

DCT領域でRDSの埋込みを行う 画像用相関型電子透かし方式に関する一検討

小田 弘*, 古田 光*

A Note on a Correlation-based Scheme of Digital Watermarking for Images embedding the RDS in DCT Domain

Hiromu KODA and Hikaru FURUTA

Abstract

In this paper, we propose a correlation based scheme of digital watermarking for images embedding the RDS (Random Dot Stereogram) in DCT (Discrete Cosine Transform) domain, and investigate the fundamental performance of the above scheme before and after attacks. First we show the definition of DCT, and describe some features of the RDS from the viewpoint of digital watermarking (i.e., information hiding) techniques. Next we explain basic procedures for the embedment and detection of our scheme. Finally we perform the computer experiments for some test images in order to examine the availability of our scheme. The experimental results show that our scheme using DCT provides better performance than the scheme using WHT (Walsh Hadamard Transform) in point of the BER (Bit Error Rate) property.

Keywords : Digital watermarking, Discrete cosine transform, Random dot stereogram, M-sequence, Bit error rate

1 はじめに

近年、デジタルコンテンツに対する不正コピーなどの不正利用の対策として、電子透かし方式の研究が進んでいる。その方式の一つとしてランダムドットステレオグラム (RDS) を透かし情報として用いた電子透かし方式が研究されてきた [1]。電子透かし方式は、透かし情報を時間領域に埋込む方式と、周波数領域に埋込む方式に大別される。文献 [2] によると、周波数領域に埋込む方式の方が、時間領域に埋込む方式と比較して、標準的な信号処理や攻撃に対して耐性があるとされている。しかしながら、先行研究 [1] では、時間領域に透かし情報を埋込む方式が検討されており、結果として、AWGN (加法性白色雑音) 付加や JPEG [3] 圧縮などの基本攻撃を受けると透かし情報が失われてしまうという欠点があった。

本稿では、周波数領域への変換の一つである、離散コサイン変換 (DCT) [4] の領域で RDS の埋込みを行う画像用相関型電子透かし方式を提案し、その処理手順 [5][6] を整理する。そして、計算機実験により、透かし入り画像に対して AWGN 付加, JPEG 圧縮, クリッピングの 3 種類の基本攻撃を行い、その攻撃耐性を調査する。さ

らに、DCT を用いた方式は、ビット誤り率 (BER) 特性の点でウォルシュ・アダマール変換 (WHT) [7] を用いた方式より相対的に良い性能を与えることを確認する。

2 2次元 DCT

DCT (Discrete Cosine Transform, 離散コサイン変換) は、直交変換の一種であり、画像信号や音声信号を圧縮する際の基礎技術として知られている。無相関化、エネルギー寄与率最大、符号化利得最大などの点で最適な直交変換である KLT (カルーネン・レーベ変換) は、隣接画素間の相関係数 ρ に対して $\rho \rightarrow 1$ の極限をとると、DCT と等しくなることが知られている [3]。つまり、 ρ が 1 に近い値をもつ多くの自然画像に対して、DCT は無相関化、エネルギー寄与率最大化、符号化利得最大化の点で最適な変換であるといえる。DCT を電子透かし方式に用いた場合にも、これらの特徴により、視覚的な影響が小さい部分に透かし情報を埋込むことや、ある程度の基本的な信号処理に対する攻撃耐性を持った電子透かし方式を実現することができる。以下に 2 次元 DCT の定義式を示す。

X を $N \times N$ の入力画像行列, Y を $N \times N$ の変換出力行列とすると, 2次元 DCT の変換式は以下で定義される.

$$\text{正変換 (DCT)} : Y = AXA^T \quad (1)$$

$$\text{逆変換 (IDCT)} : X = A^T Y A \quad (2)$$

ただし, A^T は A の転置行列を表し, A は DCT 基底行列 $[\gamma(p, q)]$ である. DCT の基底行列の各成分 $\gamma(p, q)$ は次式となる.

$$\gamma(p, q) = \sqrt{\frac{2}{N}} K(p) \cos \frac{(2q+1)p\pi}{2N} \quad (3)$$

$$(p, q = 0, 1, \dots, N-1)$$

$$K(p) = \begin{cases} 1/\sqrt{2} & (p=0) \\ 1 & (\text{otherwise}) \end{cases} \quad (4)$$

3 RDS について

人間の眼は左右に約 6cm 程度離れているため [8], 両眼に映る網膜像はわずかにずれており, このずれを両眼網膜像差 (または両眼視差) という.

両眼網膜像差を持つように描かれた左右一対の平面図形のことをステレオグラムという. その一種である, ランダムドットステレオグラム (RDS) は, 1960 年に工学者の *B. Julesz* (ユレシユ) [9] により発表され, 1971 年に書籍が出版された. これは, 両眼間の対応点を探し出す (融像する) ことにより, ランダムなドットの並びを持つ 2次元の画像 (RDS) から 3次元の画像を浮かび上がらせるという方法である [10]. 以下に RDS の描画手順を簡単に示す.

〈S1〉 擬似乱数によって, ランダムな背景画像を左右に全く同じ形で描く.

〈S2〉 同様にしてランダムな対象画像を, 2枚の背景画像 (上記 〈S1〉 で作成したもの) に, 水平方向に少し (n_0 画素) ずらして上書きする. ただし, 対象画像は背景画像よりも小さなサイズとする.

図 1 に RDS の例 (20×20 画素^{*1}, $n_0 = 1$, 知覚パターン “コ”) を示す. また, 融像した RDS の見え方の模式図を図 2 に示す. 立体視に成功した場合, 図 2 のように “コ” が浮かび上がる^{*2}. 模式図の作成には文献 [11] を参考にした. ただし, 図 2 の黒部分は影ではなく, 浮かび上がっていることを強調しているものである.

RDS の中には, オート RDS という特殊な RDS が存在する. 通常の RDS が離れた位置にある 2枚の画像を

^{*1}RDS の画像サイズは, 電子透かしの基本要件 (付録 C を参照) の 1 つである埋込み容量の目安 (42[bytes]) に近い容量 (50[bytes]) のものを用いた.

^{*2}RDS の視認の方法は平行法と交差法の 2 種類がある. 今回の RDS (図 1) は, 平行法を用いた場合は “コ” が浮かび上がるように見える. 交差法を用いた場合は, “コ” が沈み込んだように見える.

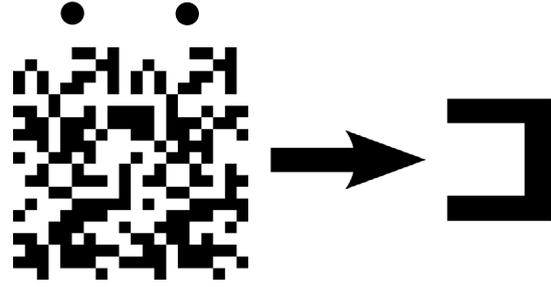


図 1: RDS の例

(20^2 画素, 知覚パターン “コ”, ●は両眼誘導用の点)

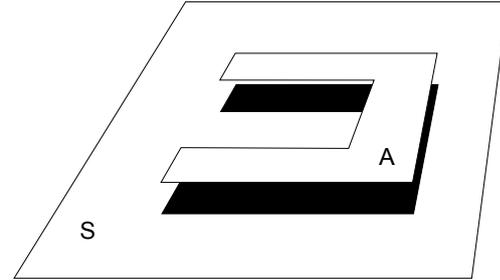


図 2: 融像した RDS の見え方の模式図 [浮かび上がり]

(A: 対象画像, S: 背景画像)

用いて融像するのに対し, オート RDS は縦に細長いランダムドットパターンが横に何周期も連続して並んでおり, 視認時にその何周期ものパターンのうち 1 周期分をずらすことで融像できるというものである. この違いにより, オート RDS は通常の RDS と比較して, 融像するまでに必要な輻輳 (ふくそう)^{*3} 変化量が小さく, 通常の RDS よりも融像難易度が低い [9]. 本稿における RDS は, 基本的な作成法は通常の RDS のものと同様であるが, 縦に長い二つの画像を合成したものであり, オート RDS のように融像しやすいよう改良されている.

4 DCT を用いた提案方式

ホスト画像^{*4}として濃淡画像を使用し, 透かし情報として RDS を DCT 領域で埋込み, 検出するための手順を以下に示す. ただし, *印の部分は, 今回新たに文献 [13] の方式 I に追加した箇所である. また, 各手順についての簡単なブロック図を図 3, 図 4 に示す.

4.1 透かし情報の埋込み方法

〈E1〉 サイズ $N_0 \times N_0$ のホスト画像をサブブロック (サイズ $N \times N = 8 \times 8$) に分割し, 各サブブロック毎に 2次元 DCT を行う. 得られた変換出力の係数行列にジグザグスキャンを行い, 低域から高域の順に並べた 1次元系列 $Y_u(i)$ ($i = 0, 1, \dots, N^2 -$

^{*3}輻輳: 単一像を得るための両眼球の回転運動 [12]

^{*4}透かし情報が埋込まれる画像

1; $u = 0, 1, \dots, N_B - 1$) を作成する. ただし, $N_B (= N_0^2/N^2)$ はサブブロックの総数であり, i は 1 サブブロック内のシーケンス番号, u は $(N_0/N) \times (N_0/N)$ 個のサブブロックをラスタスキャンの順に並べたブロック番号である (尚, 後述の検出手順の処理 (D1) では $Y_u(i)$ を $D_u(i)$ に書き直して表現する).

(E2) 各サブブロックの 1 次元系列 $Y_u(i)$ から, 特定のシーケンス成分 $Y'_u(i)$ ($i = s, s+1, \dots, s+l-1$; $u = 0, 1, \dots, N_B - 1$) を抽出する. そして, 全サブブロックの $Y'_u(i)$ を連結した 1 次元系列を $\hat{Y}(j)$ ($j = 0, 1, \dots, N_B \times l - 1$) とする. ただし, s は埋込み開始シーケンス番号, l は埋込むシーケンスの長さである (尚, 後述の検出手順の処理 (D1) では $Y'_u(i)$ を $D'_u(i)$ に, $\hat{Y}(j)$ を $\tilde{D}(j)$ に書き直して表現する).

(E3)* 透かし情報として埋込む RDS に対して, 各ドットを 2 進数で表した後, ラスタスキャンを行う. 得られた 2 進数のデータを m 個ずつ取り出し, 10 進数に変換することで M' 系列のデータ*5 を 1 本選択する.

(E4) ゲイン k を用いて, 上記 (E3) で選択した M' 系列 $W(n)$ ($n = 0, 1, \dots, L - 1$; $L (= 2^m)$ は M' 系列の長さ) を次の式 (5) で埋込む.

$$\hat{Y}(j) = \tilde{Y}(j) + k \times W(j \bmod L) \quad (5)$$

(E5) 上記 (E1) で求めた 1 次元系列 $Y_u(i)$ の内で, 透かし情報の埋込みに使用したシーケンス成分を上記 (E4) の $\hat{Y}(j)$ で置き換え, 逆ジグザグスキャンを行ってサイズ $N \times N$ のサブブロックに戻した後, 逆 DCT により透かし入り画像を作成する.

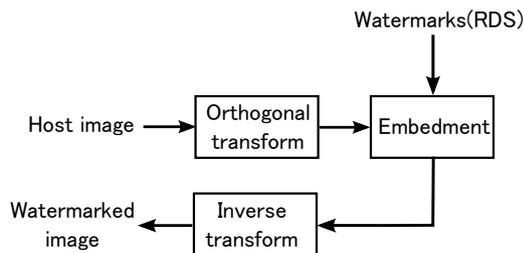


図 3: 透かし情報 (RDS) の埋込み

4.2 透かし情報の検出方法

(D1) 透かし入り画像に対して, 埋込み手順の前処理 (E1), (E2) を行い, 透かし入り系列 $\tilde{D}(j)$ ($j = 0, 1, \dots, N_B \times l - 1$) を抽出する (攻撃なしのときは, $\tilde{D}(j) = \hat{Y}(j)$ である).

*5 M' 系列: M 系列 (Maximum length sequence) の末尾に “0” を付加し, “0” を “-1” に置き換えた長さ $L = (2^m - 1) + 1 = 2^m$ [bits] の系列. この系列のデータが 256 [本] ($= 2^m, m = 8$) 用意してある [13].

(D2) 長さ L の透かし入り系列 $\tilde{D}(n)$ ($= \tilde{D}(j \bmod L)$) と透かし情報の埋込み時に用いた M' 系列 $W(n)$ ($n = 0, 1, \dots, L - 1$) との相関関数を次の式 (6) で計算し, ピークの位置 τ を透かし情報とする.

$$R(\tau) = E[\tilde{D}(n) \times W(n + \tau)] \quad (6)$$

ここで, $E[\cdot]$ *6 は期待値演算である.

(D3)* 得られた透かし情報を m ビットの 2 進数データに変換し, これを並べることによって RDS 画像 (二値画像) を再構築する.

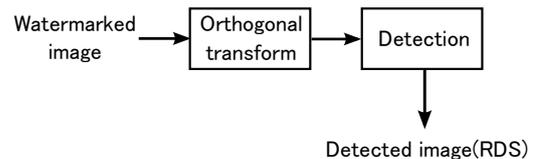


図 4: 透かし情報 (RDS) の検出

5 計算機実験

4 で述べた提案方式に対して計算機実験を行い, 攻撃前後の基本性能を調査する.

5.1 実験条件

- M' 系列: 8 次 ($m = 8$) の M' 系列, 系列の長さ $L = 256 (= 2^8 - 1) + 1$
- テスト用のホスト画像 (図 5): 標準画像 “GIRL”, “MOON” ($N_0 \times N_0 = 256^2$ 画素, 256 階調)
- 透かし情報: RDS 画像 (20² 画素, 2 階調, 知覚パターン “コ”). このときの透かし情報のデータ量は, $20^2 [\text{pels}] \times 1 [\text{bit/pel}] = 400 [\text{bits}] = 50 [\text{bytes}]$ となる.
- 埋込み領域: 4.1 の (E2) の $s = 10, l = 13$ *7
- 方式の種類:
 - (1) DCT 方式...4.1, 4.2 で述べた方式
 - (2) WHT 方式...4.1, 4.2 で述べた方式で, DCT の代わりに WHT (Walsh Hadamard Transform)[7] を使用したもの. ただし, 上記 (1) と (2) で, サブブロックサイズは共に $N \times N = 8 \times 8$ である.
- 画質の評価尺度: $\text{SNR} = 10 \log_{10}(255^2/\text{MSE})$, MSE は原画像 (ホスト画像) と透かし入り画像の濃度値の平均 2 乗誤差である.

*6 $E[\tilde{D}(n) \times W(n + \tau)]$ は, 実際には $\frac{1}{L} \sum_{n=0}^{L-1} \tilde{D}(n) \times W(n + \tau)$ として計算した.

*7 透かし情報のデータ量が 400 [bits] であるため, 容量が 400 [bits] 以上となるような最小の l の値を用いた. 具体的な計算については付録 A を参照されたい.

- 基本的な攻撃：SNR が 40[dB] 程度*⁸である透かし入り画像（SNR が 40[dB] 程度になるゲイン k の導出については付録 B 参照されたい）に対して、以下の 3 種類の攻撃を加えた。
 - (1) AWGN（加法性白色雑音）付加（平均 0, 標準偏差 $\sigma = 5, 10, \dots, 30$ ）
 - (2) JPEG 圧縮（2, 4, \dots , 16 分の 1）
 - (3) クリッピング（切り取り率 10, 20, \dots , 90[%]）

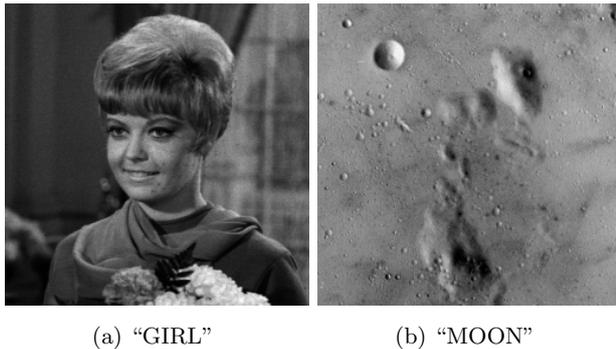


図 5: ホスト画像 (自然画像)

5.2 結果と考察

5.2.1 攻撃前の基本性能

図 6 は埋込みのゲインを変化させることで得た SNR と BER(Bit Error Rate) の関係（攻撃前）を示している。その際、WHT 方式によって透かし情報を埋込んだものと比較した。ホスト画像が“GIRL”のとき、WHT 方式は 39.616[dB] の SNR で BER=1[%] であった。それに対して、DCT 方式の場合は 39.963[dB] の SNR で BER=0[%] であった。ホスト画像が“MOON”のとき、WHT 方式は 39.610[dB] の SNR で BER=0[%] であり、DCT 方式は 39.956[dB] の SNR で BER=0[%] であった。よって、DCT 方式の性能が WHT 方式より相対的に優れていることが分かる。

次に、DCT 方式による透かし入り画像と検出画像の例（攻撃前）を図 7(“GIRL”), 図 8(“MOON”) に示す。このとき BER は 0[%] であり、透かし情報が正しく検出されていることが分かる。先行研究 [1] では、BER が 5[%] までは視認できるとしている。しかし、今回透かし情報として用いた RDS の二値画像では、少しでも誤りが生じると視認できなくなる可能性がある*⁹ため、BER は 0[%] 程度であることが望ましいと考えられる。

*⁸SNR=40[dB] では、劣化はほとんど知覚されないほど良好な画像であるとされる [14]。

*⁹本稿における RDS は、先行研究 [1] の RDS($64^2 = 4096$ 画素) と比べてサイズが小さく、少しの誤りによる影響が大きいと思われる。

5.2.2 基本的な攻撃に対する耐性

5.2.1 で述べた、SNR=40[dB] 付近での 4 種類の透かし入り画像に対して、攻撃耐性を調べた結果を以下に述べる。

◇ AWGN（加法性白色雑音）付加と誤り率

ここでは AWGN 付加に対する攻撃耐性を調査した。図 9 に白色雑音の標準偏差と BER の関係（AWGN 付加攻撃後）を示す。図 9 から、ホスト画像が“GIRL”のとき、WHT 方式は標準偏差が 5.0 で誤りがあったが、DCT 方式は標準偏差が 5.0, 10.0 で BER=0[%] であった。ホスト画像が“MOON”のとき、WHT 方式と DCT 方式は標準偏差が 5.0, 10.0 で BER=0[%] であった。よって、全体としては DCT 方式の性能が WHT 方式より相対的に優れていることが分かる。

次に、DCT 方式による透かし入り画像と検出画像の例（AWGN 付加攻撃後、標準偏差 10.0）を図 10(“GIRL”), 図 11(“MOON”) に示す。“GIRL”と“MOON”で BER=0[%] であり、視認に問題はない。

◇ JPEG 圧縮と誤り率

ここでは JPEG 圧縮に対する攻撃耐性を調査した。図 12 に JPEG 圧縮の圧縮比と BER の関係（JPEG 圧縮攻撃後）を示す。図 12 から、ホスト画像が“GIRL”のとき、WHT 方式は 1/2 圧縮で誤りがあり、DCT 方式は 1/6 圧縮までの圧縮強度で BER=0[%] であった。ホスト画像が“MOON”のとき、WHT 方式は 1/6 圧縮までの圧縮強度で BER=0[%] であり、DCT 方式は 1/8 圧縮までの圧縮強度で BER=0[%] であった。よって、DCT 方式の性能が WHT 方式より相対的に優れていることが分かる。

次に、DCT 方式による透かし入り画像と検出画像の例（JPEG 圧縮攻撃後、1/8 圧縮）を図 13(“GIRL”), 図 14(“MOON”) に示す。ホスト画像が“GIRL”のとき、BER=1.25[%] であり、若干の誤りが発生しているが、検出画像から分かる通り視認して立体視可能であった。ホスト画像が“MOON”のとき、BER=0[%] であり、視認に問題はない。

◇ クリッピングと誤り率

ここではクリッピングに対する攻撃耐性を調査した。図 15 にクリッピングの切り取り率と BER の関係（クリッピング攻撃後）を示す。図 15 から、ホスト画像が“GIRL”のとき、DCT 方式と WHT 方式に有意な差は見られなかった。ホスト画像が“MOON”のとき、攻撃が弱い場合（切り取り率 30[%] 以下）では、DCT 方式と WHT 方式でほぼ等しい BER 特性を示した。攻撃が強い場合（切り取り率 40[%] 以上）では、WHT 方式の方が DCT 方式より誤りが相対的に少ないものの、両方式で類似した BER 特性となった。

次に、DCT 方式による透かし入り画像と検出画像

の例（クリッピング攻撃後、切り取り率 50[%]）を図 16(“GIRL”), 図 17(“MOON”) に示す。ホスト画像が “GIRL” のとき、BER=14[%] であったが、視認に必要な RDS 情報 (“コ” の情報) の部分に誤りが比較的少なく、視認して立体視可能であった。一方、ホスト画像が “MOON” のときは、“GIRL” のときと同様に BER=14[%] であったが、視認に必要な RDS 情報 (“コ” の情報) の部分に誤りが比較的多く、視認がやや困難であった。

以上の結果から、RDS の立体視の可否について BER=0[%] は基準の一つとなるが、クリッピング攻撃では相対的に大きい BER (例えば BER=14[%]) で立体視可能となる場合があり、検出画像を視認し確認することが重要であるということが分かった。

6 結論

本稿では、DCT 領域で RDS の埋込みを行う画像用相関型電子透かし方式を提案し、その処理手順を整理した。また、3 種類の基本攻撃 (AWGN 付加, JPEG 圧縮, クリッピング) を導入し耐性を調べた。攻撃前後の結果から、以下のことが分かった。

(1) SNR が 40[dB] 程度である透かし入り画像を DCT 方式によって作成した場合の BER はテスト用ホスト画像で常に 0[%] となった。

(2) AWGN 付加 (標準偏差 10) と JPEG 圧縮 (1/8 圧縮) の攻撃に対する耐性が DCT 方式で見られた。クリッピング攻撃では相対的に大きい BER (例えば BER=14[%]) のときでも RDS を検出して立体視できる場合が DCT 方式で見られた。

(3) 攻撃前後において、DCT 方式の方が BER 特性の点で WHT 方式より相対的に良い性能を示す傾向にあった。

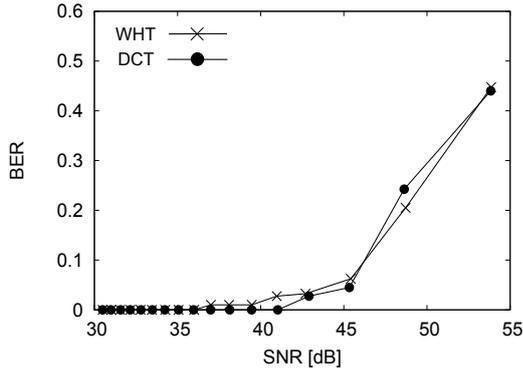
今後の課題は、更なる性能向上のため、DCT 以外の直交変換 (LOT[13], 一般化 LOT など) を用いる方式についての検討が挙げられる。

謝辞 計算機実験に協力頂いた学部生の小森真美氏 (現, (株)テレビ東京) に感謝する。

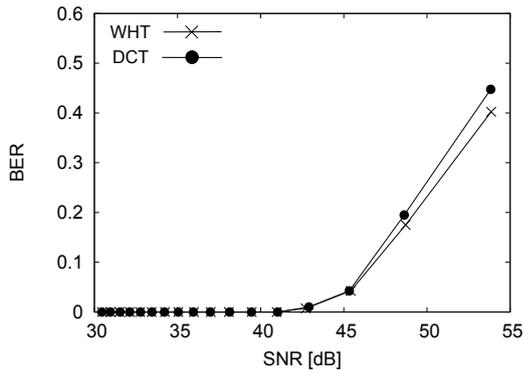
参考文献

- [1] 永野: “M 系列に基づく RDS 型電子透かし方式に関する研究”, 平成 15 年度電気通信大学 情報通信工学科 卒業論文 (2004-01).
- [2] I.J.Cox *et al.*: Secure spread spectrum watermarking for multimedia, *IEEE Trans. on Image Processing*, vol.6, no.12, pp.1673-1687(Dec. 1997).

- [3] 貴家, 村松: マルチメディア技術の基礎 DCT 入門, CQ 出版社 (1997).
- [4] N. Ahmed, T. Natarajan and K. R. Rao: “Discrete cosine transform”, *IEEE Trans. Comput.*, vol.C-23, no.1, pp.90-93(Jan. 1974).
- [5] 小森: “DCT 領域で RDS の埋込みを行う相関型電子透かし方式に関する研究”, 平成 28 年度電気通信大学 情報・通信工学科 卒業論文 (2017-01).
- [6] 古田, 小森, 小田: “DCT 領域で RDS の埋込みを行う相関型電子透かし方式の性能評価”, 2017 年電子情報通信学会総合大会 学生ポスターセッション, ISS-P-112, p.112(2017-03).
- [7] 笠原, 田中: デジタル通信工学, 昭晃堂 (1992).
- [8] 原島 (監修), 元木, 矢野 (共編): 3 次元画像と人間の科学, オーム社 (2000).
- [9] 下條: 視覚の冒険, 産業図書 (1995).
- [10] 真田, 出澤, 北岡: “ランダムドットステレオグラムにおける奥行き逆転現象に関する研究”, 電気通信大学大学院情報システム学研究科シンポジウム, pp.11-16(2000-03).
- [11] J.P. フリスビー (村山訳): シーイング, 誠信書房 (1994).
- [12] 松田: 視知覚, 培風館 (1998).
- [13] 小田, 上主: “2 次元 LOT を利用した画像用相関型電子透かし方式について”, 電気通信大学紀要, 第 23 巻, 第 1 号, pp.1-10(2011).
- [14] 貴家 (編著): 画像情報符号化, コロナ社 (2008).
- [15] A.Hanjalic *et al.*: Image and video databases - Restoration, watermarking and retrieval, *Elsevier*(2000).
- [16] 松井: 電子透かしの基礎, 森北出版 (1998).

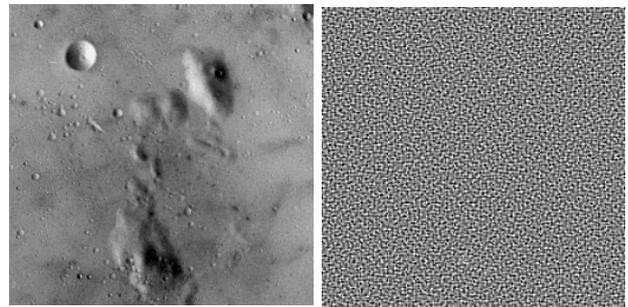


(a) "GIRL"



(b) "MOON"

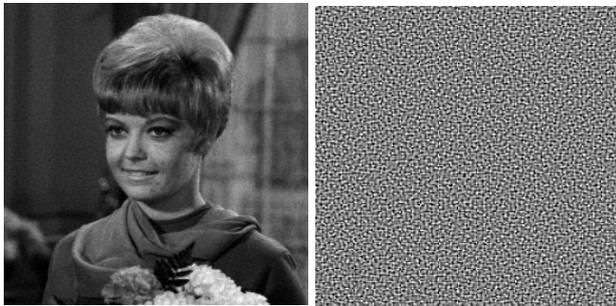
図 6: SNR と BER の関係 (攻撃前)



(a) 透かし入り画像

(b) 誤差画像 (×20)

(SNR=39.956[dB])



(a) 透かし入り画像

(b) 誤差画像 (×20)

(SNR=39.963[dB])



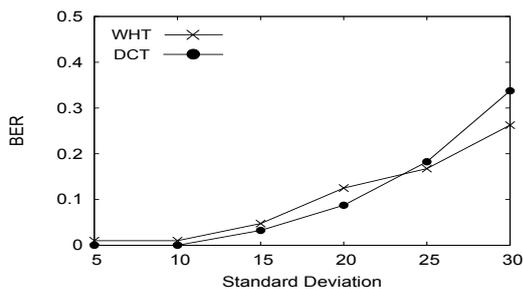
(c) 検出画像 (BER=0[%])

図 8: DCT 方式による透かし入り画像と検出画像の例 (攻撃前, "MOON")

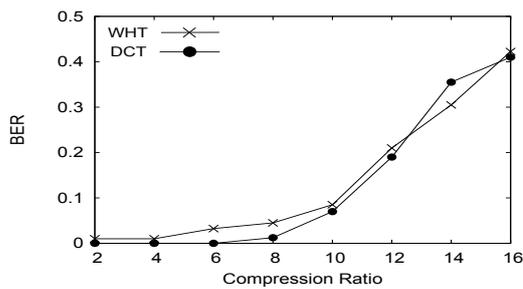


(c) 検出画像 (BER=0[%])

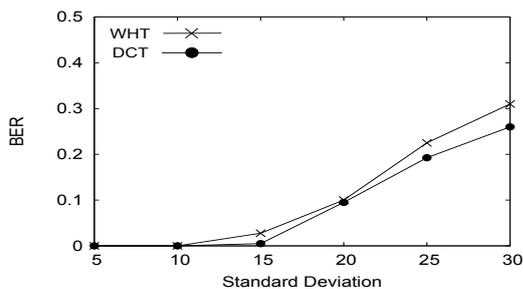
図 7: DCT 方式による透かし入り画像と検出画像の例 (攻撃前, "GIRL")



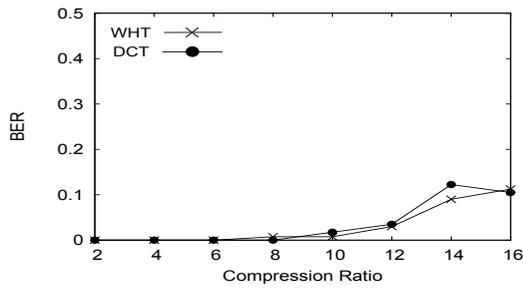
(a) "GIRL"



(a) "GIRL"



(b) "MOON"



(b) "MOON"

図 9: 白色雑音の標準偏差と BER の関係 (AWGN 付加攻撃後)

図 12: JPEG 圧縮と BER の関係 (JPEG 圧縮攻撃後)



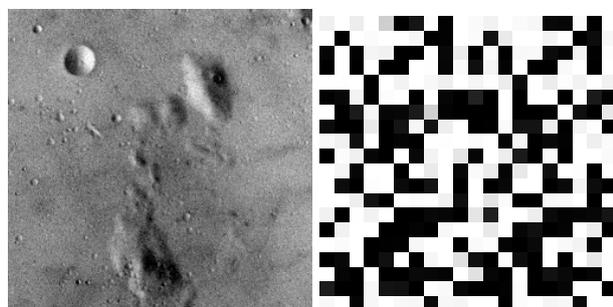
(a) 透かし入り画像 (標準偏差 = 10.0) (b) 検出画像 (標準偏差 = 10.0, BER = 0[%])

図 10: DCT 方式による透かし入り画像と検出画像の例 (AWGN 付加攻撃後, "GIRL")



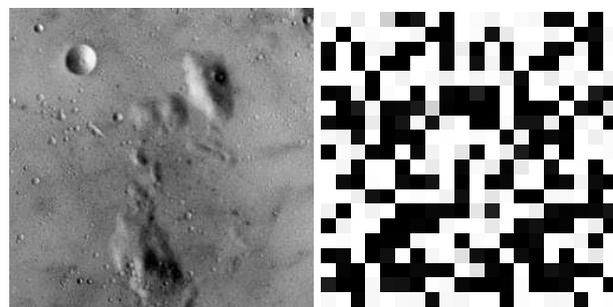
(a) 透かし入り画像 (1/8 圧縮) (b) 検出画像 (1/8 圧縮, BER = 1.25[%])

図 13: DCT 方式による透かし入り画像と検出画像の例 (JPEG 圧縮攻撃後, "GIRL")



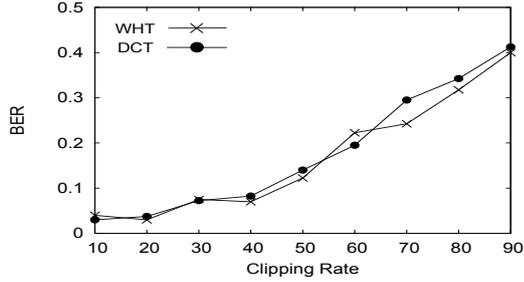
(a) 透かし入り画像 (標準偏差 = 10.0) (b) 検出画像 (標準偏差 = 10.0, BER = 0[%])

図 11: DCT 方式による透かし入り画像と検出画像の例 (AWGN 付加攻撃後, "MOON")

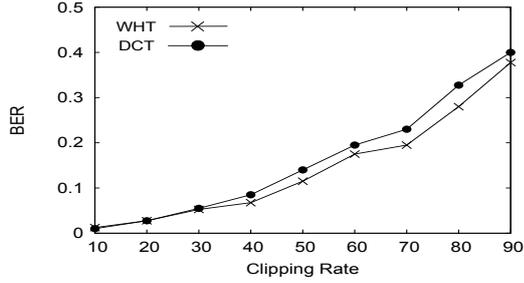


(a) 透かし入り画像 (1/8 圧縮) (b) 検出画像 (1/8 圧縮, BER = 0[%])

図 14: DCT 方式による透かし入り画像と検出画像の例 (JPEG 圧縮攻撃後, "MOON")



(a) “GIRL”



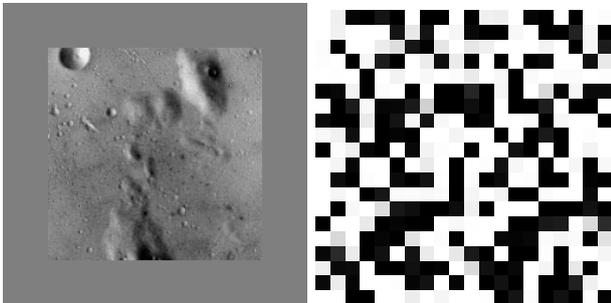
(b) “MOON”

図 15: クリッピングの切り取り率と BER の関係 (クリッピング攻撃後)



(a) 透かし入り画像 (切り取り率 50%) (b) 検出画像 (切り取り率 50%, BER = 14%)

図 16: DCT 方式による透かし入り画像と検出画像の例 (クリッピング攻撃後, “GIRL”)



(a) 透かし入り画像 (切り取り率 50%) (b) 検出画像 (切り取り率 50%, BER = 14%)

図 17: DCT 方式による透かし入り画像と検出画像の例 (クリッピング攻撃後, “MOON”)

付録 A 各サブブロックの埋込み領域の長さ l の導出

提案方式のパラメータとして, ホスト画像のサイズ $N_0 \times N_0$, 2次元の直交変換によるサブブロックのサイズ $N \times N$, m 次の M' 系列を用いるとする. このとき, 提案方式の(可能な)埋込み容量 (Payload) C は, 2^m の長さを持つ M' 系列 1 本につき m [bits] の情報の量を表現できることを考慮すると, 以下の式 (7) のように表せる.

$$C = \frac{N_0^2}{N^2} \times l \times \frac{m}{2^m} \quad (7)$$

5.1 の場合を計算すると, $N_0 = 256$, $N = 8$, $m = 8$ より, $C = 32 \times l$ となる. このとき, C が所望の透かし情報のデータ量よりも大きくなるような最小の l を求めればよいので, $32 \times 13 = 416 > 400 > 32 \times 12 = 384$ より, $l = 13$ となる. 尚, $l = 13$ を用いたため, (可能な)埋込み容量 $C = 416$ [bits] に対して必要容量が 400 [bits] となり, 容量に 16 [bits] 分の空きが生じた. この空きには, ダミーの透かし情報 (M' 系列) を埋込んだ.

付録 B 所望の SNR の透かし入り画像を生成するゲイン k の導出

ホスト画像のサイズを $N_0 \times N_0$ とするとき, 透かし入り画像の DCT 変換出力の 1 次元系列 $Y'(m)$ とホスト画像の DCT 変換出力の 1 次元系列 $Y(m)$ ($m = 0, 1, \dots, N_0^2 - 1$) との間の MSE (Mean Squared Error) は, 式 (5) のゲイン k の符号を考慮すると, 次式で与えられる.

$$\begin{aligned} \text{MSE}_{\text{DCT}} &= \frac{1}{N_0^2} \sum_{m=0}^{N_0^2-1} (Y'(m) - Y(m))^2 \\ &= \frac{1}{N_0^2} \sum_{j=0}^{L_0-1} \{(Y(j) + (+k) \times W(j \bmod L)) - Y(j)\}^2 \\ &= \frac{1}{N_0^2} \sum_{j=0}^{L_0-1} \{(+k) \times W(j \bmod L)\}^2 \\ &= \frac{1}{N_0^2} (+k)^2 \times L_0 \end{aligned} \quad (8)$$

ここで, $W(n)$ ($n = 0, 1, \dots, L-1$; $L =$ 系列の長さ) は M' 系列であり, $W^2(n) = 1$ である. また, $Y(j)$ ($j = 0, 1, \dots, L_0 - 1$) は透かし情報の埋込みに使用した DCT 変換出力係数であり, $L_0 (< N_0^2)$ はホスト画像にゲイン k で M' 系列 $W(n)$ を指定本数分埋込むために使用する DCT 変換出力係数 $Y(j)$ の総個数である.

DCT は直交変換であるので, 周波数領域と時間領域 (すなわち, 空間領域) との間でエネルギー保存則 (energy

preservation property) が成り立つ。よって、 $MSE_{DCT} = MSE_{TIME}$ となり、時間領域における SNR は次式となる。

$$SNR = 10 \log_{10} \left(\frac{A^2}{MSE_{TIME}} \right) \quad (9)$$

$$= 10 \log_{10} \left(\frac{A^2 \times N_0^2}{k^2 \times L_0} \right) \quad (10)$$

ここで A は最大階調値である。上式をゲイン k について解くと次式となり、これは文献 [13] の結果と同じである。

$$k = \frac{A \times N_0}{\sqrt{L_0 \times 10^{\frac{SNR}{10}}}} \quad (11)$$

実際に式 (11) を用いて $SNR=40.00$ [dB] となるゲイン k を導出した。ただし、5.1 の条件に従い、 $N_0 = 256$, $N = 8$, $l = 13$, $A = 255$ と設定し、 $L_0 = l \times \frac{N_0^2}{N^2} = 13 \times \frac{256^2}{8^2} = 13312$ (>12800 [ビット]= 50 [本] $\times 256$ [ビット/本]) とした。

$$k = \frac{255 \times 256}{\sqrt{13312 \times 10^{\frac{40.00}{10}}}} = 5.657942$$

上記の $k = 5.657942$ を用いて実際に透かし情報をホスト画像 “GIRL” に埋込んだところ、ホスト画像に対する透かし入り画像の SNR は $SNR=39.963$ [dB] となり、ほぼ理論値通りの値となった。また、 $k = 5.657942$ を式 (10) に代入して計算したところ、 $SNR=40.00$ [dB] となった。

付録 C 電子透かしの基本要件

電子透かしの要件として、文献 [15] では以下の 5 つが挙げられている。

- 不可知性 (Perceptual transparency) : 透かし入り画像の例から、提案方式は不可知であると言える。
- 埋込み容量 (Payload of watermarks) : 文献 [16] では 42[bytes] が埋込み容量の目安として紹介されている。これには著作権に対する識別子 (4[bytes])、識別番号 (8[bytes])、プロバイダ識別子 (4[bytes])、購入者番号 (16[bytes])、契約条件 (6[bytes])、ヘッダ等 (4[bytes]) が含まれている。提案方式では、この目安に近い容量 (50[bytes])、かつ視認して立体視が可能な RDS (図 1) を用いた。
- 強固性 (Robustness) : 計算機実験の結果から、DCT を用いた提案方式では、AWGN (加法性白色雑音) 付加 (標準偏差 $\sigma = 10$)、JPEG 圧縮 (1/8 圧縮) の攻撃ならば、ほぼ誤りなく検出できているので、提案方式は攻撃に対して耐性があると言える。
- 安全性 (Security) : 使用した 8 次の M' 系列が検出の鍵となっている。また、8 次の M' 系列のピーク位置 (256 通り) と “0”, “1” からなる 8 ビット (256 通り) との対応付け表を鍵とすれば、その対応の場合の数は 256! 通りであり、提案方式は安全と言える。

- 忘却型・非忘却型 (Oblivious vs. non-oblivious watermarking) : 透かし検出時に原画像 (ホスト画像) を必要としないため、提案方式は忘却型である。