ふ	28	へ	29	ほ	30
ま	31	み	32	む	33	め	34	も	35
や	36	空白	37	ゆ	38	空白	39	よ	40
ら	41	り	42	る	43	れ	44	ろ	45
わ	46	ん	47	を	48	空白	49	空白	50
が	51	ぎ	52	ぐ	53	げ	54	ご	55
ざ	56	じ	57	ず	58	ぜ	59	ぞ	60
だ	61	ぢ	62	づ	63	で	64	ど	65
*	66	!	67	—	68	,	69	。	70

原理で述べた順序に沿って実験を進めていく。

- ① 2つの素数 p , q を用意する。そのとき、暗号化する数値が3桁であるから、素数 p と q の積が4桁以上になるように選ぶ。ここでは、 $p = 31$, $q = 37$ と決める。
- ② $n = p \cdot q = 31 \times 37 = 1147$, $\varphi = (p - 1)(q - 1) = 1080$ とおく。
- ③ 式 $k \cdot 1080 + 1 = e \cdot d$ を満たす e , d を決める。ただし、 k は自然数、 e , d は素数とする。
 $k = 1$, $e = 23$, $d = 47$ とする。
- ④ 公開キー $e = 23$ と $n = 1147$ の組を暗号の送信者に公開する。送信者は公開キーを用いて、平文の3桁数値「 052 640 035 556 023 113 700 」を $C \equiv M^e \pmod{n}$ で暗号化する。暗号は「 420 360 994 519 325 856 534 」となる。これを、公開キーを発行した受信者に送る。
- ⑤ 秘密キーをもつ受信者は暗号文を $M \equiv C^d \pmod{n}$ で復号する。復号は「 052 640 035 556 023 113 700 」となる。これを2桁の数値に区切ると平文の2桁数値と一致する。

(3) 長所

① 安全性が高い。それは2つの素数の因数分解が困難であることに原因する。公開キーは公開されているので誰でも暗号化して送信できる。しかし、暗号化された暗号文は公開キーでは復号できない。これを復号できるのは秘密キーだけである。すなわち、誰でも暗号化して送信できるが、復号できる人は秘密キーを所有している人だけである。

② カギの管理が容易である。公開キーは公開するので秘密キーさえ厳重に管理すればよい。多人数が相互に情報交換する場合、共通キー方式に比較すると全体におけるカギの個数は少なくてよい。たとえば N 人が相互に情報交換する場合、共通キーの場合では $N(N-1)/2$ 個のカギが必要になるのに対し、全体のカギの個数は $2N$ 個だけで済む。

③ 電子署名を行うことができる点である。秘密キーで平文を暗号化すると、これは公開キーでないと復号することができない。その秘密キーはただ1個しかなく、それを所有している人は本人だけである。したがって、秘密キーで暗号化された暗号文は秘密キーを所有する人でないと作成することができない。このことが印鑑やサインの役割を果たすことになり、電子署名として活用できる。

(4) 短所

暗号化および復号の処理速度に遅いことである。バイト数が多い平文や画像のように情報量が多い場合には処理時間が長くなる。

2.5 楕円曲線暗号

(1) 原理

楕円曲線暗号は Miller と Koblitz によって、それぞれ独立に 1985 年と 1987 年に発表された暗号法 [24],[25]である。どちらも公開キー方式である。楕円曲線暗号の安全性は楕円曲線上の加算演算の困難性に基いている。点 P と点 Q が既知であっても、 $Q = n \cdot P$ を満たす加算回数 n を求めることが容易ではないからである。一般に楕円曲線暗号における楕円曲線とは、式 $y^2 = x^3 + ax + b$ (a, b : 定数) の形で表される曲線で、 x 軸を中心に上下対称な曲線である。暗号に用いるためには重解や三重解を避けなければならないので、 $4a^3 + 27b^2 \neq 0$ という制限条件を設ける。

平文や暗号は楕円曲線の点で表される。暗号化あるいは復号は楕円曲線上の点の加算が必要になる。加算の定義 [26],[27],[28],[29],[30]は次のように場合分けされる。

(1) 2 点が異なる場合の加算は、点 P と点 Q を通る直線と楕円曲線との交点を求め、その交点と x 軸に関して対称になる点 R を $R=P+Q$ と定める。それを図 2.4 (a) に示す。

(2) 2 点が重なる場合の加算は、その点 P における接線と楕円曲線との交点を求め、その交点と x 軸に関して対称になる点 R を $R=2P=P+P$ と定める。この様子を図 2.4 (b) に示す。

なお、それぞれの場合の点 R の座標は次式で与えられる。

i) 異なる 2 点 $P = (x_P, y_P)$, $Q = (x_Q, y_Q)$ のとき

$$x_R = \left(\frac{y_P - y_Q}{x_P - x_Q} \right)^2 - x_P - x_Q \quad (2.11)$$

$$y_R = \left(\frac{y_P - y_Q}{x_P - x_Q} \right) (x_P - x_R) - y_P \quad (2.12)$$

ii) 2 点が点 $P = (x_P, y_P)$ で一致するとき

$$x_R = \left(\frac{3x_P^2 + a}{2y_P} \right)^2 - 2x_P \quad (2.13)$$

$$y_R = \left(\frac{3x_P^2 + a}{2y_P} \right) (x_P - x_R) - y_P \quad (2.14)$$

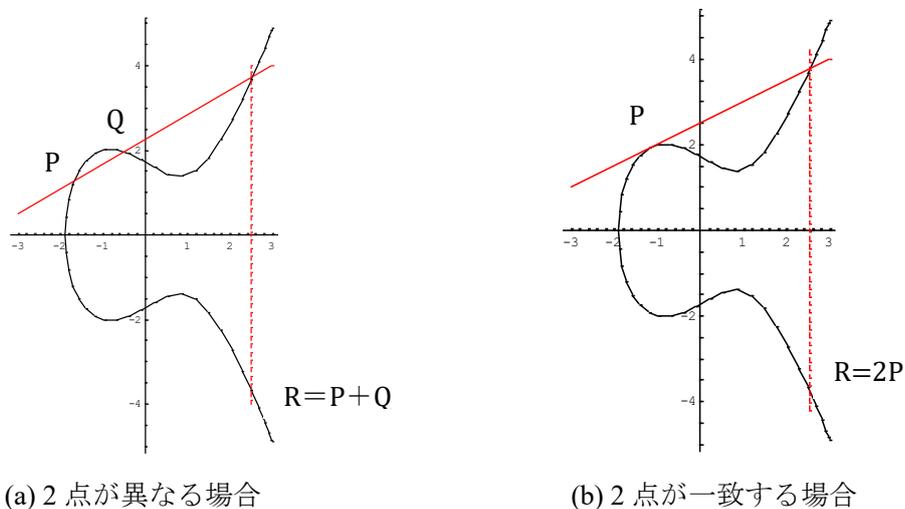


図 2.4 楕円曲線の加算

次に楕円曲線暗号の原理を述べる。楕円曲線の加算を暗号に活用するために、素数 p を法とする整数点の座標だけを用いることにする。すなわち

$$y^2 \equiv x^3 + ax + b \pmod{p} \quad (\text{ただし } 4a^3 + 27b^2 \equiv 0 \pmod{p})$$

を満たす座標である。

① グループ共通乱数を r 、ベースポイントを P_B 、送信者 A および受信者 B の公開キーをそれぞれ A_p, B_p とする。送信者と受信者の秘密キーをそれぞれ a_s, b_s とする。ベースポイント、公開キーは座標で表され、グループ共通乱数、秘密キーは1つの数値である。公開キーはベースポイントの秘密キー倍とする。すなわち $A_p = a_s \cdot P_B, B_p = b_s \cdot P_B$ である。

② 送信者 A はベースポイント P_B と受信者 B の公開キー暗号 B_p を用いて2つの暗号をつくる。第1暗号 C_1 を次式に基づいてつくる。

$$C_1 = r \cdot P_B \tag{2.15}$$

③ 第2暗号 C_2 を次式でつくる。ただし M は平文である。

$$C_2 = M + r \cdot B_p \tag{2.16}$$

④ 送信者は受信者に2つの暗号 C_1, C_2 を伝達する。

⑤ 暗号を受けた受信者は自分の秘密キー b_s を用いて、次式によって復号する。

$$C_2 - b_s \cdot C_1 \tag{2.17}$$

復号できる理由を述べる。

式(2.17)は次のように変形でき、元の平文が得られる。

$$C_2 - b_s \cdot C_1 = M + r \cdot B_p - b_s \cdot (r \cdot P_B) = M + r \cdot (b_s \cdot P_B) - b_s \cdot (r \cdot P_B) = M \tag{2.18}$$

ただし、マイナス符号が付いてある座標はその逆元をつくり加算する。すなわち、 y 座標を $p - y$ の値に変えて演算する。

(2) 模擬実験例

採用する楕円曲線は $y^2 \equiv x^3 + x$ である。そのグラフを図 2.5 に示す。法に採用する素数 p は $p = 61$ とする。暗号化と復号に採用できる点の個数は、 $y^2 \equiv x^3 + x \pmod{61}$ の場合の 73 個となる。その点を図 2.6 に示す。図には、ベースポイント P_B を番号 1 の点(59,7)とした場合のすべての可算点 73 個を番号で記してある。それぞれの点の座標を表 2.1 に示す。

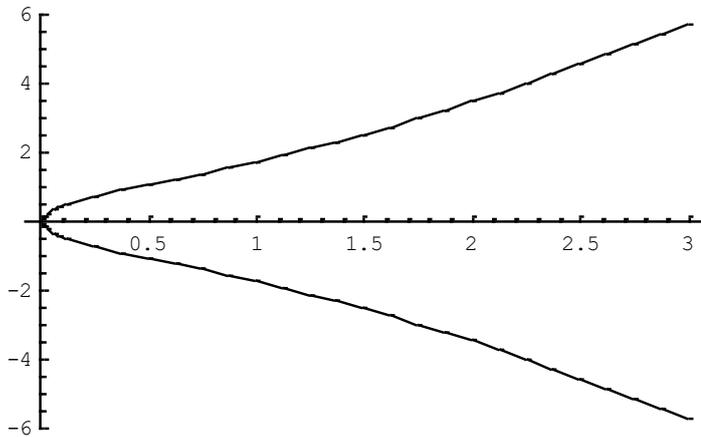


図 2.5 採用する楕円曲線

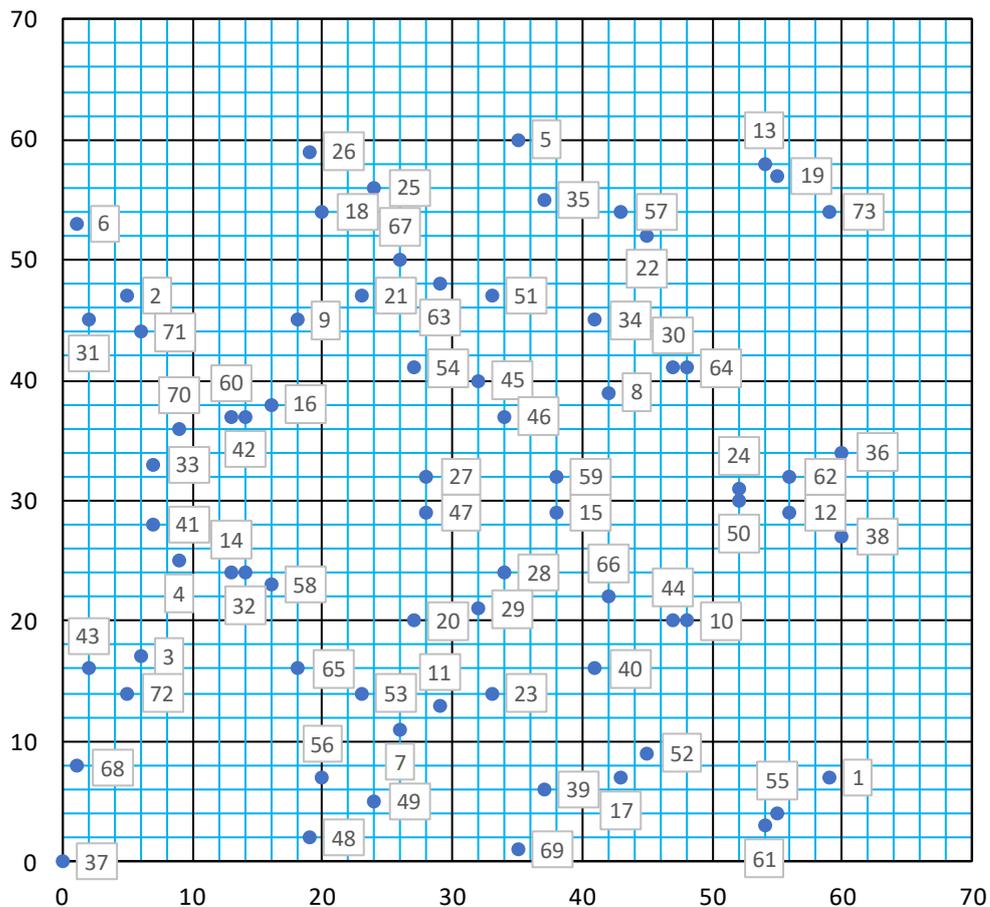


図 2.6 楕円曲線暗号の点

表 2.6 楕円曲線暗号の点の座標

No.	x	y									
1	59	7	21	23	47	41	7	28	61	54	3
2	5	47	22	45	52	42	14	37	62	56	32
3	6	17	23	33	14	43	2	16	63	29	48
4	9	25	24	52	31	44	47	20	64	48	41
5	35	60	25	24	56	45	32	40	65	18	16
6	1	53	26	19	59	46	34	37	66	42	22
7	26	11	27	28	32	47	28	29	67	26	50
8	42	39	28	34	24	48	19	2	68	1	8
9	18	45	29	32	21	49	24	5	69	35	1
10	48	20	30	47	41	50	52	30	70	9	36
11	29	13	31	2	45	51	33	47	71	6	44
12	56	29	32	14	24	52	45	9	72	5	14
13	54	58	33	7	33	53	23	14	73	59	54
14	13	24	34	41	45	54	27	41			
15	38	29	35	37	55	55	55	4			
16	16	38	36	60	34	56	20	7			
17	43	7	37	0	0	57	43	54			
18	20	54	38	60	27	58	16	23			
19	55	57	39	37	6	59	38	32			
20	27	20	40	41	16	60	13	37			

平文「おやすみなさい」を、表 2.5 を用いて数値に置き換えると、「05 36 13 32 21 11 02」となる。この数値をy座標とする座標点は「(24,5) (9,36) (29,13) (28,32) (32,21) (26,11) (19,2)」である。これを暗号化する。

- ① グループ共通乱数を $r = 3$ ，ベースポイントを $P_B = (59,7)$ ，送信者および受信者の公開キーをそれぞれ $A_p = (5,47)$ ， $B_p = (35,60)$ とする。送信者と受信者の秘密キーはそれぞれ $a_s = 2$ ， $b_s = 5$ とする。
- ② 第1の暗号 C_1 を次式に基づいてつくる。

$$C_1 = r \cdot P_B = 3 \cdot (59,7) = (6,17) \quad (2.19)$$

- ③ 第2の暗号 C_2 を平文 M と受信者の公開キーを用いてつくる。平文の第1文字の座標(24,5)を暗号化すると

$$C_2 = M + r \cdot B_p = (24,5) + 3 \cdot (35,60) = (24,5) + (38,29) = (48,41) \quad (2.20)$$

同様なことを平文の文字数だけ繰り返す。暗号 C_2 は次のようになる。

「(48,41) (29,13) (19,59) (14,37) (47,20) (45,52) (29,48)」

- ④ 送信者は受信者に2つの暗号 C_1 ， C_2 を伝達する。
- ⑤ 暗号を受けた受信者は自分の秘密キー b_s を用いて、次式によって復号化する。

$$C_2 - b_s \cdot C_1 = (48,41) - 5 \cdot (6,17) = (48,41) - (38,29) \quad (2.21)$$

ここで、マイナス符号が付いている座標はその逆元をつくる。すなわち、y座標のみを

$$p - y = 61 - 29 = 32 \quad (2.22)$$

に変えて加算する。

$$C_2 - b_s \cdot C_1 = (48,41) + (38,32) = (24,5) \quad (2.23)$$

この演算を繰り返すと、次のように復号できる。

「(24,5) (9,36) (29,13) (28,32) (32,21) (26,11) (19,2)」

(3) 長所

楕円曲線暗号の公開キーや秘密キーの長さは、RSA 暗号のそれよりも短い長さであっても、RSA 暗号と同等の安全性を達成できる。

(4) 短所

ここに掲げた楕円曲線暗号は楕円曲線上の点を用いる方法であるので、任意の整数を自由に選ぶことはできないという制約がある。したがって使用できる平文にも限界がある。これを解消したのがメンジース・ヴァンストーン暗号[31]である。楕円曲線上の点だけの制約を楕円曲線からずれた点も暗号化に使用できるように改良したものである。

以上述べてきた、バーナム暗号、DES 暗号、RSA 暗号、そして楕円曲線暗号は、節 1.1 (2)で述べた画像を暗号に変換し、それを隠さずにそのまま伝達する場合に相当する情報ハイディングである。

2.6 ステガノグラフィ

これから述べるステガノグラフィと、次節で述べる電子透かしは、節 1.1 (3)に相当する情報ハイディングである。

ステガノグラフィは情報ハイディングの1つであり、伝達したい秘匿画像や秘匿文書を任意の日常的な画像の中にデータを置換して埋め込む技術である。別の画像の中に埋め込めてしまうので、秘匿画像や秘匿文書が隠されていること自体を隠すことができる方法である。したがって、誰にも知られないように秘かに伝達できる方法[32, 33, …, 131]である。

(1) 原理

画素が8ビットの単色濃淡画像は8枚のビットプレーンに分解できる。カラー画像の場合には、さらに赤色、緑色、青色に分解できる。一般に日常的な画像は上位ビットプレーンになるほどそこに現れる画像は判読し易く、下位ビットプレーンになるほど現れる画像は乱雑になり判読し難いという性質がある。画像のこの性質を活用したのがステガノグラフィの原理である。

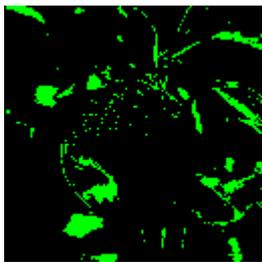
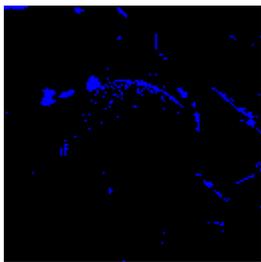
以降では、LSB (Least Significant Bit) に相当する最下位ビットプレーンをビットプレーン 0、MSB (Most Significant Bit) に相当する最上位ビットプレーンをビットプレーン7とする。

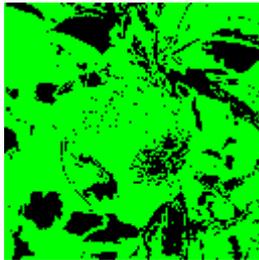
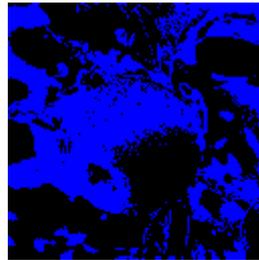
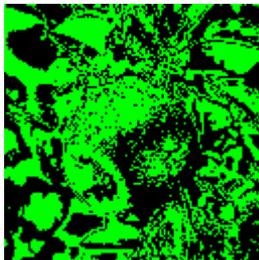
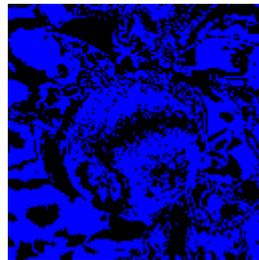
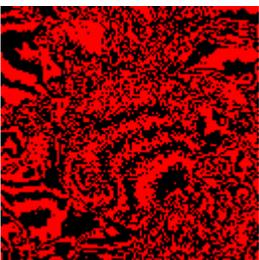
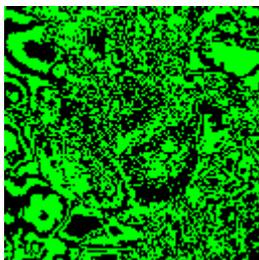
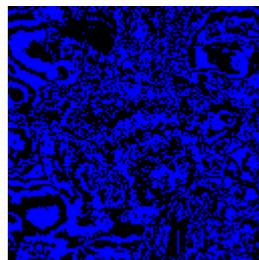
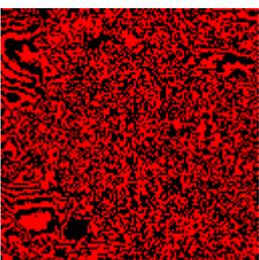
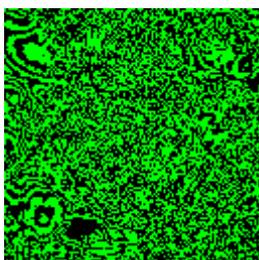
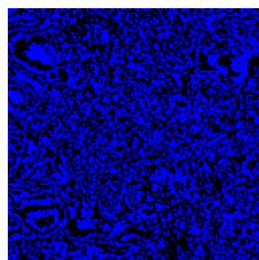
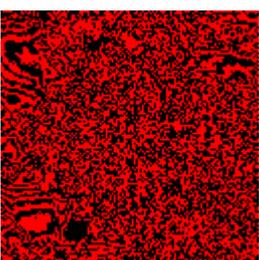
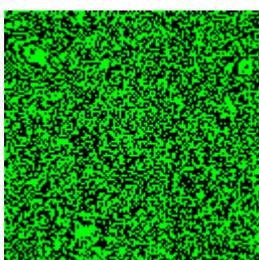
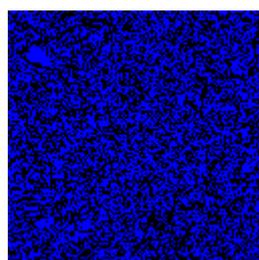
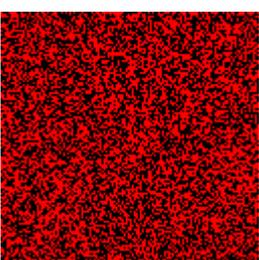
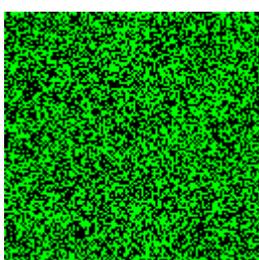
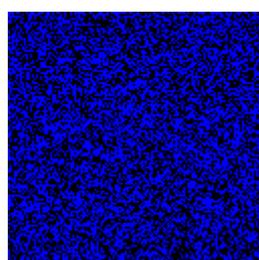
図 2.7 のカラー画像を赤色、緑色、青色のビットプレーンに分解した画像が表 2.7 である。各色のビットプレーン 0 における画像は定まった形状がなく乱雑にみえる。このビットプレーン 0 に秘匿画像や秘匿文書を埋め込むことが可能となる。なぜならば、画像や文書のデジタル情報は「0」と「1」の組み合わせであり、それらが多くなるほど乱雑な並び方になる傾向があるからである。

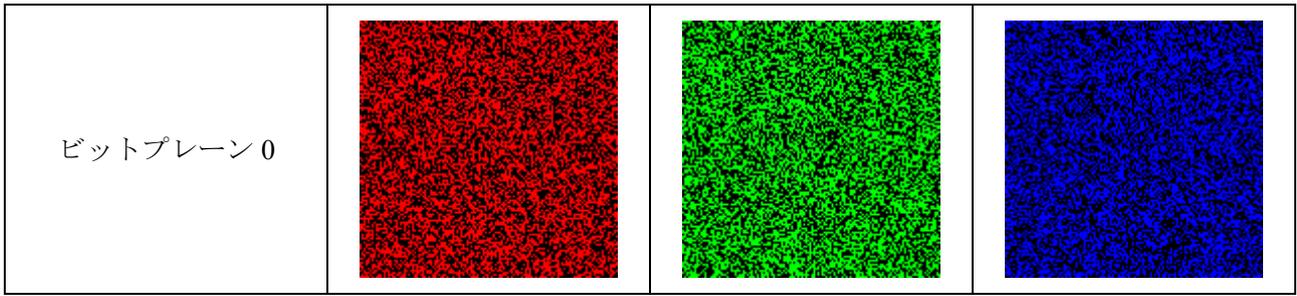


図 2.7 日常的な画像

表 2.7 図 2.7 のビットプレーン画像

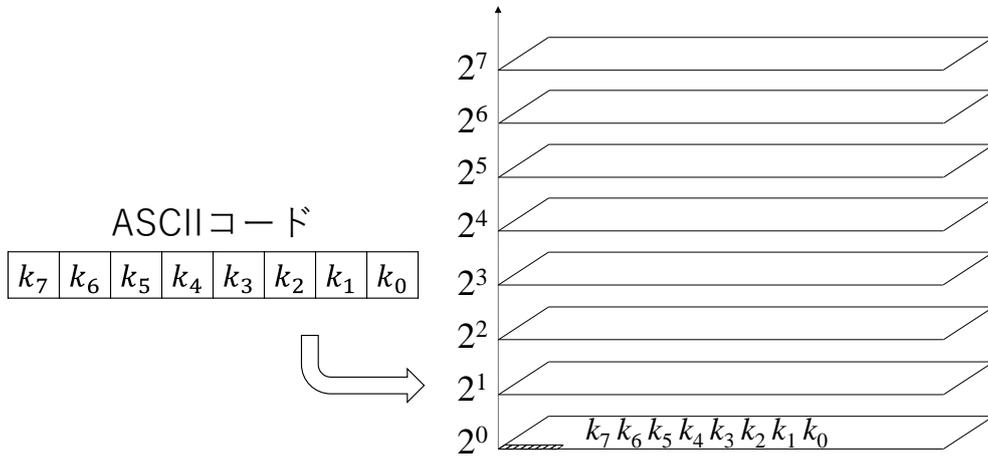
ビットプレーン番号	Red	Green	Blue
ビットプレーン7			

ビットプレーン 6			
ビットプレーン 5			
ビットプレーン 4			
ビットプレーン 3			
ビットプレーン 2			
ビットプレーン 1			

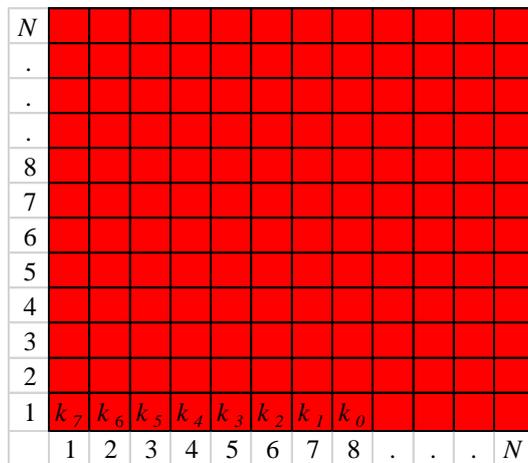


(a) 秘匿文書の埋め込み方

画素数 $N \times N$ のカラー画像の赤色ビットプレーン0にアスキーコード「 $k_7, k_6, k_5, k_4, k_3, k_2, k_1, k_0$ 」を秘匿文書として埋め込む場合を述べる。以降のビットプレーンの位置の表し方は、画像の場合と同様に、最左下角を1行1列、最右上方を N 行 N 列とする。アスキーコード「 $k_7, k_6, k_5, k_4, k_3, k_2, k_1, k_0$ 」を先頭ビット k_7 から1ビットずつ赤色ビットプレーン0の1行1列～1行8列に順に埋め込む。それを図2.8に示す。赤色ビットプレーン0内に、最大 $N \times N/8$ 個のアスキー文字を埋め込むことができる。



(a)アスキーコードが埋め込まれる赤色ビットプレーン0



(b)赤色ビットプレーン0に埋め込まれたアスキーコード

図2.8 アスキーコードを赤色ビットプレーン0に埋め込む場合

(b) 秘匿画像の埋め込み方

次に、画素数 $M \times M$ のカラー画像を画素数 $N \times N$ のカラー画像に埋め込む場合を述べる。埋め込む方法は画素値が $k_7 \times 2^7 + k_6 \times 2^6 + k_5 \times 2^5 + k_4 \times 2^4 + k_3 \times 2^3 + k_2 \times 2^2 + k_1 \times 2^1 + k_0 \times 2^0$ であるとき、図 2.9 に示すように、「 $k_7, k_6, k_5, k_4, k_3, k_2, k_1, k_0$ 」の 8 ビットをビットプレーン 0 に順番に埋め込む。これを色ごとに繰り返すと、カラー画像を埋め込むことができる。ただし、画素数 $N \times N$ の画像に埋め込める最大の画素数 $Max \times Max$ は、1 色の画素が 8 ビットで表現される場合には、 $Max^2 \leq N^2/8$ に制限される。

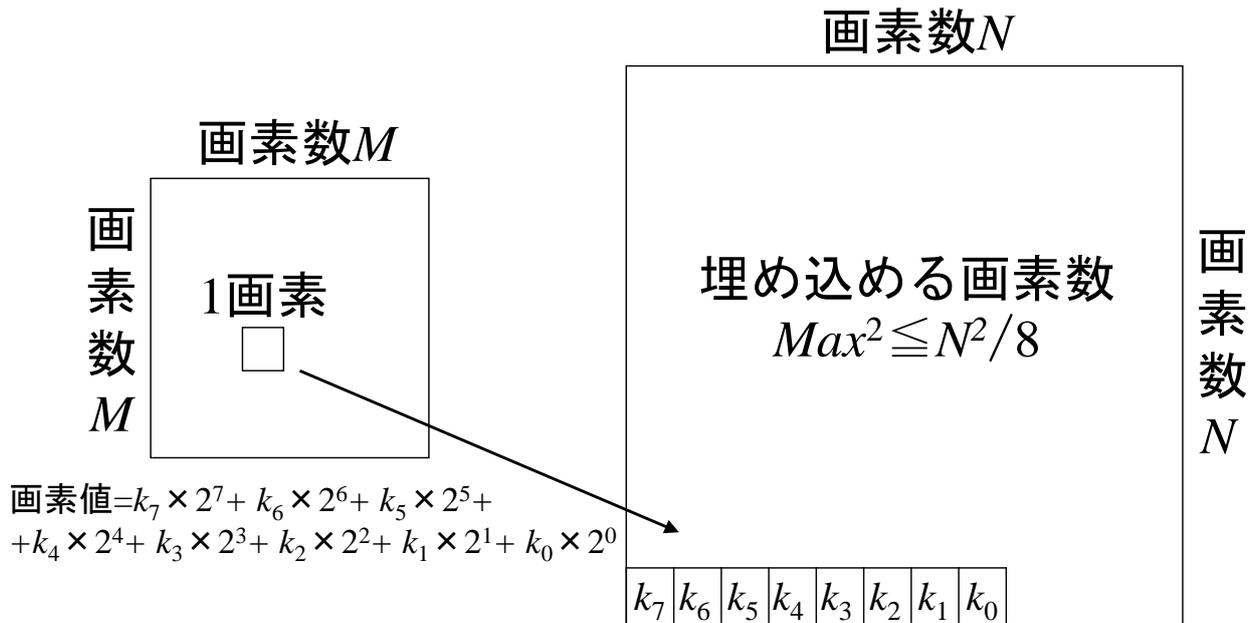


図 2.9 秘匿画像を埋め込む場合

合せて「01000001」となりアスキーコード「A」を表す。以下同様である。したがって、秘匿文書が再生されていることを確認できる。このアスキーコードを文字に変換して表示したのが図 2.13 の左下部分の赤色枠内である。

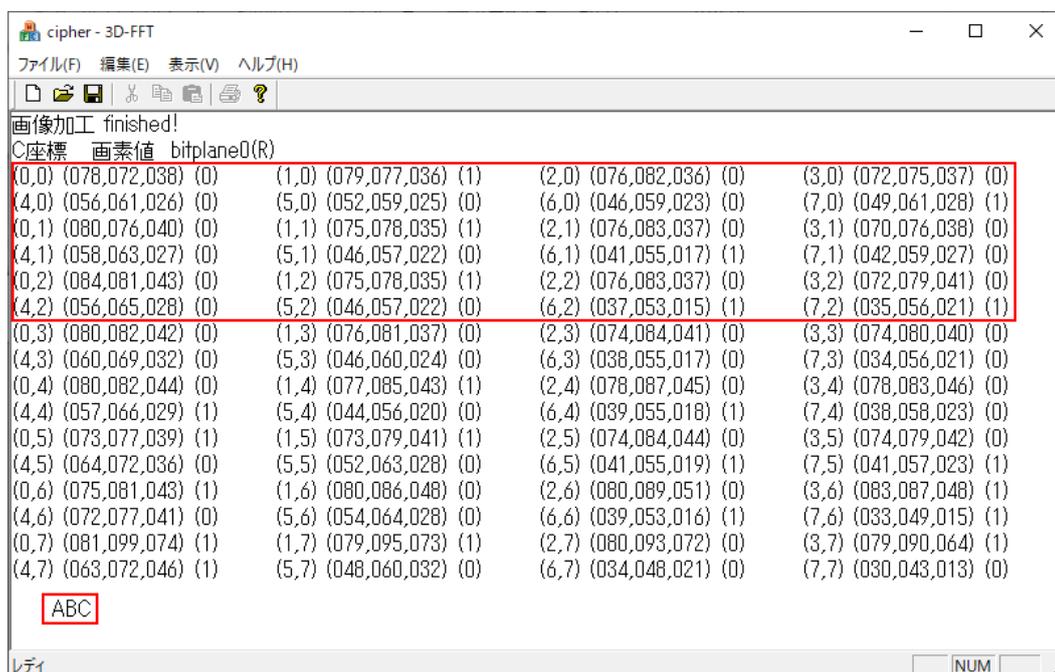


図 2.13 図 2.12 から再生した秘匿文書

③ 秘匿画像を埋め込むとき

次に、画像数 64×64 のカラー画像 A を画像数 256×256 のカラー画像 B に埋め込める場合を示す。カラー画像 A の 1 行 1 列～64 行 32 列の画素値 8 ビット「 $k_7, k_6, k_5, k_4, k_3, k_2, k_1, k_0$ 」を、カラー画像 B のビットプレーン 0 の 1 行 1 列～64 行 256 列の位置に埋め込む。これを赤色、緑色、青色の色別に行う。さらに、カラー画像 A の 1 行 33 列～64 行 64 列の画素値 8 ビットをカラー画像 B のビットプレーン 0 の 65 行 1 列～128 行 256 列の画素に埋め込む。それを表したのが図 2.14 である。

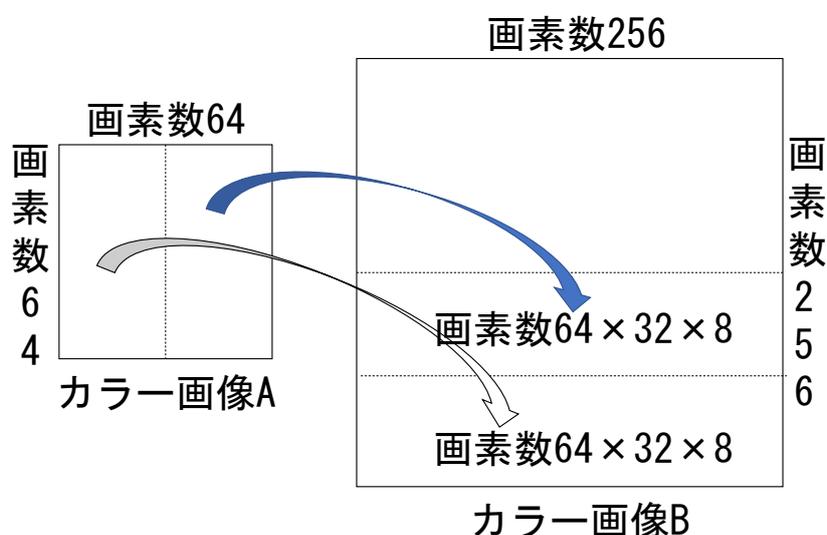


図 2.14 画像 A を画像 B に埋め込む場合

図 2.15 が埋め込む画像(画素数 64×64)である。図 2.16 はその画像を埋め込んだ画像(画素数 256×256)である。これがステガノグラフィを用いた情報ハイディング画像である。



図 2.15 埋め込む画像



図 2.16 図 2.15 を埋めた情報ハイディング画像

④ 埋め込んだ画像を再生するとき

再生は埋め込む手順の逆手順で行うことができる。図 2.16 の画像から再生した画像が図 2.17 である。

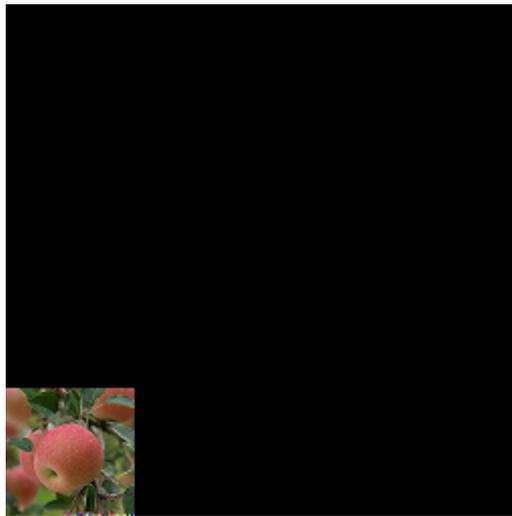


図 2.17 図 2.16 から再生した画像

(3) 長所

画像の中に秘匿文書や秘匿画像を埋め込んでいること自体を隠すことができる。したがって、秘匿文書や秘匿画像が伝達されていること隠すことができる。このことが、節 2.1～節 2.4 で述べたバーナム暗号、DES 暗号、RSA 暗号、楕円曲線暗号とは大きく異なる点である。

(4) 短所

- ① 改ざんに対する耐性が弱い。
- ② 伝達できる情報量が制限される。

2.7 電子透かし

電子透かしは伝達したい秘匿画像を別の画像の中に埋め込む技術で、情報ハイディングの1つである。別の画像の中に埋め込んでしまうので、秘匿画像が隠されているか否かは容易には区別できない。電子透かしは秘匿画像が隠されていることを知られないようにすることによって第三者による偽造や悪用することを防止しようとする技術[132, 133, …,257]である。

ここで、電子透かしとステガノグラフィの相違点を3つの観点から述べる。

第1は技術の目的が異なる点である。電子透かしは第三者が許可なくコピーしたり盗用したりすることを防止することを目的とする埋め込み技術であるのに対して、ステガノグラフィは個人情報を秘匿に伝達することを目的とする埋め込み技術である。

第2の観点は、表画像と裏画像に対する重要度の違いである。肉眼で見ることができる表画像とその内部に隠された裏画像の、どちらの画像がより重要な画像であるか。表画像は偽りのない本物で保護されるべき画像であり、偽造や複製から守られるべき画像である。それを保証するための技術が電子透かしである。それに対して、表画像は重要ではなく日常的な画像やその他どんな画像であってもよい、重要なのはその中に埋め込まれた秘匿情報である。そのための技術がステガノグラフィである。

第3の観点は、電子透かしとステガノグラフィの相違点として、取り扱う数値の種類が異なる。ステガノグラフィが取り扱う数値は、節2.1～節2.4で述べてきたバーナム暗号、DES暗号、RSA暗号、楕円曲線暗号と同様にすべて整数である。それに対して、電子透かしで取り扱う数値は実数である。このことは大きな相違である。たとえば、整数41が整数42に変化すると、電子透かし以外の情報ハイディングでは再生した秘匿文書や秘匿画像が大きく変化してしまう恐れがある。しかし、電子透かしの場合には実数を取り扱うので、実数41が実数42に変化しても大きな変化はなく、再生した画像が元の画像と類似した画像になる。

(1) 原理

制作方法と再生方法を順に述べる。最初に制作方法は次の2段階である。

① 画素数 $N \times N$ の秘匿画像 A を正規直交関数系 $\{\varphi_i(j)\}$ ($i, j = 1, 2, \dots, N$)で展開する。その展開係数 a_{mn} を次式で算出する。カラー画像の場合は赤色、緑色、青色の展開係数をそれぞれ算出する。

$$a_{mn} = \sum_{j=1}^N (\sum_{i=1}^N A_{ij} \varphi_m(i)) \varphi_n(j) \quad (2.24)$$

$(m, n = 1, 2, \dots, N)$

② 展開係数を量子化し、その量子化係数をカギ画像 K に次式のように埋め込む。以上で情報ハイディング画像 H を制作することができる。ただし、 k は任意の実数で $0 < k < 1$ 、 H_{ij} は量子化された整数で $0 \leq H_{ij} \leq 255$ とする。

$$H_{ij} = (1 - k) \cdot K_{ij} + k \cdot qa_{ij} \quad (2.25)$$

次に、再生方法は次の2段階である。原理的には制作方法の逆演算である。

③ 式(2.25)を逆算する。 a'_{ij} は②において展開係数 a_{ij} が量子化されたことにより、近似として表した実数である。

$$a'_{ij} = \frac{H_{ij} - (1 - k)K_{ij}}{k} \quad (2.26)$$

④ そして式(2.24)を逆算する.

$$A'_{ij} = \sum_{n=1}^N (\sum_{m=1}^N a'_{mn} \varphi_m(i)) \varphi_n(j) \quad (2.27)$$

以上で、秘匿画像 A に類似した画像 A' を再生することができる.

(2) 模擬実験例

2種類の実験を行う. 秘匿画像の画素数とカギ画像の画素数が異なる場合と, 等しい場合である.

最初に画素数が異なる場合の実験である.

① 画素数 $N \times N = 32 \times 32$ の秘匿画像(図 2.18)を正規直交関数系で展開する. 正規直交関数系 $\{\varphi_i(j)\}$ を

$\{\varphi_i(j)\} = \sqrt{\frac{2}{N}} \cdot C_i \cdot \cos \frac{i\pi}{2N} (2j+1)$ ($i, j = 1, 2, \dots, N$. $C_0 = \frac{1}{\sqrt{2}}$, $C_i = 1$ ($i \neq 0$))とし, 式(2.24)に基づいて赤色, 緑色, 青色の展開係数をそれぞれ算出する[β].

ここでは, 展開係数を算出する前処理として, 秘匿画像の画素値に次の乗算を行う. 赤色の場合で述べる. 範囲 $[0,1]$ の擬似乱数系列の k 番目の値 $rand_k$ が 0.5 より大きいならば「+1」を, 0.5 より小さいならば「-1」を, 秘匿画像の k 番目の画素値 R_k に乗算する. これを式(2.28)に示す.

$$R_k = \begin{cases} +R_k & (0.5 \leq rand_k \leq 1) \\ -R_k & (0 \leq rand_k < 0.5) \end{cases} \quad (2.28)$$

同様な乗算を緑色, 青色の画素値にも行う. 用いる擬似乱数系列は色ごとに異なる系列である.

② 次に展開係数を量子化する. 量子化した量子化画像を図 2.19 に示す. その量子化画像を画素数 128×128 の黒色画像の左上に上書きする. それが図 2.20 である.



図 2.18 秘匿画像



図 2.19 量子化画像

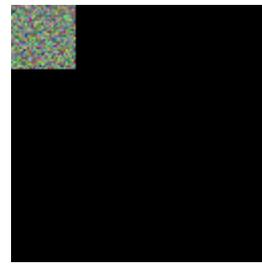


図 2.20 量子化画像を上書きした黒色画像

そして, 図 2.20 を画素数 128×128 のカギ画像に式(2.25)に基づいて埋め込む. カギ画像は図 2.21 である. 制作した画像が図 2.22 である. この画像が情報ハイディング画像である. ただし, 式(2.25)の実数 k を $k = 1/8$ と設定する.



図 2.21 カギ画像



図 2.22 情報ハイディング画像

③ 情報ハイディング画像から再生画像を再生する．再生のために，式(2.26)と式(2.27)を演算し，画素数を 32×32 に戻す．そして，式(2.28)に示した前処理に対応するため，演算数値の絶対値をとる．再生した画像が図 2.23 である．このように，表画像より小さな画像を偽造防止目的に秘かに埋め込む方法が電子透かし技術として音楽やデザインなど分野で利用されている．



図 2.23 再生画像

次に，秘匿画像とカギ画像の画素数が等しい場合の実験を述べる．

① 画素数 $N \times N = 128 \times 128$ の秘匿画像(図 2.24)を正規直交関数系で展開する．正規直交関数系 $\{\varphi_i(j)\}$ を $\{\varphi_i(j)\} = \sqrt{\frac{2}{N}} \cdot C_i \cdot \cos \frac{i\pi}{2N} (2j + 1) \quad (i, j = 1, 2, \dots, N. C_0 = \frac{1}{\sqrt{2}}, C_i = 1 (i \neq 0))$ とし，式(2.24)に基づき赤色，緑色，青色の展開係数をそれぞれ算出する．ただし前処理として，秘匿画像の画素値に擬似乱数系列を式(2.28)にしたがって乗算する．その結果の量子化画像を図 2.25 に示す．



図 2.24 秘匿画像



図 2.25 量子化画像

② 図 2.25 の量子化画像を図 2.26 のカギ画像に埋め込む．埋め込んだ画像が図 2.27 に示す情報ハイディング画像である．ただし，式(2.25)の実数 k は $k = 1/8$ と設定する．



図 2.26 カギ画像



図 2.27 情報ハイディング画像

③ 情報ハイディング画像から再生画像を再生する．再生のために，式(2.26)と式(2.27)を演算する．そして，式(2.28)に示した前処理に対応するため，演算数値の絶対値をとる．以上で図 2.28 に示す再生画像を得ることができる．



図 2.28 再生画像

(3) 長所

- ① 正規直交関数系にはいろいろな種類の関数系がある.
- ② ステガノグラフィによる画像の埋め込み可能な画素数はカギ画像の $1/8$ であるのに対して、電子透かしによる画像の埋め込み可能な画素数はカギ画像の画素数と同数まで可能である.
- ③ 著作権主張の画像や偽造防止の画像を埋め込むことができる.
- ④ 音響のような1次元データにも作曲者や作詞者のマークを不正防止目的に埋め込むことができる.

(4) 短所

実数の演算を取り扱うことから演算過程における誤差の発生は避けられない。したがって、それによる画質の劣化は抑えにくい。

以上、第2章では情報ハイディング分野を技術ごとに分類し、その概要を述べてきた。その結果、どのような技術にも長所と短所があることが明らかになる。

第3章 秘匿化のために

伝達したい画像の秘匿性を高めるためには、画像の暗号化と平坦化そして量子化が必要な条件である。暗号化は第三者に直接閲覧させないためである。平坦化は暗号化した画像の濃淡の起伏を目立たなくするためである。そして、量子化は実数データを整数データに変えるためである。この章では、これらの条件に最適な正規直交関数系を考察し提案する。

3.1 正規直交関数系とそのグラフ

画像の秘匿化のために画像を変換する方法として、次の5つの正規直交関数系を取り上げ考察する。その関数系は

- (1) 離散フーリエ変換 (Discrete Fourier Transform)
- (2) 離散コサイン変換 (Discrete Cosine Transform)
- (3) ハール関数系 (Haar function)
- (4) 選点正規直交多項式 (discrete orthogonal polynomial)
- (5) 擬似乱数系列に基づく正規直交関数系 (orthonormal system using pseudorandom series)

である。

これら5つの正規直交関数系のうち、離散フーリエ変換、離散コサイン変換、ハール関数系は超越関数グループに属し、選点正規直交多項式は代数関数グループに属する関数系である。残りの擬似乱数系列に基づく正規直交関数系はいずれにも属さない関数系である。

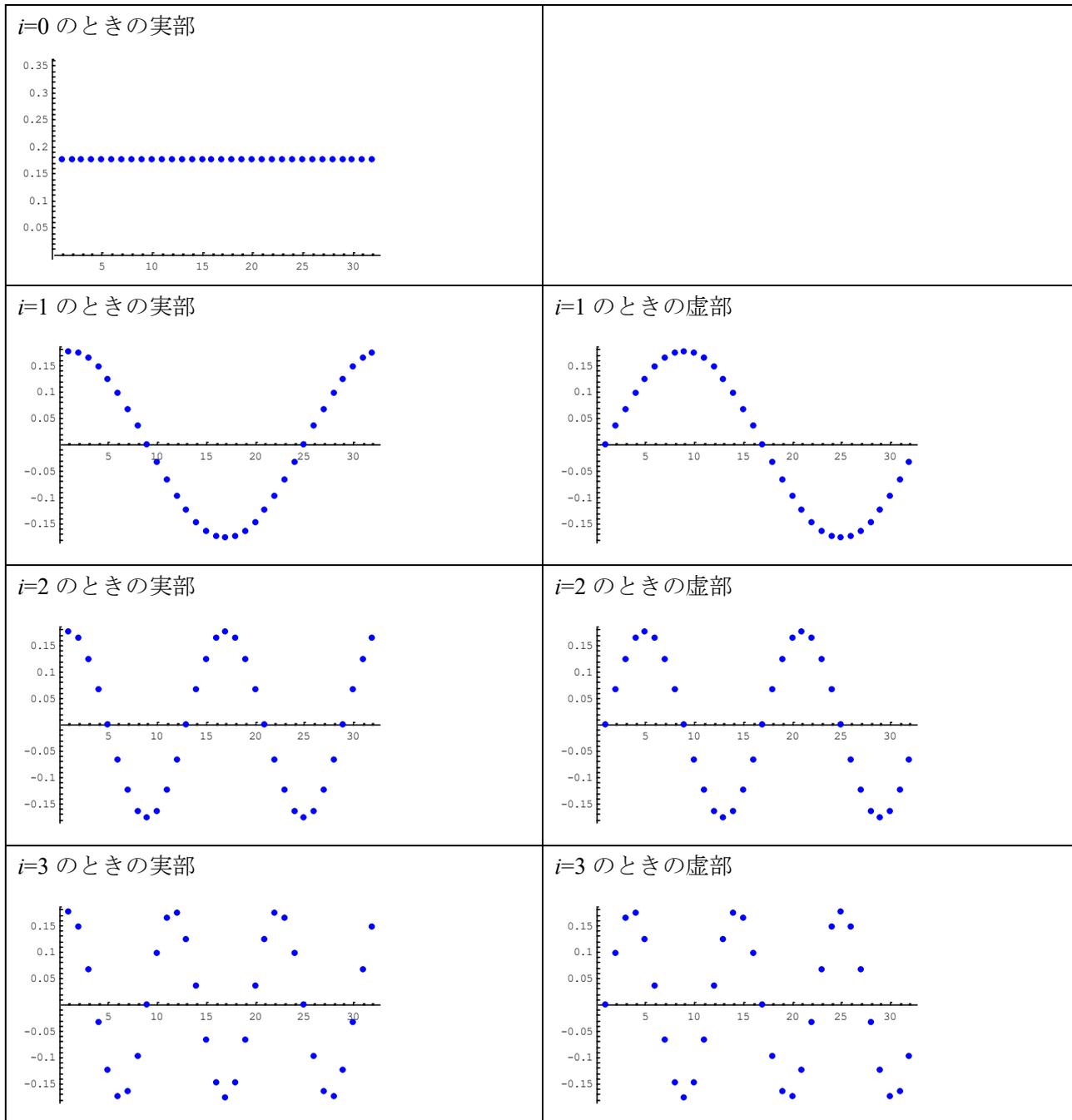
離散フーリエ変換、離散コサイン変換、そしてハール関数系は情報ハイディングに関する研究論文で数多く採用されている関数系である。しかし、選点正規直交多項式と擬似乱数系列に基づく正規直交関数系の採用は極端に少ない。

5つの正規直交関数系の数式とそのグラフ例を以下に示す.

(1) 離散フーリエ変換

$$\varphi_i(j) = \frac{1}{\sqrt{N}} e^{\sqrt{-1} 2\pi i j / N} \quad (i, j = 0, 1, 2, \dots, N-1) \quad (3.1)$$

表 3.1 離散フーリエ変換の正規直交関数 $\varphi_i(j)$ グラフ ($N=32$ の場合)



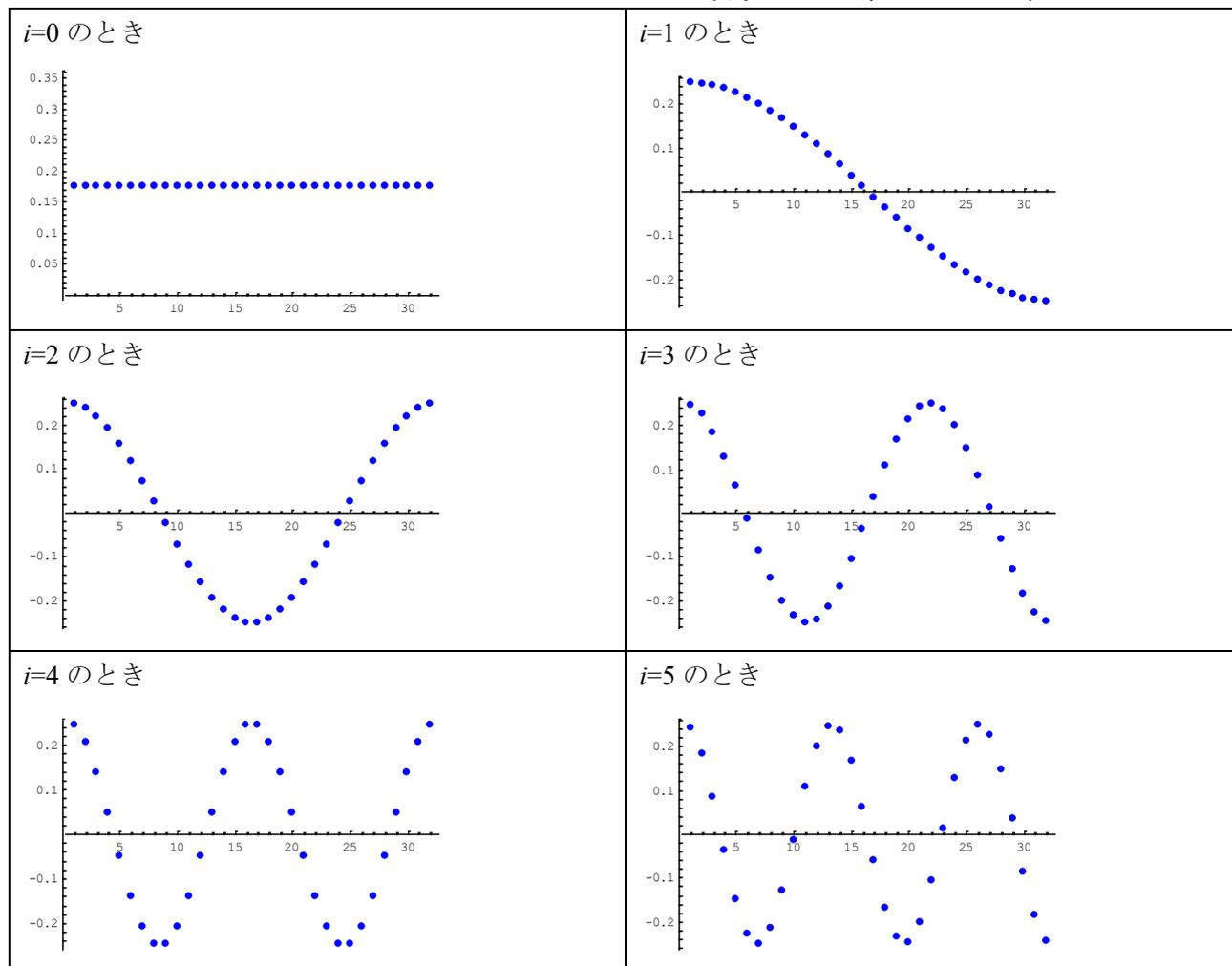
(横軸の開始位置は 1 である)

(2) 離散コサイン変換

$$\varphi_i(j) = \sqrt{\frac{2}{N}} \cdot C_i \cdot \cos \frac{i\pi(2j+1)}{2N} \quad \left(C_0 = \frac{1}{\sqrt{2}}, C_i = 1 (i \neq 0) \right) \quad (3.2)$$

$$(i, j = 0, 1, 2, \dots, N - 1)$$

表 3.2 離散コサイン変換の正規直交関数 $\varphi_i(j)$ グラフ ($N=32$ の場合)



(横軸の開始位置は 1 である)

(3) ハール関数系

区間 $0 \leq x < 1$ におけるハール関数 $x_n^{(k)}(x)$ を次のように定義する.

i) $x_0^{(0)}(x) = 1$

$$\text{ii) } x_n^{(k)}(x) = \begin{cases} \sqrt{2^n} & \left(\frac{k-1}{2^n} \leq x < \frac{k-1/2}{2^n} \right) \\ -\sqrt{2^n} & \left(\frac{k-1/2}{2^n} \leq x < \frac{k}{2^n} \right) \\ 0 & \text{(その他)} \end{cases} \quad (3.3)$$

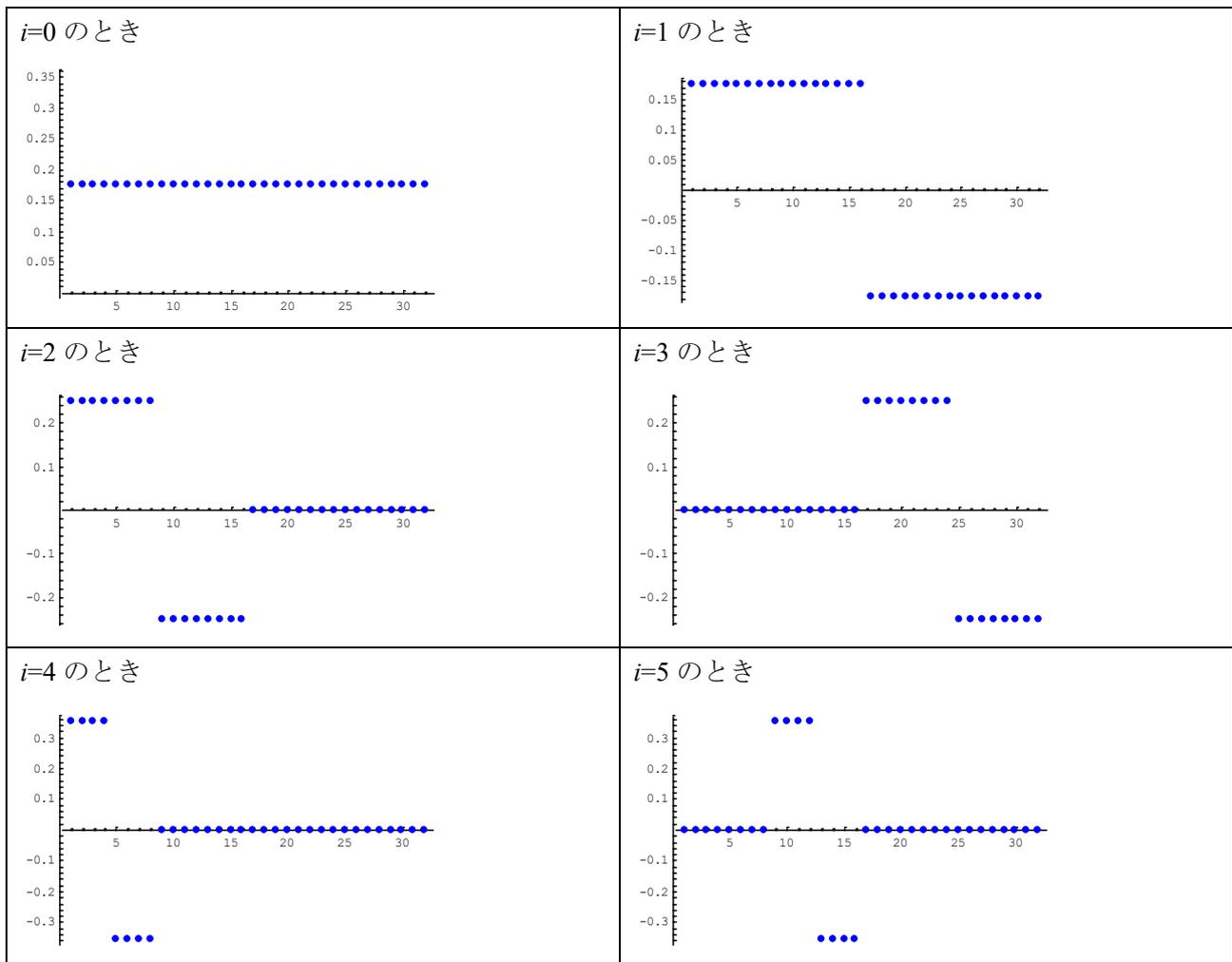
$$(n = 0, 1, 2, \dots, \log_2 N - 1. \quad k = 1, 2, \dots, 2^n)$$

区間 $0 \leq j < N$ のハール関数系の記述を簡潔化のため、次のように書き表すことにする.

$$\varphi_i(j) = x_n^{(k)}(j) \quad (i = 2^n + k - 1) \quad (3.4)$$

$$(i, j = 0, 1, 2, \dots, N - 1)$$

表 3.3 ハール関数系の正規直交関数 $\varphi_i(j)$ グラフ ($N=32$ の場合)



(横軸の開始位置は 1 である)

(4) 選点直交多項式

選点 $j = 0, 1, 2, \dots, N - 1$ に関する選点直交多項式 $\{P_i(j)\}$ は次の通りである.

$$P_i(j) = \sum_{k=0}^i (-1)^k \frac{1}{k!(i-k)!} \frac{(i+k)!}{k!} \frac{j!(N-1-k)!}{(N-1)!(j-k)!} \quad (3.5)$$

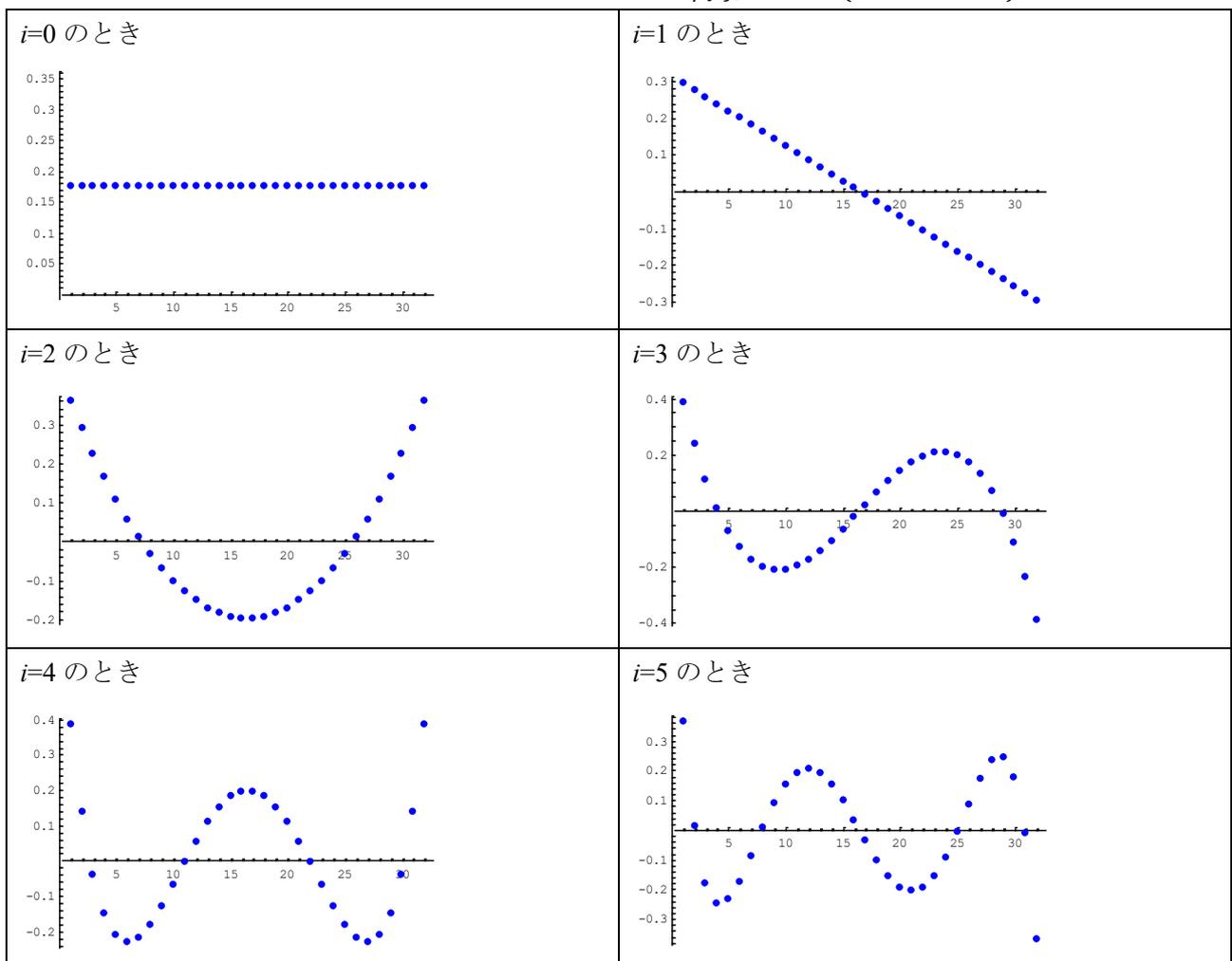
$$(i, j = 0, 1, 2, \dots, N - 1)$$

選点直交多項式の正規化を行う.

$$\varphi_i(j) = \frac{P_i(j)}{\sqrt{\sum_{j=0}^{N-1} P_i(j) \cdot P_i(j)}} \quad (3.6)$$

$$\text{ただし, } \left(\sum_{j=0}^{N-1} P_i(j) \cdot P_i(j) \right) = \frac{((N-1)+i+1)! \cdot ((N-1)-i)!}{((N-1)!)^2 \cdot (2i+1)}$$

表 3.4 選点直交多項式の正規直交関数 $\varphi_i(j)$ グラフ ($N=32$ の場合)



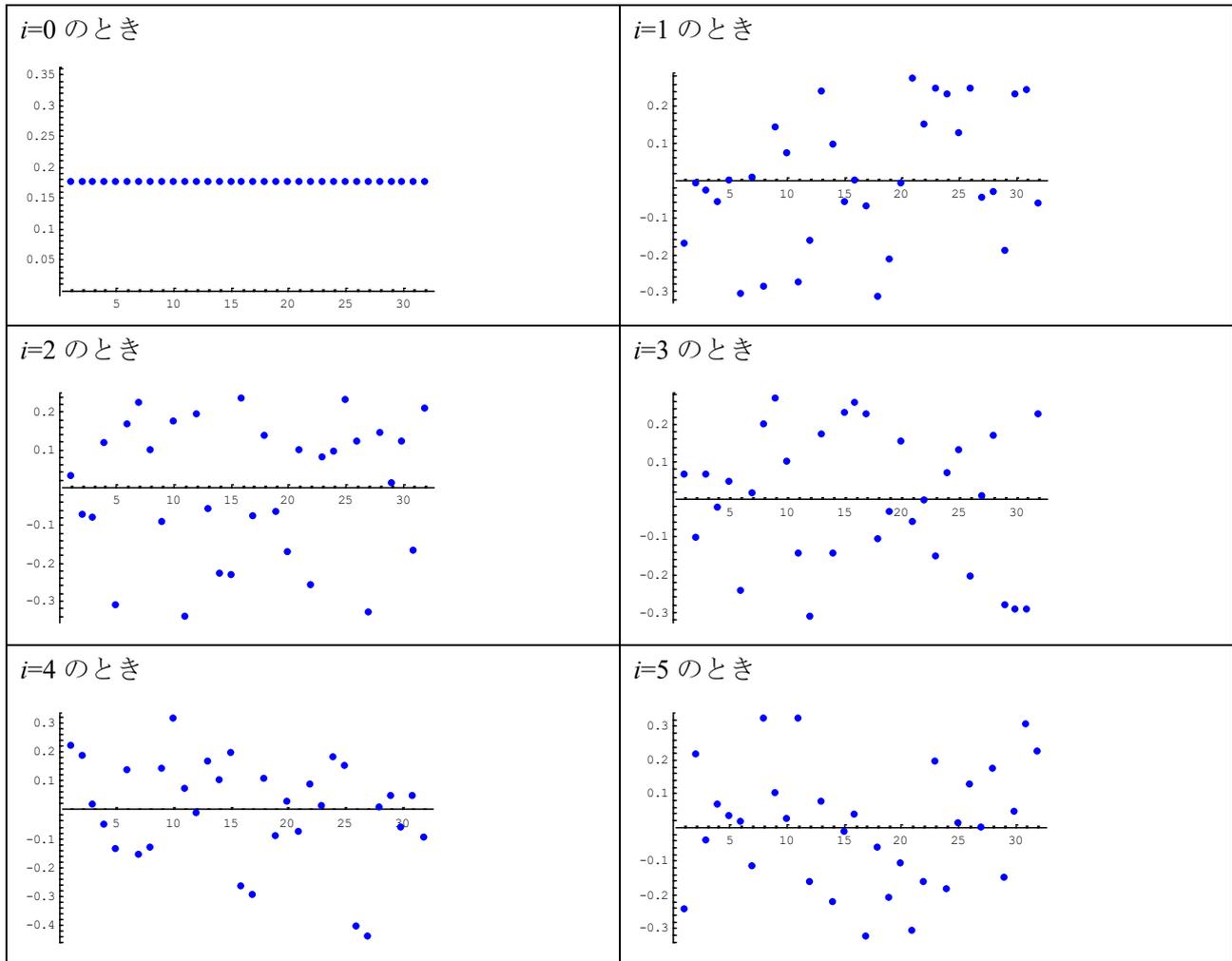
(横軸の開始位置は 1 である)

(5) 擬似乱数系列に基づく正規直交関数系

擬似乱数系列の数値から正規直交関数系 $\{\varphi_i(j)\}$ を構築する方法は次の通り.

- ① 擬似乱数系列を行列 N 行 N 列に順に並べる. 各行 $i=1, 2, \dots, N$ の擬似乱数値は列 $j=1, 2, \dots, N$ における関数値とみなすことができる.
- ② 第 1 行の関数値をすべて値 1 に置き換える.
- ③ 第 2 行以降の関数値をシュミット直交化法で直交化する.
- ④ 正規化する.

表 3.5 擬似乱数系列による正規直交関数 $\varphi_i(j)$ グラフ ($N=32$ の場合)



(横軸の開始位置は 1 である)

3.2 正規直交関数系による秘匿化

正規直交関数系を用いて画像を展開した展開係数分布図を次に調べる。調べ易くするために共通な画像を展開する。

① 共通な画像を画像Aとする。画像Aは画素数が $N \times N = 32 \times 32$ で、式(3.7)で与えられるものとする。その画像Aを図3.1に示す。

$$A_{i+1,j+1} = 127 \exp\left(-\frac{0.2}{N} \left(\left(i - \frac{N}{2}\right)^2 + \left(j - \frac{N}{2}\right)^2 \right)\right) \times \cos\left(\frac{8\pi}{N} \sqrt{\left(i - \frac{N}{2}\right)^2 + \left(j - \frac{N}{2}\right)^2}\right) + 128 \quad (3.7)$$

$(i, j = 0, 1, 2, \dots, N - 1)$

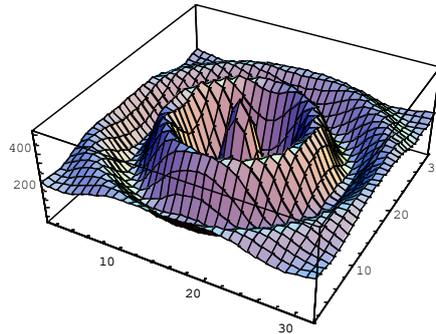


図 3.1 画像A

② 画像Aを展開したときの展開係数を a とする。展開係数 a は次式で示される。

$$a_{mn} = \sum_{j=1}^N \left(\sum_{i=1}^N A_{ij} \varphi_m(i) \right) \varphi_n(j) \quad (3.8)$$

その逆演算は次式に基づく。

$$A_{ij} = \sum_{n=1}^N \left(\sum_{m=1}^N a_{ij} \varphi_m(i) \right) \varphi_n(j) \quad (3.9)$$

③ 展開係数 a の展開係数分布図と逆演算結果を表3.6に示す。

表 3.6 正規直交関数系による展開係数分布図と逆演算結果

正規直交関数系	展開係数分布図	逆演算結果
離散フーリエ変換 (DFT)	<p>A 3D surface plot showing the expansion coefficients for the Discrete Fourier Transform (DFT). The x and y axes range from 0 to 30, and the z-axis (height) ranges from 0 to 4000. The surface is nearly flat and close to zero, indicating that the coefficients are very small.</p>	<p>A 3D surface plot showing the reconstructed image A. The x and y axes range from 0 to 30, and the z-axis (height) ranges from 0 to 200. The surface shows a central peak with a color gradient from blue to yellow, identical to Figure 3.1.</p>

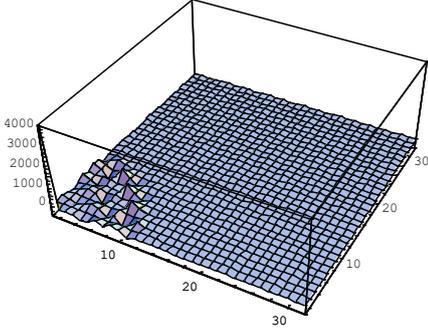
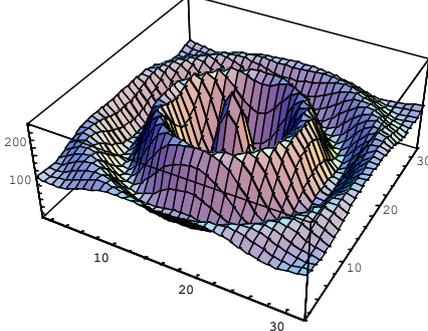
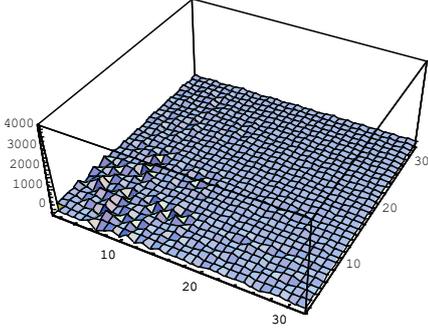
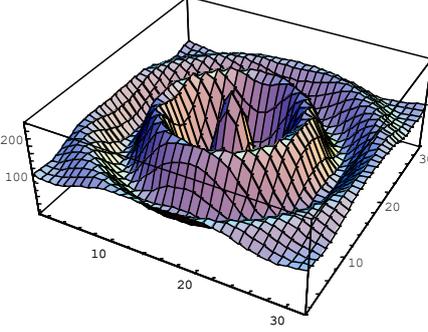
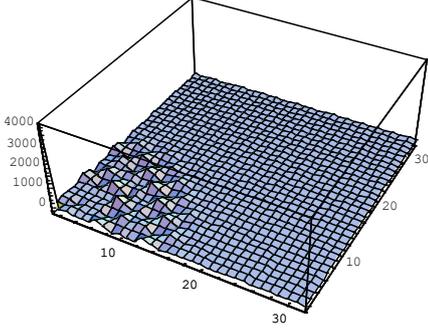
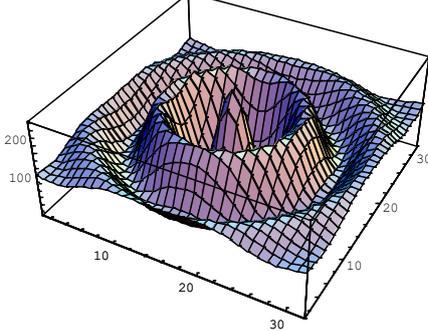
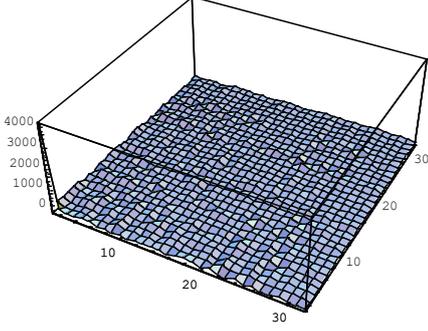
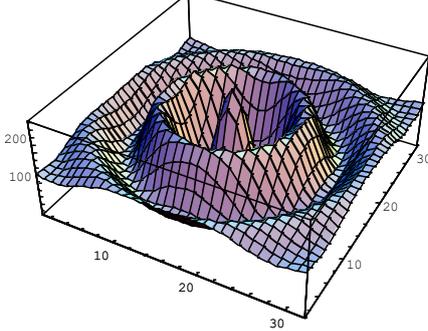
<p>離散コサイン変換 (DCT)</p>		
<p>Haar 関数系 (Haar function)</p>		
<p>選点正規直交多項式 (discrete orthogonal polynomial)</p>		
<p>擬似乱数系列に基づく正 規直交関数系 (orthonormal system using pseudorandom series)</p>		

表 3.6 が示すように、正規直交関数系を用いて画像を展開すると、その展開係数分布図は元の画像とはまったく異なる図になる。しかし、逆演算によって元の画像が再生できている。したがって、いずれの正規直交関数系による展開係数分布図は画像の秘匿化に活用することができる。

3.3 展開係数分布図の平坦性

画像を別の画像の中に埋め込むためには、埋め込む画像の起伏が平坦であれば平坦であるほど好都合である。なぜならば、埋め込む画像の起伏が小さければ、埋め込んだ後の画像にその起伏が目立たないからである。したがって、展開係数分布図の起伏が可能な限り平坦であることが必須になる。

そこで、展開係数分布図の平坦性を調べてみる。比較のため表 3.6 の展開係数 a が $a_{11} \neq 0$ の場合と、 $a_{11} = 0$ の場合を表 3.7 に併記する。なお、 a_{11} の位置は展開係数分布図の最左下 1 行 1 列の位置である。

表 3.7 展開係数分布図の比較

正規直交関数系	展開係数分布図 ($a_{11} \neq 0$ のとき)	展開係数分布図 ($a_{11} = 0$ のとき)
離散フーリエ変換 (DFT)		
離散コサイン変換 (DCT)		
Haar 関数系 (Haar function)		

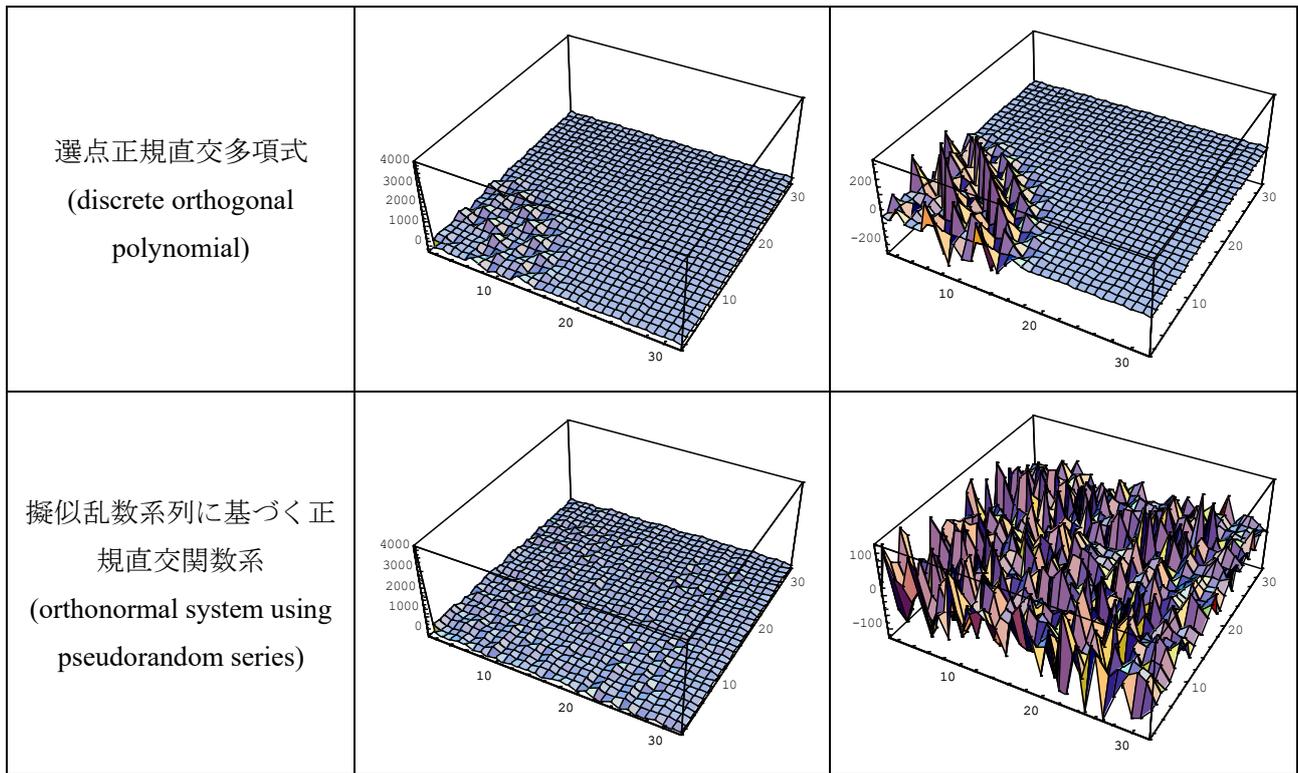


表 3.7 は展開係数分布図の起伏状態を示している。展開係数が最大値となる位置は展開係数分布図の最左下の a_{11} である。さらに、その周辺にも起伏が広がっていることがわかる。

展開係数分布図の起伏が大きい部分は画像の情報が多く集中している部分である。起伏の小さい部分は画像の情報が少ない部分である。この起伏が大きい部分と小さい部分が際立って分離しているならば、画像の情報を抽出しやすくなり、それは画像の圧縮技術に大いに役立つ。

しかし、画像を別の画像に埋め込める観点からは、展開係数分布図が平坦なほど望ましいことから、5つの正規直交関数系の中では擬似乱数系列に基づく正規直交関数系による展開係数分布図が最も望ましい分布図であるといえる。

3.4 強制的な平坦化

表 3.7 に示したように、 $a_{11} = 0$ のとき擬似乱数系列に基づく正規直交関数系以外の展開係数分布図は平坦的ではない。そこで、展開係数分布図を強制的に平坦化する方法を述べる。その方法として正規直交関数系で展開する前に任意の擬似乱数系列を乗算する方法がある。その手順を以下に述べる。

- ① 秘匿画像は式(3.7)で与えられる画像 A とする。画像 A を表 3.8 (a) に再掲する。
- ② 画像 A の展開係数を算出する前処理として、画像 A の画素値に次の乗算を行う。赤色の場合で示す。範囲 $[0, 1]$ の擬似乱数系列の k 番目の値 $rand_k$ が 0.5 より大きいならば「+1」を、 0.5 より小さいならば「-1」を、画像 A の k 番目の赤色画素値 R_k に乗算する。これを次式に示す。

$$R_k = \begin{cases} +R_k & (0.5 \leq rand_k \leq 1) \\ -R_k & (0 \leq rand_k < 0.5) \end{cases} \quad (3.10)$$

同様な乗算を緑色、青色の画素値にも行う。用いる擬似乱数系列は色ごとに異なる系列とする。なお、節 3.1 (5) の擬似乱数系列とは異なる系列である。

画像 A に擬似乱数系列を乗じた結果の画像を画像 B とし、それを表 3.8 (b) に示す。

- ③ 画像 B の展開係数を b とする。展開係数 b は次式に基づく。

$$b_{mn} = \sum_{j=1}^N (\sum_{i=1}^N B_{ij} \varphi_m(i)) \varphi_n(j) \quad (3.11)$$

- ④ 展開係数 b の逆演算は次式のように絶対値をとる。

$$B_{ij} = | \sum_{n=1}^N (\sum_{m=1}^N b_{mn} \varphi_m(i)) \varphi_n(j) | \quad (3.12)$$

展開係数 b の展開係数分布図と逆演算 B_{ij} の結果を表 3.9 に併記する。

表 3.8 用意した画像と擬似乱数系列を乗じた画像

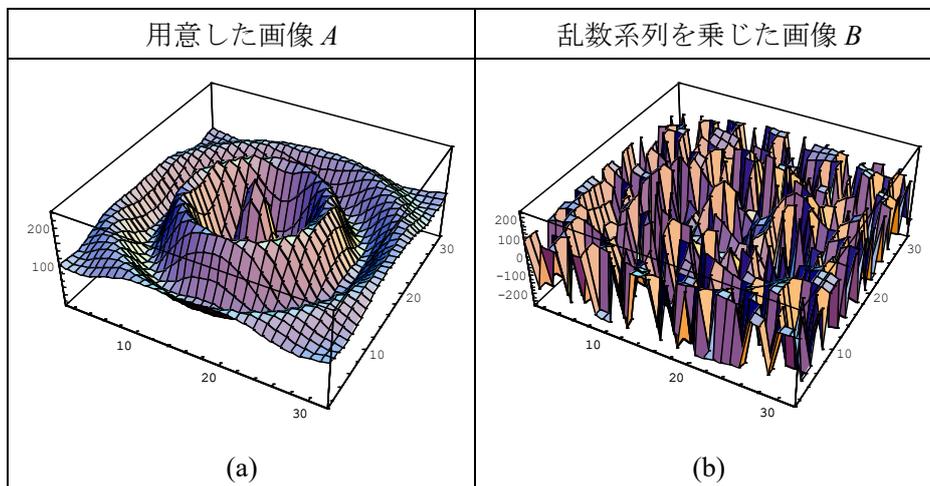
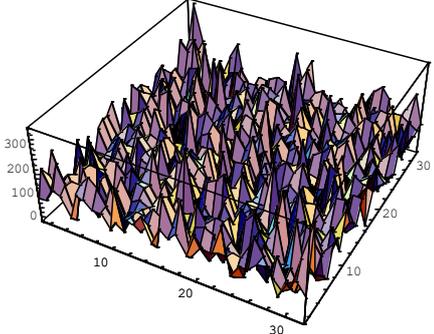
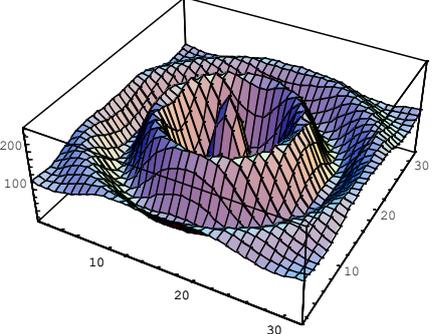
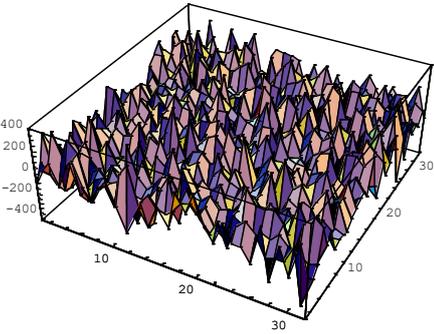
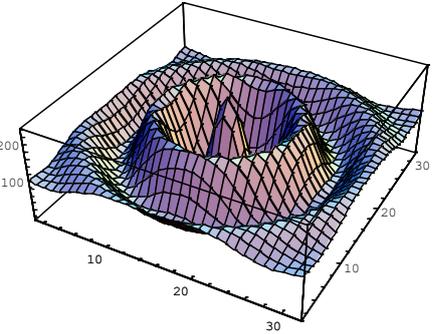
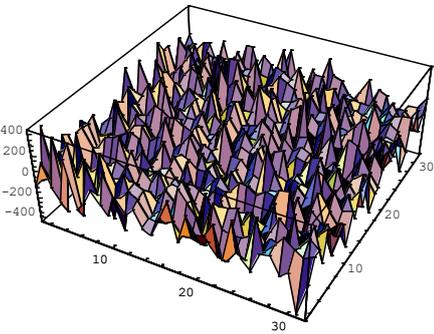
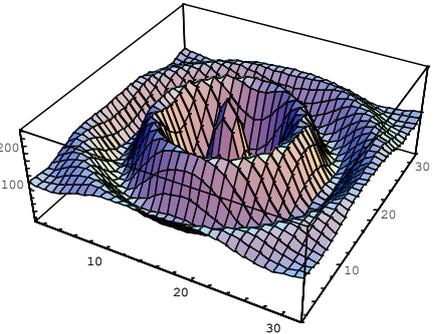
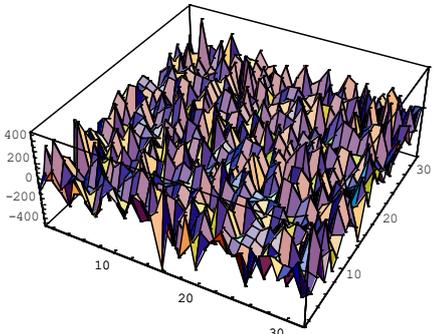
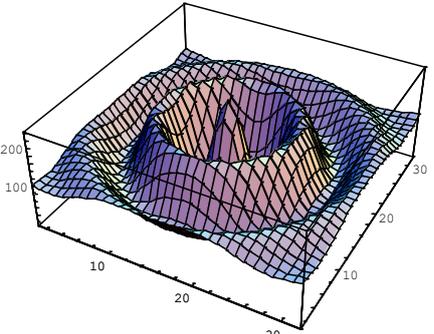
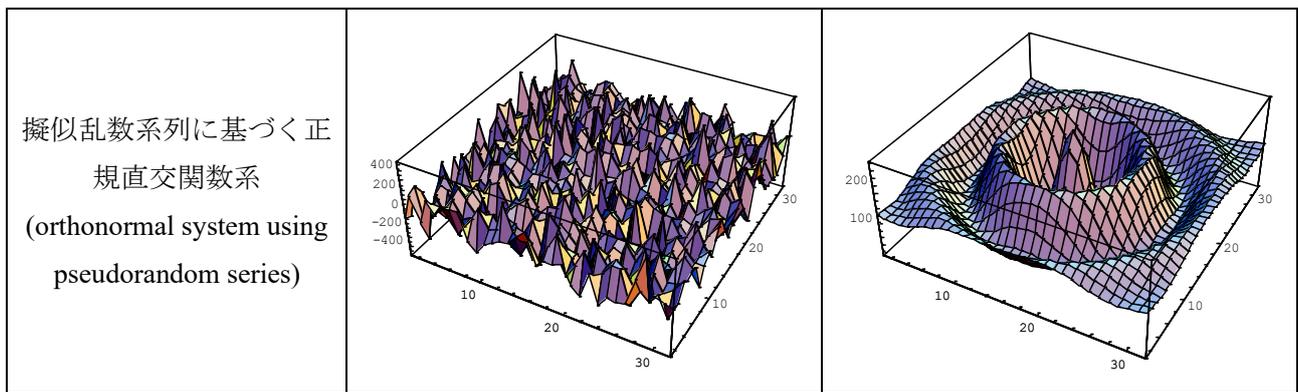


表 3.9 展開係数分布図と逆演算 B_{ij} の結果

正規直交関数系	展開係数 b の展開係数分布図	逆演算 B_{ij} の結果
離散フーリエ変換 (DFT)		
離散コサイン変換 (DCT)		
Haar 関数系 (Haar function)		
選点直交多項式 (discrete orthogonal polynomial)		



画像に擬似乱数系列を乗算することで、その展開係数分布図を強制的に平坦化できることが明らかになる。また、その逆演算の絶対値を取ることで、元の画像を再現できることが明らかになる。

この方法を活用した多重情報ハイディングに関する論文「直交関数系でつくる電子透かし」を参考論文[A]に添付する。

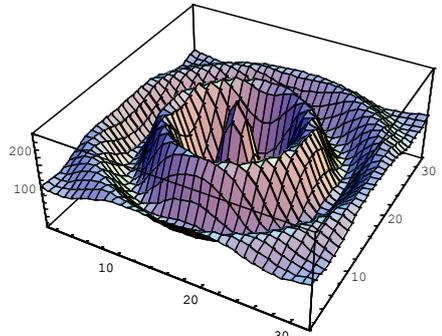
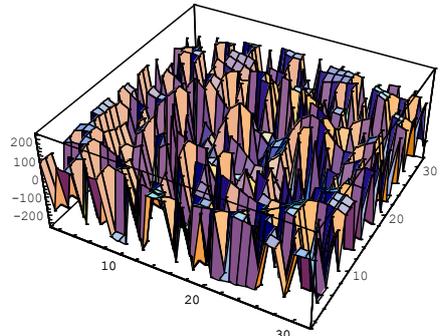
3.5 展開係数の量子化

(1) 展開係数の度数分布

画像の展開係数の量子化について考察する。BMP形式画像の画素値は0~255(8ビット)という正の整数値に限定されている。したがって、正規直交関数系で算出した展開係数分布図を画像に埋め込むためには、展開係数を最小値0, 最大値255の整数に量子化する必要がある。その量子化する方法について考察する。

最初に、画像Aそのものの展開係数分布図の度数分布と、画像Aに擬似乱数系列を乗じた節3.4の画像B展開係数分布図の度数分布を調べる。その比較の結果が表3.10である。ただし、グラフの中の赤線は最大度数の位置を指す。

表 3.10 展開係数の度数分布比較

正規直交関数系	画像Aの展開係数分布図の度数分布	画像Aに擬似乱数系列を乗じた展開係数分布図の度数分布
	 <p style="text-align: center;">画像A</p>	 <p style="text-align: center;">画像A × 擬似乱数系列(節 3.4 画像B)</p>

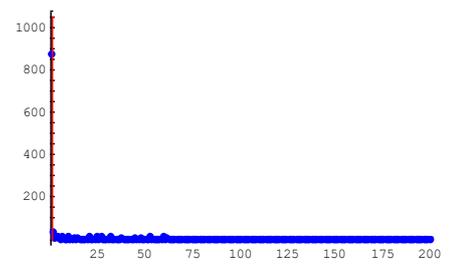
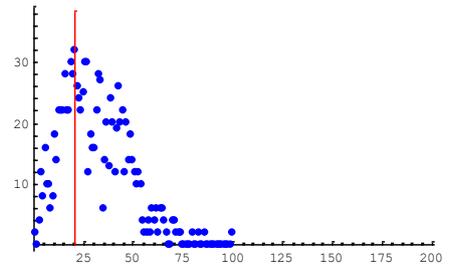
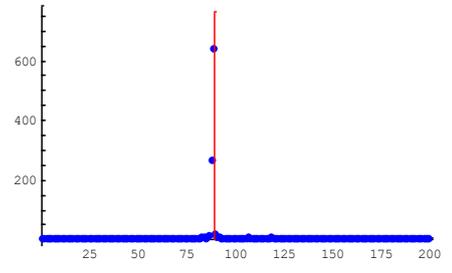
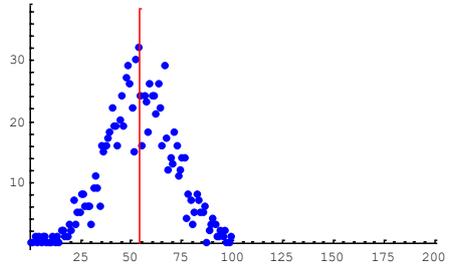
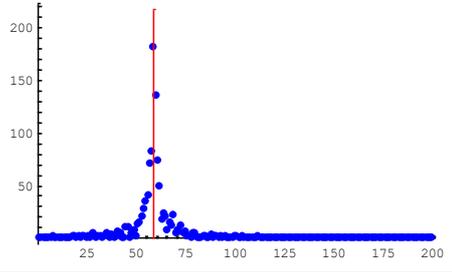
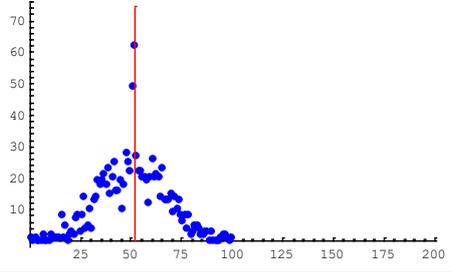
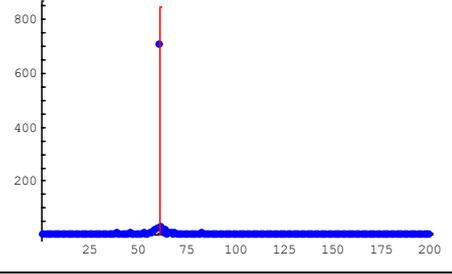
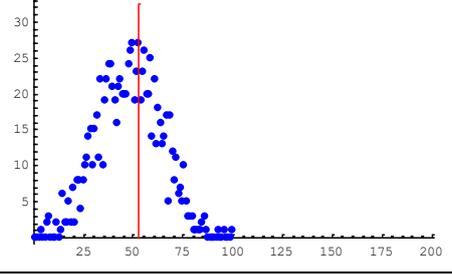
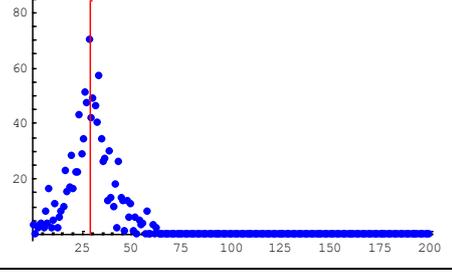
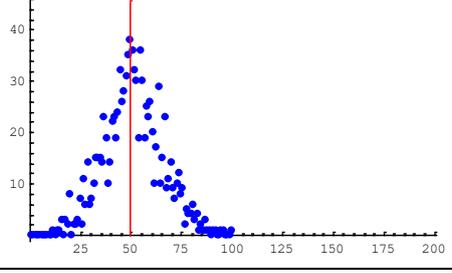
<p>離散フーリエ変換 (DFT)</p>		
<p>離散コサイン変換 (DCT)</p>		
<p>Haar 関数系 (Haar function)</p>		
<p>選点直交多項式 (discrete orthogonal polynomial)</p>		
<p>擬似乱数系列に基づく正 規直交関数系 (orthonormal system using pseudorandom series)</p>		

表 3.10 から明らかになることは

- ① すべての正規直交関数系で展開係数分布図の度数分布には偏りがあること
- ② 擬似乱数系列に基づく正規直交関数系の展開係数分布の度数分布は、擬似乱数系列を乗算しても乗算しなくても類似した形状であること

である。

(2) 量子化の方法

量子化には一般に2つの方法がある。1つは展開係数を一定の刻み幅で量子化する方法である。もう1つは展開係数を対数関数で圧縮し、その後一定の刻み幅で量子化する方法である。度数分布に偏りがある場合には後者の方法が望ましいという理由をここでは簡潔に述べる。

展開係数 a に対する量子化係数を qa とおく。量子化によって発生する量子化誤差を e とすると、次式が成り立つ。

$$qa_{ij} = \ln|a_{ij}| + e_{ij} \quad (3.13)$$

これを指数関数で伸長する。

$$\exp(qa_{ij}) = \exp(\ln|a_{ij}| + e_{ij}) = |a_{ij}| \cdot \exp(e_{ij}) \quad (3.14)$$

ここで、 e_{ij} が小さければ次式を得る。

$$|a_{ij}| \cdot (1 + e_{ij}) = |a_{ij}| + |a_{ij}| \cdot e_{ij} \quad (3.15)$$

展開係数 a と量子化誤差 e が独立で、しかも e が白色ノイズであるとする、展開係数の分散と量子化誤差の分散の比 R は

$$R = \frac{1}{\frac{1}{N^2} \sum_{i=1}^N (\sum_{j=1}^N e_{ij}^2)} \quad (3.16)$$

になる。よって、比 R は量子化の刻み幅だけに関係し、展開係数の分散とは無関係になる。論文では、このことを踏まえて、量子化方法には対数関数で圧縮する量子化方法を採用することとする。

(3) 量子化特性の設定

量子化について、さらに次のような設定を行う。なお、横軸を展開係数、縦軸を量子化係数とするグラフを以降では量子化特性と呼ぶことにする。

量子化特性の縦軸をビット数 D の画素値空間 $\{0, 1, 2, \dots, 2^D\}$ に制限する。量子化係数の画素値をこの範囲に制限した理由は、量子化係数を画素とする量子化画像を土台となるカギ画像に直接にそのままの値で埋め込むことができるようにするためである。

量子化特性の横軸を3つの区間に分割して量子化する。ただし、値 U, V は次式のように定める。

$$U = \sum_{j=1}^N (\sum_{i=1}^N 255\varphi_1(j))\varphi_{1(j)} \quad (3.17)$$

$$V = 1/\sqrt{N} \quad (3.18)$$

それぞれの区間における展開係数 a と量子化係数 qa の関係式は次のとおり。

(i) $-U < a_{mn} \leq -V$ のとき

$$qa_{mn} = \frac{2^{D-1}-1}{\log_{10} U - \log_{10} V} (\log_{10}(-a_{mn}) - \log_{10} V) + 1 \quad (3.19)$$

(ii) $-V < a_{mn} < V$ のとき

$$qa_{mn} = 0 \quad (3.20)$$

(iii) $V \leq a_{mn} \leq U$ のとき

$$qa_{mn} = \frac{2^{D-1}-1}{\log_{10} U - \log_{10} V} (\log_{10}(+a_{mn}) - \log_{10} V) + 2^{D-1} \quad (3.21)$$

これをグラフに表したのが図3.2の量子化特性である。図3.2は画素値を16個で例示してある。

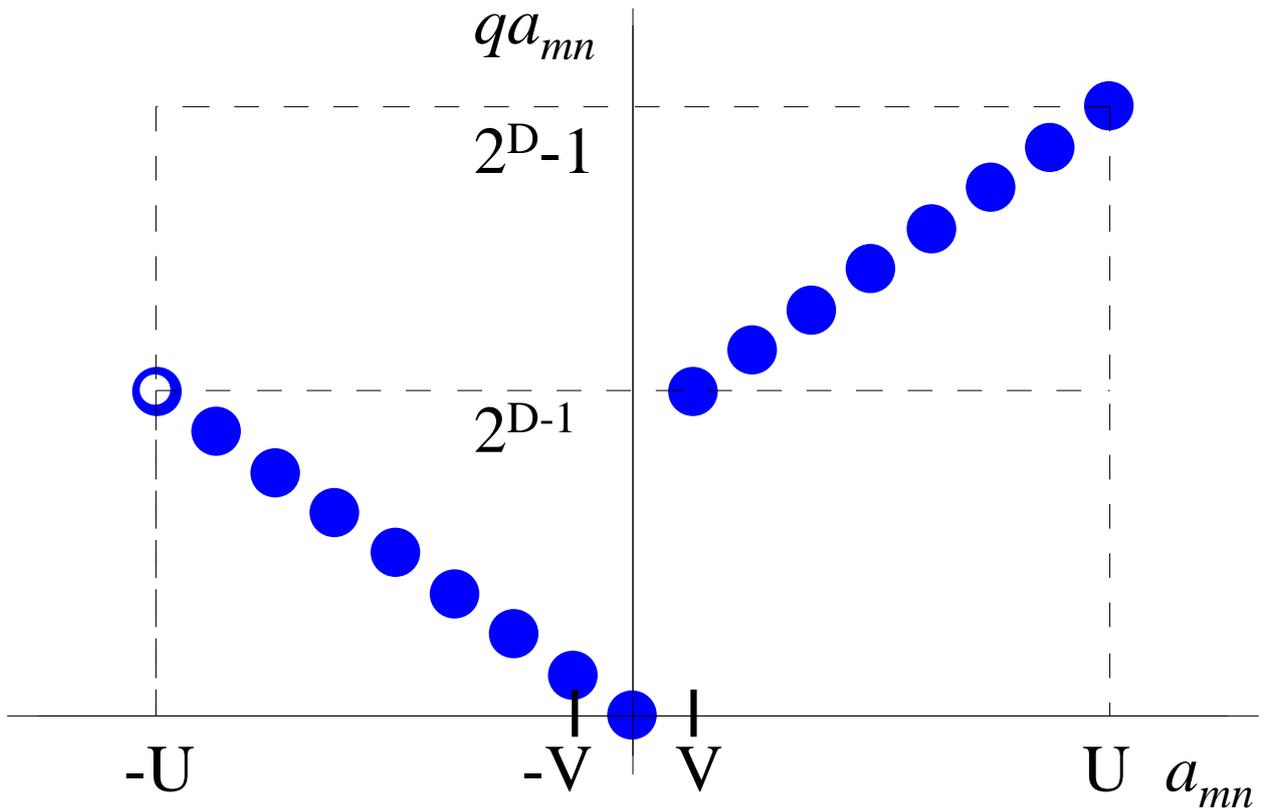


図 3.2 量子化特性

この章の結論は次の 3 点である。

- ①秘匿化のために採用する正規直交関数系を擬似乱数系列のよる正規直交関数系とすること
- ②強制的な平坦化は行わずに擬似乱数系列がもつ平坦性を活用すること
- ③量子化は対数関数を用いた量子化方法とすること

以上を踏まえて、秘匿化のために採用する正規直交関数系は擬似乱数系列に基づく正規直交関数系とすることを新規考案として提案する。

第4章 多重化のために

受信者に多くの情報を一度の伝達するためには、1枚の画像の中に複数枚の画像を埋め込むことが必要である[γ]。この章では、複数枚の画像を埋め込むための多重化方法を考察し最適な方法を提案する。

4.1 偶関数と奇関数を活用する二重化

画像の左半分、右半分、上半分、下半分のいずれかが黒色である画像は偶関数あるいは奇関数だけで構成された画像であるとみなすことができる。このことを活用すると、1枚の画像の中に2枚の画像を埋め込むことができ、再生することができる。その理由を述べる。

図4.1は区間の長さが N の1次元関数である。右半分の値はゼロである。ゼロの部分の見方には2つの見方がある。1つは左半分のグラフがそのまま繰り返されているとみる見方で図4.2(a)である。もう1つの見方は左半分のグラフの符号が反対のグラフが繰り返されているとみる見方で図4.2(b)である。(a)と(b)を加えると右半分はゼロになる。だから、2通りのグラフが同時にあると見ることができる。

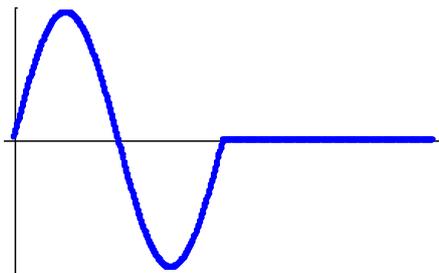
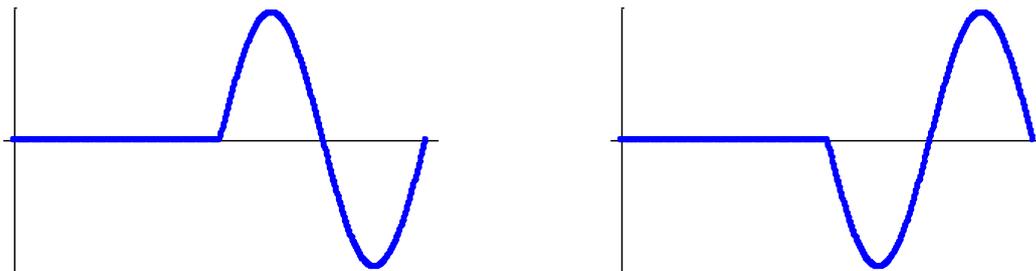


図4.1 区間の長さが N の関数



(a) 図4.1の左半分と同じグラフの繰り返し (b) 図4.1の左半分と符号が反対のグラフの繰り返し

図4.2 図4.1のゼロ部分の2つの見方

次に、図4.1と図4.2(a)を合成すると、そのグラフは中央の位置を中心とする奇関数になる。それが図4.3(a)である。または、図4.1と図4.2(b)を合成すると、そのグラフは中央の位置を中心とする偶関数になる。それが図4.3(b)である。図4.3の(a) $\times 1/2$ と(b) $\times 1/2$ を足し合わせると、図4.1と等しくなる。

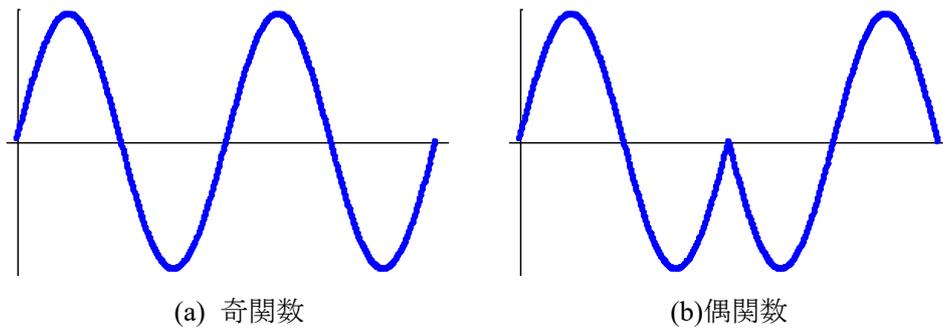


図 4.3 奇関数と偶関数

この見方は2次元画像に拡張しても同様なことがいえる。画像の左半分、右半分、上半分、下半分のいずれかが黒色である画像は偶関数あるいは奇関数で構成された画像であるとみることができる。したがって、画像の半分がゼロの画像を2枚用意して、一方の画像は偶関数だけで構成された画像、他方は奇関数だけで構成された画像であるとみることが可能である。

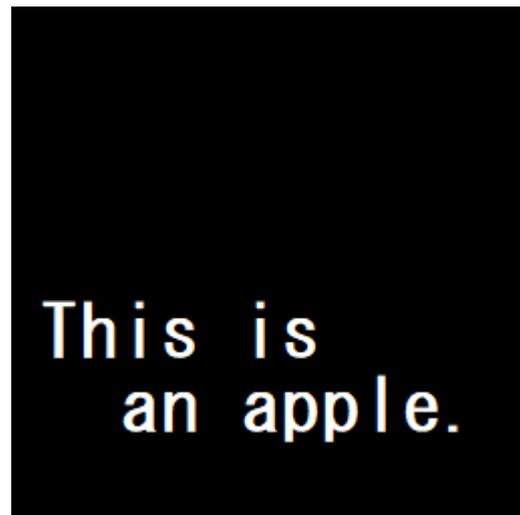
そして、偶関数と奇関数で構成された二重の画像から、それぞれを分離できる方法があれば、1枚の画像の中に2枚の画像を埋め込むことが可能となる。

離散フーリエ変換 (DFT) を活用すると、偶関数と奇関数をそれぞれ分離することができる。なぜならば、DFT の実部が偶関数を抽出することができ、虚部が奇関数を抽出することができるからである。

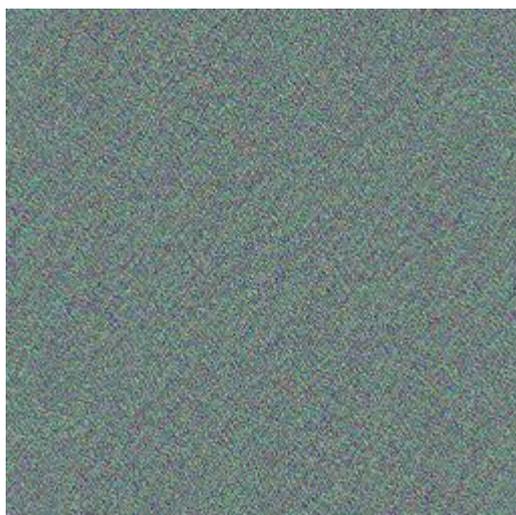
例を示す。図 4.4 (a)を偶関数の画像とする。(b)を奇関数の画像とする。この2枚の画像を二重化のために正規直交関数系でそれぞれを展開し量子化し1枚に合成した量子化画像が(c)である。そして、画像(c)から個々に再生される再生画像が(d)と(e)である。画像の最左下の位置を中心に点对称な画像が再生されている。ただし、量子化画像を強制的に平坦化(節 3.4 参照)するために、画像(a), (b)に擬似乱数系列を事前に乗算してある。再生する場合には絶対値を取る必要がある。



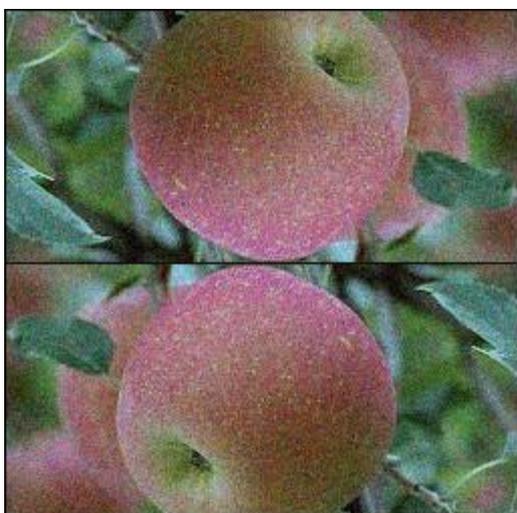
(a) 偶関数の画像



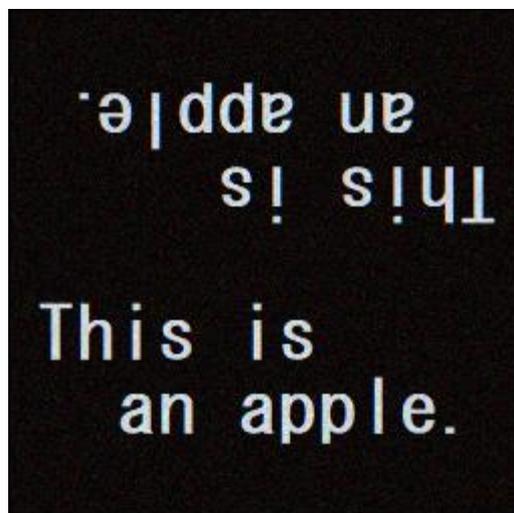
(b) 奇関数の画像



(c) (a)と(b)の量子化係数を二重化した量子化画像



(d) 再生画像



(e) 再生画像

図 4.4 偶関数と奇関数を活用する二重化

再生画像が点対称となる理由を述べる．偶関数の画像(a)を A ，奇関数の画像(b)を B とする．この2枚の画像をフーリエ変換して二重化した量子化画像(c)は次式で表される．

$$Re\left[\sum_{j=0}^{N-1} \sum_{i=0}^{N-1} A_{ij} \cdot e^{-\sqrt{-1} \cdot 2\pi \cdot (mi+nj)/N}\right] + Im\left[\sum_{j=0}^{N-1} \sum_{i=0}^{N-1} B_{ij} \cdot e^{-\sqrt{-1} \cdot 2\pi \cdot (mi+nj)/N}\right] \quad (4.1)$$

再生するためには，量子化画像を逆フーリエ変換して，偶関数と奇関数を抽出するとよい．偶関数の再生画像は次式になる．

$$\left| \frac{1}{2} A'_{i,j} + \frac{1}{2} A'_{N-i,N-j} \right| \quad (4.2)$$

奇関数の再生画像は次式になる．

$$\left| \frac{1}{2} B'_{i,j} - \frac{1}{2} B'_{N-i,N-j} \right| \quad (4.3)$$

絶対値を施す理由は量子化画像を強制的に平坦化してあるからである．

式(4.2)，(4.3)は，再生画像 $A'_{i,j}$ および $B'_{i,j}$ は元の画像 A ， B と類似した画像で，しかも画像の最左下の

位置を中心とする点対称になることを表している。なお、ここでは再生画像の縁を値ゼロとする。

この二重化を活用した文献として「偶関数と奇関数を活用した電子透かし画像の制作」(佐々木隆幸, Hi-Tec 青森, 産業技術高度化振興会, Vol.18, pp.49-53, 2014)がある。

4.2 画素平面の2分割

画素平面を2分割する方法には、縦に2分割、横に2分割などさまざまな方法がある。ここでは、左上角から右下角を結ぶ対角線で画素平面を2分割する場合を示す。その理由は、節3.3で示したように、強制的な平坦化を行わない場合、展開係数分布図の左上角と右下角を結ぶ対角線より左下側に画像データの多くが集中しているからである。

画素数 $N \times N$ の量子化画像の中から画素を以下のように抜き取る。

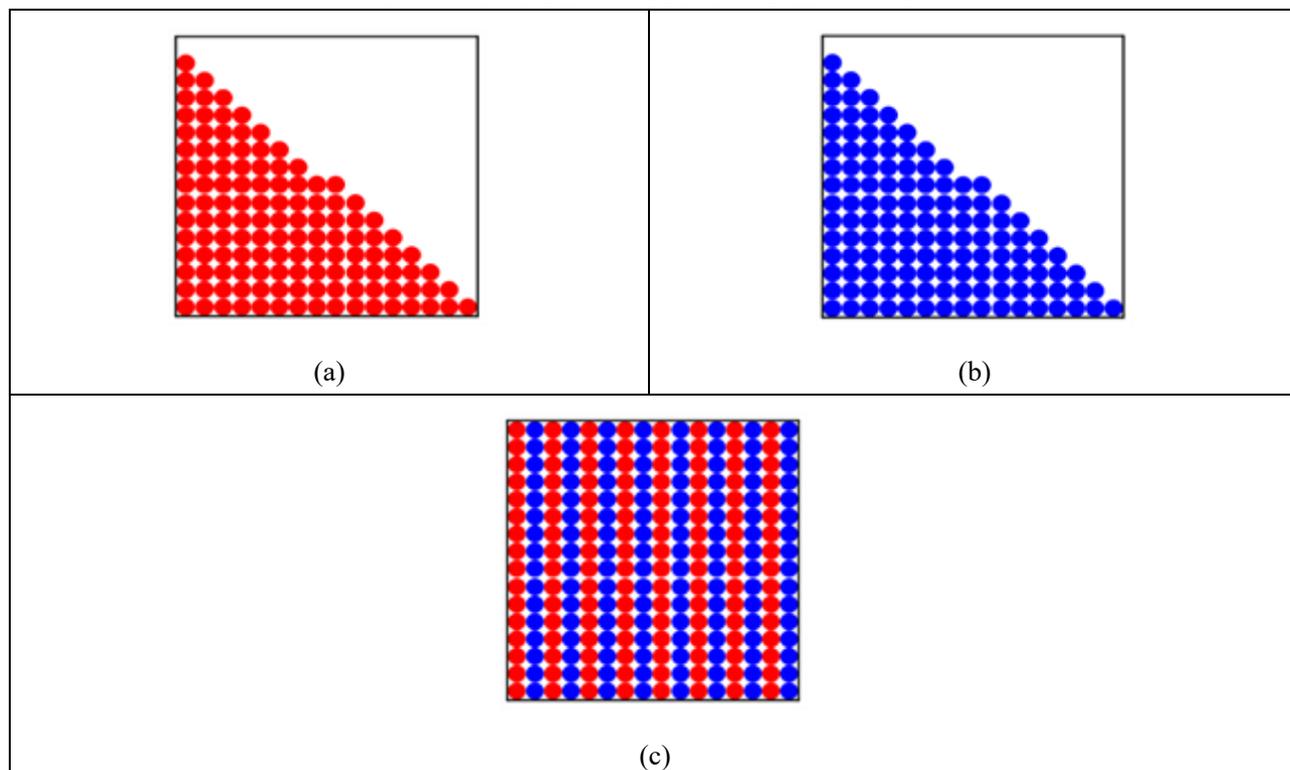
- ① 行番号 i を範囲 $1 \leq i \leq \frac{N}{2}$ で順に増加させながら、列番号 j が $1 \leq j \leq N - i + 1$ となる画素を順に抽出する。
- ② さらに i を範囲 $\frac{N}{2} + 1 \leq i \leq N - 1$ で順に増加させながら、 j が $1 \leq j \leq N + 1 - i$ となる画素を順に抽出する。
- ③ 抽出した画素に二重化のために新たに奇数の番号をつける。

以上で1枚目の量子化画像から画素値を抽出できる。

- ④ 同様に2枚目の量子化画像から画素値を抽出し、新たに偶数の番号をつける。表4.1(a), (b)が画素数 $N \times N = 16 \times 16$ の量子化画像2枚の中から抽出したそれぞれの画素値の例である。

- ⑤ 二重化のために、それぞれの画素値を1枚の量子化画像に合成する。表4.1(c)が画素値を交互に並べた二重の量子化画像である。

表 4.1 画素平面を2分割する場合の二重化



画像を再生する場合には、二重の量子化画像から奇数列と偶数列に分けて抽出し、それぞれの量子化画像に戻す。その様子が図 4.5 である。

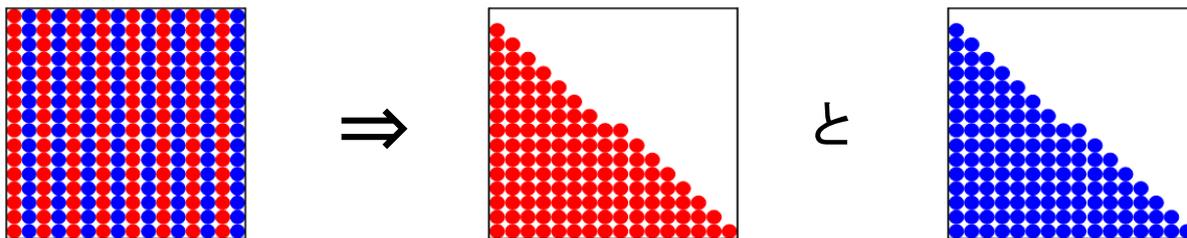


図 4.5 再生する場合は画素値を元の状態に戻す

この方法に基づいた二重情報ハイディングに関する論文「Constructing Digital Watermark Based on Orthogonal Functions」が参考論文[B]である。

4.3 画素空間の 2 分割

この二重化は画素値空間をタテ軸方向に 2 分割する方法である。その手順は以下のとおり。

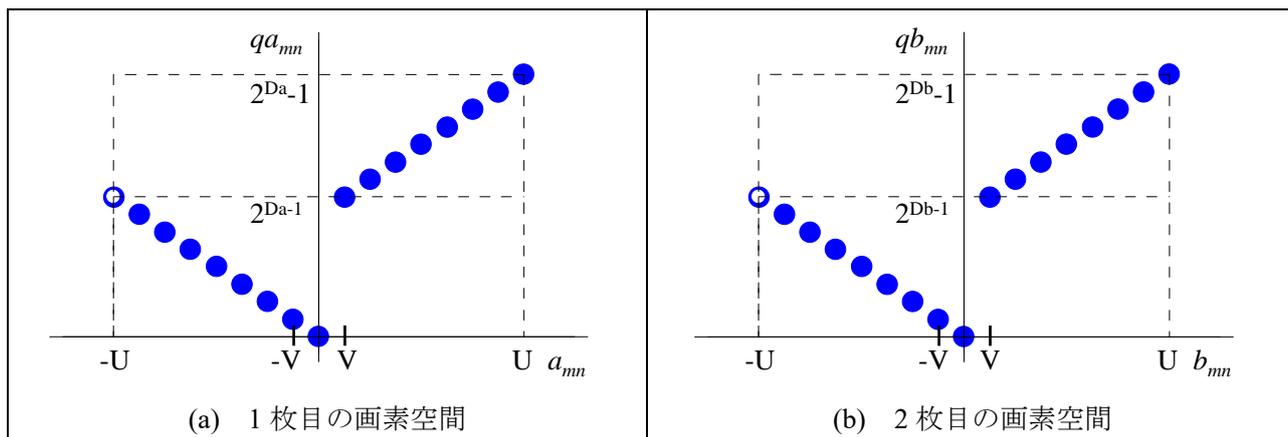
- ① 1 枚目の展開係数分布図をビット数 D_a の画素空間 $\{0, 1, 2, \dots, 2^{D_a}\}$ に量子化する。
- ② 2 枚目の展開係数分布図をビット数 D_b の画素空間 $\{0, 1, 2, \dots, 2^{D_b}\}$ に量子化する。
- ③ 二重化は

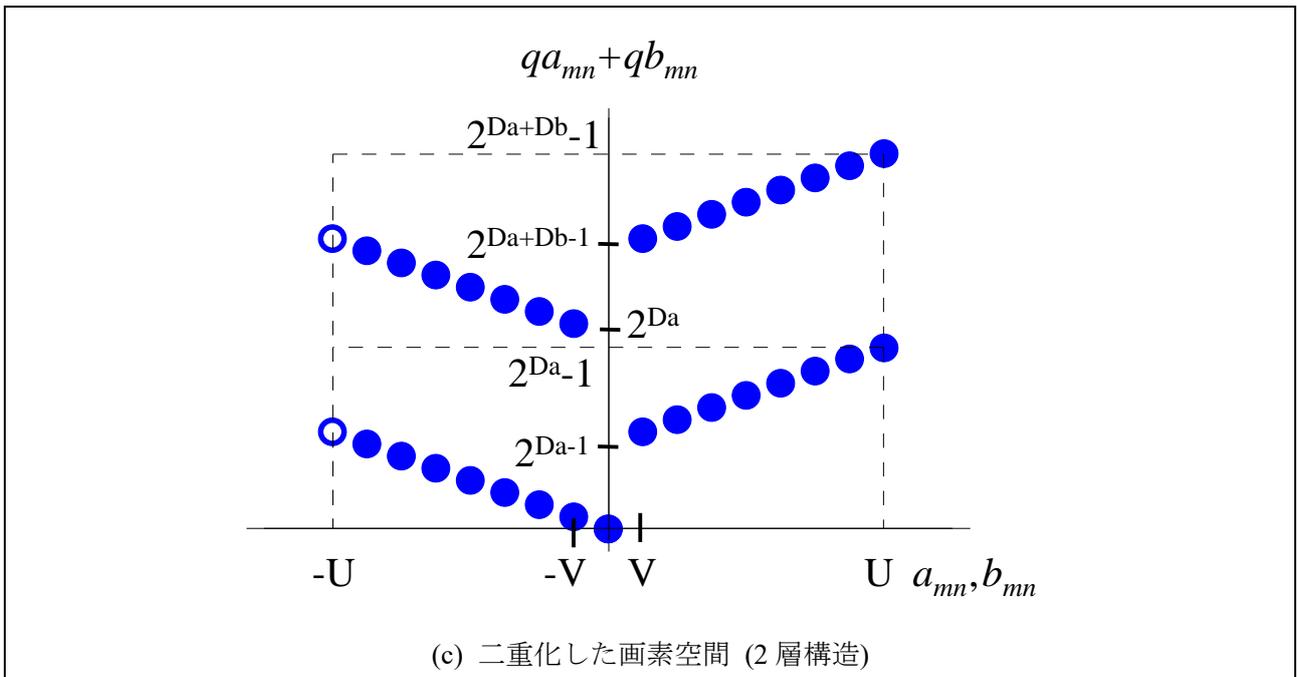
$$\{0, 1, \dots, 2^{D_a} - 1\} + \{0, 1, \dots, 2^{D_b} - 1\} \times 2^{D_a} \quad (4.4)$$

に基づいて行う。

画素空間における上記の 2 層構造が二重化の原理である。表 4.2 (a), (b) に 1 枚目, 2 枚目の画素空間をそれぞれ示す。表 4.2 (c) がそれらを二重化した画素空間の 2 層構造である。

表 4.2 画素空間の二重化





この方法に基づいた多重情報ハイディングに関する論文「擬似乱数系列でつくる二重情報ハイディング」を参考論文[C]に示す.

4.4 画像の三重化方法

1枚の画像の中に3枚の画像を埋め込む方法を示す. BMP形式画像は赤(R)、緑(G)、青(B)の3色で構成されている。それらの画素値は赤色、緑色、青色のデータ系列として個々に記録されている。したがって、各色のデータ系列に単色の濃淡画像を埋め込むことによって、三重の濃淡画像を1枚のカラー画像に埋め込むことができる。

一般的な三重の埋め込みはカラー画像3枚を埋め込むことを指すが、ここでは図4.6に示すように赤色の濃淡画像、緑色の濃淡画像、青色の濃淡画像を赤色、緑色、青色のデータ系列にそれぞれ埋め込むことによって三重化する方法を示す。

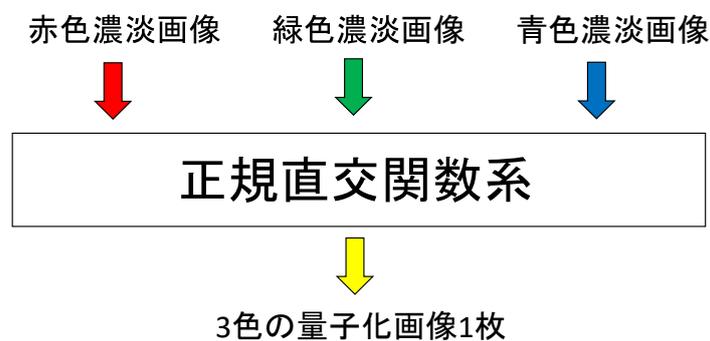


図 4.6 画像の三重化

この方法に基づいた多重情報ハイディングに関する論文「三重電子透かし画像づくり」を参考論文[D]に示す.

4.5 ステガノグラフィと電子透かしによる二重化

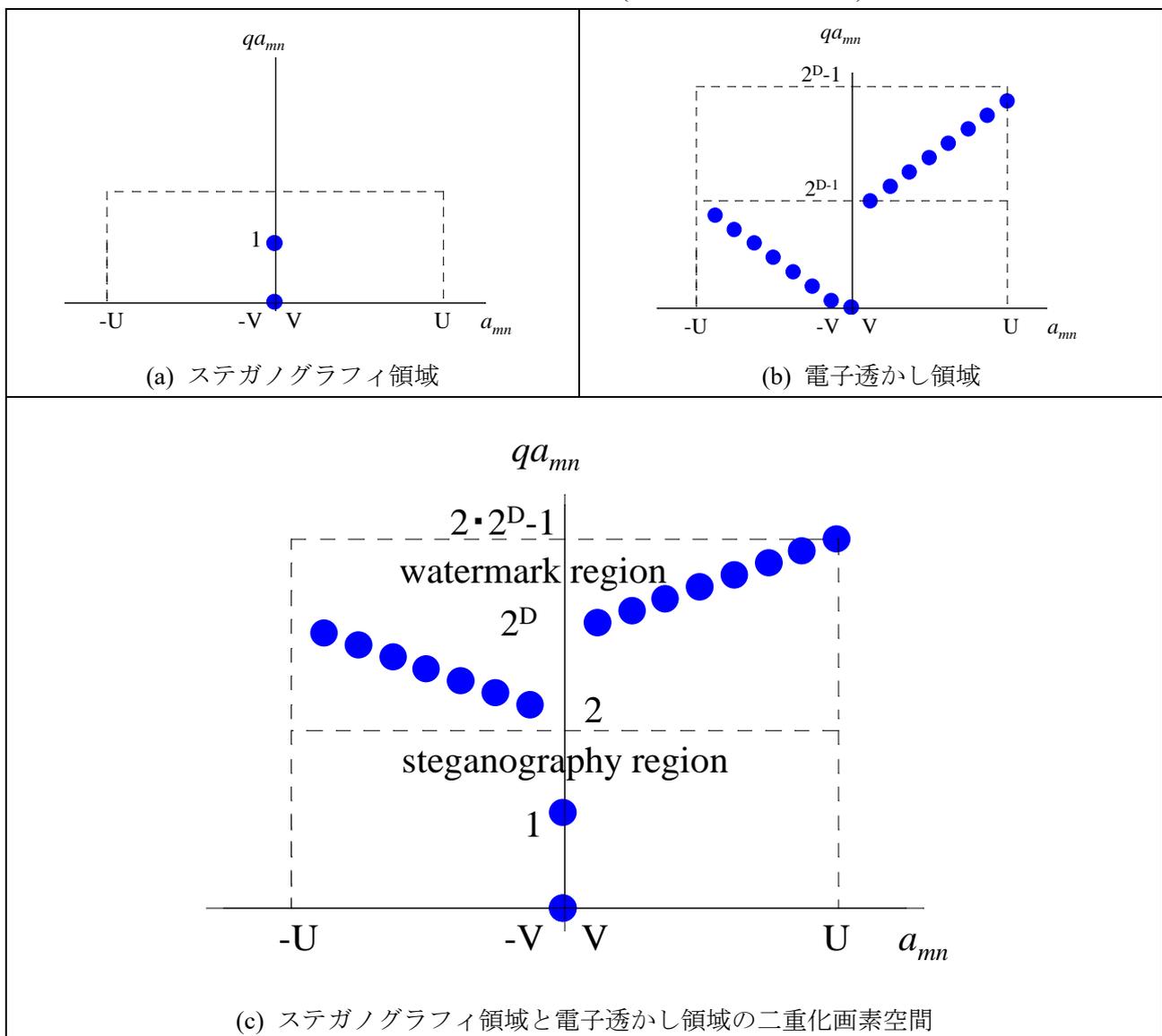
この二重化は節 4.3 で述べた 2 層構造の画素空間を変更したものである。下段の 1 層をビット数 1 のビットプレーン 0 だけのステガノグラフィ領域に変更した 2 層構造である。ビットプレーン 0 の領域にアスキーコードの秘匿文書を埋め込めるようにする。すなわち、この二重化は次のようになる。

- ① 第 1 層目をビット数 1 の画素空間 $\{0, 1\}$ のステガノグラフィ領域とする。
- ② 第 2 層目をビット数 D の画素空間 $\{0, 1, 2, \dots, 2^D\}$ の電子透かし領域とする。
- ③ 画素空間を次式のような 2 層構造とする。

$$\{0, 1\} + \{0, 1, \dots, 2^D - 1\} \times 2 \quad (4.5)$$

表 4.3 (a), (b) に第 1 層, 第 2 層の画素空間を示す。表 4.3 (c) がそれらを二重にした 2 層構造である。

表 4.3 量子化画像の二重化(画素空間の 2 層構造)



ここまで述べてきたいろいろな多重化を踏まえて、この論文では二重化方法として、ステガノグラフィ画素空間と電子透かし画素空間を二重にした 2 層構造の画素空間を新規考案として提案する。

第5章 安全のために

多重情報ハイディング画像の伝達中における安全のための条件をプライバシー保護の観点から次の目標を設定する。

- (1) 秘匿画像は改ざんされても耐えられる画像とする。
- (2) 秘匿文書は改ざんを受けたら壊れやすい文書とする。
- (3) 二重情報ハイディング画像の画質を高くする。

この設定を可能にする方法として、ビットプレーン転置を新規考案として提案する。その理由は3つある。1つは、ビットプレーン転置それ自体が安全対策になるからである。第三者は伝達中の多重ハイディング画像からビットプレーン転置に関する情報を知り得ることはほぼ不可能で、ビットプレーンを転置前に戻すことはできないからである。第2は、ビットプレーン転置による効果として改ざん範囲を集約化できることである。そして、第3は情報ハイディング画像の画質を向上できる効果である。以降に、第2と第3の理由を概説的に述べる。

5.1 改ざん範囲の集約化

この論文においては、ビットプレーンを次のように転置する。ビットプレーン $(D-1)$ をビットプレーン 0 に移し替える。ビットプレーン 0 はその1つ上のビットプレーン 1 に、ビットプレーン 1 はビットプレーン 2 に、と順に1つ上のビットプレーンに移し替える。最後にビットプレーン $(D-2)$ をビットプレーン $(D-1)$ に移し替える。この様子を図5.1に示す。以上でビットプレーン転置は完了する。なお、ビットプレーンを転置すると、画素値 $n_{D-1} \times 2^{D-1} + \dots + n_1 \times 2^1 + n_0 \times 2^0$ は $n_{D-2} \times 2^{D-1} + \dots + n_0 \times 2^1 + n_{D-1} \times 2^0$ に変化する。ただし、 n_k ($k = 0, 1, \dots, D-1$)は転置前ビットプレーン k における値「0」か「1」を表す。

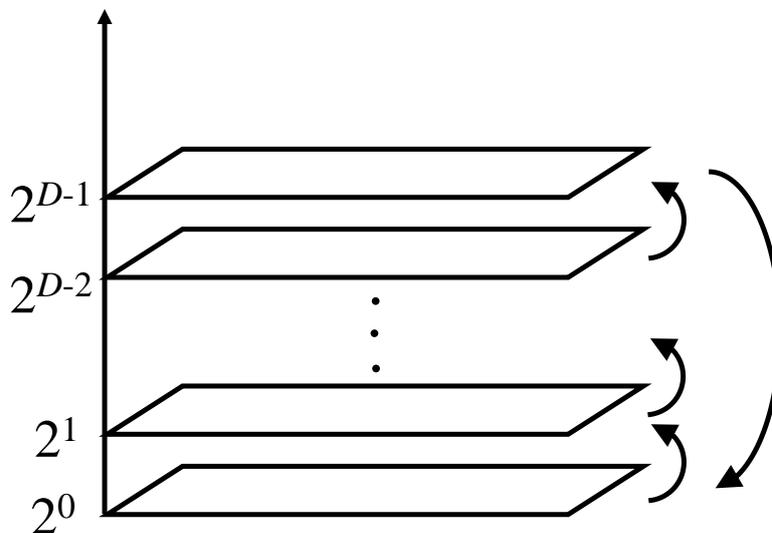


図 5.1 ビットプレーンの転置方法

ビットプレーン転置によって量子化特性は図 5.2 の(a)から(b)に変わる. 左側の画素値が $\{1, 2, 3, \dots, 2^{D-1} - 1\}$ から $\{2, 4, 6, \dots, 2^D - 2\}$ の偶数値に変わり, 右側の画素値 $\{2^{D-1}, 2^{D-1} + 1, 2^{D-1} + 2, \dots, 2^D - 1\}$ は $\{1, 3, 5, \dots, 2^D - 1\}$ の奇数値に変わる. 縦軸の画素値の順番が交互の順番に変わる.

したがって, ビットプレーン転置前の量子化特性を逆演算したグラフと, ビットプレーン転置後の量子化特性を逆演算したグラフも異なる. その違いをグラフで表したのが図 5.3 (a), (b)である. 展開係数 a の絶対値が大きい部分が図 5.3(a)では 2 ヲ所あるが, (b)では 1 ヲ所に集約する. このことを改ざん範囲の集約化とここでは呼ぶことにする.

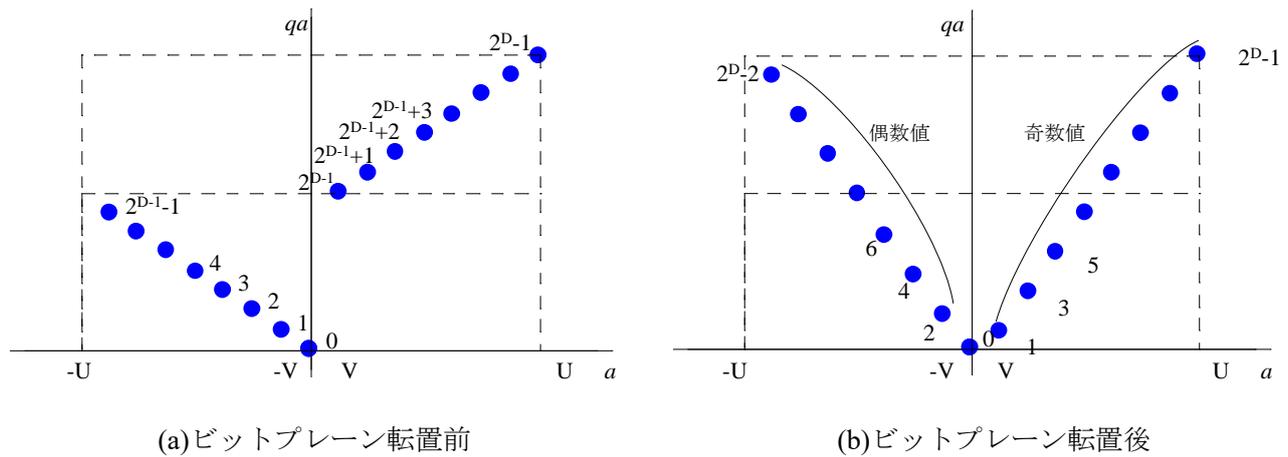


図 5.2 ビットプレーン転置前後の量子化特性

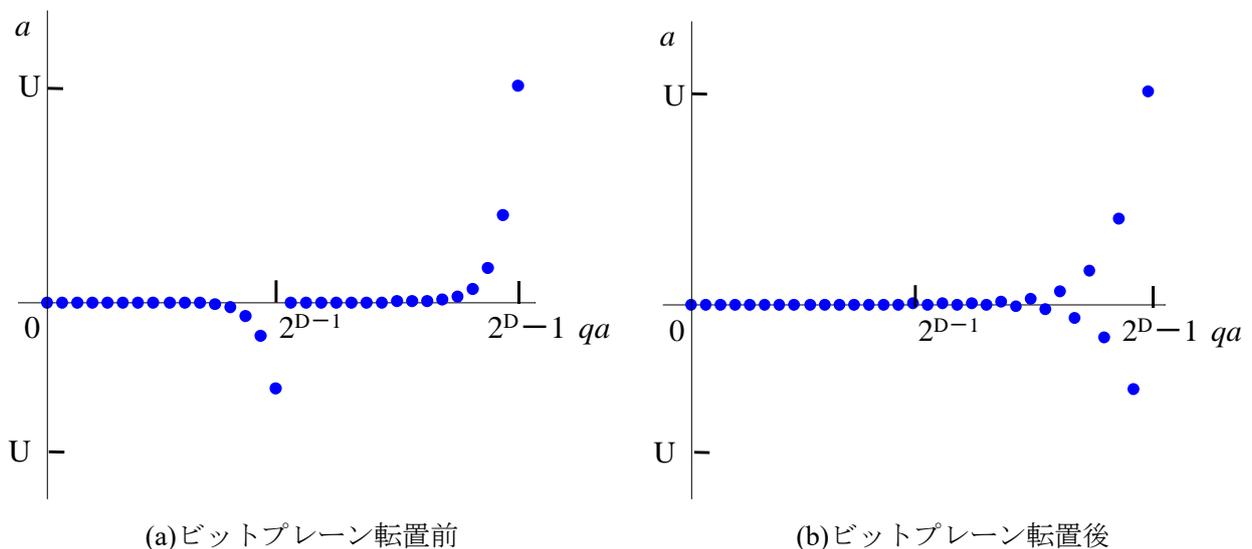


図 5.3 ビットプレーン転置前後の量子化特性の逆演算グラフ

5.2 情報ハイディング画像の高画質化

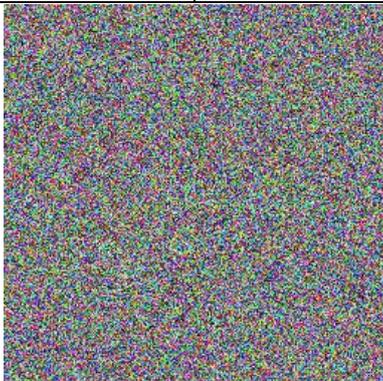
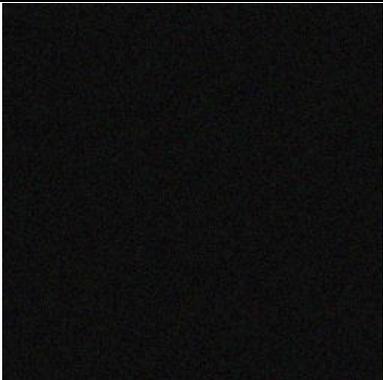
ビット数 D の画素空間に量子化された画像は D 枚のビットプレーンに分解できる。以降、ビットプレーン上の数値が 1 である点の個数をそのビットプレーンの度数と定める。この度数を用いて情報ハイディング画像の画質について考察する。ただし、ビット数 D を $D=5$ と設定する。その理由は節 6.3 (5) に示す。

考察に用いる画像は起伏の激しい画像とする。ここでは 256×256 個の擬似乱数系列を行列 256 行 256 列に配列したカラー画像を選ぶ。これを表 5.1 (a) に示す。この画像を別の擬似乱数系列で構築した正規直交関数系を用いて展開し量子化した画像が表 5.1 (b) である。この画像はビットプレーンを転置する前の量子化画像である。ビットプレーンを転置した後の転置後量子化画像が表 5.1 (c) である。

ビットプレーン転置前後におけるビットプレーン 0~7 の度数をそれぞれ表 5.1 (d), (e) に示す。併せて、色ごとの分散を (f), (g) に示し、色ごとの平均を (h), (i) に示す。

ビットプレーン転置後の平均値は転置前のそれとほぼ等しいが、転置後の分散(表 5.1 (g))は転置前のそれ(表 5.1 (f))よりも小さい数値である。この数値の違いが情報ハイディング画像の画質差となって現れる。すなわち、ビットプレーンの並び方の違いが画質差となって現れるのである。その具体例を節 7.3(2) で述べる。

表 5.1 ビットプレーンの度数分布と分散

	ビットプレーン転置前	ビットプレーン転置後
擬似乱数系列を配列した画像	 (a)	
正規直交関数系で展開した量子化画像	 (b)	 (c)

ビットプレーンの度数分布	<p>(d)</p>	<p>(e)</p>	
	分散	(57, 57, 57) (f)	(6, 6, 6) (g)
	平均	(14, 15, 14) (h)	(14, 14, 14) (i)

ここで、ビットプレーン転置前のビットプレーン3の度数が最小になる理由を、図5.4に示す画素数 256×256 の擬似乱数系列の単色画像を用いて述べる。この画像の展開係数の度数分布が図5.5である。ビット数は $D=5$ とし、量子化係数は節3.5(2)の図3.2に従うとする。図5.5の横軸数値8, 9, 10, 11, 24, 25, 26は量子化係数の開始位置を示す。たとえば量子化係数が8になる区間は[8,9)である。赤色の実線、破線はそれぞれ基準0の位置、標準偏差 ± 73.55 の位置を示す。ビットプレーン3の度数は量子化係数が区間8~15と区間24~31の総合計度数である。したがって、図5.5のように区間[8,9)が負側の標準偏差の位置を含むか、あるいはそれより負側領域に位置する場合には、ビットプレーン3の度数が他のビットプレーンの度数より少なくなり、最小になる。

なお、表5.1(d)のビットプレーン0の度数がほぼ50%(RGB平均 $\div(256 \times 256)$)である理由は量子化係数が偶数奇数のうち奇数になる割合と等しいからである。またビットプレーン4の度数がほぼ50%(RGB平均 $\div(256 \times 256)$)である理由は量子化係数が0~31のうち16~31になる割合と等しいからである。

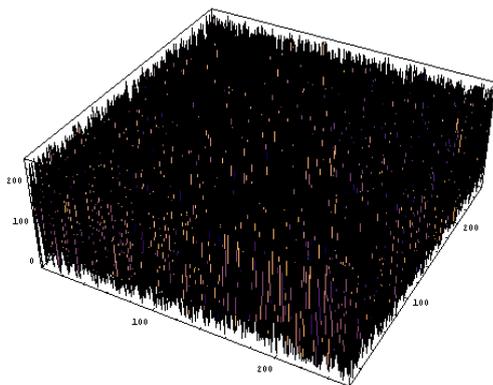


図5.4 単色画像

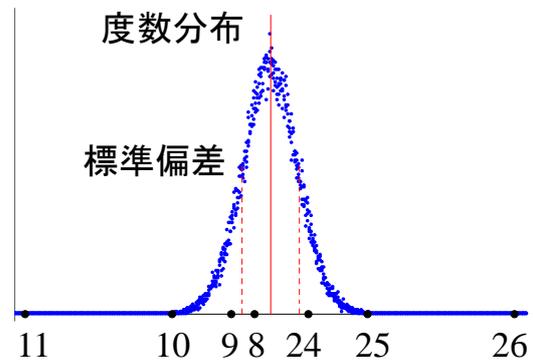


図5.5 展開係数度数分布

第6章 アルゴリズムと実験

この章の前半では、二重情報ハイディング画像を制作するアルゴリズムと、それを再生するアルゴリズムを作成する。

そのアルゴリズムは

- (1) 第3章で提案した擬似乱数系列で構築する正規直交関数系
- (2) 第4章で提案したステガノグラフィと電子透かしによる2層構造の画素空間
- (3) 第5章で提案したビットプレーン転置

を取り入れたものである。

そして、後半ではそのアルゴリズムを用いて二重情報ハイディング画像を制作する実験および再生する実験を行う。

6.1 制作アルゴリズム

アルゴリズムを制作する前に、擬似乱数系列で構築する正規直交関数系を次の5つの手順で用意しておく。

- ① 個数 N^2 個の擬似乱数をもつ系列を用意する。乱数の値が $0\sim 1$ 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 N 個ずつ区切り N 行 N 列の行列に配置替える。ここで、各行の横並びの擬似乱数を、列 $j=1, 2, \dots, N$ において定義される関数値とみなす。そうすると関数の個数は全部で N 個になる。第 i 行 ($i=1, 2, \dots, N$) 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 $\psi_i(j)$ を順次に直交化する。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。

$$\begin{cases} \phi_1(j) = \psi_1(j) \\ \phi_i(j) = \psi_i(j) - \sum_{k=1}^{i-1} \frac{(\phi_k(j), \psi_i(j))}{(\phi_k(j), \phi_k(j))} \phi_k(j) \end{cases} \quad (6.1)$$

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

- ⑤ 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。

$$\varphi_i(j) = \frac{\phi_i(j)}{\sqrt{(\phi_i(j), \phi_i(j))}} \quad (6.2)$$

$\varphi_i(j)$ は次の関係を満たす。

$$(\varphi_i(j), \varphi_k(j)) = \delta_{ik} \quad (\delta_{ik} \text{はクロネッカーのデルタ}) \quad (6.3)$$

以上の手順で、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 $\{\varphi_i(j)\}$ が構築される。

次に，秘匿画像と秘匿文書を埋め込むための制作アルゴリズムを，図 6.1 に示す二重情報ハイディング画像の制作過程に沿いながら作成する．

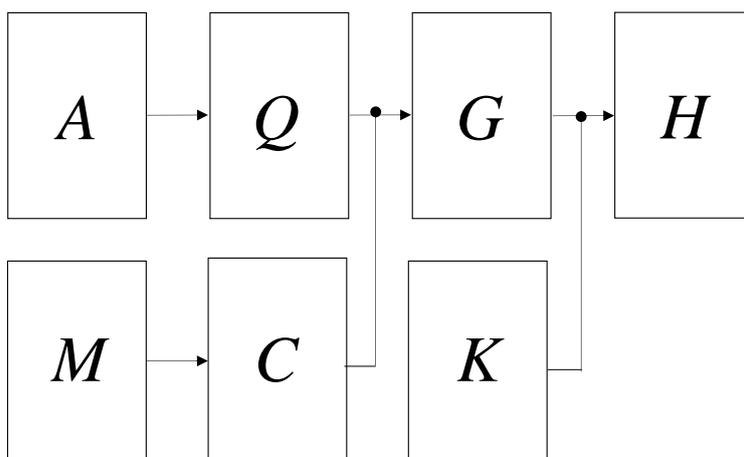


図 6.1 二重情報ハイディング画像の制作過程

- ① 秘匿画像 1 枚と秘匿文書 1 枚を用意する．それらをそれぞれ A ， M とする．さらに，カギ画像 K を 1 枚と，画素値がすべて 0 の空白画像を 1 枚用意する．
- ② 秘匿画像 A を正規直交関数系で展開したときの展開係数 a を算出する．その算出方法は次式を用いて行う．

$$a_{mn} = \sum_{j=1}^N (\sum_{i=1}^N A_{ij} \varphi_m(i)) \varphi_n(j) \quad (6.4)$$

カラー画像を対象にするので，赤色，緑色，青色の 3 つの展開係数を算出する．

- ③ 秘匿文書 M のアスキーコードを空白画像のビットプレーン 0 に置換する．それをサイファ画像 C とする．埋め込むアスキーコード個数は赤色ビットプレーン 0 に $(N \times N) \div 8$ 個以内，緑色ビットプレーン 0 に $(N \times N) \div 8$ 個以内，そして青色ビットプレーン 0 に $(N \times N) \div 8$ 個以内とする．
- ④ 展開係数 a を D ビットの画素空間 $\{0, 1, \dots, 2^D - 1\}$ 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，カギ画像に埋め込むとき，その画素値のまま直接に埋め込むようにするためである．展開係数を量子化する方法は，(i)，(ii)，(iii) の 3 つの区間に分けて量子化する．ただし，値 U, V を

$$U = \sum_{j=1}^N (\sum_{i=1}^N 255 \varphi_1(i)) \varphi_1(j) \quad (6.5)$$

$$V = 1/\sqrt{N} \quad (6.6)$$

とする． U は式(6.4)の A 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 $\varphi_1(j)$ ($j = 1, 2, \dots, N$) の関数値である．

- (i) $-U < a \leq -V$ のとき

$$qa_{mn} = \frac{2^{D-1}-1}{\log_{10} U - \log_{10} V} (\log_{10}(-a_{mn}) - \log_{10} V) + 1 \quad (6.7)$$

- (ii) $-V < a < V$ のとき

$$qa_{mn} = 0 \quad (6.8)$$

- (iii) $V \leq a \leq U$ のとき

$$qa_{mn} = \frac{2^{D-1}-1}{\log_{10} U - \log_{10} V} (\log_{10}(+a_{mn}) - \log_{10} V) + 2^{D-1} \quad (6.9)$$

量子化係数 qa を画素値とする画像が量子化画像である．

展開係数 a と量子化係数 qa の関係をグラフに表したのが図 6.2 の量子化特性である。ただし、図 6.2 は qa の画素値を 16 個で例示したものである。

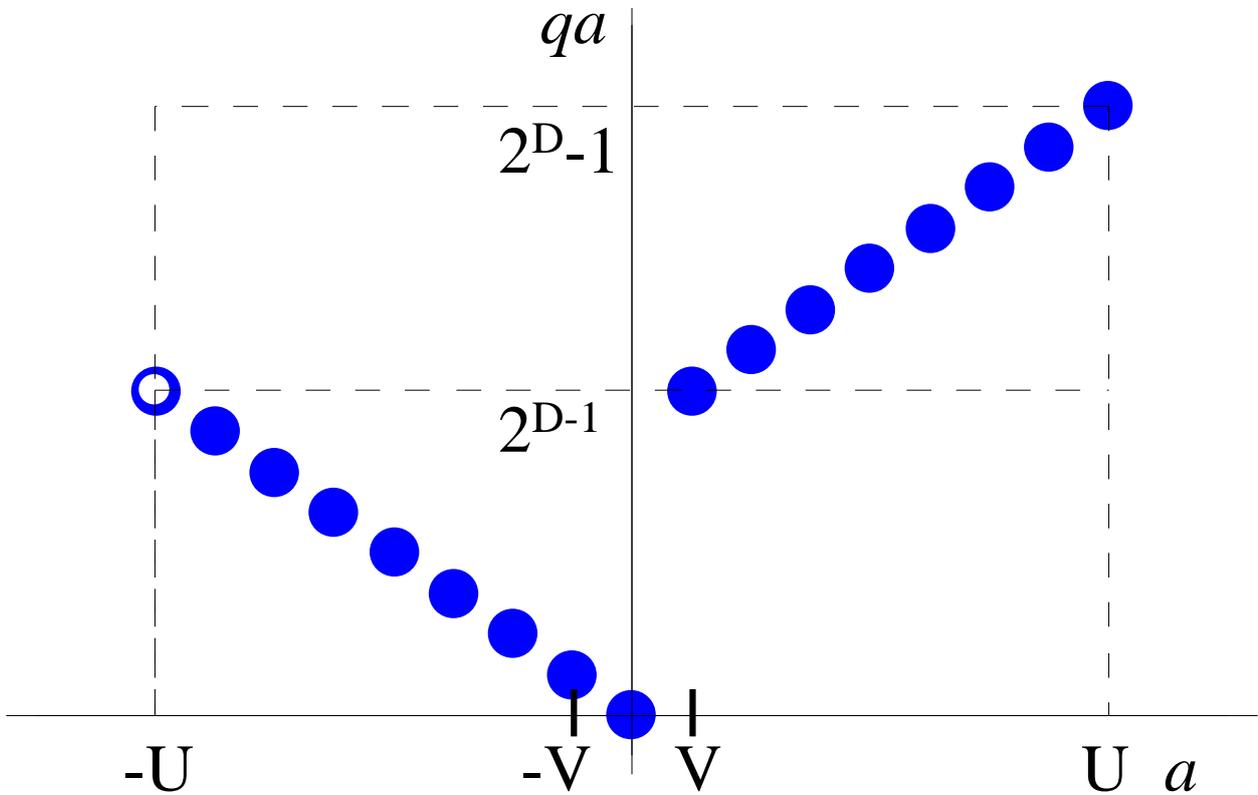


図 6.2 量子化特性

⑤ 次に、量子化画像のビットプレーンを転置する。 D ビット画素空間の転置は、最上位のビットプレーン $(D-1)$ を最下位のビットプレーン 0 に転置し、ビットプレーン 0 は 1 つ上のビットプレーン 1 へ、ビットプレーン 1 はビットプレーン 2 へと順次 1 つ上のビットプレーンに転置する。最後にビットプレーン $(D-2)$ をビットプレーン $(D-1)$ に転置して、ビットプレーンの転置は完了する。これを画素値の変化で示すと、式(6.10)、式(6.11)になる。式(6.10)は転置前で、これを画像にしたのが量子化画像である。式(6.11)は転置後で、これを画像にしたのが転置後量子化画像 Q である。

$$n_{D-1} \times 2^{D-1} + \dots + n_1 \times 2^1 + n_0 \times 2^0 \quad (6.10)$$

$$n_{D-2} \times 2^{D-1} + \dots + n_0 \times 2^1 + n_{D-1} \times 2^0 \quad (6.11)$$

ただし、 n_k ($k = 0, 1, \dots, D-1$) は転置前ビットプレーン k における数値「0」または「1」

⑥ 転置後量子化画像 Q とサイファ画像 C を 1 枚のホログラム画像 G に合成する。その合成方法は式(6.12)で行う。

$$\{0, 1, \dots, 2^D - 1\} \times 2 + \{0, 1\} \quad (6.12)$$

つまり、ホログラム画像 G は $\{0,1,\dots,2^{D_a}-1\} \times 2$ である電子透かし領域と、ビットプレーン 0 の $\{0,1\}$ を画素値とするステガノグラフィ領域から構成される2層構造である。この2層構造が二重情報ハイディング画像の仕組みである。ホログラム画像の画素空間の2層構造を図 6.3 に示す。

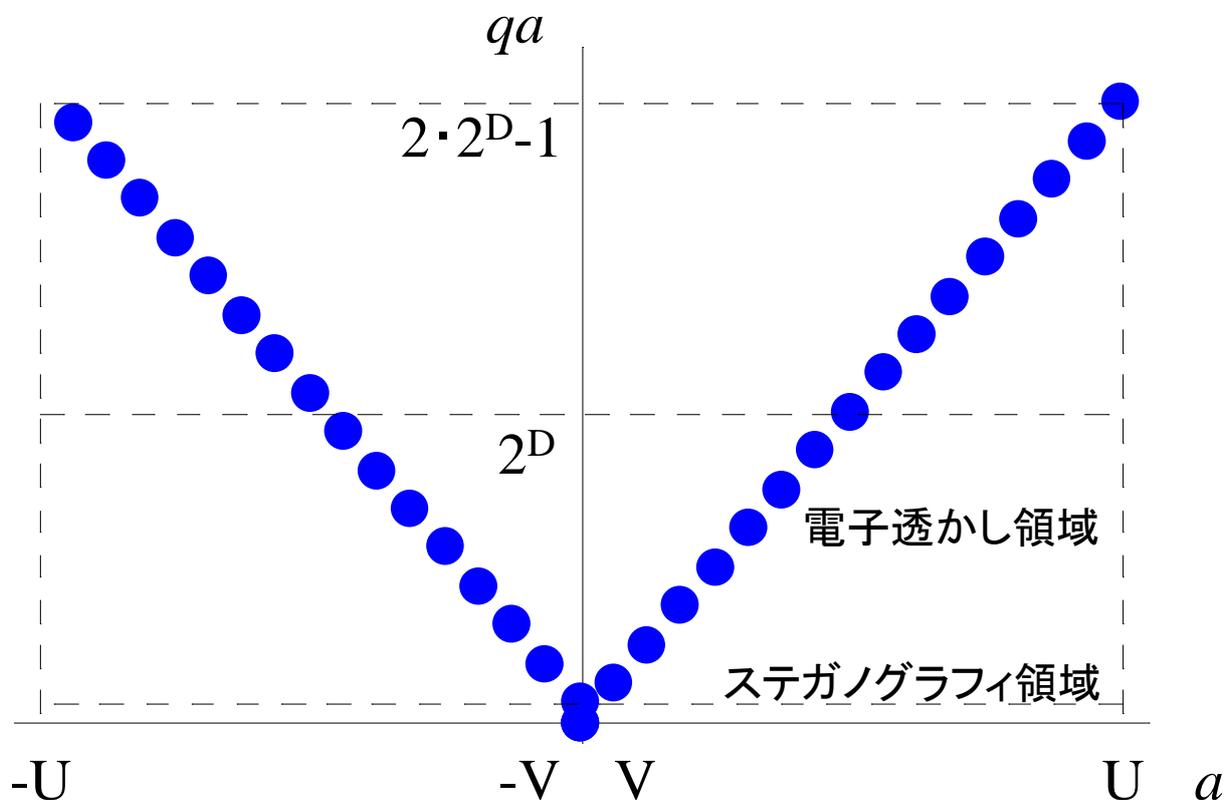


図 6.3 ホログラム画像の2層構造

⑦ 最後にホログラム画像 G をカギ画像 K に次式で埋め込む。以上で二重情報ハイディング画像 H を制作することができる。

$$H = G + \frac{256-2^{D+1}}{255}K \tag{6.13}$$

6.2 再生アルゴリズム

二重情報ハイディング画像を再生するアルゴリズムを、図 6.4 に示す二重情報ハイディング画像の再生過程に沿いながら作成する。再生アルゴリズムは原理的には制作アルゴリズムの逆過程である。

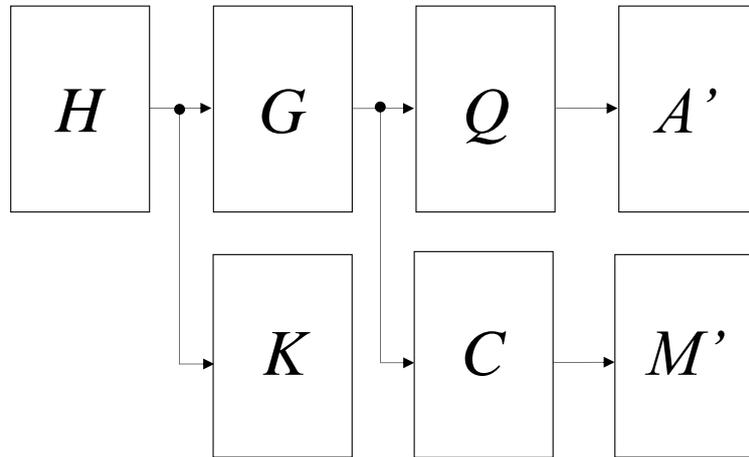


図 6.4 二重情報ハイディング画像の再生過程

- ① 最初に、二重情報ハイディング画像 H からカギ画像 K を差し引く。2層構造のホログラム画像 G を得ることができる。
- ② ホログラム画像から各層ごとに画素空間を抽出する。第1層はビットプレーン0の $\{0,1\}$ をそのまま抽出したものである。それがサイファ画像 C である。残り1層はホログラム画像を 2^{-1} 倍して得る。これでビットプレーン転置された転置後量子化画像 Q を得ることができる。
- ③ 次に、ビットプレーン転置された転置後量子化画像のビットプレーン転置を元の状態に戻す。以上で、正規直交関数系で展開した直後の量子化展開係数を得ることができる。
- ④ 式(6.7), 式(6.8), 式(6.9)の逆演算を行う。それを a' とする。
- ⑤ そして、 a' から再生画像 A' を再生する。その再生方法は次式のとおりである。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。

$$\begin{cases} X_{ij} = \sum_{n=1}^N (\sum_{m=1}^N a'_{mn} \varphi_m(i)) \varphi_n(j) \\ A'_{ij} = \frac{X_{ij} - \min\{X_{ij}\}}{\max\{X_{ij}\} - \min\{X_{ij}\}} \times 255 \end{cases} \quad (6.14)$$

- ⑥ 最後に、サイファ画像 C のビットプレーン0のビットを読み込む。それらをアスキー文字に変換すると、再生文書 M' を得ることができる。

6.3 制作実験

1枚の画像の中に秘匿画像1枚と秘匿文書1枚を埋め込む二重情報ハイディングの実験例を示す。最初に実験条件を設定する。

(1) 設定1

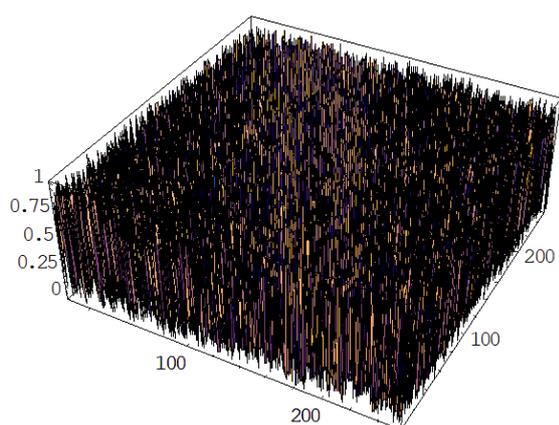
実験の画像形式はBMP形式とする。画像の画素数 $N \times N$ は横256画素、縦256画素とする。この場合、式(6.5)の U は $U=65280$ 、式(6.6)の V は $V=0.0625$ になる。

(2) 設定2

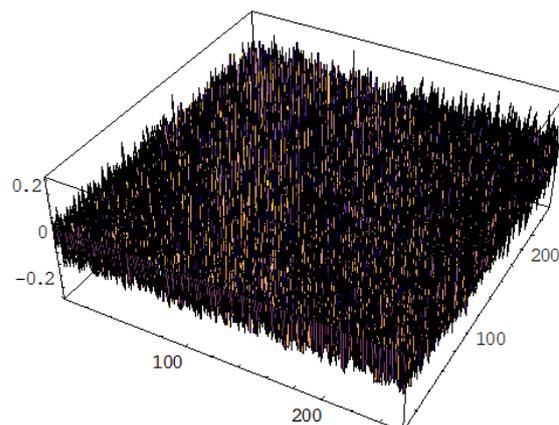
実験に採用した擬似乱数系列は「Mathematica」(Wolfram Research社)が発生したものである。その擬似乱数系列の乱雑さを確認しておく。確認にはカイ二乗検定を用いる。表6.1は発生した $N \times N=65536$ 個の擬似乱数をそれぞれ10倍したときの整数値の出現度数を示す。表6.1のカイ二乗の値は11.8である。この値は自由度9で危険率0.01の場合のカイ二乗の値21.7より小さな値であることから、擬似乱数は99%の確率で均等に出現していることになる。擬似乱数系列を256行256列の平面に表したグラフが図6.5(a)である。この擬似乱数系列を用いて構築した正規直交関数系 $\varphi_i(j)$ ($i, j = 1, 2, \dots, 256$) が図6.5(b)である。

表 6.1 擬似乱数の出現度数

整数値	0	1	2	3	4	5	6	7	8	9
出現度数	6397	6637	6570	6537	6650	6561	6427	6481	6647	6629



(a) 擬似乱数系列による 256×256 行列



(b) 構築した正規直交関数系 $\varphi_i(j)$

図 6.5 擬似乱数系列による行列と正規直交関数系

(3) 設定3

画素空間の2層構造を次のように設定する。サイファ画像にはビットプレーン0の1ビットの画素空間を設定する。埋め込み可能なアスキーコード個数は赤色ビットプレーン0の1行1列~1行256列に32個、緑色ビットプレーン0の1行1列~1行256列に32個、そして青色ビットプレーン0の1行1

列～1行 256列に 32個, 合計 96個とする.

(4) 設定 4

この実験で用いる秘匿文書は赤色ビットプレーン 0 に「Sasaki Takayuki (male)」, 緑色ビットプレーン 0 に「Aomori (0173-**-****)」, 青色ビットプレーン 0 に「Good-feeling (cold)」書き込むこととする. 空白含めて 83 (=32+32+19)個のアスキーコードである.

(5) 設定 5

転置後量子化画像には 5 ビットの画素空間を用いる. 秘匿文書のビット数 1 と合計すると, ビット数 D は合計で $D = 6$ になる. $D = 6$ とした理由は, 式(6.13)の二重情報ハイディング画像 H とカギ画像 K の相関係数が 0.5 以上となる最大の D を採用したからである. ただし, このときのホログラム画像 G 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, 青色の色で異なる擬似乱数系列でつくられる画像である. 実験に採用するビットプレーン転置後の 2 層構造は図 6.6 になる.

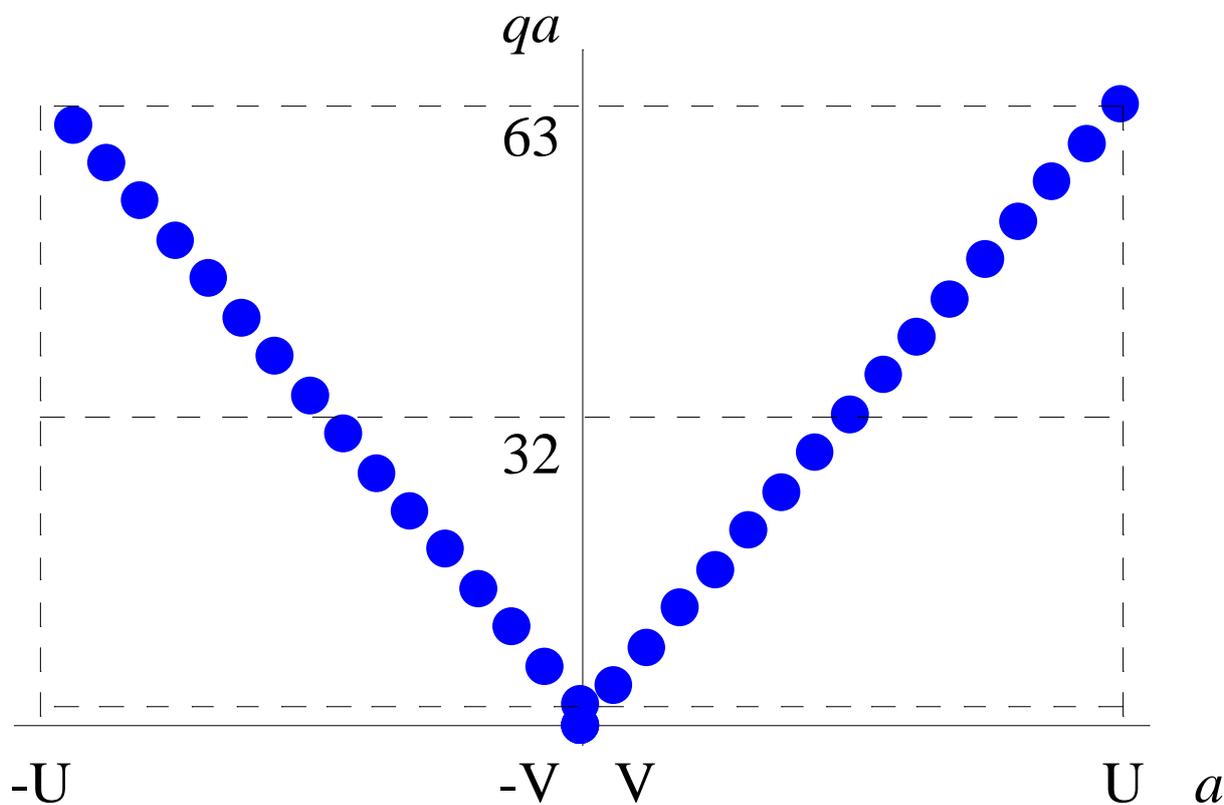


図 6.6 実験に採用する 2 層構造の画素空間(ビットプレーン転置後)

図 6.1 の二重情報ハイディング画像の制作過程に制作途中の画像と文書を挿入したのが図 6.7 である。

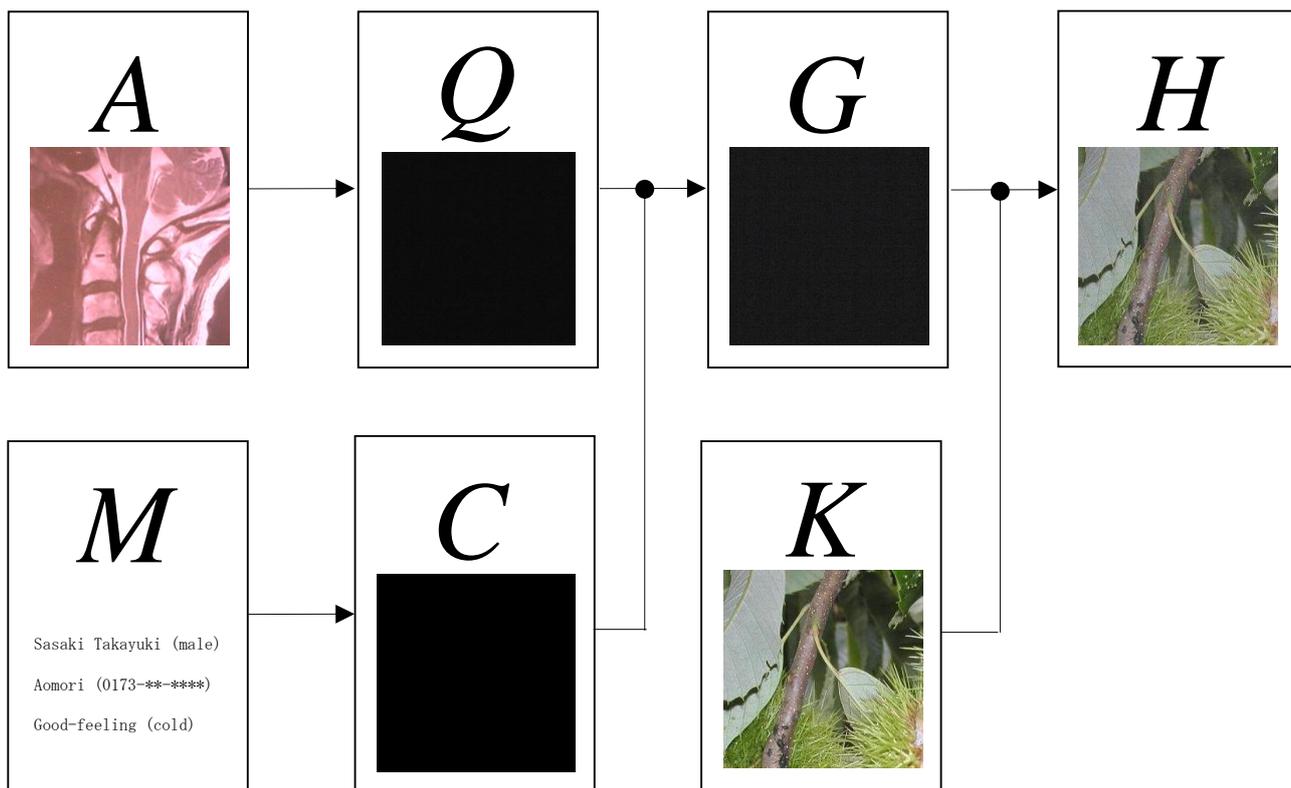
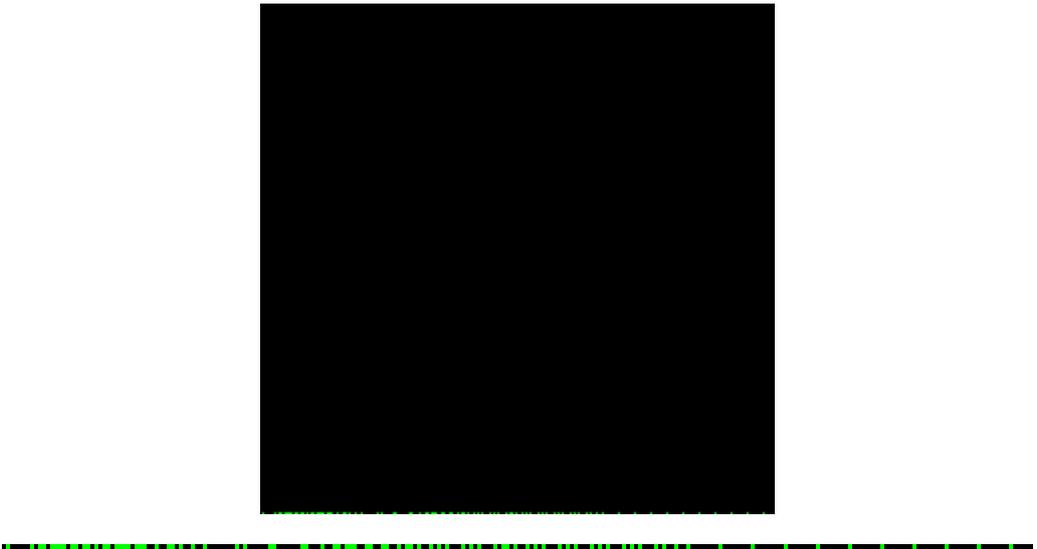
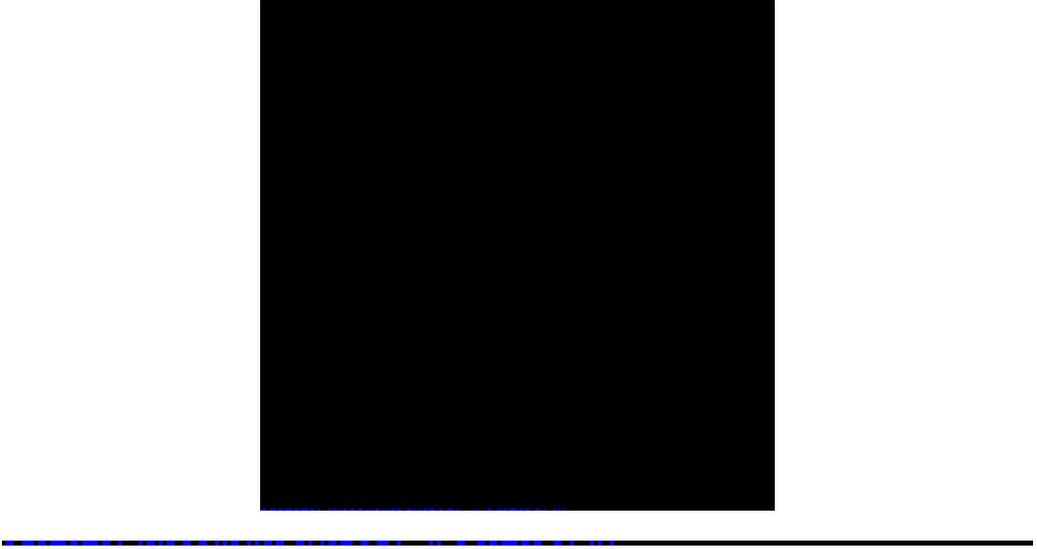


図 6.7 二重情報ハイディング画像の制作過程(画像と文書を挿入)

制作過程のサイファ画像 C を表 6.2 に示す。色ごとのビットプレーン 0 全面と、ビットプレーン 0 の 1 行 1 列～1 行 256 列を縦 2 倍×横 2 倍し画素値を 255 倍した拡大図をその下に併記する。色ごとの明るい位置が数値 1 で、暗い位置が数値 0 である。

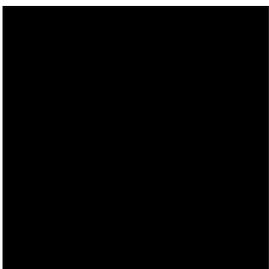
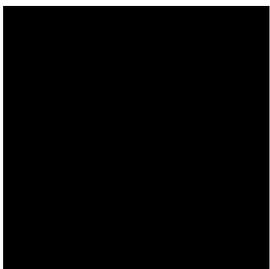
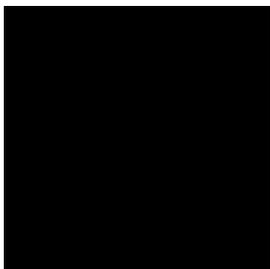
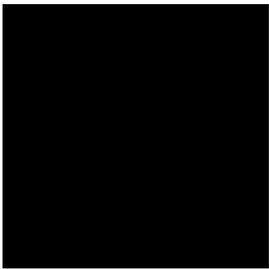
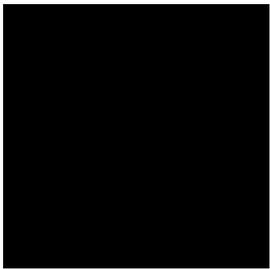
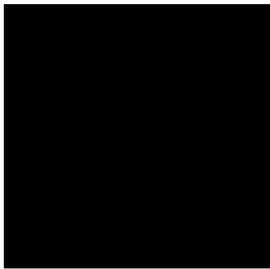
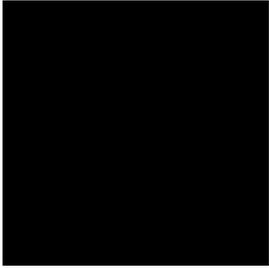
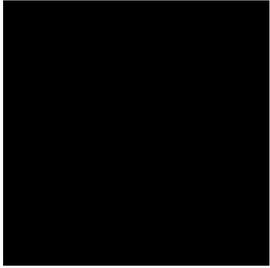
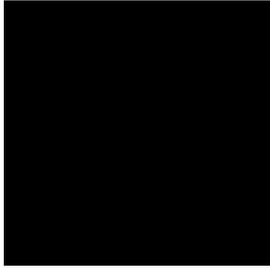
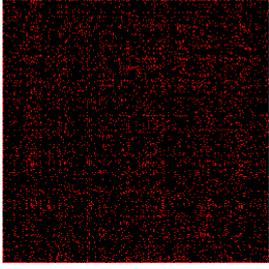
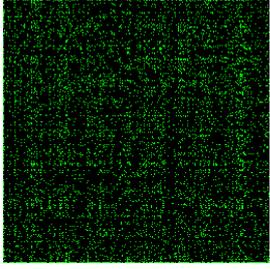
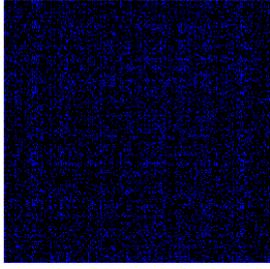
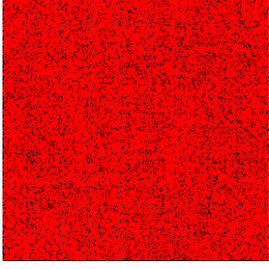
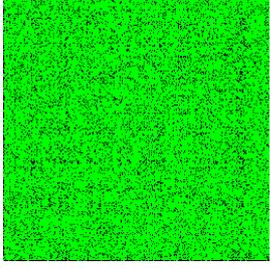
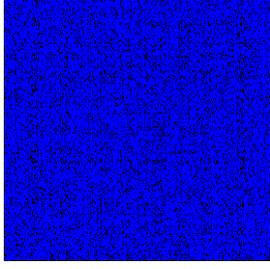
表 6.2 秘匿文書が埋め込まれたサイファ画像 C のビットプレーン 0

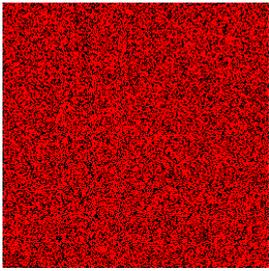
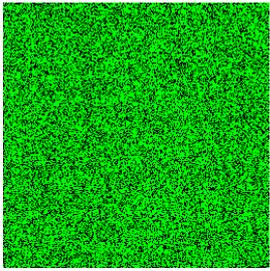
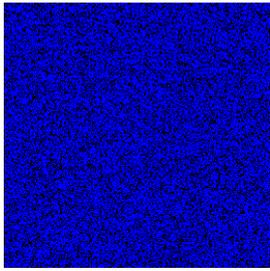
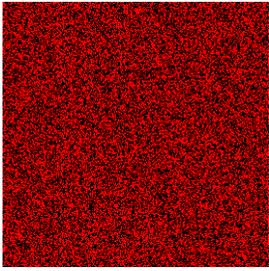
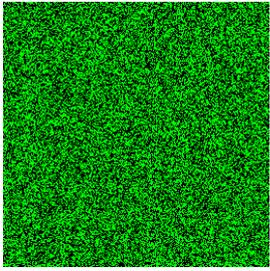
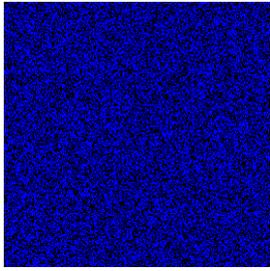
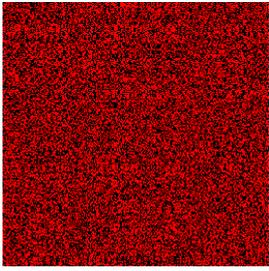
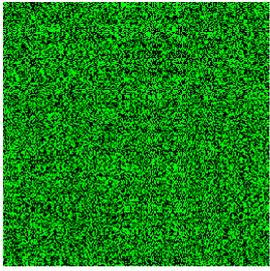
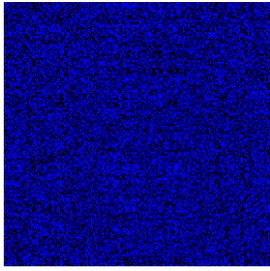
色	各色のビットプレーン 0 画面 (上図) 1 行 1 列～1 行 256 列を縦 2 倍×横 2 倍し画素値を 255 倍した拡大図(下図)
赤色	

緑色	
青色	

次に、秘匿画像を展開し量子化し、さらにビットプレーン転置した転置後量子化画像 Q の各色ビットプレーン 0~7 を表 6.3 に示す。

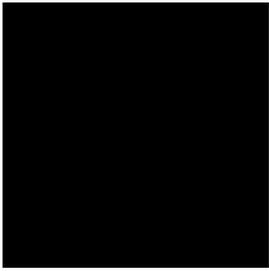
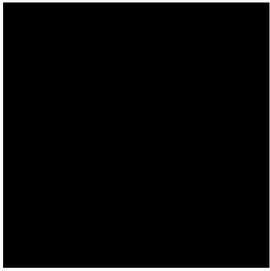
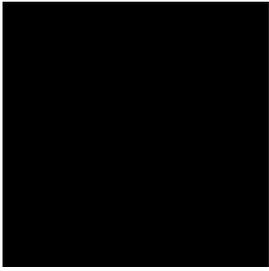
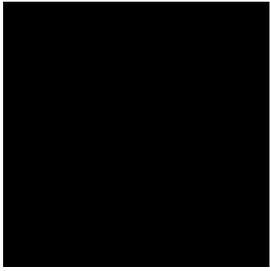
表 6.3 転置後量子化画像 Q のビットプレーン

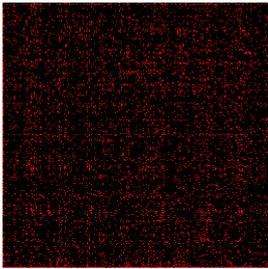
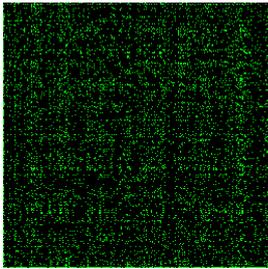
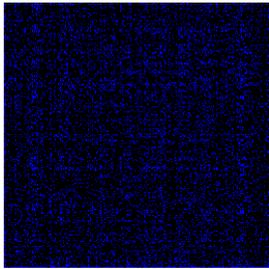
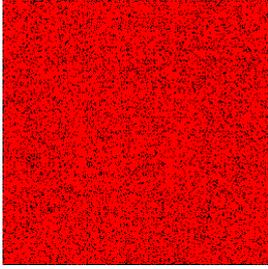
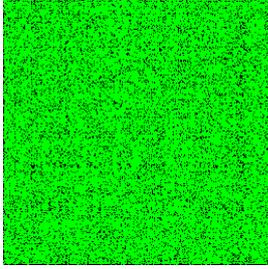
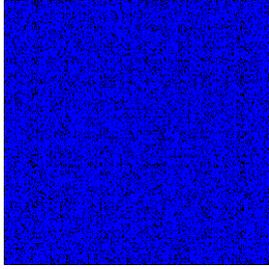
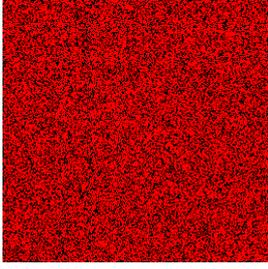
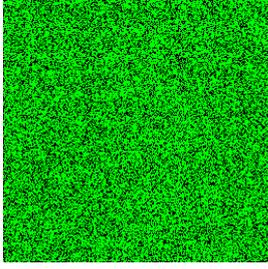
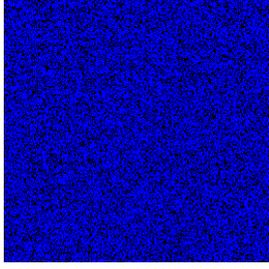
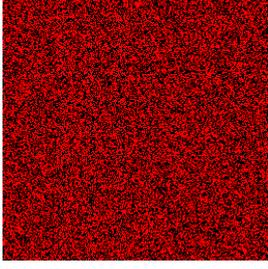
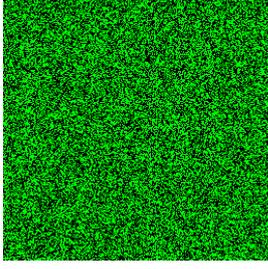
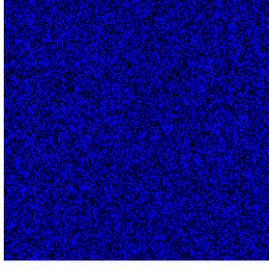
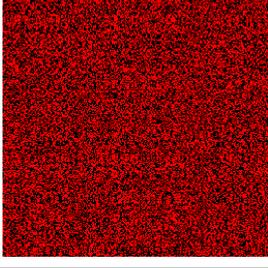
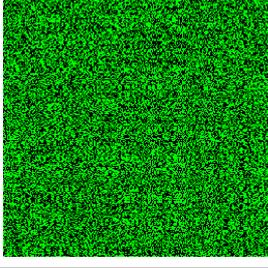
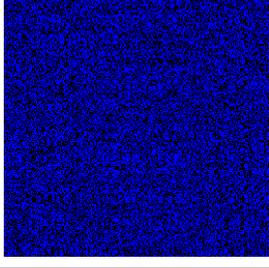
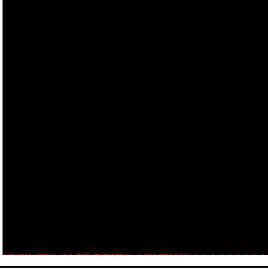
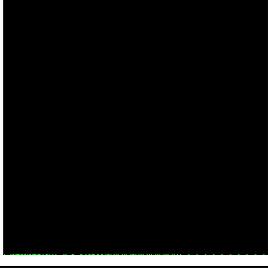
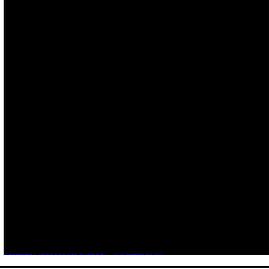
ビットプレーン No.	赤色	緑色	青色
ビットプレーン 7			
ビットプレーン 6			
ビットプレーン 5			
ビットプレーン 4			
ビットプレーン 3			

ビットプレーン2			
ビットプレーン1			
ビットプレーン0			

サイファ画像 C と転置後量子化画像 Q を合成したホログラム画像 G の各色ビットプレーン 0~7 を表 6.4 に示す.

表 6.4 ホログラム画像 G のビットプレーン

ビットプレーン No.	赤色	緑色	青色
ビットプレーン7			
ビットプレーン6			

ビットプレーン 5			
ビットプレーン 4			
ビットプレーン 3			
ビットプレーン 2			
ビットプレーン 1			
ビットプレーン 0			

6.4 再生実験

図 6.4 の二重情報ハイディング画像の再生過程に再生途中における画像と文書を挿入したのが図 6.8 である。

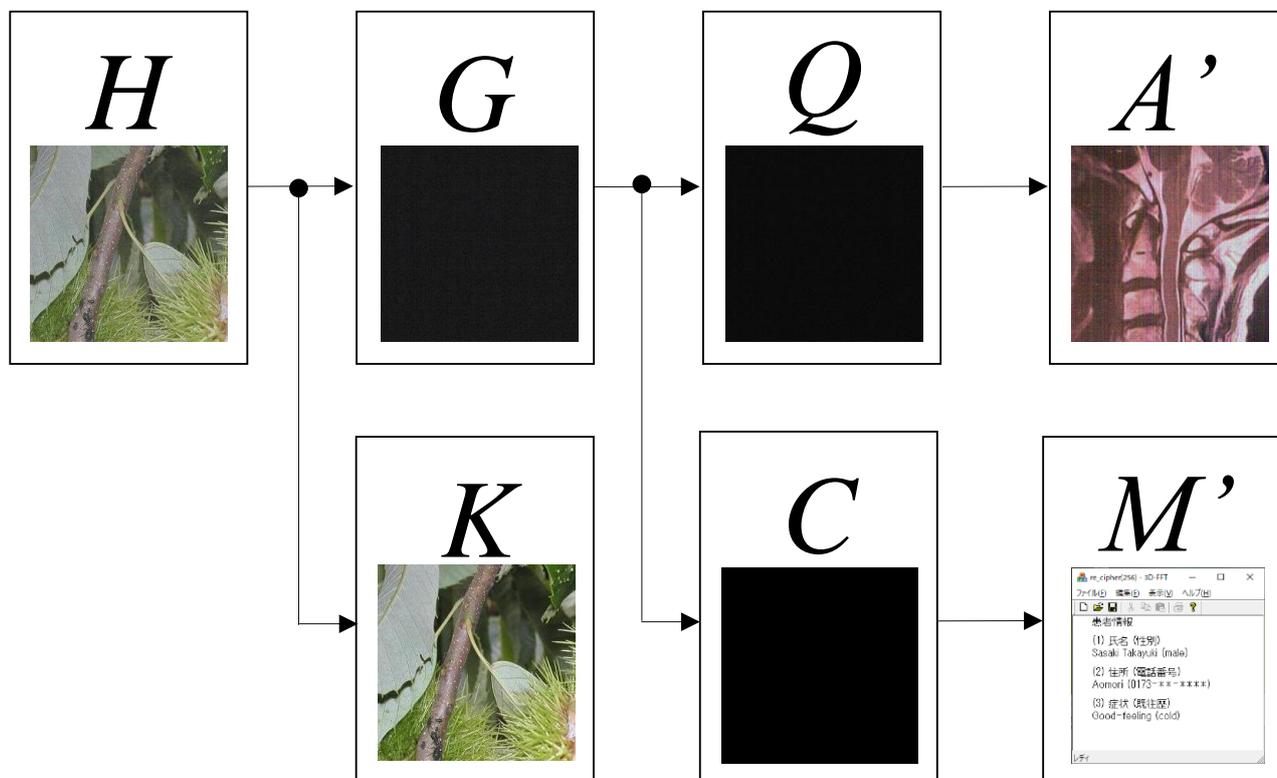


図 6.8 二重情報ハイディング画像の再生過程(画像と文書を挿入)

再生された秘匿文書 M' の拡大画面を図 6.9 に示す。赤色枠内のアスキー文字が秘匿文書の再生である。それ以外は実験のために設定した画面様式である。

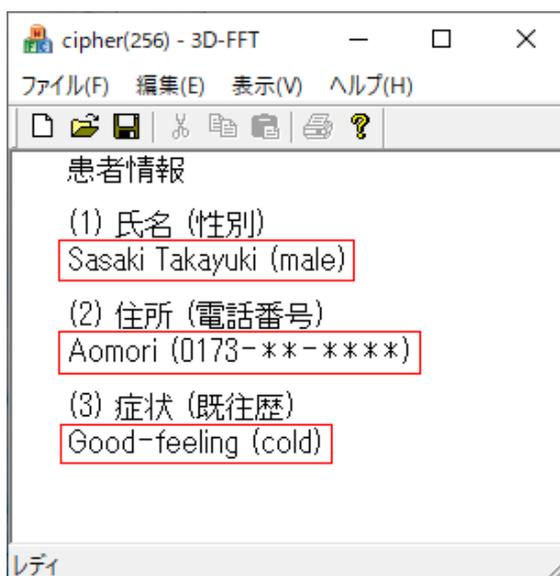


図 6.9 秘匿文書の再生画面

第7章 測定と評価

最初に制作実験と再生実験で得た画像を測定し評価する。その次に、二重情報ハイディング画像が伝達途中で改ざんを受けた場合、どのような改ざん痕跡が現れるかを実験して測定と評価をする。最後に、ビットプレーン転置の効果を実験して測定し評価する。画像の測定方法は PSNR (Peak Signal to Noise Ratio, 単位[dB])測定と、相関係数 (coefficient of correlation)測定の2種類である。以降では PSNR の単位[dB]は省略する。

7.1 制作・再生実験の測定と評価

(1) 制作した二重情報ハイディング画像 H (図 7.1) とカギ画像 K (図 7.2) の PSNR および相関係数を測定する。その結果が表 7.1 である。



図 7.1 二重情報ハイディング画像



図 7.2 カギ画像

表 7.1 二重情報ハイディング画像とカギ画像の PSNR と相関係数

	赤色	緑色	青色
PSNR	24.28	23.94	24.58
相関係数	0.991	0.991	0.992

(2) 再生画像 A' (図 7.3) と秘匿画像 A (図 7.4) の PSNR および相関係数を測定する。その結果が表 7.2 である。

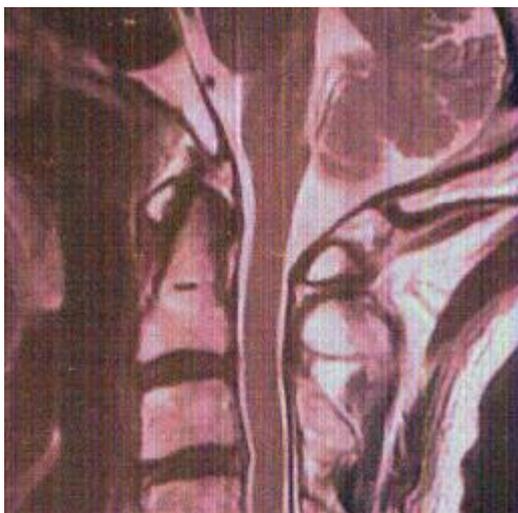


図 7.3 再生画像

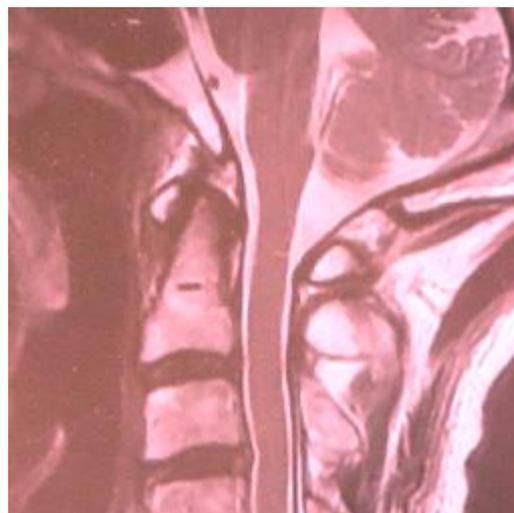


図 7.4 秘匿画像

表 7.2 再生画像と秘匿画像の PSNR と相関係数

	赤色	緑色	青色
PSNR	11.58	16.15	15.59
相関係数	0.967	0.968	0.968

(3) 再生文書の測定は再生した文字で確認する。再生文書には秘匿文書「Sasaki Takayuki (male) Aomori (0173-**-****) Good-feeling (cold)」が図 7.5 の赤色枠内に示すように空白も含めて正確に再生されている。



図 7.5 再生文書

実験で制作した二重情報ハイディング画像を評価する。評価方法は参考論文[C]の場合と比較する。比較する項目は相関係数のみとする。理由は参考論文[C]では相関係数だけで評価しているからである。その比較を表 7.3 に示す。ただし、参考論文[C]における画像の画素数は 128×128 ピクセルである。

表 7.3 二重情報ハイディング画像とカギ画像の相関係数の比較

	赤色	緑色	青色
本論文の場合の 二重情報ハイディング画像と カギ画像の相関係数	0.991	0.991	0.992
参考論文[C]の場合の 二重情報ハイディング画像と カギ画像の相関係数	0.933	0.934	0.942

よって、二重情報ハイディング画像の画質は参考論文[C]の場合より平均55/1000だけ向上している。なお、参考論文[C]ではビットプレーンを転置していない。

次に、実験で再生した再生画像を評価する。評価方法は参考論文[C]の場合と比較する。比較する項目は相関係数のみである。その比較を表 7.4 に示す。

表 7.4 再生画像と秘匿画像の相関係数の比較

	赤色	緑色	青色
本論文の場合の 再生画像と秘匿画像 の相関係数	0.967	0.968	0.968
参考論文[C]の場合の 再生画像と秘匿画像の 相関係数	0.970	0.970	0.971

よって、再生画像の画質は参考論文[C]の場合より平均3/1000だけ劣化している。しかし、画素数の違いを考慮すると差異があるとは言えないだろう。

7.2 改ざん実験の測定と評価

二重情報ハイディング画像が伝達途中で改ざんを受けた場合、再生画像にどのような改ざん痕跡が現れるかを実験し測定と評価を行う。

(1) 改ざん痕跡の現れ方

改ざん痕跡の現れ方を、再生画像の場合と再生文書の場合に分けて以下に述べる。

(a) 再生画像の場合

二重情報ハイディング画像 H の位置 i 行 j 列の 1 画素が改ざんを受けると、その影響が再生画像にどのように現れるかを求めてみる。二重情報ハイディング画像 H_{ij} 、ホログラム画像 G_{ij} 、カギ画像 K_{ij} の関係式は次式である。

$$G_{ij} = H_{ij} - \frac{256-2^{D+1}}{255} K_{ij} \quad (7.1)$$

また、 G_{ij} は転置後量子化画像 Q_{ij} 、サイファ画像 C_{ij} を用いると次式で表される。

$$G_{ij} = Q_{ij} \times 2 + C_{ij} \quad (7.2)$$

したがって、二重情報ハイディング画像が ΔH_{ij} 変化すると、転置後量子化画像 Q が受ける影響は次式になる。

$$\Delta H_{ij} = \Delta(Q_{ij} \times 2 + C_{ij}) \quad (7.3)$$

これを再生すると、再生画像には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、転置後量子化画像に変化 ΔQ_{mn} が発生したとする。この変化は式(6.7)、式(6.8)、式(6.9)を介して展開係数に変化 $\Delta a'_{mn}$ を与え、その変化が式(6.14)を介して再生画像に与える。よって、再生画像の変化 $\Delta A'_{ij}$ は

$$\Delta A'_{ij} = \varphi_m(i) \varphi_n(j) \Delta a'_{mn} \quad (7.4)$$

になる。すなわち、再生画像には正規直交関数 $\varphi_m(i)$ の形状が現れることになる。

(b) 再生文書の場合

二重情報ハイディング画像 H 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、サイファ画像 C_{ij} は式(7.3)の影響を受ける。

これを再生すると、再生文書に改ざん痕跡が現れる。たとえば、ビットプレーン 0 上の位置 i 行 j 列の画素値が改ざんを受け、0 が 1 に、あるいは 1 が 0 に変化すると、再生されるアスキー文字は変化を受ける。したがって、再生文書の文字は秘匿文書と異なる文字に変化する。

(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(a)」と正方形に塗りつぶす「実験(b)」,そしてビットプレーン0の1ビットを改ざんする「実験(c)」である。以降,画素値の表現を(赤色, 緑色, 青色)の形式で記述する。

「実験(a)」 1画素改ざん実験

改ざん画素値が異なる場合の実験(a-1)と実験(a-2)を行う。改ざん位置は両方とも128行128列とする。ただし, $D = 5$ であるから式(6.13)の $H = G + (256 - 2^{D+1})K/255$ の第2項は $192K/255$ になる。そして, 位置128行128列における $192K/255$ の画素値は (51, 54, 37) である。

実験(a-1): 二重情報ハイディング画像 $H_{128,128} = (83, 90, 73)$ を(114,117,100)に改ざんする実験

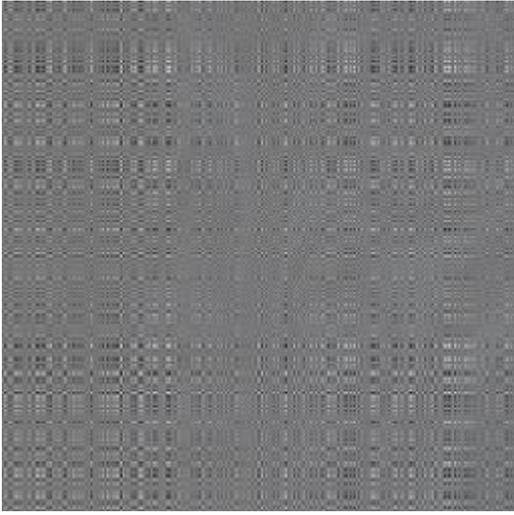
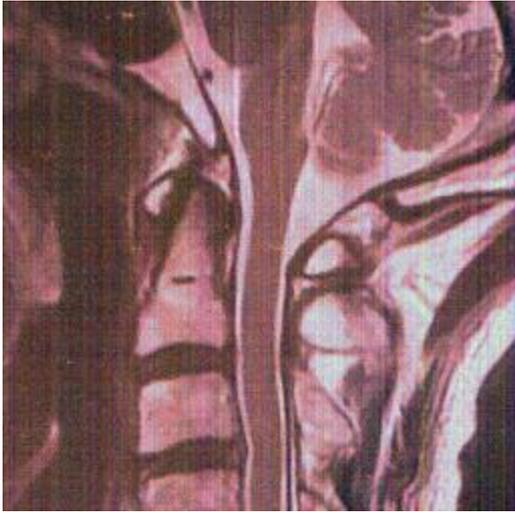
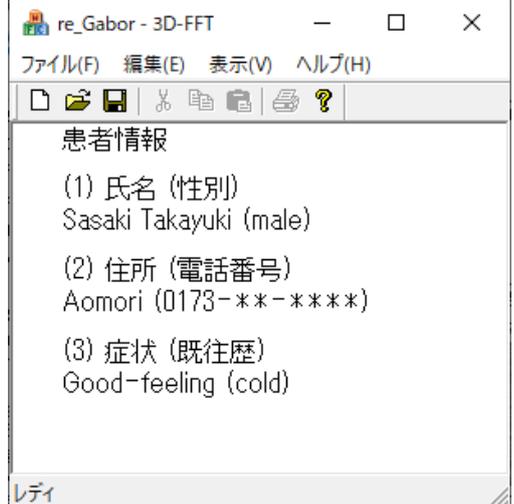
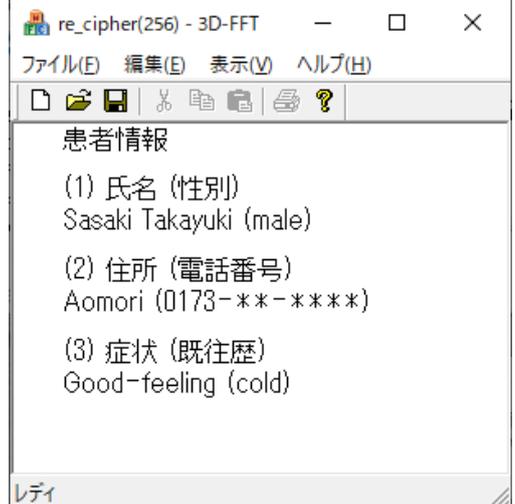
これは, $192/255$ 倍したカギ画像の画素値 (51, 54, 37) を引き算すると, ホログラム画像 G の画素値 $G_{128,128}$ が $G_{128,128} = (63, 63, 63)$ に変化する場合である。言い換えると, $G_{128,128}$ が2層構造の画素空間における最大値63に改ざんされる場合である。この実験結果の再生画像と再生文書を表7.5の第2列に示す。

実験(a-2): 二重情報ハイディング画像 $H_{128,128} = (83, 90, 73)$ を(115,118,101)に改ざんする実験

これは, $192/255$ 倍したカギ画像の画素値 (51, 54, 37) を引き算すると, ホログラム画像 G の画素値 $G_{128,128}$ が $G_{128,128} = (64, 64, 64)$ に変化する場合である。つまり, $G_{128,128}$ が2層構造の画素空間における最大値63を1だけ超えた改ざん値になる場合である。この実験結果の再生画像と再生文書を表7.5の第3列に示す。

表 7.5 1画素改ざんの実験(a-1)と実験(a-2)の結果

	実験(a-1) 二重情報ハイディング画像の画素値を (83,90,73)から(114,117,100)に改ざん	実験(a-2) 二重情報ハイディング画像の画素値を (83,90,73)から(115,118,101)に改ざん
改ざん位置 128行128列 (赤○印内)		

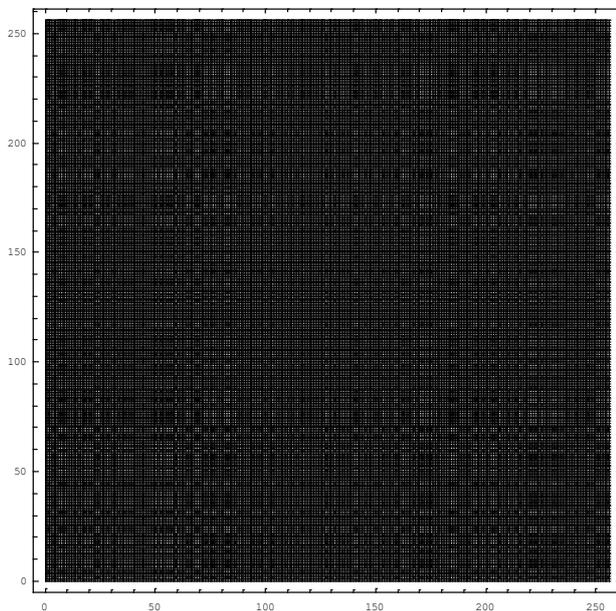
<p>再生画像 および 秘匿画像(図 7.4)に対する PSNR と 相関係数</p>	 <p>PSNR=(8.93,14.93,13.27) 相関係数=(0.089,0.093,0.116)</p>	 <p>PSNR=(11.58,16.15,15.59) 相関係数=(0.967,0.968,0.968)</p>
<p>再生文書</p>		

この実験結果は、改ざん画素値が次式を満たすならば、改ざんの影響はほとんど再生画像に現れない
ということを示している。

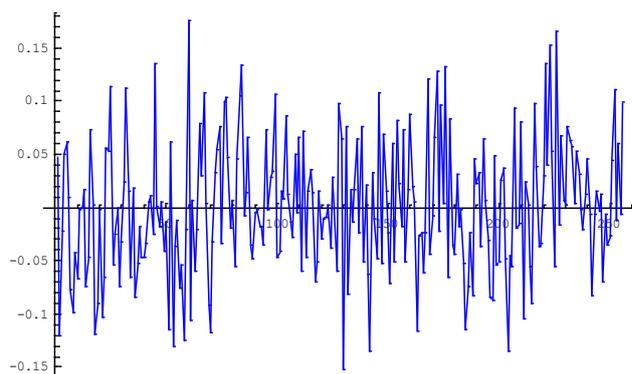
$$(\text{改ざん画素値}) - (192/255 \text{倍したカギ画像の画素値}) \geq 64 \quad (7.5)$$

すなわち、画素値が大きな数値の改ざん攻撃に対しては強い耐性をもつということである。

ここで表 7.5 の実験(a-1)欄の再生画像についてもう少し述べる. この実験は 128 行 128 列の画素値を改ざんした実験である. それゆえに, 再生画像には式(7.4)から 2 つの正規直交関数による画像 $\varphi_{128}(i)\varphi_{128}(j)$ の模様痕跡が現れている. 2 つの正規直交関数系による画像 $\varphi_{128}(i)\varphi_{128}(j)$ そのものと正規直交関数 $\varphi_{128}(i)$ のグラフをそれぞれ図 7.6 の(a), (b)に示す.



(a) 2 つの正規直交関数 $\varphi_{128}(i)\varphi_{128}(j)$ による画像



(b) 正規直交関数 $\varphi_{128}(i)$ のグラフ

図 7.6 画像 $\varphi_{128}(i)\varphi_{128}(j)$ と正規直交関数 $\varphi_{128}(i)$ グラフ

1 画像改ざんによる痕跡が 2 つの正規直交関数の模様になることを, 参考のために, 参考論文[B]の場合の改ざん例で示す. 参考論文[B]は, 2 つの異なる正規直交関数系として奇数列に Haar 関数系, 偶数列に選点正規直交多項式を用いて二重情報ハイディング画像を制作している.

二重情報ハイディング画像の奇数列 11 行 121 列の画素値を画素値(255,255,255)に改ざんした場合の改ざん痕跡が図 7.7 (a)である. Haar 関数で構成された長方形が出現している. 一方, 偶数列 23 行 18 列の画素値を画素値(255,255,255)に改ざんした場合の改ざん痕跡が図 7.7 (b)である. 選点正規直交多項式で構成された格子的な模様が現れているのがわかる.



(a) Haar 関数による長方形



(b) 直交多項式による格子状模様

図 7.7 参考論文[B]の場合の 1 画素改ざん痕跡

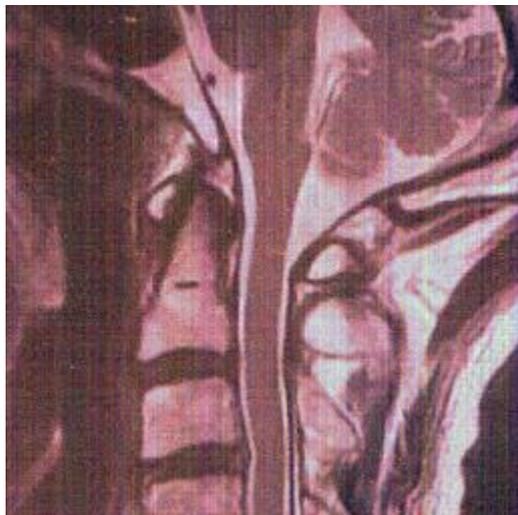
「実験(b)」 正方形に塗りつぶす実験

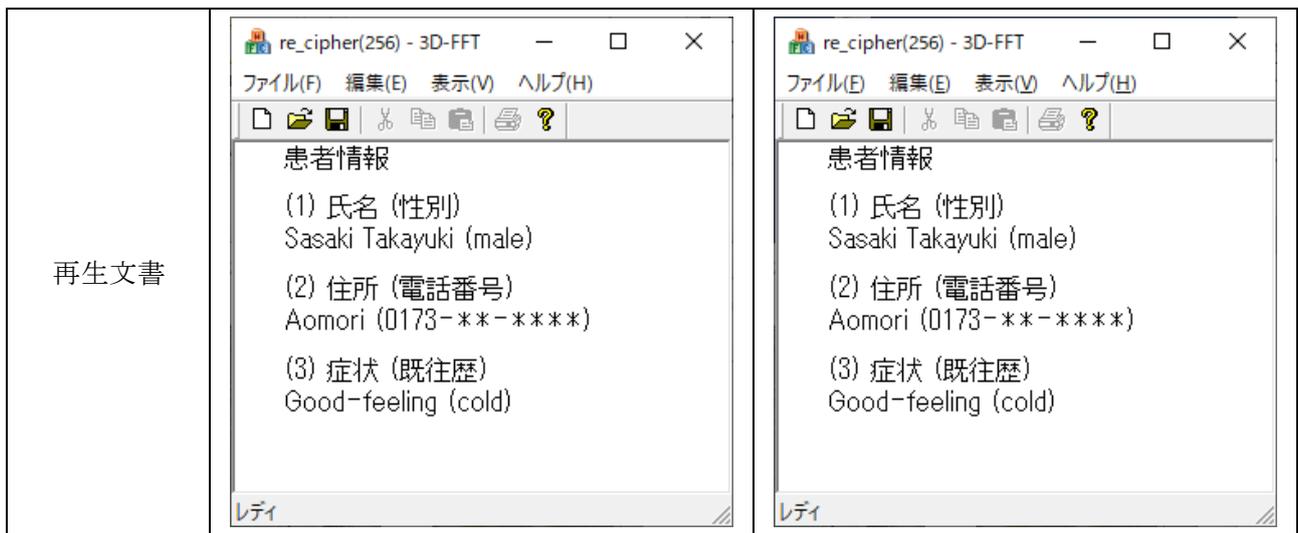
塗りつぶす色が異なる場合の実験(b-1)と実験(b-2)を行う。塗りつぶす色はそれぞれ白色と黒色とする。

実験(b-1)： 二重情報ハイディング画像を白色正方形に塗りつぶす実験

実験結果を表 7.6 に示す。この実験で使用したカギ画像は 2 つある。式(6.13)の $(256 - 2^{D+1}) K/255$ の値を $192 K/255$ とする場合と、 $191 K/255$ とする場合である。前者の場合を表 7.6 の第 2 列に、後者の場合を第 3 列に示す。

表 7.6 白色正方形に塗りつぶす実験(b-1)の結果

	192 K/255 とする場合	191 K/255 とする場合
塗りつぶした部分 (位置 127 行 127 列を中心 に左右上下± 15 画素)		
再生画像 および 秘匿画像(7.4) に対する PSNR と 相関係数	 PSNR=(11.75,15.64,16.09) 相関係数=(0.963,0.104,0.964)	 PSNR=(11.75,16.00,16.09) 相関係数=(0.963,0.964,0.964)



実験(b-1)の結果は、カギ画像の画素値範囲は 0~255 であるから

$$(白色改ざん画素値 255) - (192/255倍したカギ画像) \geq 63 \quad (7.6)$$

である。したがって位置によっては 2 層構造の最大値 63 の画素値になることがある。

しかし、実験(b-2)の結果は

$$(白色改ざん画素値 255) - (191/255倍したカギ画像) \geq 64 \quad (7.7)$$

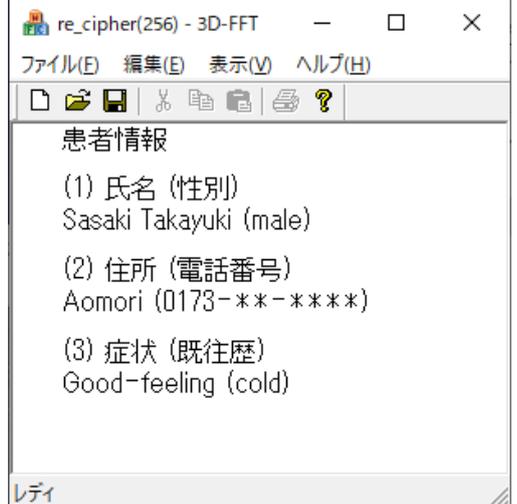
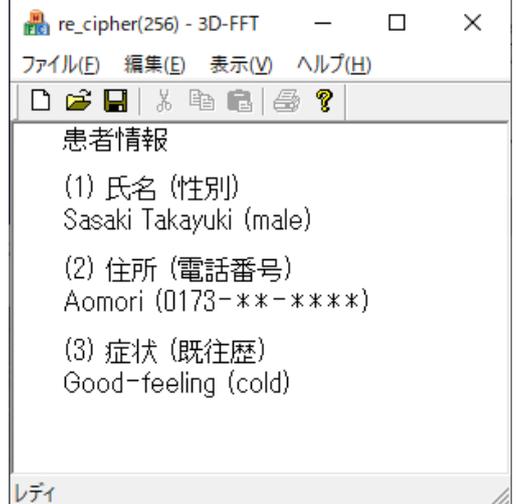
である。よって、大きな数値の改ざんには強い耐性をもつことが確認できる。

実験(b-2)： 二重情報ハイディング画像を黒色正方形に塗りつぶす実験

実験結果を表 7.7 に示す。この実験で使用したカギ画像は 2 つある。式(6.13)の $(256 - 2^{D+1}) K/255$ の値を $192 K/255$ とした場合と、 $191 K/255$ とした場合の 2 つである。前者の場合を表 7.7 の第 2 列に、後者の場合を第 3 列に示す。

表 7.7 黒色正方形に塗りつぶす実験(b-2)の結果

	192 K/255 とする場合	191 K/255 とする場合
塗りつぶした部分 (位置 127 行 127 列を中心 に左右上下± 15 画素)		

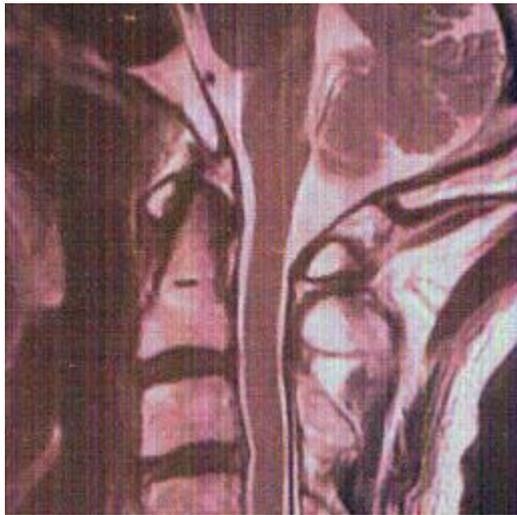
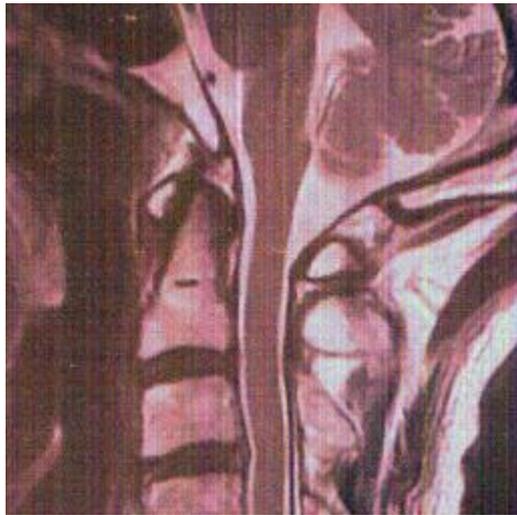
<p>再生画像 および 秘匿画像(7.4) に対する PSNR と 相関係数</p>	 <p>PSNR=(11.75,16.00,16.09) 相関係数=(0.963,0.964,0.964)</p>	 <p>PSNR=(11.75,16.00,16.09) 相関係数=(0.963,0.964,0.964)</p>
<p>再生文書</p>	 <p>患者情報 (1) 氏名 (性別) Sasaki Takayuki (male) (2) 住所 (電話番号) Aomori (0173-**-****) (3) 症状 (既往歴) Good-feeling (cold)</p>	 <p>患者情報 (1) 氏名 (性別) Sasaki Takayuki (male) (2) 住所 (電話番号) Aomori (0173-**-****) (3) 症状 (既往歴) Good-feeling (cold)</p>

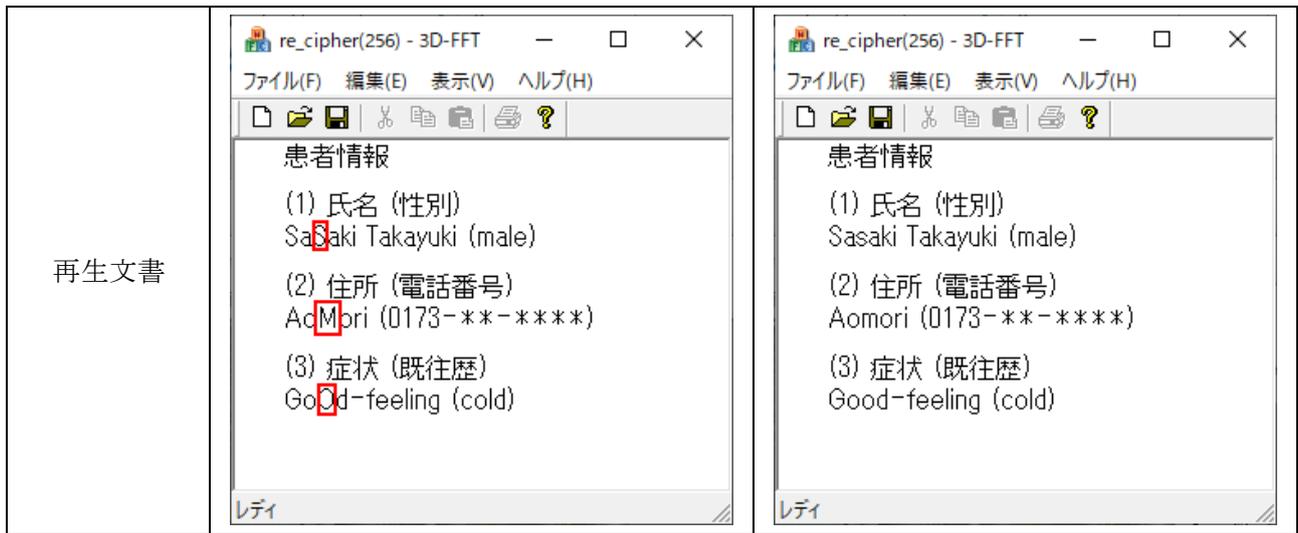
黒色に塗りつぶす実験結果は、どちらの改ざんであっても、改ざんには強い耐性をもつことが確認できる。

「実験(c)」 ビットプレーン0の1ビット改ざん実験

ビットプレーン0の1ビットだけを改ざんする実験である。実験は二重情報ハイディング画像の位置1行19列の画素値(83,93,41)を画素値(0,0,0)に改ざんする。すなわち、ビットプレーン0の画素値を(1,1,1)から(0,0,0)に改ざんする実験である。その結果を表7.8に示す。

表 7.8 ビットプレーン0の1ビット改ざん実験(c)の結果

	改ざん後	改ざん前
改ざん位置 (位置1行19列(赤○印内))		
再生画像 および 秘匿画像(7.4) に対する PSNR と 相関係数	 PSNR=(11.44,16.13,15.76) 相関係数=(0.967,0.968,0.968)	 PSNR=(11.59,16.16,15.60) 相関係数=(0.967,0.968,0.968)



改ざん痕跡が表 7.8 の第 2 列の再生文書に現れている。赤色四角内のアスキー文字が小文字から大文字に変化している。ビットプレーン 0 の 1 ビット改ざんはアスキーコードを容易に改変できる。したがって、ステガノグラフィ領域は改ざんに対する耐性が弱い領域である。逆にみると、この領域は改ざんに対して敏感な領域になる。

7.3 ビットプレーン転置効果の検証

ビットプレーン転置がある場合とビットプレーン転置がない場合を比較する。そして、ビットプレーン転置がある場合の方が2点において有益であることを検証する。1点は大改ざん痕跡を残す画素値を1カ所に集約できること、もう1点は二重情報ハイディング画像を高画質化できることである。

この実験で述べているビットプレーン転置とはビットプレーンを次のように移し替えることを指す。秘匿画像の量子化画像のビットプレーン4をビットプレーン0に移し替える、ビットプレーン0をその上のビットプレーン1に移し替える、ビットプレーン1をその上のビットプレーン2に移し替える、ビットプレーン2をビットプレーン3に移し替える、そしてビットプレーン3をビットプレーン4に移し替えることである。その様子を図7.7に示す。すなわち、画素値 $n_4 \times 2^4 + \dots + n_1 \times 2^1 + n_0 \times 2^0$ はビットプレーンを転置することによって画素値 $n_3 \times 2^4 + \dots + n_0 \times 2^1 + n_4 \times 2^0$ に変化する。ただし、 n_i ($i = 0,1,2,3,4$) は数「0」か「1」のいずれかである。なお、ビットプレーン転置の対象は秘匿画像の量子化画像のみで、秘匿文書は対象外とする。

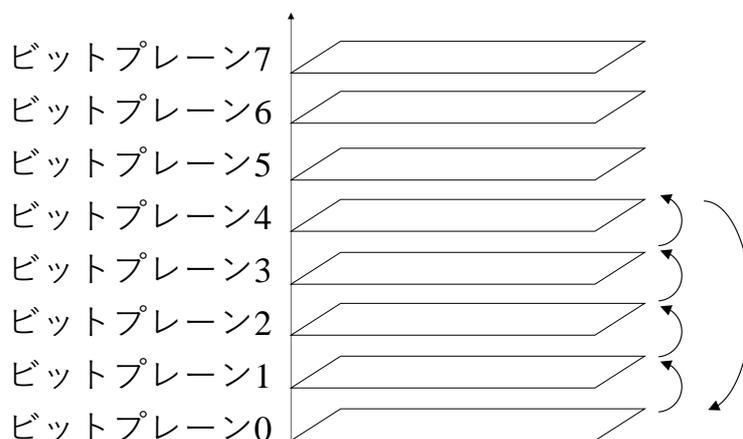


図 7.8 量子化画像のビットプレーン転置方法

(1) 大きな改ざん痕跡を残す画素値の集約化

大きな改ざん痕跡を残す画素値の集約化を調べるために、2つのホログラム画像を用意する。1つはビットプレーン転置後の転置後量子化画像とカギ画像を合成したホログラム画像で、もう1つはビットプレーン転置前の量子化画像とカギ画像を合成したホログラム画像である。それぞれの場合を区別するために添え字 *after*, *before* をそれぞれに付与する。ビットプレーン転置した場合の二重情報ハイディング画像 H_{after} は次式で表される。

$$H_{after} = G_{after} + \frac{192}{255}K \quad (7.8)$$

一方、ビットプレーン転置しない場合の二重情報ハイディング画像 H_{before} は次式で表される。

$$H_{before} = G_{before} + \frac{192}{255}K \quad (7.9)$$

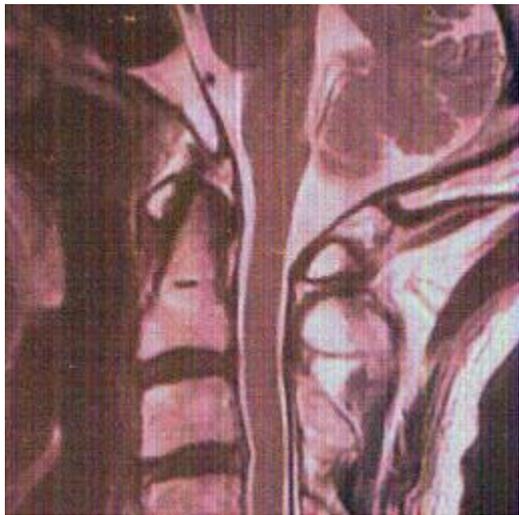
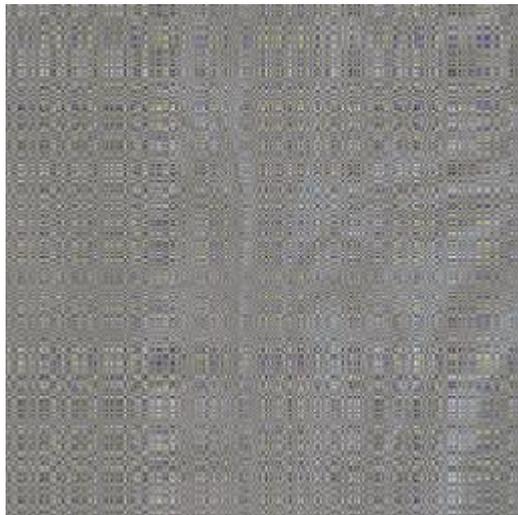
ただし、カギ画像 K はビットプレーン転置に関係しないので、添え字の付与をしていない。

位置 128 行 128 列におけるビットプレーン転置後の画素値は $H_{after,128,128} = (83,90,73)$ 、位置 128 行 128 列におけるビットプレーン転置前の画素値は $H_{before,128,128} = (67,72,55)$ 、同位置におけるカギ画像の画素値 $\frac{192}{255}K_{128,128}$ は $(51,54,37)$ である。

以上のことから、ホログラム画像を $G_{after,128,128} = G_{before,128,128} = (31,31,31)$ に改ざんするために、二重情報ハイディング画像を $H_{after,128,128} = (82,85,68)$, $H_{before,128,128} = (82,85,68)$ に改ざんする。

その改ざんの実験結果を表 7.9 に示す。第 2 列がビットプレーン転置後の場合で、第 3 列がビットプレーン転置前の場合である。

表 7.9 ビットプレーン転置の前・後における再生画像と再生文書

	ビットプレーン転置後の場合	ビットプレーン転置前の場合
二重情報ハイディング画像 (位置 128 行 128 列(赤○印 内))		
再生画像 および 秘匿画像(7.4) に対する PSNR と 相関係数	 PSNR=(11.58,16.14,15.58) 相関係数=(0.967,0.968,0.968)	 PSNR=(10.61,16.17,14.53) 相関係数=(0.248,0.264,0.312)

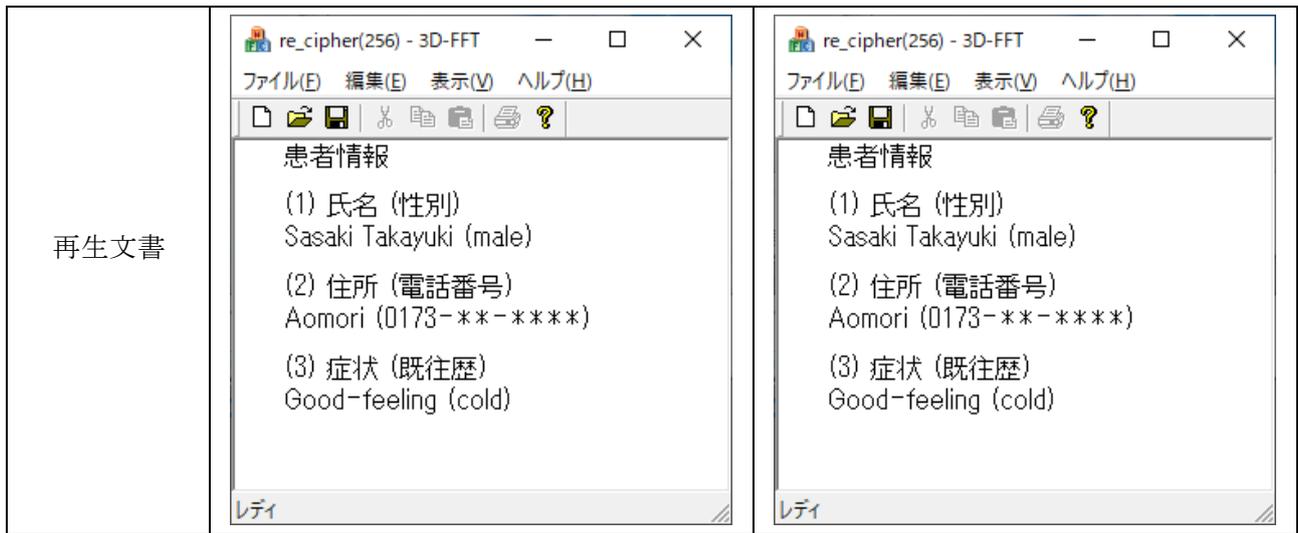


表 7.9 が示すように、ホログラム画像の位置 128 行 128 列の画素が (31, 31, 31) になるように二重情報ハイディング画像の画素値を改ざんすると、ビットプレーン転置前の場合は再生画像に改ざん痕跡が大きく現れている。しかし、ビットプレーン転置後の場合は改ざん影響が現れていない。これはビットプレーンを転置することによって改ざん影響が大きく現れる領域が集約化するからである。その理由を、節 5.1 で概説的に述べているが、ここでは実験で考察してみる。

ビットプレーンを転置することによって量子化特性は図 7.9 の(a)から(b)に変わる。横軸は転置前と同じままであるが、量子化画像が埋め込められる第 2 層の縦軸の画素値の順番が変わる。図 7.9 (a)では負の展開係数 a の量子化係数 qa は $\{2,4,6,\dots,31\}$ の整数値で、正の展開係数 a の量子化係数 qa は $\{32,34,36,\dots,63\}$ の整数値である。しかし、図 7.9 (b)では負の展開係数 a の量子化係数 qa は $\{4,8,12,\dots,60\}$ の整数値に、正の展開係数 a の量子化係数 qa は $\{2,6,10,\dots,62\}$ の整数値に置き換わる。

したがって、ビットプレーン転置前の量子化特性を逆演算したグラフと、ビットプレーン転置後の量子化特性を逆演算したグラフも異なる。それぞれのグラフを図 7.10 の(a), (b)に示す。展開係数 a の絶対値が大きい領域が図 7.9 (a)では 2 ヶ所あるが、(b)では 1 ヶ所に集約化されている。

したがって、ホログラム画像の画素値が(31,31,31)に変化すると、ビットプレーン転置前の場合には大きな展開係数になるため、再生画像に大きな改ざん痕跡が現れる。しかし、ビットプレーン転置後の場合には展開係数が小さな変化であるため、大きな改ざん痕跡は現れないことになる。これがビットプレーン転置の効果の 1 つである。

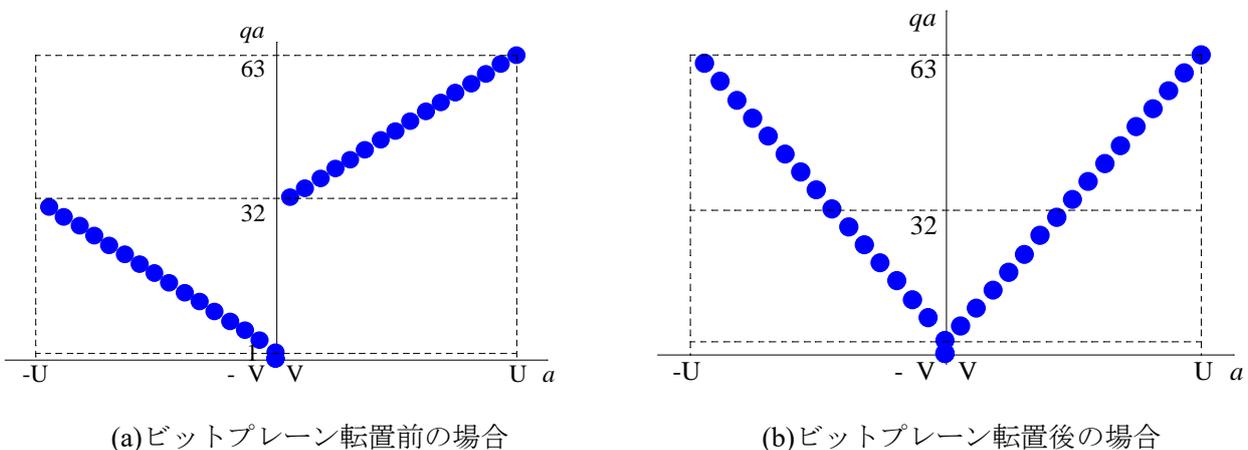
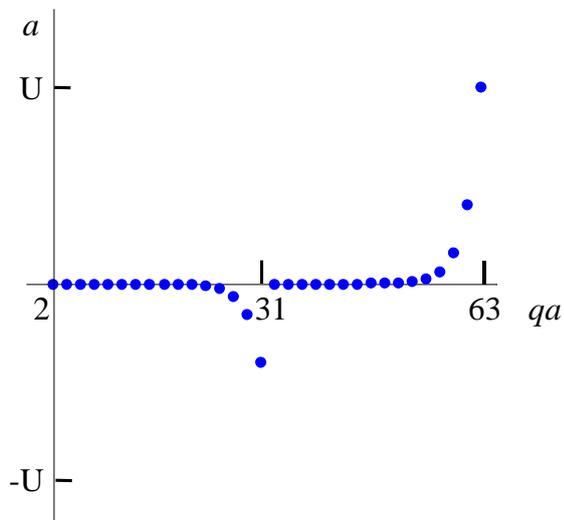
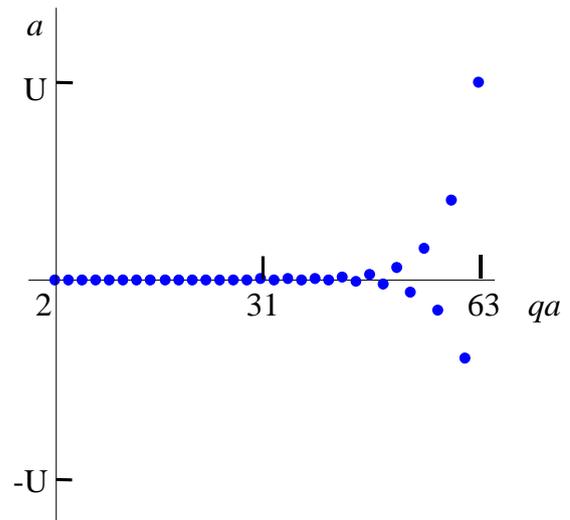


図 7.9 ビットプレーン転置前後の量子化特性



(a)ビットプレーン転置前の場合



(b)ビットプレーン転置後の場合

図 7.10 ビットプレーン転置前・後の量子化特性の逆演算グラフ

次に、量子化係数 qa に対する再生画像の PSNR および相関係数を実験測定する。実験方法は次の通り。

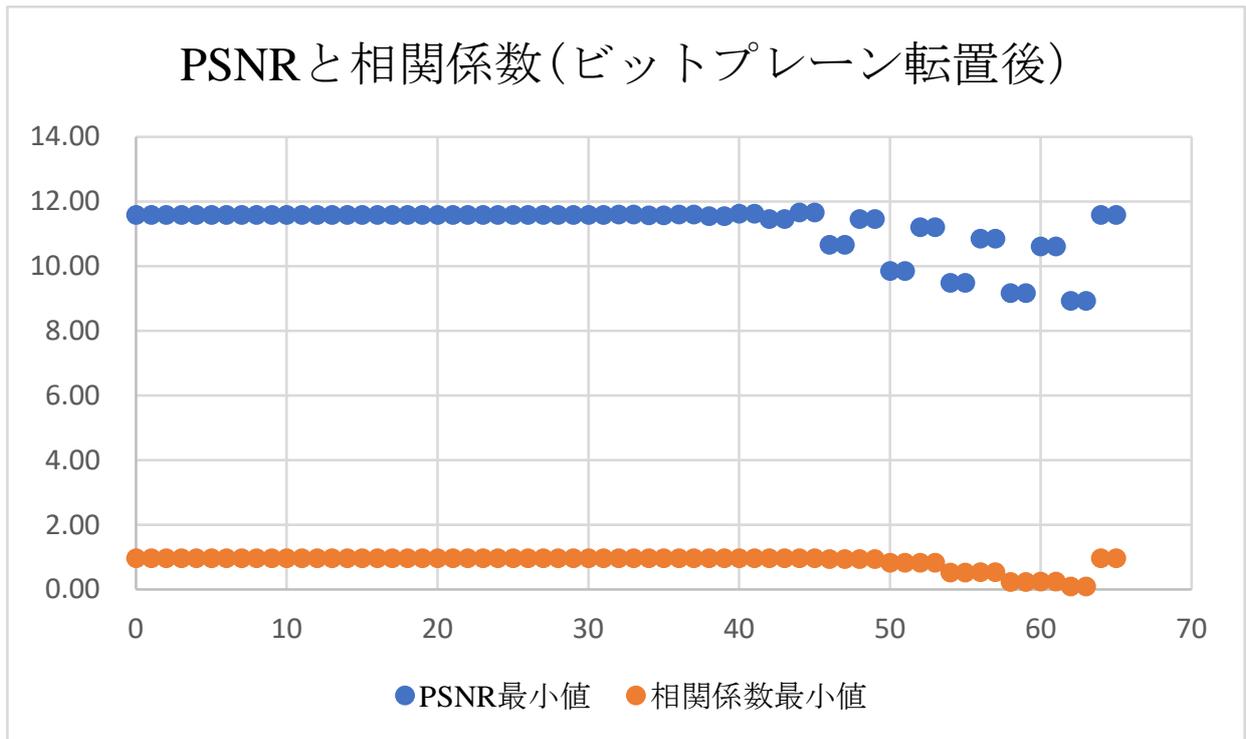
- ①転置後量子化画像の位置 128 行 128 列の画素値(32,36,36)を(0,0,0)～(65,65,65)に順に変える
- ②それぞれの画素値における秘匿画像(図 7.4)に対する再生画像の PSNR と相関係数を測定する

ビットプレーン転置後の場合における測定結果を図 7.11 (a)に示す。ビットプレーン転置前の場合における測定結果を図 7.11 (b)に示す。グラフの横軸は量子化係数 qa 、縦軸は PSNR または相関係数である。ただし、グラフはいずれも赤色、緑色、青色の 3 色中の最小値で表す。色ごとの測定値は表 7.10, 表 7.11 にそれぞれ表す。

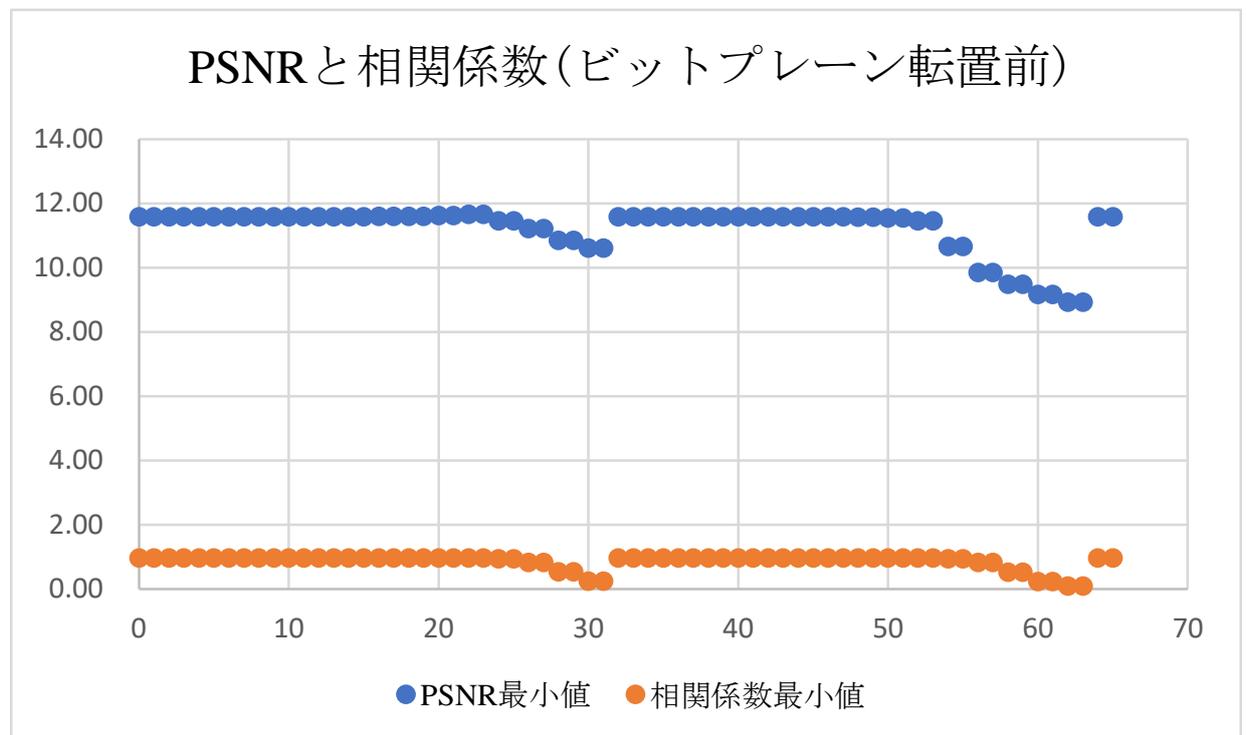
以上から、改ざん痕跡が強く現れる部分が

- ①ビットプレーン転置前では 2 ヲ所あること
- ②ビットプレーン転置後では 1 ヲ所あること

を確認することができる。



(a)ビットプレーン転置後の場合



(b)ビットプレーン転置前の場合

図 7.11 ビットプレーン転置前および後における量子化係数に対する PSNR または相関係数

表 7.10 ビットプレーン転置後の場合における量子化係数に対する PSNR または相関係数

qa	PSNR				相関係数			
	red	green	blue	PSNR最小値	red	green	blue	相関係数最小値
0	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
1	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
2	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
3	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
4	11.58	16.14	15.58	11.58	0.967	0.968	0.968	0.967
5	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
6	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
7	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
8	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
9	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
10	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
11	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
12	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
13	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
14	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
15	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
16	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
17	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
18	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
19	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
20	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
21	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
22	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
23	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
24	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
25	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
26	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
27	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
28	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
29	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
30	11.58	16.14	15.58	11.58	0.967	0.968	0.968	0.967
31	11.58	16.14	15.58	11.58	0.967	0.968	0.968	0.967
32	11.59	16.15	15.59	11.59	0.967	0.968	0.968	0.967
33	11.59	16.15	15.59	11.59	0.967	0.968	0.968	0.967
34	11.57	16.13	15.57	11.57	0.967	0.968	0.968	0.967
35	11.57	16.13	15.57	11.57	0.967	0.968	0.968	0.967
36	11.60	16.16	15.60	11.60	0.967	0.968	0.968	0.967
37	11.60	16.16	15.60	11.60	0.967	0.968	0.968	0.967
38	11.54	16.11	15.54	11.54	0.966	0.967	0.968	0.966
39	11.54	16.11	15.54	11.54	0.966	0.967	0.968	0.966
40	11.62	16.18	15.64	11.62	0.967	0.968	0.968	0.967
41	11.62	16.18	15.64	11.62	0.967	0.968	0.968	0.967
42	11.46	16.02	15.23	11.46	0.962	0.963	0.965	0.962
43	11.46	16.02	15.23	11.46	0.962	0.963	0.965	0.962
44	11.66	16.19	16.36	11.66	0.963	0.965	0.966	0.963
45	11.66	16.19	16.36	11.66	0.963	0.965	0.966	0.963
46	10.66	16.46	15.58	10.66	0.938	0.941	0.950	0.938
47	10.66	16.46	15.58	10.66	0.938	0.941	0.950	0.938
48	11.46	18.13	17.02	11.46	0.942	0.946	0.953	0.942
49	11.46	18.13	17.02	11.46	0.942	0.946	0.953	0.942
50	9.85	16.95	15.36	9.85	0.820	0.832	0.870	0.820
51	9.85	16.95	15.36	9.85	0.820	0.832	0.870	0.820
52	11.21	18.84	17.04	11.21	0.828	0.843	0.878	0.828
53	11.21	18.84	17.04	11.21	0.828	0.843	0.878	0.828
54	9.48	16.15	14.38	9.48	0.518	0.538	0.612	0.518
55	9.48	16.15	14.38	9.48	0.518	0.538	0.612	0.518
56	10.85	17.39	15.57	10.85	0.531	0.556	0.626	0.531
57	10.85	17.39	15.57	10.85	0.531	0.556	0.626	0.531
58	9.17	15.38	13.65	9.17	0.232	0.244	0.295	0.232
59	9.17	15.38	13.65	9.17	0.232	0.244	0.295	0.232
60	10.61	16.17	14.53	10.61	0.248	0.264	0.312	0.248
61	10.61	16.17	14.53	10.61	0.248	0.264	0.312	0.248
62	8.93	14.93	13.27	8.93	0.089	0.093	0.116	0.089
63	8.93	14.93	13.27	8.93	0.089	0.093	0.116	0.089
64	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
65	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967

(注意) 改ざん位置は128行128列

表 7.11 ビットプレーン転置前の場合における量子化係数に対する PNSR または相関係数

qa	PSNR				相関係数			
	red	green	blue	PSNR最小値	red	green	blue	相関係数最小値
0	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
1	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
2	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
3	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
4	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
5	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
6	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
7	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
8	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
9	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
10	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
11	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
12	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
13	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
14	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
15	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
16	11.59	16.15	15.59	11.59	0.967	0.968	0.968	0.967
17	11.59	16.15	15.59	11.59	0.967	0.968	0.968	0.967
18	11.60	16.16	15.60	11.60	0.967	0.968	0.968	0.967
19	11.60	16.16	15.60	11.60	0.967	0.968	0.968	0.967
20	11.62	16.18	15.64	11.62	0.967	0.968	0.968	0.967
21	11.62	16.18	15.64	11.62	0.967	0.968	0.968	0.967
22	11.66	16.19	16.36	11.66	0.963	0.965	0.966	0.963
23	11.66	16.19	16.36	11.66	0.963	0.965	0.966	0.963
24	11.46	18.13	17.02	11.46	0.942	0.946	0.953	0.942
25	11.46	18.13	17.02	11.46	0.942	0.946	0.953	0.942
26	11.21	18.84	17.04	11.21	0.828	0.843	0.878	0.828
27	11.21	18.84	17.04	11.21	0.828	0.843	0.878	0.828
28	10.85	17.39	15.57	10.85	0.531	0.556	0.626	0.531
29	10.85	17.39	15.57	10.85	0.531	0.556	0.626	0.531
30	10.61	16.17	14.53	10.61	0.248	0.264	0.312	0.248
31	10.61	16.17	14.53	10.61	0.248	0.264	0.312	0.248
32	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
33	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
34	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
35	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
36	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
37	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
38	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
39	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
40	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
41	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
42	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
43	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
44	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
45	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
46	11.58	16.14	15.58	11.58	0.967	0.968	0.968	0.967
47	11.58	16.14	15.58	11.58	0.967	0.968	0.968	0.967
48	11.57	16.13	15.57	11.57	0.967	0.968	0.968	0.967
49	11.57	16.13	15.57	11.57	0.967	0.968	0.968	0.967
50	11.54	16.11	15.54	11.54	0.966	0.967	0.968	0.966
51	11.54	16.11	15.54	11.54	0.966	0.967	0.968	0.966
52	11.46	16.02	15.23	11.46	0.962	0.963	0.965	0.962
53	11.46	16.02	15.23	11.46	0.962	0.963	0.965	0.962
54	10.66	16.46	15.58	10.66	0.938	0.941	0.950	0.938
55	10.66	16.46	15.58	10.66	0.938	0.941	0.950	0.938
56	9.85	16.95	15.36	9.85	0.820	0.832	0.870	0.820
57	9.85	16.95	15.36	9.85	0.820	0.832	0.870	0.820
58	9.48	16.15	14.38	9.48	0.518	0.538	0.612	0.518
59	9.48	16.15	14.38	9.48	0.518	0.538	0.612	0.518
60	9.17	15.38	13.65	9.17	0.232	0.244	0.295	0.232
61	9.17	15.38	13.65	9.17	0.232	0.244	0.295	0.232
62	8.93	14.93	13.27	8.93	0.089	0.093	0.116	0.089
63	8.93	14.93	13.27	8.93	0.089	0.093	0.116	0.089
64	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967
65	11.58	16.15	15.59	11.58	0.967	0.968	0.968	0.967

(注意) 改ざん位置は128行128列

(2) 二重情報ハイディング画像の高画質化

表 7.12 はビットプレーン転置の前後における二重情報ハイディング画像，再生画像，再生文書を併記したものである。

表の中で異なる点は二重情報ハイディング画像の画質差である。ビットプレーン転置後の PSNR と相関係数の数値がビットプレーン転置前の数値より大きな数値である。このことは，ビットプレーン転置後の二重情報ハイディング画像がビットプレーン転置前のそれより高画質であることを意味する。

ここでは，ビットプレーン転置すると，なぜ二重情報ハイディング画像が高画質になるのかを考察する。節 5.2 で既に擬似乱数系列による画像を用いて概説しているが，実験に用いた画像で再度述べる。

表 7.12 ビットプレーン転・置の前後における二重情報ハイディング画像と再生画像と再生文書

	ビットプレーン転置の後	ビットプレーン転置の前
二重情報ハイディング画像 および カギ画像(図 7.2)に対する PSNR と 相関係数	 PSNR=(24.28,23.94,24.58) 相関係数=(0.991,0.991,0.992)	 PSNR=(21.93,21.82,21.69) 相関係数=(0.933,0.933,0.942)
再生画像 および 秘匿画像(図 7.4)に対する PSNR と 相関係数	 PSNR=(11.58,16.15,15.59) 相関係数=(0.967,0.968,0.968)	 PSNR=(11.58,16.15,15.59) 相関係数=(0.967,0.968,0.968)

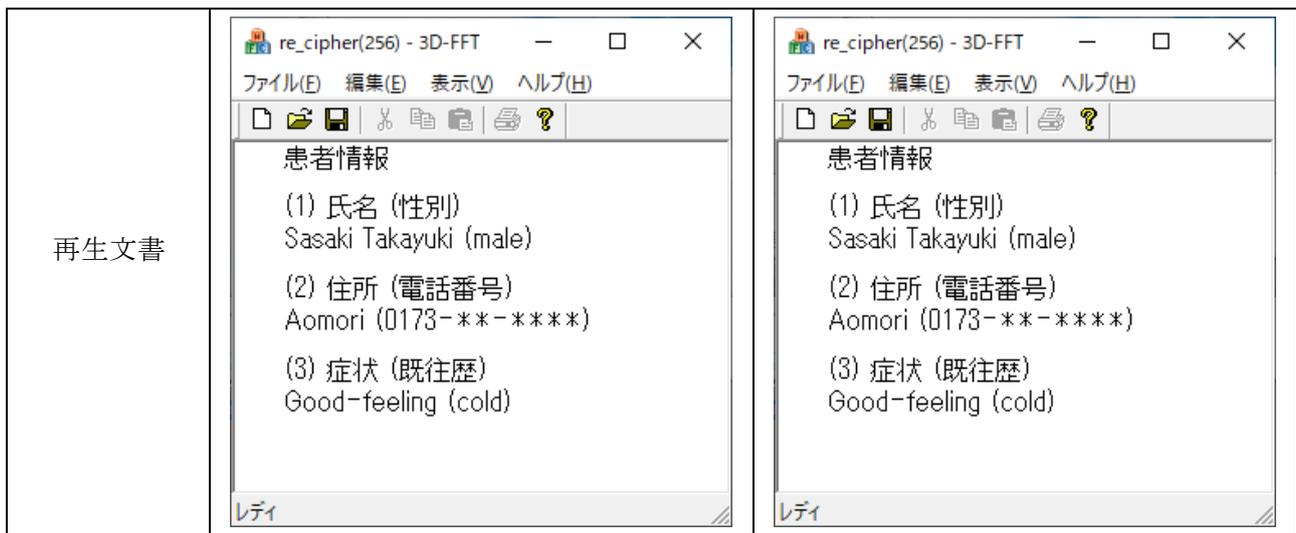


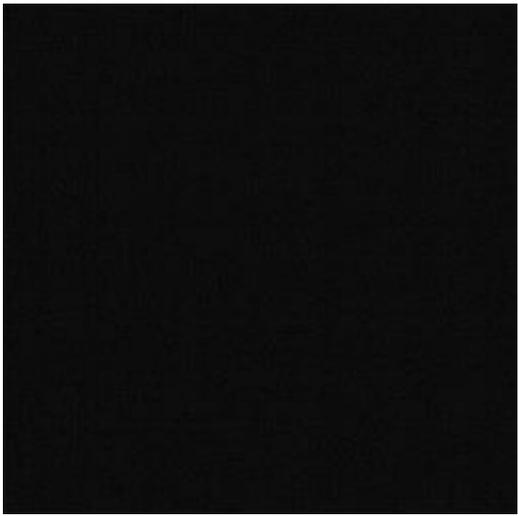
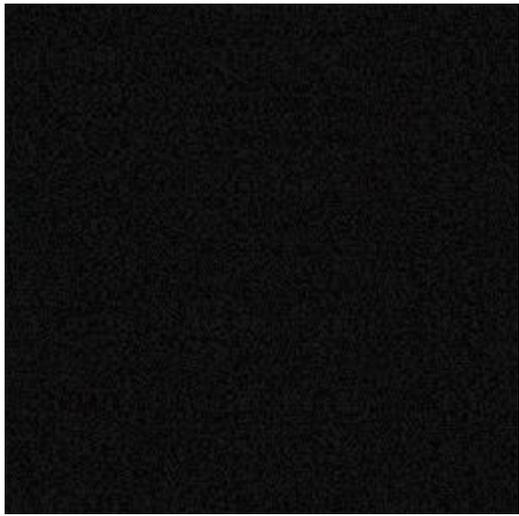
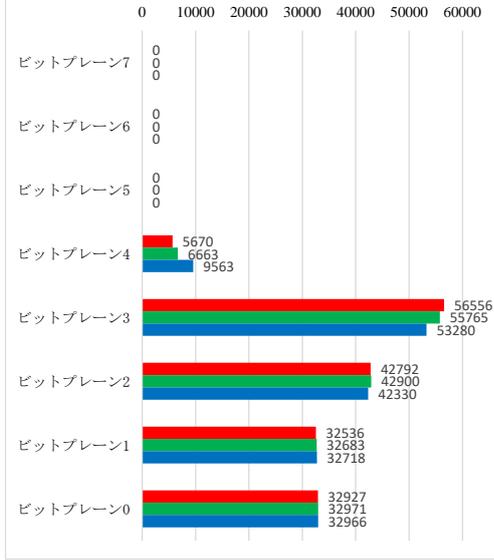
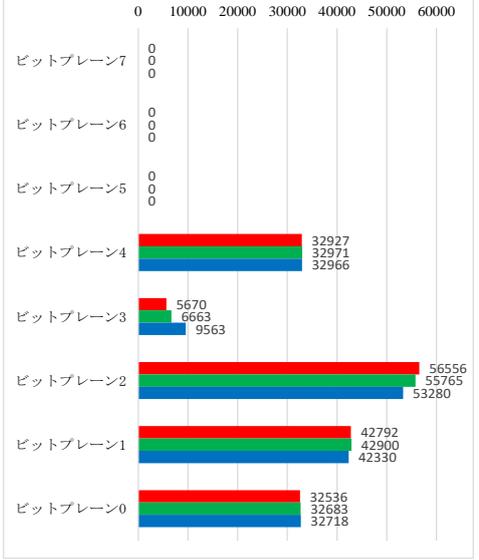
表 7.13 (a)に示す秘匿画像を正規直交関数系で展開し量子化した直後の画像(量子化画像)が図 7.13(c)で、それをさらにビットプレーン転置した画像(転置後量子化画像)が表 7.13 (b)である。転置後量子化画像と量子化画像のビットプレーンの度数を表 7.13 (d), (e)にそれぞれ示す。それらの画像をカギ画像(図 7.2)にそれぞれ埋め込めた画像が表 7.12 の二重情報ハイディング画像の左と右である。その画質差の違いは節 5.2 で述べたように表 7.13(d)と(e)の違いによるものである。そのことを二重情報ハイディング画像のビットプレーンの模様並び方で確認してみる。

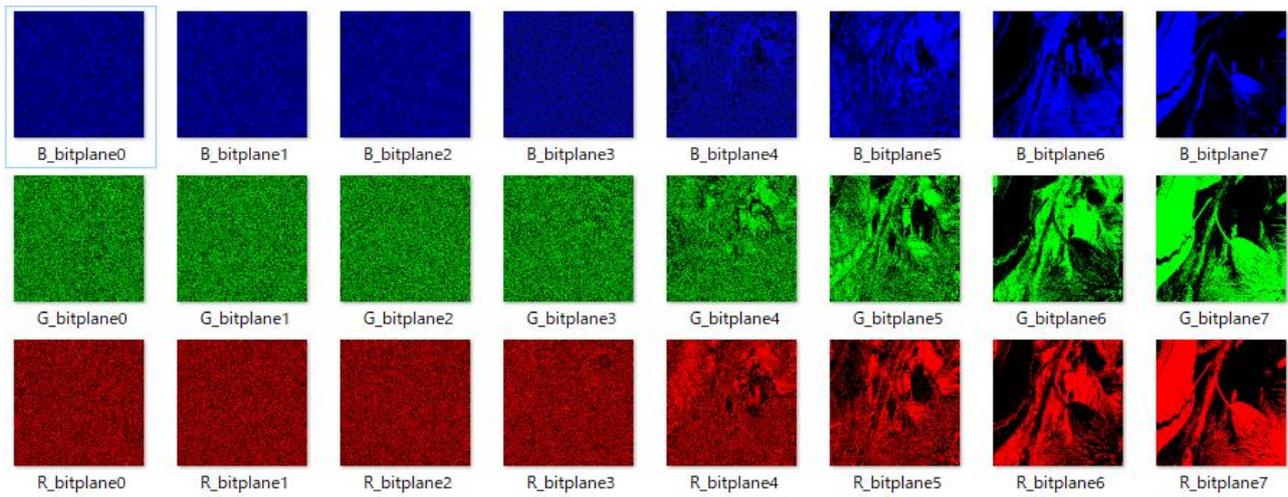
カギ画像に表 7.13(d)を埋め込めた二重情報ハイディング画像(表 7.12 左)のビットプレーンが図 7.12(a)である。表 7.13(e)を埋め込めた二重情報ハイディング画像(表 7.12 右)のビットプレーンが図 7.12(b)である。図 7.12(b)において、ランダム模様のビットプレーン 5 が、形状を有する模様の 2つのビットプレーン 4 と 6 の間に位置している。それに対して図 7.12(a)においては、左側に位置するビットプレーンほどランダム模様の模様で、右側に位置するほど形状を有する模様である。比較のため、カギ画像のビットプレーンを図 7.12(c)に示す。左側ほどランダム模様の模様で右側ほど形状を有する模様のビットプレーンである。以上のことから、高画質化の理由はビットプレーンの模様の連続性にあるといえる。

表 7.13 ビットプレーン転置の前後の度数分布と分散

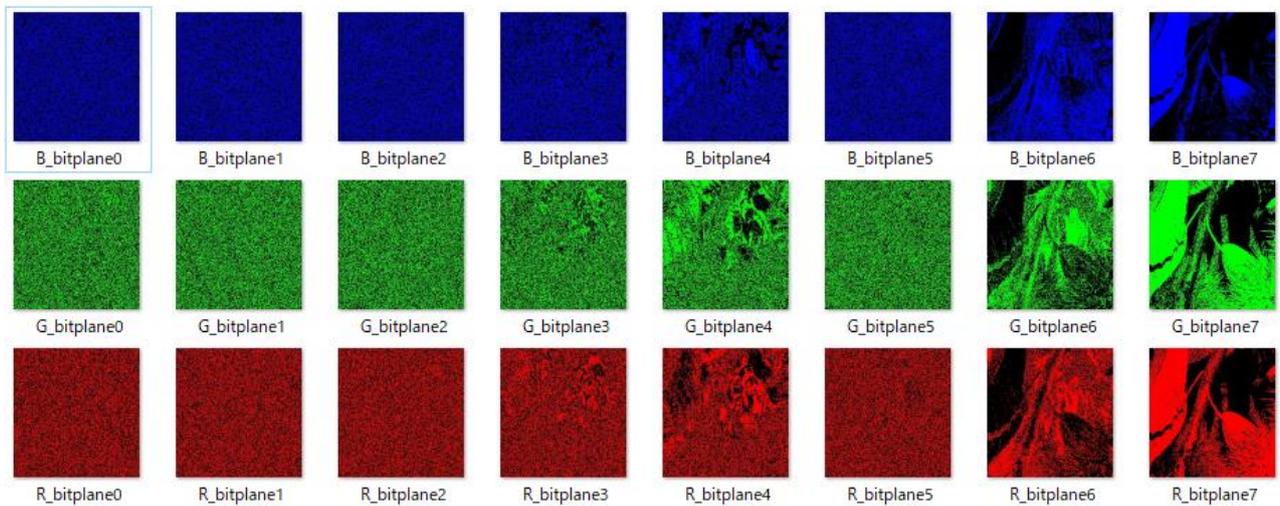
	ビットプレーン転置後	ビットプレーン転置前
秘匿画像		

(a) 秘匿画像

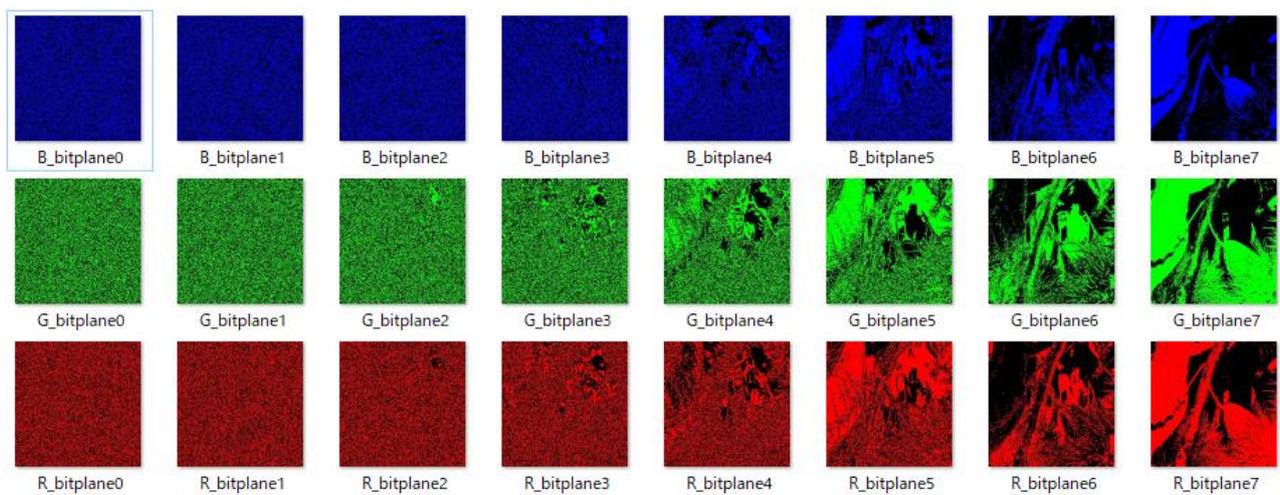
量子化画像	 <p>(b) 転置後量子化画像</p>	 <p>(c) 量子化画像(転置前)</p>
ビットプレーンの度数分布	 <p>(d)</p>	 <p>(e)</p>
分散	(6, 6, 6) (f)	(58, 58, 58) (g)
平均	(12, 12, 12) (h)	(13, 14, 14) (i)



(a) ビットプレーン転置後の二重情報ハイディング画像のビットプレーン



(b) ビットプレーン転置前の二重情報ハイディング画像のビットプレーン



(c) カギ画像(192/255倍)のビットプレーン

図 7.12 ビットプレーン転置前後の二重情報ハイディング画像とカギ画像のビットプレーン

第 8 章 結論

この論文は個人情報秘匿に大量に安全に伝達することを目的とした論文である。想定している個人情報は秘匿画像たとえば医療画像と秘匿文書たとえば患者カルテである。

この論文の独創的な特徴は 3 つある。

第 1 の特徴は画像を暗号化するために用いる正規直交関数系を擬似乱数系列から構築した点である。多くの文献で採用される正規直交関数系は超越関数グループに属する三角関数やハール関数などである。しかし、ここでは秘匿性を高めるために擬似乱数系列から構築した正規直交関数系を採用する。

第 2 の特徴は 1 枚の画像の中に大量の個人情報を埋め込むために多重の埋め込みを可能にした点である。1 枚の画像の中に多重に埋め込むことによって個人情報を大量に伝達することができる。

そして第 3 の特徴は量子化画像のビットプレーンを転置する点である。ビットプレーン転置によって、二重情報ハイディング画像を高画質化する効果を得る。これは第三者による傍受を回避するのに役立つ。また、改ざん耐性を強化にする効果を得る。しかし、この改ざん耐性の強化は秘匿画像の場合だけに適用するものであり、秘匿文書の改ざん耐性に対してはビットプレーン転置の効果はない。

制作した二重情報ハイディング画像に埋め込まれた秘匿画像は改ざんに対して耐性が強く、秘匿文書は改ざんに対しては耐性が弱い。秘匿画像が改ざんに強い理由は、秘匿画像の量子化範囲を限定して埋め込んでいるからである。改ざん画素値が量子化範囲を超えた大きな数値であるならば改ざんの影響をほとんど受けない。

それに対して、秘匿文書は改ざんに対して弱い。その理由は、ビットプレーン 0 (LSB) の 1 バイトが秘匿文書のアスキーコードと 1 対 1 対応しているため、1 ビットの書き換えがそのまま秘匿文書のアスキーコードの書き換えとなるからである。したがって、この論文の二重情報ハイディング画像は改ざん耐性が強い面と弱い面の両面をもつ画像である。

改ざん耐性が一方では強く他方では弱いという両面をもつことが有効な場合もある。それをプライバシー保護の観点からみても。想定している秘匿画像は、個人を特定できる顔写真ではなく、医療画像そのものである。したがって、第三者に傍聴されても個人が特定されるケースは少ないだろう。他方、秘匿文書は文字そのもので個人名や住所や電話番号などである場合が多く、個人が特定されやすい。

したがって、個人が特定されやすい秘匿文書が改ざんに弱いことは好都合であるといえる。また、改ざんに敏感ならば、改ざんを受けたか否かを確認するのに有益なこともある。

これまで論じてきたように情報ハイディング分野には多くの技術がある。どの技術も完全であるとはいえず一長一短がある。この論文の二重情報ハイディング画像もその通りである。長所は秘匿画像が改ざん攻撃に対して強い耐性をもつことである。とくに、改ざんの画素値が大きな数値ならば改ざんによる影響がほとんど再生画像に現れてこない点である。しかし短所としては、限られた画素空間に 2 枚の

秘匿情報を埋め込むために、一重の場合に比べてコンテンツの劣化が抑えにくい点がある。

今後は二重情報ハイディング画像および再生画像の画質をより一層に高画質にすることが望まれる。また、研究精度を向上させるためには2枚の画像の類似性を比較する新規の測定方法が求められる。相関係数やPSNR以外の有効的な比較方法の開発が急務である。たとえば、画像の輝度を用いる方法や明瞭度による比較方法などである。

最後に、これらの技術開発の集約の先端には信頼性の高い情報ハイディング技術が確立されるものと確信している。

参考論文

- [A] 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
- [B] 佐々木 隆幸, 長瀬 智行: “Constructing Digital Watermark Based on Orthogonal Functions”, 2018 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom) (China), pp.140-143, 2018
- [C] 佐々木 隆幸, 長瀬 智行: “擬似乱数系列でつくる二重情報ハイディング”, 情報処理学会論文誌, Vol.8, No.1, pp.11-19, 2020
- [D] 佐々木 隆幸, 川守田 聡: “三重電子透かし画像づくり”, 職業能力開発報文誌, Vol. 31, No. 1, pp. 1-8, 2019

研究報告

- [a] 佐々木 隆幸: “直交関数系による電子透かしづくり2例”, 情報処理学会東北支部研究会 (弘前大学), 2017/2/20
- [b] 佐々木 隆幸, 長瀬 智行: “3重電子透かしづくりと部分再生に関する定性的考察”, 電気関係学会東北支部連合大会 (弘前大学), 2017/8/24
- [c] 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”, 情報処理学会デジタルコンテンツクリエーション研究会 (東京藝術大学), Vol.2018-DCC-19 No.5, 2018/6/16
- [d] 佐々木 隆幸, 長瀬 智行: “擬似乱数でつくる一重と二重の電子透かし画像”, 情報処理学会デジタルコンテンツクリエーション研究会 (東北大学), Vol.2018-DCC-20, No.7, 2018/11/7
- [e] 佐々木 隆幸, 長瀬 智行: “情報ハイディング画像の高画質化”, 情報処理学会デジタルコンテンツクリエーション研究会 (愛知県日間賀島アイランドホテル浦島), Vol.2019-DCC-22, No.6, 2019/6/8

参考講義

- [α] 長瀬智行, “セキュリティ信号処理特論”, 2016年
- [β] 別宮耕一, “離散アルゴリズム特論”, 2016年
- [γ] 小野口一則, “三次元画像認識特論”, 2016年

参考文献

- [1] OECD Guidelines for the Security of Information Systems and Networks TOWARDS A CULTURE OF SECURITY, 2002
- [2] Hardikkumar V. Desai: Steganography, Cryptography, Watermarking: A Comparative Study, Journal of Global Research in Computer Science, Volume 3, No. 12, 2012
- [3] Tej R. Joshi: Hardware of watermarking Based on DCT, International Journal of Engineering Development and Research (IJEDR), Volume 2, Issue 1, ISSN: 2321-9939, 2014
- [4] 久保田英之: 情報セキュリティの基礎技術 ～暗号技術～, NTT Facilities Research Institute, Annual Report No. 29, 2018
- [5] R. Ganesan, K. Vivekanandan: COMPARATIVE ANALYSIS OF HIGHER GENUS HYPERELLIPTIC CURVE CRYPTOSYSTEMS OVER FINITE FIELD FP , ICTACT Journal on communication Technology, Vol. 02, ISSUE 01, 2011
- [6] A. Michael Froomkin: THE METAPHOR IS THE KEY: CRYPTOGRAPHY, THE CLIPPER CHIP, AND THE CONSTITUTION, Published at 143 U. Penn. L. Rev. 709, 1995
- [7] C. E. Shannon: A Mathematical Theory of Communication, The Bell System Technical Journal, Vol. 27, pp. 379–423, 623–656, July, October, 1948
- [8] C. E. Shannon: Communication Theory of Security Systems, N. J. A. Sloana and A. D. Wyner, editors, Claude Elwood Shannon: Collected Papers, IEEE Press, pp84-143, 1949
- [9] C. Paar, J. Pelzl: Understanding Cryptograph Chapter 2 Stream Ciphers, Springer-Verlag Berlin Heidelberg, 2010
- [10] Olivier Bonaventure: Network Security, Department of Computing Science and Engineering Université catholique de Louvain (UCL), 2008
- [11] 高田豊, “わかりやすい暗号学”, 米田出版, 2000
- [12] 神永正博, “現代暗号入門”, 講談社, 2017
- [13] 大村平, “改訂版情報数学のはなし”, 日科技連出版社, 2018
- [14] Federal Information Processing Standard Publication: GUIDELINES FOR IMPLEMENTING AND USING THE NBS DATA ENCRYPTION STANDARD, 1981
- [15] National Institute of Standards and Technology: The Economic Impacts of NIST’s Data Encryption Standard (DES) Program, 2001
- [16] Awakash Mishra, Deo Brat Ojha: SECURE E-MESSAGING SCHEME USING SYMMETRIC KEY ENCRYPTION -EHDES, Journal of Global Research in Computer Science, Vol. 1, No. 3, 2010
- [17] National Institute of Standards and Technology, “Announcing the Advanced Encryption Standard (AES)”, FIPS Publication 197, 2001
- [18] R. L. Rivest, A. Shamir, L. M. Adleman: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Association for Computing Machinery (ACM), 1977
- [19] 平成 16 年度情報基盤対策技術開発等推進事業（電子商取引（EC）技術基盤の相互運用性に関する調査研究）調査報告 公認制度調査, (財)日本情報処理開発協会(平成 17 年), 2005
- [20] Kavita Rawat, Mr. Shambhu Sah: A Study- To Combined Cryptography and Steganography Methods, International Journal of Computer Science Trends and Technology (IJCST), Vol. 4, Issue 5, 2016

- [21] 花岡悟一郎: 1 群 (信号・システム) -- 3 編 (暗号理論) 5 章 公開鍵暗号, 電子情報通信学会「知識ベース」, ver.1, 2010
- [22] 馬場 良始: 暗号—小学校専門科目「数学」での実践—, 数学教育研究, 第 44 号, 2015
- [23] 荒井 千里: 数式処理を用いた暗号アルゴリズムの実験的評価, 数式処理 J.JSSAC, Vol. 12, No. 4, pp. 9–17, 2006
- [24] Victor S. Miller: Use of Elliptic Curves in Cryptography, Exploratory Computer Science, Advances in Cryptology - CRYPTO '85, LNCS 218, pp. 417-426, 1986
- [25] Neal Koblitz: Elliptic Curve Cryptosystems, Mathematics Of Computation, Vol. 4X, No. 177, pp.201-209 JANUARY IW7. PAGES 203-209
- [26] 高木 剛: 1 群 (信号・システム) -- 3 編 (暗号理論) 7 章 楕円曲線暗号とペアリング, 電子情報通信学会「知識ベース」, ver.1, 2010
- [27] 堀内 啓次, 布田 裕一, 境 隆一, 金子 昌信, 笠原 正雄: 素数位数を有する楕円曲線の構成とその計算量評価, 電子情報通信学会論文誌 A, Vol. j82-A, No. 8, pp. 1269-1277, 1999
- [28] 宮地 充子: 楕円曲線暗号, 数理解析研究所講究録, 1098 巻, pp. 138-146, 1999
- [29] 加塩 朋和: 代数学と楕円曲線暗号, kashio_tomokazu@ma.noda.tus.ac.jp
- [30] 赤根大吾: ビットコインをきっかけに学ぶ暗号技術入門, 平成 29 年度 CITP フォーラム/JUAS アドバンスド研究会 活動報告書, 2017
- [31] A. Menezes, P. van Oorschot, S. Vanstone: Handbook of Applied Cryptography, 1996
- [32] SHRIKANT S. KHAIRE, SANJAY L. NALBALWAR: Review: Steganography – Bit Plane Complexity Segmentation (BPCS) Technique, International Journal of Engineering Science and Technology, Vol. 2(9), 4860-4868, 2010
- [33] Koichi Nozaki, Michiharu Niimi, Richard O. Eason, Eiji Kawaguchi: A Large Capacity Steganography Using Color BMP Images, Proceedings of ACCV'98, pp. 112-119, 1998
- [34] Abbas Cheddad, Joan Condell, Kevin Curran Paul Mc Kevitt: Information hiding-enabled data transmission framework, International Journal of Information Studies, Volume 1, Issue 3, PP.159-164, 2009
- [35] Ravi Saini: Comparative Study of Current Image Steganography Techniques, International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. 5, Issue 1, pp. 308-310, 2018
- [36] N.F. Johnson, S. Jajodia: Exploring steganography: Seeing the unseen, IEEE Computer, 1998
- [37] J.C. Judge: Steganography: Past, present, future, SANS Institute 2000-2005
- [38] N. Provos, P. Honeyman: Hide and seek: An introduction to steganography, IEEE Security and Privacy, pp. 32-44, 2003
- [39] Hieu Van Dang: A Perceptual Data Hiding Technique for Color Image Protections, University of Manitoba Department of Electrical & Computer Engineering, 2012
- [40] 河口英二: BPCS-Steganography の原理(Bit-Plane Complexity Segmentation に基づくデータの埋込み), KIT ステガノグラフィ 研究グループ, 2019
- [41] S. Lyu, H. Farid: Steganalysis Using Higher-Order Image Statistics, IEEE Transactions on Information Forensics and Security, pp. 111-119, 2006
- [42] D. Kahn: The Codebreakers: The Story of Secret Writing, The Macmillan Company, 1973
- [43] Ashikali M. Hasan: IMPLEMENTING SECURITY LAYERS ON FILE SYSTEM, Journal of Theoretical and Applied Information Technology, pp. 137-139, 2010

- [44] Gustavus J. Simmons: The prisoners' problem and the subliminal channel, pp. 51-67, 1984
- [45] Yvo G. Desmedt, Shuang Hou, Jean-Jacques Quisquater: Cerebral Cryptography, David Aucsmith (Ed.): Information Hiding 1998, LNCS 1525, pp. 62–72, 1998
- [46] T.L. Thomas, Al Qaeda and the Internet: The danger of “cyberplanning”, Parameters, US Army War College Quarterly-Spring 2003. Available from: www.carlisle.army.mil/usawc/Parameters/03spring/thomas.pdf
- Robert Hossal: The Evolution of al-Qaeda's Strategy after Afghanistan
- [47] Chet Hosmer, Christopher Hyde: Discovering Covert Digital Evidence, WetStone Technologies Inc., DFRWS – 2003. www.wetstonetech.com, 2003
- [48] Julio C. Hernandez-Castroa, Ignacio Blasco-Lopezb, Juan M. Estevez-Tapiadora, Arturo Ribagorda-Garnachoa: Steganography in games: A general methodology and its application to the game of Go, Computers and Security, Elsevier Science, 25, pp. 64-71, 2006
- [49] Andrew Rukhin: Testing Randomness : Physical Generators and Statistical Procedures, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, 2017
- [50] W. Bender, W. Butera, D. Gruhl, R. Hwang, F.J. Paiz, S. Pogreb: Applications for data hiding, IBM Systems Journal, Vol. 39, NOS 3&4, pp. 547-568, 2000
- [51] T. D. Sairam, K. Boopathybagan: Computational intelligence-based steganalysis comparison for RCM-DWT and PVA-MOD methods, <https://doi.org/10.1080/00051144.2019.1579434>, 2019
- [52] Raju, Mohit Dhanda: Improved LSB Steganography Technique for grayscale and RGB image, Journal of Engineering Research and Applications www.ijera.comISSN, Vol. 4, Issue 10(Part -2), pp.36-38, 2014
- [53] Allen Tom, Anu V Thomas, Jerin Jose, Maria Jose, P. Darsana: Hiding Host Image using a Cover Image, International Journal of Engineering Research & Technology (IJERT), Vol. 3, Special Issue 05, 2015
- [54] Neha Saxena: Complete Study On Different Methods For Producing Stegoimage, IJLTEMAS ISSN 2278 – 2540, Volume II, Issue VI, pp.66-72, 2013
- [55] Mamta Juneja, Parvinder Singh Sandhu: Improved information security using Steganography and Image Segmentation during transmission, Computer Science and Engineering Department, Rayat and Bahra Institute of Engineering and Technology (RBIET), Sahauran (Punjab), India
- [56] H. Farid: A Survey of image forgery detection, IEEE Signal Processing Magazine, 16-25, 2009
- [57] A. Cheddad, J. Condell, K. Curran and P. Mc Kevitt, A secure and improved self-embedding algorithm to combat digital document forgery, Signal Processing, 89, pp. 2324-2332, 2009
- [58] N.F. Johnson and S.C. Katzenbeisser: A survey of steganographic techniques, Information hiding techniques for steganography and digital watermarking, pp.43-78, 2006
- [59] Khan Muhammad, Jamil Ahmad, Muhammad Sajjad, Sung Wook Baik: Evaluating the Suitability of Color Spaces for Image Steganography and its Application in Wireless Capsule Endoscopy, IEEE, 2016
- [60] Yoan Miche, Patrick Bas, Amaury Lendasse, Christian Jutten, Olli Simula: Une méthodologie pour la Sélection de Variables pour la Stéganalyse A Feature Selection Methodology for Steganalysis, traitement du signal, volume 26, numéro 1, pp.13-30, 2009
- [61] Abednego Jaya Setiawan, dan Sari Wijayanti, M.Kom: PERANCANGAN APLIKASI PENGIDENTIFIKASI DATA BERDASAR METADATA PADA PLATFORM ANDROID, JURNAL TEKNIK INFORMATIKA UDINUS, 2013
- [62] Ruchi Jain, Piyush Singh: EMSEMBLE APPROACH FOR HIDDING DATA IN STEGANOGRAPHY,

International Journal of Application or Innovation in Engineering & Management, Vol. 3, pp.327-330, Issue 10, 2014

[63] M.H. Shirali-Shahreza, M. Shirali-Shahreza: STEGANOGRAPHY IN PERSIAN AND ARABIC UNICODE TEXTS USING PSEUDO-SPACE AND PSEUDO CONNECTION CHARACTERS, Journal of Theoretical and Applied Information Technology, pp.682-687, 2005

[64] E.T. Lin and E.J. Delp, A review of data hiding in digital images, IS&T's 1999 PICS Conference, pp.274-278, 1999

[65] Jessica Fridrich, Miroslav Goljan, Rui Du: Reliable Detection of LSB Steganography in Color and Grayscale Images, SUNY Binghamton, 2001

[66] S.Balusamy: Authentication of Grey Level Images using a Watermarking Scheme, SSRG International Journal of Computer Science and Engineering (SSRG-IJCSE), volume 1, Issue 1, 2014

[67] Eugenijus Margalikas, Simona Ramanauskaitė: Image steganography based on color palette transformation in color space, EURASIP Journal on Image and Video Processing volume 2019, Article number: 82, 2019

[68] Jessica Fridrich, Miroslav Goljan, Dorin Hoge: Steganalysis of JPEG Images: Breaking the F5 Algorithm, Proceedings of Information Hiding: 5th International Workshop, pp. 310-311, 2002

[69] Ki-Hyun Jung, Kee-Young Yoo: Data hiding method using image interpolation, Computer Standards & Interfaces, CSI-02600, 2008

[70] R Anushiadevi, Kolluri Chennakesava Vinay, Majety B V S K Sita Ram, Katta Bala Anil Kumar, Katti Krishna Murthy: IMPROVED LOSSLESS DATA HIDING SCHEME USING HISTOGRAM OF ADJACENCY PIXEL DIFFERENCE, International Journal of Pharmacy & Technology, Vol. 8, No.3, pp.18239-18246, 2016

[71] Aswathy Soman, Sowmya K S: International Journal of Advance Research in Computer Science and Management Studies, , January 2015, ISSN: 232 7782, Vol.3, Issue 1, pp.276-278, 2015

[72] Pasquet Jérôme, Sandra Bringay, Marc Chaumont: Steganalysis with Cover-Source Mismatch and a Small Learning Database, European Signal Processing Conference 2014, Lisbon – Portugal, 2014

[73] Vlado Kitanovski, Marius Pedersen: Detection of Orientation-Modulation Embedded Data in Color Printed Natural Images, MDIP, Computational Color Imaging, 2018

[74] Balakrishnan Ramalingam, Rengarajan Amirtharajan, John Bosco Balaguru Rayappan: Stego on FPGA: An IWT Approach, Scientific World Journal, 2014

[75] Jessica Fridrich, Miroslav Goljan, Rui Du: Detecting LSB Steganography in Color and GrayScale Images, IEEE, Multimedia and Security, pp.22-28, 2001

[76] N.Vinothkumar, T.Vigneswaran: Steganographic Method Image Security Based on Optimal Pixel Adjustment Process and Integer Wavelet Transform, International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE), Vol. 2, Issue 3, pp.261-264, 2013

[77] Dalia Battikh, Safwan El Assad, Thang Manh Hoang, Bassem Bakhache, Olivier Deforges, Mohamad Khalil: Comparative Study of Three Steganographic Methods Using a Chaotic System and Their Universal Steganalysis Based on Three Feature Vectors, Entropy 2019, 21(8), 748, <https://doi.org/10.3390/e21080748>

[78] Raja K B, Shankara N, Venugopal K Ra, L M Patnaik: Steganalysis of LSB Embedded Images Using Variable Threshold Color Pair Analysis, International Journal of Information Processing, Vol. 1, No. 1, pp.30-39, 2007

[79] Shanqing Zhang, Shengqi Su, Li Li, Qili Zhou, Jianfeng Lu, Chin-Chen Chang: An Image Style Transfer

- Network Using Multilevel Noise Encoding and Its Application in Coverless Steganography, *Symmetry* 2019, 11(9), 1152; <https://doi.org/10.3390/sym11091152>, 2019
- [80] Tom'as Pevn'y, Jessica Fridrich: Merging Markov and DCT Features for Multi-Class JPEG Steganalysis, Binghamton University, State University of New York
- [81] Richa Khare, Dr. Kuldeep Raghuwanshi: A REVIEW OF VIDEO STEGANOGRAPHY METHODS, *International Journal of Research in Advent Technology*, Vol. 2, Issue 1, pp.447-451, 2014
- [82] Niels Provos: Defending Against Statistical Steganalysis, Center for Information Technology Integration University of Michigan, technical report, 2001
- [83] N. Provos, P. Honeyman: Detecting steganographic content on the Internet, Center for Information Technology Integration, University of Michigan, technical report, 2001
- [84] A. Westfeld: F5-A steganographic algorithm High Capacity Despite Better Steganalysis, *IH 2001, LNCS 2137*, pp. 289-302, 2001,
- [85] Samir Kumar Bandyopadhyay, Suman Chakraborty: IMAGE STEGANOGRAPHY USING DNA SEQUENCE, *Asian Journal Of Computer Science And Information Technology* 1:2 India, pp. 50 – 52, 2011
- [86] J. Fridrich, M. Goljan, D. Soukal: Perturbed Quantization Steganography, *ACM Multimedia and Security Journal*, Vol.11, No.2, pp.98-107, 2005
- [87] Kaushal Solanki, Anindya Sarkar, B. S. Manjunath: YASS: Yet Another Steganographic Scheme that Resists Blind Steganalysis, *ONR # N00014-05-1-0816*, University of California Santa Barbara, CA 93106
- [88] Manoj Nagar, Pinky Brahmabhatt, Dr. M. Sarada Devi: DETECTION OF TAMPERING IN COLOR IMAGE, *International Research Journal of Engineering and Technology*, Vol.02 Issue 02, 2015
- [89] Rajendraprasad K, Dr. V. B. Narasimha: Steganography Images Detection using Different Steganalysis Techniques with Markov Chain Features, *Global Journal of Computer Science and Technology: G Interdisciplinary*, Volume 15, Issue 3, Version 1.0, 2015
- [90] Nidhal Abdulaziz, Abdullatif Glass, K. Khee Pang: Embedding Data in Images Using Turbo Coding, Department of Electrical and Computer Systems Engineering Monash University, pp.88-92
- [91] Hayfaa Abdulzahra Atee, Robiah Ahmad, Norliza Mohd Noor, Abdul Monem S. Rahma, Yazan Aljeroudi: Extreme learning machine based optimal embedding location finder for image steganography, <https://doi.org/10.1371/journal.pone.0170329>, 2017
- [92] Vijay Kumar, Dinesh Kumar: Performance Evaluation of Modified Color Image Steganography Using Discrete Wavelet Transform, *Journal of Intelligent Systems*, Vol.28, Issue 5, <https://doi.org/10.1515/jisys-2017-0134>
- [93] Kolsoom Shahryari1, Mehrdad Gholami: High Capacity Secure Image Steganography Based on Contourlet Transform, *ACSIIJ Advances in Computer Science: an International Journal*, Vol. 2, Issue 4, No.5, 2013
- [94] M. Kharrazi, H.T. Sencar and N. Memon, Performance study of common image steganography and steganalysis techniques, *Journal of Electrical Imaging*, 15 (4) 1-16, 2006
- [95] Rui S. Rodrigues, Diogo M. Lourenço, Sara L. Paulo, Joana M. Mateus, Miguel F. Ferreira, Francisco M. Mouro, João B. Moreira, Filipa F. Ribeiro, Ana M. Sebastião, Sara Xapelli: Cannabinoid Actions on Neural Stem Cells: Implications for Pathophysiology, *MDPI Emerging Topics in (Endo)Cannabinoid Signalling*, 2019
- [96] M.Vijay, V.VigneshKumar: Image Steganography Method Using Integer Wavelet Transform, *International Journal of Innovative Research in Science, Engineering and Technology*, Vol. 3, Special Issue 3, 2014

- [97] Jan Kodovský, Jessica Fridrich: Influence of Embedding Strategies on Security of Steganographic Methods in the JPEG Domain, Department of Electrical and Computer Engineering, Binghamton University, State University of New York
- [98] Amer A. Al-Lehiebe: Ciphered Text Hiding in an Image using RSA algorithm, J. Of College Of Education For Women, vol. 26 (3), 2015
- [99] Shaik Rahamtula, K. Veera Swamy: An Improved Face Recognition using Dimensionality Reduction Technique, International Conference on Electronics and Communication Engineering (ICECE), 2012
- [100] Gumma Prasad, V.Sathya Narayanan: Data Hiding Scheme For Side Match Vector Quantization and Arnold Decoding, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
- [101] Saeed Toosizadeh, Seyyed Mohammad Reza Farshchi: A Hybrid Steganography Algorithm based on Chaos & BPCS, Department of Electrical Engineering, Mashhad Branch, Islamic Azad University (Mashhad, Iran)
- [102] Ashish Chawla, Pranjal Shukla: Comparison of Arnold and Matrix Rotation Using DWT Image Steganography, International Journal of Scientific & Engineering Research, Vol. 5, Issue 2, 2014
- [103] Y. Srinivasan: High Capacity Data Hiding System Using BPCS Steganography, Submitted to the Graduate Faculty of Texas Tech University in Partial Fulfillment, 2003
- [104] Jeremiah Spaulding, Hideki Noda, Mahdad N. Shirazi, Michiharu Niimi, Eiji Kawaguchi: BPCS Steganography Using EZW Encoded Images, Digital Image Computing Techniques and Applications, 2002
- [105] Jessica Fridrich: Application of Data Hiding in Digital Images, Tutorial for the ISSPA'99, Brisbane, Australia, August 22-25 1999.
- [106] Zhenhao lud, Wei Xie, Baosheng Wang, Yong Tang, Qianqian Xing: EasyStego: Robust Steganography Based on Quick-Response Barcodes for Crossing Domains, College of Computer, National University of Defense Technology, Changsha 410073, China, 2019
- [107] Deo Brat Ojha, Ramveer Singh, Ajay Sharma, Abhishek Shukla: A Model of Anonymous cum Idiosyncratic Machiavellian Mailing System using Steganographic Scheme, International Journal of Computer Applications Vol. 8, No.14, 2010
- [108] C.C. Chang, W.L. Tai , C.C. Lin: A Reversible Data Hiding Scheme Based on Side Match Vector Quantization, IEEE Transactions on Circuits and Systems for Video Technology, Vol.16, No.10, pp.1301-1308, 2006
- [109] IRajani, Muhammad Tauheed Khan: Data Hiding In Digital Image Processing Using Steganography: A Review, International Journal of Engineering Development and Research (IJEDR), Volume 2, Issue 3, ISSN: 2321-9939, pp.2994-2996, 2014
- [110] S.P. Maity, M.K. Kundu: Performance Improvement in Spread Spectrum Image Watermarking Using Wavelets, International Journal of Wavelets, Multiresolution and Information Processing Vol. 9, No. 1, pp.1-33, 2011
- [111] T.Tuncer, E. Avci: BRAILLE ALFABESİ TABANLI OLASILIKSAL GÖRSEL SIR PAYLAŞIMI METODU, BRAILLE ALFABESİ TABANLI OLASILIKSAL GÖRSEL SIR PAYLAŞIMI METODU
- [112] M.W. Chao, C.H. Lin, C.W. Yu, T.Y. Lee: A high Capacity 3D Steganography Algorithm, IEEE Transactions on Visualization and Computer Graphics, Vol.20, No.3, 2009
- [113] Xinbo Gao, Cheng Deng, Xuelong Li, Dacheng Tao: Geometric Distortion Insensitive Image Watermarking in Affine Covariant Regions, IEEE Transactions on systems, Man, and Cybernetics-Part C: Applications and Reviews, Vol. 40, No. 3, 2010

- [114] Cheng Deng, Xinbo Gao, Xuelong Li, Dacheng Tao: Local histogram based geometric invariant image watermarking, ELSEVIER Signal Processing 90, pp.3256-3264, 2010
- [115] Ranjan KUMAR Arya, Shalu Singh, Ravi Saharan: A Secure Non-blind Block Based Digital Image Watermarking Technique Using DWT and DCT, IEEE International Conference on Advances in Computing, Communications and Informatics, 2015
- [116] Y. H. Yu, C.C. Chang, I.C. Lin, A new steganographic method for color and grayscale image hiding, Computer Vision and Image Understanding, 107, pp.183-194, 2007
- [117] M.S. Drew, S. Bergner: Spatio-Chromatic Decorrelation for Color Image Compression, Technical Report, School of Computing Science, Simon Fraser University, Vancouver, Canada, 2007
- [118] M. Saenz, R. Oktem, K. Egiazarian, E. Delp: Color Image Wavelet Compression Using Vector Morphology, Center for Education and Research Information Assurance and Security Purdue University, West Lafayette, CERIAS Tech Report, 2001
- [119] S.J. Banerjee, M.Azharuddin, D. Sen, S. Savale, H. Datta, A.K. Dasgupta, S. Roy: Using complex networks towards information retrieval and diagnostics in multidimensional imaging, naturesearch, PMID: 26626047, 2015
- [120] M. Galar, A. Jurio, C. Lopez-Molina, D. Paternain, J. Sanz, H. Bustince: Aggregation functions to combine RGB color channels in stereo matching, Optical Society of America, 2012
- [121] M. Kutter, F.P. Petitcolas: A fair benchmark for image watermarking systems, Electronic Imaging '99, Security and Watermarking of Multimedia Contents, Vol. 3657, San Jose, California, U.S.A, 1999
- [122] Balakrishnan Ramalingam, Rengarajan Amirtharajan, John Bosco Balaguru Rayappan: Stego on FPGA: An IWT Approach, The Scientific World Journal, PMID: 24723794, 2014
- [123] Micah K. Johnson, Siwei Lyu, Hany Farid: Steganalysis of Recorded Speech, Computer Science Department, Dartmouth College, Hanover
- [124] Samir Kumar Bandyopadhyay: A Proposed Method for Image Steganography, Research in Medical & Engineering Science, ISSN 2576-8816, 2018
- [125] Shafi Goldwasser, Mihir Bellare: Lecture Notes on Cryptography, MIT Computer Science and Artificial Intelligence Laboratory, Cambridge, Massachusetts, July 2008
- [126] Jishen Zeng, Shunquan Tan, Bin Li, Jiwu Huang: Large-scale JPEG image steganalysis using hybrid deep-learning framework, Shenzhen University 518060 China
- [127] Mohammed Al-Mualla, Hussain Al-Ahmad: Information Hiding: Steganography and Watermarking, Etisalat College of Engineering College of Engineering, P.O.Box: 980, P.O.Box: 980, Sharjah Sharjah, UAE
- [128] Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt: Towards Objectifying Information Hiding, School of Computing and Intelligent Systems, Faculty of Computing and Engineering, University of Ulster, Derry, 2010
- [129] A. Nikolaidis, I. Pitas: Region-Based Image Watermarking, IEEE Transactions on Image Processing, Vol.10, No.11, pp. 1726-1740, 2001
- [130] A. Nikolaidis and I. Pitas, Robust Watermarking of Facial Images Based on Salient Geometric Pattern Matching, IEEE Transactions on Multimedia, Vol.2, No.3, pp.172-184, 2000
- [131] Yu-Guang Yang, Qing-Xiang Pan, Si-Jia Sun, Peng Xu: Novel Image Encryption based on Quantum Walks, naturesearch, Scientific reports, PMID: 25586889, 2015

- [132] Nidhi H. Divecha, N. N. Jani: “Image Watermarking Algorithm using Dct, Dwt and Svd, National Conference on Innovative Paradigms in Engineering & Technology (NCIPET-2012) Proceedings published by International Journal of Computer Applications® (IJCA), 2012
- [133] 江島 将高, 宮崎 明雄: 画像の走査線信号を利用した電子透かし方式, 電子情報通信学会論文誌 A, Vol. J82-A, No. 7, pp. 1083-1091, 1999
- [134] J.-P. Linnartz, T. Kalker, and J. Haitsma, “Detecting electronic watermarks in digital video,” in Proc. 1999 IEEE Int. Conf. Acoustics, Speech, and Signal Processing, vol. 4, Phoenix, AZ, pp. 2071–2074, 1999
- [135] 崔 潤基, 相澤 清晴: DCT 係数のブロック間相関を利用した電子透かし法, 電子情報通信学会論文誌 D-II, Vol. J83-D-II, No. 7, pp. 1620-1627, 2000
- [136] 岩村 恵市, 桜井 幸一, 今井 秀樹: 2 次配布に対して安全な電子透かしシステム, 電子情報通信学会論文誌 A, Vol. J84-A, No. 5, pp. 624-632, 2001
- [137] 岡本 晃宏, 宮崎 明雄: モルフォロジカル信号処理を利用した電子透かし方式, 電子情報通信学会論文誌 A, Vol. J84-A, No. 8, pp. 1037-1044, 2001
- [138] Yüksel Tokur, Ergun Erçelebi: SPREAD SPECTRUM AUDIO WATERMARKING SCHEME BASED ON PSYCHOACOUSTIC MODEL, Gaziantep University, Electrical & Electronics Engineering, Turkey
- [139] 江島 将高, 宮崎 明雄: 周波数領域利用形電子透かし方式の性能評価について, 電子情報通信学会論文誌 A, Vol. J84-A, No. 10, pp. 1272-1281, 2001
- [140] Hardikkumar V. Desai: Steganography, Cryptography, Watermarking: A Comparative Study, Journal of Global Research in Computer Science, Volume 3, No. 12, 2012
- [141] P.Gitanjali, R.Manikandan: A Novel Approach for Parallel Encoder by Pixel Bit Manipulation, International Journal of Engineering and Technology (IJET), Vol 5, No 1, 2013
- [142] 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
- [143] Joshua R. Smith, Barrett O. Comiskey: Modulation and Information Hiding in Images, Proceedings of the First Information Hiding Workshop, Isaac Newton Institute, Cambridge, Volume 1174, 1996
- [144] 水本 匡, 松井 甲子雄: DCT を用いた電子透かしの印刷取り込み体制の検討, 電子情報通信学会論文誌 A, Vol. J85-A, No. 4, pp. 451-459, 2002
- [145] Weiming Zhang, Shiqu Li: Security Measurements of Steganographic Systems, ACNS 2004, LNCS 3089, pp. 194–204, 2004
- [146] Brian Chen, Gregory W. Wornell: Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding, IEEE Transactions on Information Theory, Vol. 47, No. 4, 2001
- [147] Pierre Moulin, Joseph A. O’Sullivan: Information-Theoretic Analysis of Informations Hiding, IEEE Transaction on Information Theory, Vol. 49, No. 3, 2003
- [148] Ofer Zeitouni, Jacob Ziv, Felh, Neri Merhav: When is the Generalized Likelihood Ratio Test Optimal?, IEEE Transactions on Information Theory, Vol. 38, No. 5, 1992
- [149] Young-Han Kim, Arak Sutivong, Styrmir Sigurj’onsson: Multiple User Writing on Dirty Paper, IEEE ISIT 2004, Chicago, USA, 2004
- [150] Wen Chen, Shuichi Itoh, Junji Shiki: On Sampling in Shift Invariant Spaces, IEEE Transactions on Information Theory, Vol. 48, No. 10, 2002
- [151] Vikrham Gowreesunker: EE 8510: Multi-user Information Theory Distributed Source Coding for Sensor

Networks: A Coding Perspective

- [152] Ingemar J. Cox, Matt L. Miller, Andrew L. McKellips: Watermarking as communications with side information, the Proceedings of the IEEE, Vol. 87, No. 7, pp.1127-1141, 1999
- [153] Frank Hartung, Martin Kutter: Multimedia Watermarking Techniques, Proceedings of the IEEE, Vol. 87, No. 7, 1999
- [154] 江島 将高, 宮崎 明雄: 相関利用型電子透かし方式の解析について, 電子情報通信学会論文誌 A, Vol. J85-A, No. 11, pp. 1273-1283, 2002
- [155] A.Z.Tirkel, G.A.Rankin, R.M.van Schyndel, W.J.Ho, N.R.A.Mee, C.F.Osborne: ELECTRONIC WATER MARK, Scientific Technology, 21 Walstab St, E. Brighton 3187, Australia
- [156] A.Anitha Rani, A.Kirthika: A Novel Digital Video Watermarking Algorithm for Video Authentication., International Journal of Scientific & Engineering Research, Vol. 4, Issue 5, 2013
- [157] Nidhi H. Divecha, N. N. Jani: Image Watermarking Algorithm using Dct, Dwt and Svd, National Conference on Innovative Paradigms in Engineering & Technology (NCIPET), 2012
- [158] Brian Chen, Gregory W. Wornell: Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding, IEEE Trans. Inform. Theory, 2000
- [159] 木野 将人, 和田 成夫: ビットデータを埋込み可能なウェ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
- [160] Hüseyin Abut: EE658 ADVANCED DSP APPLICATIONS and DATA COMPRESSION TECHNIQUES For Speech, Image and Video Coding, <http://anadolu.sdsu.edu/abut/Courses.html>, 2006
- [161] Meir Feder: A Note on the Competitive Optimality of the Huffman Code, IEEE Transactions on Information Theory, Vol. 38, No. 2, 1992
- [162] Thomas M. Cover, Joy A. Thomas: Elements of Information Theory, John Wiley & Sons, Inc., ISBN 0-471-06259-6, 1991
- [163] Neri Merhav, Tsachy Weissman: Coding for the Feedback Gel'fand–Pinsker Channel and the Feedforward Wyner–Ziv Source, IEEE Transactions on Information Theory, Vol. 52, No. 9, pp.4207-4211, 2006
- [164] Ashish Khisti, Uri Erez and Gregory Wornell: Writing on Many Pieces of Dirty Paper at Once: The Binary Case, ISIT 2004, Chicago, USA, June 27 – July 2, 2004
- [165] 村松 巖, 荒川 薫: オクターブ類似性に基づくオーディオ信号への電子透かし, 電子情報通信学会論文誌 A, Vol. J87-A, No. 6, pp. 787-796, 2004
- [166] Jonathan Scarlett, Vincent Y. F. Tan, Giuseppe Durisi: The Dispersion of Nearest-Neighbor Decoding for Additive Non-Gaussian Channels, Laboratory for Information and Inference Systems, Ecole Polytechnique Fédérale de Lausanne
- [167] Feng-Wen Sun: Decoding Techniques and A Modulation Scheme for Band-limited Communications, geboren te Heilongjiang, China, 1993
- [168] Ingemar J. Cox, Matt L. Miller: ELECTRONIC WATERMARKING: THE FIRST 50 YEARS, the Proceedings of the IEEE 2001 Int. Workshop on MultiMedia Signal Processing, 2001
- [169] Zoran Duric, Michael Jacobs, Sushil Jajodia: Information Hiding: Steganography and Steganalysis, Center for Secure Information Systems George Mason University Fairfax, VA 22030, 2004
- [170] Pierre Moulin: Fundamentals of Watermarking and Data Hiding, ISIT Tutorial, Seattle, 2006
- [171] Zhicheng Wei, Hao Li, Jufeng Dai, Sashuang Wang: IMAGE WATERMARKING BASED ON GENETIC

ALGORITHM, IEEE, ICME, pp.1117-1120, 2006

[172] 太田 正哉, 佐藤 晃久, 山下 勝己: DCT 係数を考慮したフラクタル符号化に基づく電子透かし, 電子情報通信学会論文誌 A, Vol. J87-A, No. 6, pp. 797-804, 2004

[173] Saraju P. Mohanty, K.R. Ramakrishnan, Mohan S Kankanhalli: An Adaptive DCT Domain Visible Watermarking Technique for Protection of Publicly Available Images, University of South Florida Tampa, FL 33620

[174] 戸根 瑞紀, 浜田 望: スケール変換と回転等への耐性をもつ電子透かし手法, 電子情報通信学会論文誌 D-I, Vol. J88-D-I, No. 12, pp. 1750-1759, 2005

[175] Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, Ton Kalker: Digital Watermarking and Steganography Second Edition, 1999

[176] M. Kuttera, F. A. P. Petitcolas: A fair benchmark for image watermarking systems, Electronic Imaging '99. Security and Watermarking of Multimedia Contents, vol. 3657, 1999

[177] Kieran G. Larkin, Peter A. Fletcher, Stephen J. Hardy: Tenacious tagging of images using the complex correlation of hyperbolic chirps, Canon Information Systems Research Australia, 2013

[178] S. Voloshynovskiy, S. Pereira, T. Pun, J.J. Eggers, J.K. Su: Attacks on Digital Watermarks: Classification, Estimation-based Attacks and Benchmarks, University of Erlangen-Nuremberg

[179] 伊藤 浩, 馬養 浩一, 鈴木 光義, 浅井 光太郎: 画像電子透かしに対する局所的な信号の相関に基づくリプレース攻撃, 電子情報通信学会論文誌 D, Vol. J89-D, No. 2, pp. 237-249, 2006

[180] 稲葉 宏幸, 山本 由紀子: プライバシーと著作権を考慮したコンテンツ配信に関する提案, 電子情報通信学会論文誌 D, Vol. J89-D, No. 12, pp. 2536-2542, 2006

[181] 山本 奏, 中村 高雄, 片山 淳, 安野 貴之: 単一周波数平面スペクトル拡散を利用した時間同期外し耐性をもつ動画電子透かし, 電子情報通信学会論文誌 D, Vol. J90-D, No. 7, pp. 1755-1764, 2007

[182] Yun Q. Shi, Zhicheng Ni, Nirwan Ansari: Stirmark Attack Resistant Fractal Transform-based Information Hiding, Department of Electrical and Computer Engineering New Jersey Institute of Technology Newark, NJ 07102, USA

[183] 北村 至, 吉田 真紀, 藤原 融: 画素空間へのパットワーク法と相関型電子透かし法の検出誤り確率の比較, 電子情報通信学会論文誌 D, Vol. J91-D, No. 11, pp. 2605-2615, 2008

[184] Shouyuan Yang, Zhanjie Song, Zhijun Fang, Jucheng Yang: A Novel Affine Attack Robust Blind Watermarking Algorithm, Symposium on Security Detection and Information Processing, 2010

[185] Hoong-Cheng Soong: Applying Yellow Colour Markings as Low-level Security Watermarking of Grayscale Photocopied Documents, International Conference on Information and Knowledge Management (ICIKM), IPCSIT vol.45, 2012

[186] 藤村 誠, 宮田 慎一, 濱野 和正, 黒田 英夫, 今村 弘樹: 電子透かし技術を用いた JPEG 方式の高効率符号化, 電子情報通信学会論文誌 D, Vol. J92-D, No. 9, pp. 1672-1676, 2009

[187] Vijaya Kumar. Kurapati, Venu Gopal. K, M.Nagaraju: Multiple Watermarking Techniques using Visual Cryptography for Secured Copyright Protection, International Journal of Scientific & Engineering Research Volume 4, Issue 1, 2013

[188] 村田 晴美, 萩原 昭夫, 岩田 基, 汐崎 陽: 音楽電子透かしにおける埋込多重化に対する直流成分を用いた音質改善, 電子情報通信学会論文誌 A, Vol. J93-A, No. 3, pp. 171-180, 2010

[189] Chengyou Wang, Heng Zhang, Xiao Zhou: Review on Self-embedding Fragile Watermarking for Image Authentication and Self-recovery, Journal of Information Processing Systems, ISSN: 2092-805X, Vol. 14, No. 2,

pp. 510 – 522, 2018

- [190] Megha Goel, M. Chaudhari: SECURED DATA HIDING BY USING EXTENDED VISUAL CRYPTOGRAPHY, International Journal of Research in Engineering and Technology, Volume 03, Issue 11, 2014
- [191] Ching-Sheng Hsu, Shu-Fen Tu: Digital Watermarking Scheme with Visual Cryptography, Proceedings of the International MultiConference of Engineers and Computer Scientists, Vol. 1, 2008
- [192] A. K. Singh, A. A. Mohanty, R. Sharma, S. Dixit: Internet Service Provider : Review paper, International Journal of Electrical Electronics & Computer Science Engineering, Special Issue – ICSCAAIT, 2018
- [193] S. Rathod, R. Jadhav, D. Pawade, H. Sonkamble: Visual Cryptography Schemes Using Secrete Sharing: Survey Report, IJCST Vol. 4, Issue Spl - 1, 2013
- [194] 寺西 直緒, 川村 正樹: スペクトル拡散モデルにおける非同期確率アルゴリズム及び温度スケジューリングによる復号の性能評価, 電子情報通信学会論文誌 A, Vol. J96-A, No. 7, pp. 452-461, 2013
- [195] Xiaodan Jiang, Zheming Lu, Xiajun Ding: A SEMI-FRAGILE BLIND WATERMARKING SCHEME FOR COLOR IMAGES BASED ON VISUAL CRYPTOGRAPHY AND DISCRETE COSINE TRANSFORM, International Journal of Innovative Computing, Information and Control, Vol. 13, No. 5, 2017
- [196] Mr.Thorat N.N , Mr.Patil P.P, Prof.Thakur Ritesh ,Ms.Kiranmai B: Visual Cryptography Schemes for Secret Colour Images Sharing, International Journal of Engineering Research & Technology (IJERT), Vol. 2 Issue 11, 2013
- [197] Sathiya K, Senthamilarasi K, Janani G, Akila victor: International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 2, Issue 2, 1 2013
- [198] Carlo Blundo, Alfredo De Santis, Moni Naor: Visual cryptography for grey level images, ELSEVIER, Information Processing Letters, 75, pp.255-259, 2000
- [199] 海老澤 竜, 藤井 康広, 高橋 由泰, 山田 隆亮: 切れ目補正処理を用いた 2 値画像電子透かしの画質維持, 電子情報通信学会論文誌 D, Vol. J96-D, No. 1, pp. 183-194, 2013
- [200] Chao-Wen Chan, Yi-Da Wu: A Visual Information Encryption Scheme Based on Visual Cryptography and D-H Key Agreement Scheme, International Journal of Computer Science and Network Security, Vol. 8 No. 4, 2008
- [201] 大西 淳児, 小野 東: 電子しかしを用いた印刷画像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. 1483-1494, 2007
- [202] 藤井 康広, 中野 和典, 越前 功, 吉浦 裕, 手塚 悟: 局所特徴量を用いた二値画像用電子透かしの画質維持方式, 情報処理学会論文誌, Vol. 44, No. 8, 2003
- [203] 小堀 紀子, 岩切 宗利, 松井 甲子雄: 画素分布による 2 値漫画への電子透かしの一方式, 情報処理学会論文誌, Vol. 42, No. 3, 2001
- [204] 越前 功, 吉浦 裕, 安細 康介, 田口 順一, 黒須 豊, 佐々木 良一, 手塚 悟: 輪郭保存に基づく画質維持方式, 情報処理学会論文誌, Vol. 41, No. 6, 2000
- [205] Maneesh Kumar: Study of (2, n) – Threshold Visual Cryptography Scheme using Different Techniques, International Journal of Science and Research (IJSR), Volume 3, Issue 5, 2014
- [206] Sruthy K Joseph, Ramesh R: Diverse Visual Cryptography Schemes: A Glimpse, International Journal of Engineering Research & Technology (IJERT), Vol. 4, Issue 07, 2015
- [207] 粕 正充: ステガノグラフィや電子透かしの手法を利用した画像ファイルへの情報の埋め込みとその利用法について, 情報処理学会, 第 47 回プログラミングシンポジウム, 2006
- [208] 松井 甲子雄, 中里 隆博: 攻撃耐性を強化した離散コサイン変換による電子透かしの一方法, 情

- [209] Rafael C. Gonzalez, Richard E. Woods: Digital Image Processing Third Edition, Pearson Prentice Hall, 2008
- [210] Anil K. JAIN: Fundamentals of Digital Image Processing - Image Representation by Stochastic Models -, PRENTICE HALL, Englewood Cliffs, NJ 07632, pp.189-232
- [211] R.Charanya, T. Vijayan: Halftone Visual Cryptography & Watermarking, International Journal of Scientific & Engineering Research, Vol. 4, Issue 5, 2013
- [212] Vijaya Kumar. Kurapati, Venu Gopal. K, M.Nagaraju: Multiple Watermarking Techniques using Visual Cryptography for Secured Copyright Protection, International Journal of Scientific & Engineering Research Vol. 4, Issue 1, 2013
- [213] Ingemar J. Cox¹, Gwenaëlle Doërr, Teddy Furon: Watermarking is not Cryptography, University College London Adastral Park, Ross Building 2, Martlesham IP5 3RE, United Kingdom, 2006
- [214] C. E. SHANNON: A Mathematical Theory of Communication, Reprinted with corrections from The Bell System Technical Journal, Vol. 27, pp. 379–423, 623–656, 1948.
- [215] JOSEPH P. CAMPBELL, RICHARD A. DEAN: A History of Secure Voice Coding: Insights Drawn from the Career of One of the Earliest Practitioners of the Art of Speech Coding, Cryptologic Quarterly, DOCID: 3860926
- [216] Anuj Kumar Sharma, Shiv kumar: Resource Allocation in Cognitive Radio Network using Dirty Paper Coding, National Conference on Future Aspects of Artificial intelligence in Industrial Automation (NCFAAIIA), pp.28-30, 2012
- [217] Krishnamoorthi R., Sheba Kezia Malarchelvi: Image Adaptive Watermarking with Visual Model in Orthogonal Polynomials based Transformation Domain, International Journal of Information and Communication Engineering, 5, 2, 2009
- [218] Anumol Joseph, K. Anusudha: Robust watermarking based on DWT SVD, International Journal of Signal & Image Processing, Issue. 1, Vol. 1, 2013
- [219] Francois Cayre, Caroline Fontaine, Teddy Furon: Watermarking Security: Theory and Practice, IEEE Transactions on Signal Processing, Supplement on secure media III, 53 (10), pp.3976-3987, 2005
- [220] J. E. Vila-Forcena, S. Voloshynovskiy, O. Koval, F. Pérez-González, T. Pun: Worst case additive attack against quantization-based data-hiding methods, University of Geneva Department of Computer Science Switzerland
- [221] Aruna Varanas, G.Ravi, D.Veerender: RRW -A ROBUST AND REVERSIBLE WATERMARKING TECHNIQUE FOR RELATIONAL DATA, International Journal of Professional Engineering Studies, Volume VIII, Issue 4, 2017
- [222] Ingemar J. Cox, Joe Kilian, F. Thomson Leighton, Talal Sharnoon: Secure Spread Spectrum Watermarking for Multimedia, IEEE Transactions on Image Processing, Vol. 6, No. 12, 1997
- [223] Salahuddin Swati, Khizar Hayat, Zafar Shahid: A Watermarking Scheme for High Efficiency Video Coding (HEVC), PMCID: PMC4140792, 2014
- [224] Teddy FURON, Pierre DUHAMEL: An Asymmetric Public Detection Watermarking Technique, THOMSON multimedia R/D France
- [225] Chinmay Tirthgirikar, Onkar Kajale, Jonny Tahilramani, Wasudeo Rahane: Enhanced Mechanism for Protection and Detection of Digital Watermarks in Digitized Data, International Journal for Scientific Research &

Development| Vol. 3, Issue 01, 2015

- [226] Teddy Furon, Pierre Duhamel: An Asymmetric Watermarking Method, IEEE Transactions on Signal Processing, Vol. 51, No. 4, 2003
- [227] 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(49), 2018
- [228] 大西 淳児, 松井 甲子雄: ウェーブレットを利用した著作権保護のための画像符号化, 情報処理学会論文誌, Vol. 38, No. 3, 1997
- [229] HUBERT ZIMMERMANN: OS1 Reference Model-The ISO Model of Architecture for Open Systems Interconnection, IEEE Transactions on communications, Vol. COM-28, No. 4, 1980
- [230] Chun-Shien Lu, Chao-Yong Hsu: CONTENT-DEPENDENT MULTIPURPOSE WATERMARKING RESISTANT AGAINST GENERALIZED COPY ATTACK, IEEE 0-7803-8603-5/04, 2004
- [231] 酒井 康行, 石塚 裕一, 櫻井 幸一: 著作権保護のためのウェーブレット変換を用いた電子透かし方式の安全性評価, 情報処理学会論文誌, Vol. 38, No. 12, 1997
- [232] Wade Trappe, Min Wu, Z. Jane Wang, K. J. Ray Liu: Anti-collusion Fingerprinting for Multimedia, IEEE Transactions on Signal Processing, Vol. 51, No. 4, 2003
- [233] Marc Chaumont: Ensuring security of H.264 videos by using watermarking, "Mobile Multimedia/Image Processing, Security, and Applications 2011", Part of SPIE'2011, Defense, Security, and Sensing, Orlando USA, 2011
- [234] Eugene T. Lin, Edward J. Delp: Temporal Synchronization in Video Watermarking, IEEE Transactions on Signal Processing, Vol. 52, No. 10, pp.3007-3022, 2004
- [235] 荒木 貴志, 宮崎 明雄, 井上 尚: 画像の多重解像度解析を利用した電子透かし方式, 情報処理学会, オーディオビジュアル複合情報処理 26-7, 2001
- [236] Matt L. Miller, Gwena"el J. Do"err, Ingemar J.Cox: Applying Informed Coding and Embedding to Design a Robust, High Capacity Watermark.
- [237] 中村 康弘, 松井 甲子雄: 著作権保護のための電子文書のハードコピーへの署名の埋め込み, 情報処理学会論文誌, Vol. 36, No. 8, 1995
- [238] 中村 康弘, 松井 甲子雄: 著作権保護のための和文印刷文書への署名情報の埋め込み, 情報処理学会, 第 50 回(平成 7 年前期)全国大会, 3-203, 1995
- [239] 大中 雅憲, 中山 心太, 後守 裕介, 越前 功, 吉浦 裕: カラー画像の 2 つの色成分の関係に基づいて多様な幾何変形に対応する画像電子透かし方式, 情報処理学会論文誌, Vol. 49, No. 3, 2008
- [240] ウィセッスト ビヤビスト, 松井 甲子雄: カラー画像への可変表示型電子透かしの提案, 情報処理学会論文誌, Vol. 40, No. 12, 1999
- [241] 黒田 英夫, 藤村 誠, 今村 弘樹: 電子透かし技術を用いた画像符号化の画像処理への発展について, 情報処理学会 研究報告, IPSJ SIG Technical Report 2008-AVM-60 (6), 2008
- [242] QIBIN SUN, SHUIMING YE: A CRYPTO SIGNATURE SCHEME FOR IMAGE AUTHENTICATION OVER WIRELESS CHANNEL, International Journal of Image and Graphics, Vol. 5, No. 1, pp.1-14, 2005
- [243] Susie J. Wee, John G. Apostolopoulos: SECURE SCALABLE STREAMING ENABLING TRANSCODING WITHOUT DECRYPTION, IEEE International Conference on Image Processing, Thessaloniki, Greece, 2001
- [244] S. C. Cheung, Dickson K. W. Chiu, Cedric Ho: The Use of Digital Watermarking for Intelligence Multimedia Document Distribution, Department of Computer Science and Engineering, Hong Kong University of

Science and Technology, 2008

- [245] Edward J. Delp: Digital Watermarking: An Introduction, Purdue University School of Electrical and Computer Engineering Purdue Multimedia Testbed Video and Image Processing Laboratory, 2003
- [246] Abdelmgeid A. Ali, Ahmed H. Ismail: Cryptography Based MSLDIP Watermarking Algorithm, International Journal of Computer Science and Security (IJCSS), Vol.9, Issue 4, 2015
- [247] 宮田 慎一, 黒田 英夫, 藤村 誠, 今村 弘樹: 電子透かし技術を用いた JPEG 画像符号化, 情報処理学会 研究報告, 2007-AVM-58 (11), 2007
- [248] 津下 浩一郎, 野上 保之, 森川 良孝: 多重解像度近似に PN 拡散と 1 次元フーリエ変換を用いた画像電子透かし埋め込み法, 情報処理学会, オーディオビジュアル複合情報処理 35-9, 2001
- [249] 越智宏, 黒田英夫, ”JPEG&MPEG 図解でわかる画像圧縮技術”, (株)日本実業出版社, 1999
- [250] 伏見康治, 赤井逸, ”復刊直交関数系増補版”, 共立出版(株), 2011
- [251] 高橋健人, ”物理数学”, (株)培風館, 1968
- [252] Ming Li, Qian Liu, Yanqing Guo, Bo Wang: Optimal M-PAM Spread-Spectrum Data Embedding with Precoding, Circuits Syst Signal Process (2016) 35, pp. 1333–1353, 2016
- [253] Roland Kwitt, Peter Meerwald, Andreas Uhl: A Lightweight Rao-Cauchy Detector for Additive Watermarking in the DWT-Domain, Dept. of Computer Sciences University of Salzburg Austria
- [254] Mya Thidar Kyaw, Kyi Soe: A New Scheme of Neural Network and DCT-Domain Based Digital Watermarking, International Conference on Advances in Engineering and Technology (ICAET'2014), 2014
- [255] 遠藤 靖: ウォルシュ解析, 東京電機大学出版局, 1993
- [256] L. R. Rabiner, R. W. Schafer (鈴木 久喜 訳): 音声のデジタル信号処理(上・下), コロナ社, 1983
- [257] D.Gabor : ”A new microscopic principle”, Nature, 1948