複素アダマール変換を用いた擬似計算機ホログラムの合成とディザ画像への埋込みの応用

Computer-generated Pseudo Holograms Using Complex Hadamard Transform and Application of Embedding into Dithered Images

正会員 田中賢一[†], 藤田泰仁[†], 磯井亮太[†]

Ken-ichi Tanaka[†], Yasuhito Fujita[†] and Ryota Isoi[†]

Abstract A computer-generated pseudo hologram was synthesized using the complex Hadamard transform instead of the Fourier transform used to synthesize a computer-generated hologram. As a result, an image was reconstructed through a simulation, and a result that was similar to that from the Fourier transform was obtained for the binary phase quantization, although a physical image (optical reconstructed image) was obtained. In addition, we propose the application of computer-generated pseudo holograms, which are used to hide the confidential information in a dither image. The strength of a StirmMark attack on a dithered image embedded with computer-generated pseudo holograms is weaker than the results of that using the Fourier transform hologram. It was previously reported that there was the possibility of the use of the computer generated holograms for information security.

キーワード：複素アダマール変換, 擬似計算機ホログラム, ディザ法, データハイディング

1. ま え が き

擬似中間調処理¹⁾された画像は、一つの画素を少ないビット数で表現しており、きわめて冗長性が乏しく、秘密画像を埋込むことは非常に困難である。また、電子メディア上では、濃淡画像の下位ビットへ埋込んだ秘密画像をデジタル画像処理によって取り出すことができるが、プリンタ等でハードコピー化されたものにおいては、下位ビットの埋込み情報だけを取り出す方法は使用できない。

しかしながら、このような擬似中間調処理された2値画像に対しても秘密画像を埋込むためにいくつかの方法が提案されている。例えば、金田らによる誤差拡散を用いた方法²⁾、松井らによるディザ法を用いた方法³⁾⁴⁾等である。これらの方法は、埋込んだ情報が2値化されていて冗長性の高い情報となっているために、情報の伝送の際に行われるJPEGなどへのデータの圧縮に対して、有効な方法と考えられる。また、2値画像であるということから、Fax伝送などにも有効であると思われる。しかし、これらは秘密画像をカバー画像の一部分に埋込む方法であり、その部分を

切り取られることで容易に秘密画像が失われてしまうという問題点があった。また、画質への影響を考慮すると埋込む情報量も少ないものとなってしまう。

このことから、筆者らはディザ画像に対してフーリエ変換型計算機ホログラム (Computer-Generated Hologram: CGH)^{5)~7)}を埋込み、各種攻撃耐性に強いデータハイディングの方法と提案した⁸⁾。ここで本論文では、フーリエ変換型計算機ホログラムをCGHと記すものとする。ところで、文献8)の方法は、CGHの有する幾何学変換や損傷に対する高い攻撃耐性を有するので耐性型電子透かしの応用としてとらえることができる。ただし、このままだと、本物をコピーして複製物を作った場合でも複製物にまで秘密情報がコピーされる。このため、本物だけに秘密情報が残り、複製物には秘密情報が残らないようにするような脆弱型電子透かし⁹⁾としての特徴はないことになる。この脆弱型電子透かしに関しては、秘密情報を埋め込むカバー画像として濃淡画像が対象になっているが、2値画像すなわちディザ画像に対する応用例は見当たらない。

ところで本論文では、幾何学変換や損傷に対して脆弱な電子透かしの応用手法を提案する。すなわち、本物であれば秘密情報が取り出せるが、偽物であれば秘密情報が取り出せないようにするための、2値画像に対する秘密情報の埋込み方法を提案する。例えば、複製を行った場合には、スキャナや顕微鏡などでビットマップの構造を読取ってそれ

2008年3月30日受付, 2008年8月25日最終受付, 2008年9月16日採録

[†] 明治大学 理工学部 電気電子生命学科

(〒214-8571 川崎市多摩区東三田 1-1-1, TEL 044-934-7326)

[†] School of Science and Technology, Meiji University

(1-1-1, Higashi-Mita, Tama, Kawasaki 214-8571 Japan)

を転写することが考えられるが、その場合においてビットマップの構造が少しでも変化すると埋込んだ情報が取り出せなくなるような方法を考えることが一案であると考えられる。すなわち、StirMark 攻撃に対して脆弱な性質である方法を考える必要がある。

このような背景をかんがみて、本論文では、各種攻撃に脆弱な擬似中間調処理における秘密画像の埋込み方法を提案する。すなわち、秘密画像を複素アダマル変換 (Complex Hadamard Transform)^{10)~13)} を用いた擬似計算機ホログラム (Computer-Generated Psuedo Hologram: CGPH) の形に変換し、その形状によって組織的ディザ法¹⁾のディザ行列を変化させることで、CGH を画像全体に埋込むものである。この方法によって、回転や切り取りなどの改ざんによっても秘密情報が消失し、複製物であるか否かを判別することが可能になると考えられる。なお本論文では、CGH の合成におけるフーリエ変換の代わりに複素アダマル変換を用いた、計算機ホログラムすなわち擬似計算機ホログラムのことを CGPH と呼ぶことにする。

2. 複素アダマル変換を用いた擬似計算機ホログラム (CGPH)

2.1 複素アダマル変換

ここでは、複素アダマル変換について述べる。アダマル変換は直交変換のひとつとして挙げられるが、その行列を 2 行 2 列で表すと、次式となる。

$$H = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad (1)$$

この式 (1) は、実数型のアダマル変換であるが、本論文で用いる複素アダマル変換の変換行列 H は、その行列を 2 行 2 列で表すと、次式となる。

$$H = \begin{bmatrix} 1 & i \\ -i & -1 \end{bmatrix} \quad (2)$$

複素アダマル行列の種類についてはいくつかあると思われるが、逆行列が同じものになる直交行列であるもののひとつを式 (2) に挙げた。この行列を 4×4 に拡大した行列は次式のようにになる。

$$H = \begin{bmatrix} 1 & i & i & -1 \\ -i & -1 & 1 & -i \\ -i & 1 & -1 & -i \\ -1 & i & i & 1 \end{bmatrix} \quad (3)$$

このアダマル行列をクロネッカー積を利用して、 128×128 の行列や 256×256 としたうえで、複素アダマル変換を行う。なお、2 次元の複素アダマル変換は、2 次元 DCT などと同様、まず行方向の複素アダマル変換を行い、次に列方向の複素アダマル変換を行うことで、実行が可能となる。

図 1 原画像
Original image.

2.2 CGPH の合成

CGH は、入力物体を複素フーリエ変換して、複素振幅を量子化して表示することによって合成される。この CGH からの再生は CGH のパターンを読み込んで複素フーリエ変換することによって得ることができる。この章では、CGH での回折計算に用いられる複素フーリエ変換に代わり、複素アダマル変換を利用した場合についての像の性質について検討する。CGH は複素フーリエ変換の計算をベースにしていることから、複素アダマル変換を利用して複素数値を CGH と同じように量子化したものについては“擬似計算機合成ホログラム”(CGPH) と呼ぶことにする。

CGPH における入力物体には、ランダム位相を付加する。すなわち、入力物体の振幅を $f(i, j)$ とするとランダム位相 $\phi_R(i, j)$ を付加した複素振幅 $f_R(i, j)$ は以下のようにになる。

$$f_R(i, j) = f(i, j) \exp(-j\phi_R(i, j)) \quad (4)$$

ただし、 (i, j) は物体平面状の座標であり、ランダム位相 $\phi_R(i, j)$ は $-\pi \sim \pi$ の一様乱数であるものとする。

このランダム位相を付加した入力物体 $f_R(i, j)$ を複素アダマル変換し、 $F(u, v)$ を得る。

$$F(u, v) = H[f_R(i, j)] \quad (5)$$

ただし、 $H[\cdot]$ は $\cdot$ の複素アダマル変換を意味する。この複素アダマル変換をフーリエ変換とした場合には従来の計算機ホログラム⁵⁾と同じになる。

この $F(u, v)$ を、次式にしたがって、位相情報を抽出し、必要な量子化数にしたがって量子化する。

$$F'(u, v) = Q[\arg\{F(u, v)\}] \quad (6)$$

ただし、 $Q[\cdot]$ は $\cdot$ を量子化することを意味する。たとえば、量子化数を 2 とすると、

$$Q[\phi] = \begin{cases} 1 & (-\pi/2 \leq \phi \leq \pi/2) \\ -1 & (otherwise) \end{cases} \quad (7)$$

となる。

この $F'(u, v)$ を CGPH とする。

ここで、式 (6) で量子化数が 3 以上となった場合を擬似キノフォームとし、量子化数が 2 のときに CGPH と呼ぶことにする。したがって、表 1 に示すように、回折計算の

表 1 計算機ホログラムならびに擬似計算機ホログラムの分類
Classification of Computer-Generated Holograms and
Computer-Generated Pseudo Holograms.

回折計算	位相量子化数	本論文での名称
フーリエ変換	2	計算機ホログラム (CGH)
フーリエ変換	3 以上	キノフォーム
複素アダマール変換	2	擬似計算機ホログラム (CGPH)
複素アダマール変換	3 以上	擬似キノフォーム

(a) 擬似キノフォーム (b) その再生像

図 2 擬似キノフォームとその再生像 (原画像は図 1)
Pseudo Kinoform and Reconstructed Image (Original Image is Fig.1).

種類, 位相量子化数の観点から分類し, 本論文ではそのように呼ぶものとする. たとえば, 式 (5) においてフーリエ変換を用いた場合で, ここで, 式 (6) で量子化数が 3 以上となった場合はキノフォーム¹⁴⁾と呼ばれる.

2.3 CGPH と再生像

(1) 擬似キノフォーム

複素アダマール変換を用いて, 位相量子化数を 255 とした場合の擬似キノフォームならびにその再生像を図 2 に示す. ここで, 原画像は図 1 としており, 本論文で一貫して扱う原画像としている. この場合の擬似キノフォーム (図 2(a)) は位相を 256 段階に量子化したものである. この擬似キノフォームを複素アダマール変換することによって得られる再生像 (図 2(b)) は文字 “F” が 1 箇所再生されている. 図 3 は, フーリエ変換を用いたキノフォーム¹⁴⁾とその再生像を示しているが, 再生像においては文字 “F” が 1 箇所再生されている. このことから, 図 2(b) と図 3 を対比させると, 雑音の発生の様子は異なるものの, 文字 “F” の出現数ならびに出現位置は同様になることがいえる. したがって, キノフォームの合成過程におけるフーリエ変換を複素アダマール変換に置き換え, 再生像を得る際にもフーリエ変換を複素アダマール変換に置き換えた場合には, キノフォームと同じような像再生結果が得られることがわかる.

(2) CGPH

前述の擬似キノフォームに関して, 位相量子化数を 2 とした場合である CGPH ならびにその再生像を図 4 に示す. この場合の CGPH (図 4(a)) は図 2(a) を 2 値画像にしたような形状となっており, それを複素アダマール変換することによって得られる再生像 (図 4(b)) は図 5 に示すように CGH からの再生像と類似したものとなっている. このことから, CGH の合成過程におけるフーリエ変換を複素ア

(a) キノフォーム (b) その再生像

図 3 キノフォームとその再生像
Kinoform and Reconstructed Image (Original Image is Fig.1).

(a) CGPH (b) その再生像

図 4 CGPH とその再生像 (原画像は図 1)
Pseudo Computer-Generated Hologram and Reconstructed Image (Original Image is Fig.1).

(a) CGH (b) その再生像

図 5 CGH とその再生像 (原画像は図 1)
Computer-Generated Hologram and Reconstructed Image (Original Image is Fig.1).

ダマール変換に置き換え, 再生像を得る際にもフーリエ変換を複素アダマール変換に置き換えた場合には, 図 5 に示すように CGH と同じような像再生結果が得られることがわかる.

3. 2 値画像への CGPH の埋込み

ここでは, 複素アダマール変換を用いた擬似計算機ホログラムの応用事例として, 白黒 2 値画像への CGPH の埋込み方法について述べる. これは, 文献 8) をベースとしたものであるが, 埋込む秘密画像として CGH に代えて CGPH を用いたものである.

3.1 組織的ディザ法の原理

組織的ディザ法とは, ハーフトーン処理における代表的なもののひとつとして知られているものである. すなわち, 2 値に量子化する際の閾値を画素ごとに変化させ, 擬似的

0	8	2	10
12	4	14	6
3	11	1	9
15	7	13	5

 D_1
(a-1) Bayer Dither (Type 1)

8	0	10	2
4	12	6	14
11	3	9	1
7	15	5	13

 D_0 | 0 | 8 | 2 | 10 |
12	4	14	6
3	11	1	9
15	7	13	5
 D_1
(a-2) Bayer Dither (Type2)

0	12	3	15
8	4	11	7
2	14	1	13
10	6	9	5

 D_0 | 11 | 4 | 6 | 9 |
12	0	2	14
7	8	10	5
3	15	13	1
 D_1
(b-1) Meshed Dither (Type 1)

11	12	7	3
4	0	8	15
6	2	10	13
9	14	5	1

 D_0 | 11 | 4 | 6 | 9 |
12	0	2	14
7	8	10	5
3	15	13	1
 D_1
(b-2) Meshed Dither (Type 2)

11	4	6	9
12	9	2	14
7	8	2	5
3	15	13	1

 D_0 | 11 | 4 | 6 | 9 |
12	0	2	14
7	8	10	5
3	15	13	1
 D_1
(b-3) Meshed Dither (Type 3)

11	4	6	9
12	15	2	14
7	8	10	5
3	0	13	1

 D_0 | 7 | 10 | 13 | 0 |
12	1	6	11
2	15	8	5
9	3	3	14
 D_1
(c) Pan Magic Dither
 D_0

図 9 ディザ行列の組合せ
Pair of the Dither Matrix.

を抽出することができる。

4.2 ディザ行列の組合せに対する効果について

本手法ではカバー画像におけるディザ行列を2種類用いるが、ディザ行列の組合せ方によって、得られる出力画像の画質やテクスチャ、秘密画像の再生像の画質などが異なる。ここでは様々なディザ行列の組合せでどういった画像が得られるかを比較した。図9に実験で用いたディザ行列の組合せを示す。またそれを用いて実際に秘密画像を埋込んだ画像とその再生像を示す。ここで表のタイトルはディザ行列の組合せの名前である。表中の D_1 と D_0 は前節で示したようにCGHが1（白）の場合と0（黒）の場合に用いるディザ行列である。

まず、それぞれのCGHを埋込んだ画像をみると、通常のディザ法の画像と比較して画質の劣化はほとんど目立たないことがわかる。これはディザ法による画像を観察する場合において、人間の目の空間周波数特性により、画像と目との距離が離れると視覚的にグレースケールを表現するためのものである。本論文の方法では、CGHを埋込むために各ブロックの規則的なノイズを2種類のディザ行列を

(a) Bayer Dither

(b) Meshed Dither

(c) Pan Magic Dither

図 10 CGHを埋込んでいない2値画像
Binary Image embedding the non CGH.

用いて与えている。そのために図10に示すような通常のディザ行列を用いたディザ画像と比較して、不規則的なディザ模様になってきているが、図11～図16に示すように、画質の劣化は気にならない程度のものであることがわかる。表2に図11～図16に示す実験結果で示した2値画像の階調表現に関するコスト E_m を示す¹⁶⁾。コスト E_m は次式で計算される。

$$E_m = \sum_{(i,j) \in \text{block}} \frac{1}{N_p} |g(i,j) - b_g(i,j)| \quad (9)$$

ここで、座標 (i,j) における原画像の階調濃度を $g(i,j)$ 、再生像の階調濃度を $B(i,j)$ とする。また、 $b_g(i,j)$ は2値パターンにガウシアンフィルタを畳み込んだものの階調濃度、 N_p は block 内の画素数である。この式における block はカバー画像全体の領域を意味する。

(a) Binary Image embedding the CGPH

(b) Simulation of the Reconstruction from (a)

図 11 CGPH を埋込んだ 2 値画像と再生シミュレーション (図 9(a-1))

Binary Image with Confidential CGPH and The Simulation of the Reconstruction (Fig.9(a-1)).

(a) Binary Image embedding the CGPH

(b) Simulation of the Reconstruction from (a)

図 12 CGPH を埋込んだ 2 値画像と再生シミュレーション (図 9(a-2))

Binary Image with Confidential CGPH and The Simulation of the Reconstruction (Fig.9(a-2)).

表 2 に示すように、CGH の埋込みを行う場合と行わない場合とのコスト E_m の差は、いずれのディザ法についても非常に少ないといえる。

それぞれの埋込み画像 (図 11(a)~図 16(a)) を見ると、図示した大きさでは、ディザ画像に何かが入っている感じにくいものとなっている。これは、埋込んだ CGPH が図 8(b) に示すように、SA を用いて最適化したものを用いたものであるため、CGPH パターンが複雑なものになっているためである。組織的ディザ法では各ブロックに規則的なノイズを与えることで、階調特性を向上させている。本論文の方法では、CGH を埋込むために各ブロックの規則的なノイズを 2 種類のディザ行列を用いて与えている。そのために、図 10 に示すような通常のディザ行列を用いたディザ画像と比較して、図 11(a)~図 16(a) に示す 2 値画像は不規則なディザ模様になっていると考えられる。二つのディザ行列を用いる本方法において、用いる 2 種類の行列の成分配置の差異が少なければ少ないほど、不規則なディザ模様の出現が目立たなくなるために画質は向上すると考えられる。また、これらの CGPH を埋込んだ画像そのものを CGPH とみなして秘密画像を抽出した結果 (図 11(b)~図 16(b)) を見ると、図 12(b) が秘密画像である “F” が最も明確に再生されていることがわかる。

(a) Binary Image embedding the CGPH

(b) Simulation of the Reconstruction from (a)

図 13 CGPH を埋込んだ 2 値画像と再生シミュレーション (図 9(b-1))

Binary Image with Confidential CGPH and The Simulation of the Reconstruction (Fig.9(b-1)).

(a) Binary Image embedding the CGPH

(b) Simulation of the Reconstruction from (a)

図 14 CGPH を埋込んだ 2 値画像と再生シミュレーション (図 9(b-2))

Binary Image with Confidential CGPH and The Simulation of the Reconstruction (Fig.9(b-2)).

(a) Binary Image embedding the CGPH

(b) Simulation of the Reconstruction from (a)

図 15 CGPH を埋込んだ 2 値画像と再生シミュレーション (図 9(b-3))

Binary Image with Confidential CGPH and The Simulation of the Reconstruction (Fig.9(b-3)).

(a) Binary Image embedding the CGPH

(b) Simulation of the Reconstruction from (a)

図 16 CGPH を埋込んだ 2 値画像と再生シミュレーション (図 9(c))

Binary Image with Confidential CGPH and The Simulation of the Reconstruction (Fig.9(c)).

表 2 階調表現の評価
Evaluation of tone expression.

ディザの種類	CGH の埋込み	処理画像	コスト E_m
Bayer	なし	図 10(a)	16.07
Bayer (図 9(a-1))	あり	図 11	17.79
Bayer (図 9(a-2))	あり	図 12	19.30
網点	なし	図 10(b)	31.15
網点 (図 9(b-1))	あり	図 13	32.21
網点 (図 9(b-2))	あり	図 14	31.94
網点 (図 9(b-3))	あり	図 15	31.98
魔方陣	なし	図 10(c)	18.01
魔方陣 (図 9(c))	あり	図 16	21.33

4.3 文献 8) における秘密情報抽出結果との差異

図 12(a) に示す複素アダマール変換を利用した CGPH を埋込んだ 2 値画像からの秘密画像抽出は、図 12(a) を複素アダマール変換を行うことにより図 12(b) のような結果となり、秘密情報 “F” が 2 箇所に現れる結果となる。これは、文献 8) のプロセスにおけるフーリエ変換を複素アダマール変換に置き換えた場合の結果といえる。

この図 12(a) を作製するプロセスにおける複素アダマール変換をフーリエ変換に置き換え、秘密情報の抽出における複素アダマール変換をフーリエ変換として置き換えた場合の結果を図 17 に示す。ただし、秘密情報は図 18 に示すようなものであり、図 18(b) の作製過程においてはフーリエ変換を用いたものである。また、図 17(a) 作成におけるディザ行列の組合せは Fig.9(a-2) を用いている。図 17(b)

(a) Binary Image embedding the CGH

(b) Simulation of the Reconstruction from (a)

図 17 CGH を埋込んだ 2 値画像と再生シミュレーション (図 9(a-2))

Binary Image with Confidential CGH and The Simulation of the Reconstruction (Fig.9(a-2)).

をみると、秘密情報“F”が多くの箇所が発生しており、図 18(c) が複数枚タイル状に組合さったようになっている。

その理由は、次のようになる。図 12(a) には図 8(b) に示す $128(H) \times 128(V)$ 画素の CGH を $512(H) \times 512(V)$ 画素に拡大した状態で埋め込まれている。図 19(a) に示すような $128(H) \times 128(V)$ 画素の CGH (図 18(b)) を $512(H) \times 512(V)$ 画素に拡大したものをフーリエ変換すると図 19(b) となり、図 18(c) が複数枚タイル状につなげたような形状になっている。これはフーリエ変換における拡大縮小の性質であるため、図 17(a) をフーリエ変換した面すなわち図 17(b) のようになると考えられる。

ところが、複素アダマル変換では、拡大縮小における周波数軸の変化がフーリエ変換の場合とは同じであるとは限らない。図 20(a) は図 18(a) を縦横 4 倍に拡大したものであり、これを複素アダマル変換すると図 20(b) になり、物体“F”の大きさも 4 倍になってしまう。このことから、図 12(b) のように秘密情報“F”が 2 箇所にはしか現れないような大きさとなると考えられる。

このことから、文献 8) のようにフーリエ変換を用いた場合と、本論文のように複素アダマル変換を用いた場合とでは、得られる秘密情報の大きさが異なってくることがわかる。

(a) Confidential image (b) CGH of (a)

(c) Reconstructed image from (b)

図 18 秘密画像 (フーリエ変換) Confidential image (Fourier).

4.4 攻撃耐性に関する評価

ここでは、各種攻撃に対する秘密画像の取得に対する影響を考察する。なお、この考察を行うにあたり、StirMark ベンチマークによる各種の変形を行った後、複素アダマル変換を用いて再生シミュレーションを行い、秘密情報である文字“F”が再生されるかどうかで耐性を評価するものとした。ここで、二つのディザ行列の組は図 9(a-2) に示したものをを用いるものとし、図 12(a) に示す埋込み画像に対して StirMark の攻撃を加えるものとした。なお、秘密情報は図 8(b) に示すように、CGPH に変換されているので、秘密情報自体 (図 8(a) のようなもの) の複雑さはここでは問題とならない。

この章では、CGPH を埋込んだ画像においては StirMark 攻撃に脆弱であり、CGH を埋込んだ画像においては StirMark 攻撃に対するロバスト性があることを示す。

このことについて、複素アダマル変換の場合と、フーリエ変換の場合との比較を行うため、秘密画像の原画像は図 8(a) ならびに図 18(a) に示すように、同じものをを用いるものとする。また、CGH を埋込んだ画像は図 17(b) に示すものを StirMark 攻撃を行いフーリエ変換による秘密画像の抽出を行うものとした。加えて、CGPH を埋込んだ画像は図 12(a) に示すものを StirMark 攻撃を行い複素アダマル変換による秘密画像の抽出を行うものとした。さらに、CGPH ならびに CGH を埋め込む際のディザ行列の組合せはいずれも図 9(a-2) に示したものをを用いるものとした。したがって、いずれの場合も、これらの両者の間で異なるのは秘密情報埋込み画像の作製から秘密情報抽出に至るまでのプロセスにおいて、一貫して複素アダマル変換を利用しているか、一貫してフーリエ変換を利用しているかの違いだけである。

(a) Binary Image enlarging the CGH

(b) Simulation of the Reconstruction from (a)

図 19 CGH (図 18(b)) を 4 倍に拡大した 2 値画像とフーリエ変換を利用した再生シミュレーション

Enlarging CGH (Fig.18(a)) and The Simulation of the Reconstruction using Fourier Transform.

(a) Binary Image embedding the CGPH

(b) Simulation of the Reconstruction from (a)

図 21 拡大攻撃の影響 (150%) (アダマール変換)
Influence of size expansion attack(150%)(Hadamard).

(a) Binary Image enlarging the CGPH

(b) Simulation of the Reconstruction from (a)

図 20 CGPH (図 8(b)) を 4 倍に拡大した 2 値画像と複素アダマール変換を利用した再生シミュレーション

Enlarging CGPH (Fig.8(a)) and The Simulation of the Reconstruction using Complex Hadamard Transform.

(a) Binary Image embedding the CGPH

(b) Simulation of the Reconstruction from (a)

図 22 拡大攻撃の影響 (200%) (アダマール変換)
Influence of size expansion attack(200%) (Hadamard).

(1) 拡大縮小に対する影響

ここでは、拡大縮小 (RESC) の攻撃を受けた状態について述べる。

まず、図 21(a) は図 12(a) に寸法で 150% の拡大攻撃 (RESC-150) * を加えたものであり、図 21(b) は図 21(a) を複素アダマール変換して秘密画像を抽出した結果を示したものである。この画像は、縦 768 ピクセル、横 768 ピクセルとなっており、再生シミュレーションに複素アダマール変換を用いた計算を利用している理由から、縦 1024 ピクセル、横 1024 ピクセルとして計算した。縦横 256 ピクセル分は、ブランクを挿入することとしている。CGPH からの再生においてアダマール変換を利用すると観点から、図 21(a) のように埋込み画像を拡大した場合には、秘密画像が出現しなくなっている。

次に、図 22(a) は図 12(a) に寸法で 200% の拡大攻撃 (RESC-200) を加えたものであり、図 22(b) は図 22(a) を複素アダマール変換して秘密画像を抽出した結果を示したものである。この画像は、縦 1024 ピクセル、横 1024 ピクセルとして計算した。この場合は、ビットマップを単純に縦横 2 倍に拡大したものとなっているため、図 12(a) の 1 画素を単純に 2×2 画素に拡大したものとなっていることから、ビットマップの形状を崩さずに拡大した場合 (図 22(a)) には、秘密画像も比例して大きさが拡大していることがわかる。

また、図 23(a) は図 12(a) に寸法で 75% の縮小攻撃 (RESC-75) を加えたものであり、図 23(b) は図 23(a) を複素アダマール変換して秘密画像を抽出した結果を示したものである。縮小された画像は縦 384 ピクセル、横 384 ピクセルであるため、秘密情報抽出を考慮して、縦 512 ピクセル、横 512 ピクセルのブランク領域に組み込んで、余った領域はブランク (黒) を挿入している。また、縮小するとディザパターンの模様がつぶれることになるが、補間処理をしているものとしている。CGPH からの再生においてアダマール変換を利用している観点から、埋込み画像を縮小した場合 (図 23(a)) には、図 12(a) の 4×4 画素を 3×3 画素に縮小して表示をしていることから、ビットマップ構造が崩れているために秘密情報である文字 “F” がわからなくなっている。

このことから、図 22 に示すようにビットマップの 1 画素を 2 画素 $\times$ 2 画素のように整数倍にする操作以外では、CGPH を埋込んだ画像から秘密情報を取り出すことはできないということができる。

ところで、図 24、図 25、図 26 は、それぞれ、図 21、図 22、図 23 におけるすべての複素アダマール変換の処理をフーリエ変換に置き換えた場合、すなわち文献 8) の方法のものである。この場合は秘密情報の “F” が再生されていることから、フーリエ変換の場合では拡大縮小に対してロバ

ストであるが、複素アダマール変換の場合には脆弱になっていることがわかる。ここで、秘密情報である “F” の大きさが小さくなっているが、これは前節で示したようにフーリエ変換を用いた場合の性質に起因するものである。

(2) 埋込み画像の一部消去に対する影響

まず、クロッピング攻撃について示す。ここでは、縦横寸法で 75% の領域だけをのこしてあとは情報を捨てた場合 (CROP-75) の実験例を示す^{**}。図 27(a) は図 12(a) の一部を消去した場合のものであり、図 27(b) は図 27(a) を複素アダマール変換して秘密画像の抽出をした結果を示したものである。なお、一部を消去した画像は縦 512 ピクセル、横 512 ピクセルよりも小さくなっているため、余った領域はブランク (黒) を埋込んであるものとしている。図 27(b) より秘密情報である “F” は雑音に埋もれていることがわかる。

図 28 は、図 27 に関するすべての複素アダマール変換の処理をフーリエ変換に置き換えたもの (すなわち文献 8) の方法において、秘密情報の一部消去攻撃 (CROP-75) を加えた場合の結果である。この場合は、秘密情報である “F” が再生されているので、フーリエ変換を用いた場合はロバスト性があり、複素アダマール変換を用いた場合には脆弱であるということができる。

つぎに、リムーブライン攻撃について示す。ここでは、RML 攻撃の中でデータの改ざん規模が最も小さい RML-100^{***} の攻撃を加えたもので、縦横 3 ラインを均一に消去したものである。図 29(a) は図 12(a) の一部のラインを消去した場合のものであり、図 29(b) は図 29(a) を複素アダマール変換して秘密画像を抽出した結果を示したものである。なお、図 29(a) において一部を消去した画像は縦 512 ピクセル、横 512 ピクセルよりも小さくなっているため、余った領域はブランク (黒) を埋込んでいるものとしている。図 29(b) より秘密情報である “F” が再生されていない。このような RML 攻撃の場合、CGPH のディザパターンが崩れているということから、秘密情報が抽出できないということができる。

図 30 は、図 29 に関するすべての複素アダマール変換の処理をフーリエ変換に置き換えたもの (すなわち文献 8) の方法において、秘密情報の一部消去攻撃 (RML-100) を加えた場合の結果である。この場合は、秘密情報である “F” が再生されているので、フーリエ変換を用いた場合はロバスト性があり、複素アダマール変換を用いた場合には脆弱であるということができる。

このことから、CGH に多少の損傷を入れたとしても CGH からは像が再生されるという性質¹⁷⁾ は CGH の場合における性質であり、CGPH にはあてはまらないことが考えら

* StirMark における拡大攻撃においては 150% の寸法に拡大するものと、200% の寸法に拡大するものの 2 通りである。

** CROP 攻撃には、情報を残す割合として 75%、50%、25% などがあり、もっとも多くの情報が残るのは CROP-75 すなわち 75% である。

*** ライン消去攻撃 RML においては、RML-100、RML-90、RML-80 などあるが、この数字が小さくなるほど消去するライン数が多くなる。

(a) Binary Image embedding the CGPH

(b) Simulation of the Reconstruction from (a)

図 23 縮小攻撃の影響 (アダマール変換)
Influence of size reduction attack (Hadamard).

(a) Binary Image embedding the CGH

(b) Simulation of the Reconstruction from (a)

図 25 拡大攻撃の影響 (200%) (フーリエ変換)
Influence of size expansion attack(200%) (Fourier).

(a) Binary Image embedding the CGH

(b) Simulation of the Reconstruction from (a)

図 24 拡大攻撃の影響 (150%) (フーリエ変換)
Influence of size expansion attack(150%) (Fourier).

(a) Binary Image embedding the CGH

(b) Simulation of the Reconstruction from (a)

図 26 縮小攻撃の影響 (フーリエ変換)
Influence of size reduction attack (Fourier).

れる．すなわち，フーリエ変換を複素アダマール変換に置き換えた場合にはホログラムの情報一部消去に関する性質は保存されないことになる．

(3) 回転攻撃に対する影響

図 31(a) は図 12(a) を 0.25° 回転させた場合 (ROT-0.25) のものであり，図 31(b) は図 31(a) を複素アダマール変換した秘密画像の抽出結果を示したものである*．なお，縦 512 ピクセル，横 512 ピクセルよりはみ出した領域については切り取っている．図 31(a) より埋込み画像のディザパターンが回転の影響で精緻に再現されていない理由から，秘密画像 “F” が取り出せないことがわかる．すなわち，回転が伴った場合でもビットマップの構造に影響を及ぼす場合には，秘密画像を取り出すことはできないといえることができる．

また，回転を伴う攻撃には，ROTCROP, ROTSCALE などがあるが，いずれの場合も，埋込み画像においてビットマップにおける白黒の構造に変化をきたすため，CGPH を埋込んだ画像からの秘密画像の抽出はできないことが考えられる．このことは，先述の拡大縮小 (RESC) や回転 (ROT) ならびに情報の一部切り取り (CROP) における知見から，類推されるものである．

図 32(a) は図 17(a) を 0.25° 回転させた場合 (ROT-0.25) のものであり，図 32(b) は図 32(a) をフーリエ変換した秘密画像の抽出結果を示したものである．すなわち，図 31 における複素アダマール変換をフーリエ変換に置き換えた場合のものであるが，回転攻撃 (ROT-0.25) を加えても図 32 に示すように，秘密情報である “F” は再生されることがわかる．したがって，フーリエ変換の場合には回転攻撃に対してロバスト性があるが，複素アダマール変換の場合には回転攻撃に対して脆弱であるといえることができる．

(4) 平滑化フィルタ攻撃に対する影響

図 33(a) は図 12(a) に平滑化フィルタ (SS-3 攻撃) を用いた場合のものであり，図 33(b) は図 33(a) を複素アダマール変換して秘密画像を抽出した結果を示したものである．図 33(b) より，秘密画像 “F” はこの場合も再生されていないことがわかる．このことから，平滑化フィルタ攻撃を行う場合も，ディザパターンが崩れてしまっているため，秘密画像は抽出できないので，幾何学的変換にくわえ，平滑化フィルタ攻撃に対しても脆弱であるといえることができる．

図 34(a) は図 17(a) に平滑化フィルタ (SS-3 攻撃) を用いたものであり，図 34(b) は図 34(a) をフーリエ変換して秘密画像を抽出した結果を示したものである．すなわち，図 33 に示した結果を得るまでのすべての複素アダマール変換のプロセスをフーリエ変換に置き換えたものであるが，この場合は平滑化フィルタ攻撃 (SS-3 攻撃) に対してロバストであることがいえる．

平滑化フィルタ攻撃においても，フーリエ変換の場合は

* 回転攻撃には，回転角が 0.25° ， 0.5° ， 0.75° ， 1° などとあり，もっとも回転角の小さいものは 0.25° である．

(a) Binary Image embedding the CGPH

(b) Simulation of the Reconstruction from (a)

図 27 一部消去攻撃 (クロッピング) の影響 (アダマール変換)
Influence of cropping attack (Hadamard).

(a) Binary Image embedding the CGH

(b) Simulation of the Reconstruction from (a)

図 28 一部消去攻撃 (クロッピング) の影響 (フーリエ変換)
Influence of cropping attack (Fourier).

(a) Binary Image embedding the CGPH

(b) Simulation of the Reconstruction from (a)

図 29 一部消去攻撃（ラインの間引き）の影響（アダマール変換）

Influence of remove line attack (Hadamard).

(a) Binary Image embedding the CPGH

(b) Simulation of the Reconstruction from (a)

図 31 回転攻撃の影響（ 0.25° ）（アダマール変換）
Influence of rotation attack (0.25°) (Hadamard).

(a) Binary Image embedding the CGH

(b) Simulation of the Reconstruction from (a)

図 30 一部消去攻撃（ラインの間引き）の影響（フーリエ変換）
Influence of remove line attack (Fourier).

(a) Binary Image embedding the CGH

(b) Simulation of the Reconstruction from (a)

図 32 回転攻撃の影響（ 0.25° ）（フーリエ変換）
Influence of rotation attack (0.25°) (Hadamard).

ロバスト性があり、複素アダマール変換の場合は脆弱であるといえることができる。

(5) JPEG 攻撃に対する影響

図 35(a) は図 12(a) に対して、圧縮率 90% の JPEG 圧縮攻撃 (JPEG) をした場合のもので、図 35(b) は図 35(a) を複素アダマール変換して秘密情報を抽出した結果である。この場合は、JPEG 攻撃を行っても白黒 2 値画像における白黒のディザパターンがほとんど変化しないため、秘密情報を抽出は影響がないといえることができる。すなわち、JPEG は非可逆符号化を用いた情報の圧縮を利用したものであるため、圧縮率が高くなればもとのディザパターンと異なってくる可能性があるが、2 値画像の場合は圧縮前のディザパターンと圧縮後のディザパターンとの間の差異がほとんどないことから、秘密情報を抽出において画質への影響はほとんどないといえることができる。

このことから、JPEG 攻撃の影響を受けにくい 2 値画像に対しては JPEG 攻撃を行っても埋込み画像のディザパターンに変化が及ばないため、秘密情報の抽出画像の画質に影響はないと考えられる。図 36(a) は図 17(a) に対して圧縮率 90% の JPEG 圧縮攻撃 (JPEG) をした場合のもので、図 36(b) は図 36(a) を複素アダマール変換して秘密情報を抽出した結果である。すなわち、図 36 は図 35 におけるすべての複素アダマール変換の処理をフーリエ変換に置き換えた場合の結果である。この場合も、JPEG 攻撃を行っても埋込み画像のディザパターンに変化が及ばないと考えられることから、秘密情報の抽出画像において画質に影響が及ばないといえることができる。

(6) 各種の形状歪みを加えた場合の影響

この場合の一例として、アフィン変換攻撃に対する影響について述べる。ここでは、アフィン変換攻撃のなかでデータ改ざんの規模の最も小さいものの一例として AFFINE-4* を加えた場合の結果を示している。図 37(a) は図 12(a) を AFFINE-4 なるアフィン変換攻撃を行ったものであり、図 37(b) は図 37(a) を複素アダマール変換して秘密情報を抽出した結果である。このように、StirMark ベンチマークに用意されている程度のアフィン変換の変形程度であっても、秘密情報を埋込んだ画像のディザパターンに変化を及ぼしているため、秘密情報 “F” の抽出はできなくなっているといえる。

逆にフーリエ変換による場合は図 38 に示すように、AFFINE-4 攻撃を加えた場合でも秘密情報の抽出は可能であることがわかる。

他の攻撃として、ディストーション攻撃 (RNDDIST, LATESTRNDDIST) を加えた場合などが挙げられるが、これらについては秘密情報埋込み画像のディザパターンの形状が大きく崩れることから、この場合も秘密情報の抽出

* StirMark 攻撃における AFFINE 攻撃は AFFINE-1 から AFFINE-8 までであるが、データ改ざん規模の最も小さいものでも 1 軸方向に 1% 程度の寸法の変形しか加えられていない。

(a) Binary Image embedding the CGPH

(b) Simulation of the Reconstruction from (a)

図 33 平滑化フィルタ攻撃の影響 (アダマール変換)
Influence of smoothing filter attack (Hadamard).

(a) Binary Image embedding the CGH

(b) Simulation of the Reconstruction from (a)

図 34 平滑化フィルタ攻撃の影響 (フーリエ変換)
Influence of smoothing filter attack (Fourier).

(a) Binary Image embedding the CGPH

(b) Simulation of the Reconstruction from (a)

図 35 JPEG 攻撃の影響 (アダマール変換)
Influence of affine JPEG attack (Hadamard).

(a) Binary Image embedding the CGH

(b) Simulation of the Reconstruction from (a)

図 36 JPEG 攻撃の影響 (フーリエ変換)
Influence of affine JPEG attack (Fourier).

は困難になると考えられる。

(7) デイザ画像への CGPH の埋込みの応用可能性

前節までの結果から、デイザ画像への CGPH の埋込んだ場合は、各種 StirMark 攻撃に対して脆弱な攻撃耐性を示していることがわかった。複素アダマール変換を用いた CGPH ではなくて、フーリエ変換を用いた CGH を埋込んだ場合は、文献 8) に示すように各種 StirMark 攻撃に対してロバストな攻撃耐性を示している。このことから、秘密情報として埋込むホログラムが CGH の場合と CGPH の場合とでは攻撃耐性が大きく異なることがわかった。ところで、各種 StirMark 攻撃に対して脆弱な攻撃耐性を有するデータハイディングの応用としては、改ざんを加えたものからは本物であるという認証が取れないような目的のものが適していると考えられる。すなわち、それを複写しようとしてスキニングしても、ビットマップ形状を正確に保持できなかった場合には秘密情報は取り出せないため、秘密情報が抽出できないものは偽物として判別することが可能になると考えられる。

5. む す び

本論文では、CGH における回折計算であるフーリエ変換を複素アダマール変換に置き換えた CGPH を合成し、デイザ画像に対して CGPH を埋め込む方法を応用例として提案し、その性質について検討した。

まず、複素アダマール変換を用いた擬似計算機ホログラムにおける再生像の性質について検討した。直交変換を利用したものであることから、フーリエ変換の場合であれ、複素アダマール変換の場合であれ、類似した結果となることがわかった。

次に、CGPH の埋込みについて検討した。埋め込む CGH は SA によって最適化したものであるものとしたが、CGH の埋込みの有無に対して、デイザ法を施した画像の画質評価を階調表現の観点から行った結果、CGH を埋め込むことによる画質の変化は少ないことがわかった。このことは、本論文に示した図程度の大きさであれば画質には大きな問題とはなりにくいことを示している。

また、秘密情報の埋め込まれた 2 値画像に各種攻撃を加え、その耐性について検討した。StirMark 攻撃において、拡大、縮小、回転、平滑化フィルタ、アフィン攻撃において、最も程度の少ない攻撃であっても、秘密情報が取り出せないことがわかった。逆にいえば、白黒 2 値画像のデイザパターンが崩れない場合にだけ秘密情報が取り出せることから、幾何学的変換に対して、脆弱な秘密情報埋込み方式であることがわかった。このことから、各種攻撃に対して脆弱な耐性を持つ方式であることがわかった。

以上のことから、デイザ画像に対して CGPH を埋め込むと、文献 8) のような強い攻撃耐性が得られないかわりに、2 値画像のコピー防止の観点から有効な方法であることが示された。今後の課題としては、CGPH の再生像改善手法

(a) Binary Image embedding the CGH

(b) Simulation of the Reconstruction from (a)

図 37 アフィン変換攻撃の影響 (アダマル変換)
Influence of affine transform attack (Hadamard).

(a) Binary Image embedding the CGH

(b) Simulation of the Reconstruction from (a)

図 38 アフィン変換攻撃の影響 (フーリエ変換)
Influence of affine transform attack (Fourier).

の確立や、情報セキュリティ分野での実用の可能性について試行を含めた詳細の検討などが挙げられる。

本研究は、文部科学省科学研究費補助金 (若手研究 (B) 課題番号 15760278) の支援を受けました。ここに感謝の意を表します。

〔文 献〕

- 1) B.E. Bayer, "An optimum method for two-level rendition of continuous-tone pictures", Internl. Conf. on Comm., **50**, pp.69-77, (1976)
- 2) 荻原剛志, 小出信也, 金田悠紀夫: "誤差拡散法を利用した2値画像への情報埋め込み手法", 信学論, **J82-A**, 10, pp.1555-1562(1999)
- 3) 田中清, 中村康弘, 松井甲子雄: "組織的ディザ画像への属性情報の埋め込み", 信学論, **J72-D-II**, 6, pp.880-886 (1989)
- 4) 松井甲子雄: "電子透かしの基礎", 森北出版株式会社 (1998)
- 5) 田中賢一: "GA を用いた計算機プログラムにおける最適誤差拡散係数の推定", 映情学誌, **54**, 3, pp.394-401 (2000)
- 6) 青木由直: "計算機プログラムを用いた電子透かし法", 信学論, **J82-A**, 7, pp.1092-1100 (1999)
- 7) Brown B. R. and Lohmann A. W.: "Complex spatial filtering with binary masks", Appl. Opt., **5**, 6, pp. 967-969 (1966)
- 8) 田中賢一, 石附英昭: "ディザ画像への計算機プログラムの埋込み", 映情学誌, **60**, 9, pp.1459-1472 (2006)
- 9) 田森秀明, 青木直史, 山本強: "数論変換による電子透かしを用いた改ざん位置検出法", 信学論, **J86-A**, 8, pp. 872-879 (2003)
- 10) 喜安善市: "アダマル行列とその応用 - 構成理論からウォルシュ関数まで -", 電子通信学会 (1983)
- 11) 浜田高宏, 松本修一: "アダマル変換を用いたコンボジット動き補償 NTSC フレーム間直接符号化方式", 信学論, **J77-B-I**, 7 pp.475-482 (1994)
- 12) Matsufuji S., Suehiro N.: "Complex Hadamard Matrices Related to Bent Sequences", IEEE Trans. Info. Theory, **42**, 2, p.637 (1996)
- 13) 田中賢一, 藤田泰仁, 磯井亮太: "複素アダマル変換における振幅ならびに位相の性質", 信学技報, **107**, 358, pp.7-10 (2007)
- 14) Lesem L. B., Hirsch P. M. and Jordan. Jr. J. A.: "The Kinoform: A new wavefront reconstruction device", IBM J. Res. Develop., **13**, 3, pp. 150-155 (1969)
- 15) 田中賢一, 坂本賢政, 下村輝夫: "シミュレーテッドアニーリングを用いた計算機プログラムにおけるコスト関数の影響", 信学論, **J80-C-I**, no.2, pp. 100-104 (1997)
- 16) 田中賢一: "SA を用いた疑似中間調処理画像の改良", 映情学誌, **54**, 7, pp.1450-1459, (2000)
- 17) 大越孝敬: "ホログラフィ", 電子通信学会

たなか けんいち
田中 賢一 1992 年, 九州工業大学工学部電気工学科卒, 1994 年, 同大学院修士課程修了。九州工業大学工学部助手, 明治大学理工学部電気電子工学科講師を経て, 2007 年, 明治大学理工学部電気電子生命学科准教授, 現在に至る。計算機ホログラフィ, ハーフトーン処理, 電子透かしなどの研究に従事。工博。正会員。

ふじた やすひと
藤田 泰仁 2007 年, 明治大学理工学部電気電子工学科卒業, 現在, 同大学院博士前期課程電気工学専攻在学中。複素アダマル変換の応用に関する研究に従事。

いそい りょうた
磯井 亮太 2006 年, 明治大学理工学部電気電子工学科卒業, 2008 年, 大学院博士前期課程電気工学専攻修了。在学中, 計算機プログラムの研究に従事。