アダマール行列を鍵系列として用いた画像電子透かし法

濱野恵太　　中本昌由　　雛元孝夫
(広島大学大学院工学研究科)

1　はじめに

電子透かしは，対象のディジタルコンテンツに透かしデータを埋め込むことによって著作権を保護する手法である [1]．本研究では，相関値を利用した画像電子透かし法に対し，アダマール変換された領域に透かし情報を埋め込む手法を提案する．一般に，変換核で用いられるアダマール行列は無数に存在するので，これを鍵系列として保持することにより，コンテンツ所有者の証とすることができる．また，焼きなまし法（SA）[2] を用いることにより，各種攻撃の耐性を高めるためのアダマール行列（鍵系列）の設計法についても述べる．最後に，シミュレーションによって電子透かしの JPEG 圧縮に対する耐性を示す．

2　アダマール変換 [3]

まず，変換に用いられるアダマール行列について説明する．アダマール行列 $\boldsymbol{H}$ は，次の 3 条件を満たす行列として定義される．

1. $\boldsymbol{H}$ は正方行列である．
2. $\boldsymbol{H}$ の要素は 1 か -1 である．
3. $\boldsymbol{H}$ の任意の異なった二つの行列は直交行列となっている．

また，定義から次のような性質が導かれる．

1. $\boldsymbol{H}$ の任意の行あるいは列を入れ替えてもアダマール行列となる．
2. $\boldsymbol{H}$ の任意の行あるいは列に -1 を掛けてもアダマール行列となる．

アダマール行列において，行 (列) に沿った符号の変化数は行 (列) のシーケンシーと呼ばれる．シーケンシーが大きいほど，高い周波数に対応している．また，アダマール行列 $\boldsymbol{H}_m$ を $m \times m$ 行列として，$m = 2^p$ (2 は正の整数) の場合を考えると，$\boldsymbol{H}_m$ は次の漸化式によって求めることができる．

$$\boldsymbol{H}_{2m} = \begin{bmatrix} \boldsymbol{H}_m & \boldsymbol{H}_m \\ \boldsymbol{H}_m & -\boldsymbol{H}_m \end{bmatrix}, \quad m = 2, 4, \cdots, \frac{N}{2} \tag{1}$$

$$\boldsymbol{H}_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{2}$$

$N \times N$ の入力信号を $\boldsymbol{X}$，出力信号を $\boldsymbol{Y}$ とすると，2 次元アダマール変換は次式のようになる．

$$\boldsymbol{Y} = \boldsymbol{H}_N \boldsymbol{X} \boldsymbol{H}_N \tag{3}$$

逆変換は

$$\boldsymbol{X} = \frac{1}{N^2} \boldsymbol{H}_N^T \boldsymbol{Y} \boldsymbol{H}_N^T \tag{4}$$

と表される．このように，$1/N^2$ 以外はすべて加減算で計算を実行することができる．

3　アダマール変換を用いた画像電子透かし法

3.1　透かしの埋め込み

透かしの埋め込み方法と検出方法は DWT を利用した手法 [4] と同様であるが，本論文では，アダマール行列が鍵系列となっているので埋め込みの際には鍵系列を必要としない．画像のサイズを $N \times N$ とし，元画像の RGB 成分から輝度成分 $\boldsymbol{X}$ を求め，得られた $\boldsymbol{X}$ に対して周波数変換を施し $\boldsymbol{Y}$ を得る．$\boldsymbol{Y}$ の i, j 要素は $Y(i, j)$ と表記する．また，埋め込むビットパターンは n ビットとし，$b_k \in \{1, 0\}, k = \{1, 2, \cdots n\}$ とする．$p = iN + j$ とおくと，透かし信号 $w(i, j)$ は以下のように構成される．

$$w(i, j) = \sigma_{p \bmod n} \tag{5}$$

ただし

$$\sigma_k = \begin{cases} 1, & \text{if} \quad b_k = 1 \\ -1, & \text{if} \quad b_k = 0 \end{cases} \tag{6}$$

透かし信号は，次式で埋め込まれる．

$$Y'(i, j) = Y(i, j) + \alpha w(i, j) \tag{7}$$

ただし，α は透かしの強度を表している．透かし信号を埋め込んだ後，逆変換により透かし入り画像を得る．

本論文では，空間領域から周波数領域に変換する方法としてアダマール変換を利用し，透かし信号を埋め込む式 (7) は，行または列のシーケンシーが大きい領域にのみ適用する．このように画像の周波数成分ごとに指定して埋め込みを行うことにより，画像情報を大きく壊すことなく透かし情報を埋め込むことが可能となる．

3.2　鍵の設計

アダマール行列 $\boldsymbol{H}$ は 1 と -1 からなる行列であるので，変換に用いたアダマール行列を鍵系列として透かしデータの埋め込みを行う．ここで，アダマール行列の性質より，任意の行または列を入れ替えるという操作と，任意の行または列に -1 を掛けるという操作は，アダマール行列の性質を保存する．これらの操作を繰り返し，透かしの相関値が大きくなるようにアダマール行列 (鍵) を設計する．

相関値の観点から鍵系列の設計法について述べる．式 (7) を式 (12) に代入すると

$$\rho_k = \sum_{\substack{i,j \\ p \bmod n=k}} \{Y(i,j) + \alpha\sigma_k\} \tag{8}$$

両辺に σ_k を掛けて

$$\rho_k\sigma_k = \sum_{\substack{i,j \\ p \bmod n=k}} \{Y(i,j)\sigma_k + \alpha\} \tag{9}$$

となる．ここで，右辺の第 1 項に着目し，以下のような評価値を定義する．

$$s_k = \sum_{\substack{i,j \\ p \bmod n=k}} Y(i,j)\sigma_k \tag{10}$$

s_k が大きな値となるように鍵系列を設計すれば，正しくもとのビットパターンを復元できる確率が高くなる．

本研究では，鍵の設計には焼きなまし法（SA）を用いた．これは，組み合わせ最適化問題を解くための繰り返し手法の一つである．評価値が改善される解を採択することに加えて，局所解を回避するためにある制限のもとで評価値が悪化する解も採択する点が特徴である．現在の解 (鍵) を $\boldsymbol{\chi}$，近傍解を $\boldsymbol{\chi}'$ とする．$\boldsymbol{\chi}'$ は等確率で $\boldsymbol{\chi}$ の任意の行 (列) を入れ替えるか，または -1 を乗じたものである．評価関数 $F(\boldsymbol{\chi})$ は，s_k を昇順に 10 個抽出したものの平均とし，焼きなましスケジュールに従って大きくする．遷移確率 p は

$$p = \begin{cases} 1 & \text{if} \quad F(\boldsymbol{\chi}) < F(\boldsymbol{\chi}') \\ e^{-\frac{F(\boldsymbol{\chi})-F(\boldsymbol{\chi}')}{T}} & \text{if} \quad F(\boldsymbol{\chi}) \geq F(\boldsymbol{\chi}') \end{cases} \tag{11}$$

とする．ただし，T は温度である．SA によって各 s_k の値を大きくするようにアダマール行列を設計することにより，電子透かしの各種攻撃に対する耐性を向上させることができる．

3.3 透かしの検出

透かし入り画像の輝度成分に対して周波数変換を用いて $\boldsymbol{Y'}$ を求める．次に，以下のように鍵と係数の相関値を計算する．

$$\rho_k = \sum_{\substack{i,j \\ p \bmod n=k}} Y'(i,j) \tag{12}$$

また，ビット列は以下のように復元される．

$$b_k = \begin{cases} 1, & \text{if} \quad \rho_k > 0 \\ 0, & \text{if} \quad \rho_k \leq 0 \end{cases} \tag{13}$$

4 シミュレーション

サイズ $256 \times 256 (N = 256)$ の画像 Lenna にサイズ $10 \times 10 (n = 100)$ の透かし情報を埋め込み，攻撃に対する耐性を調べた．画質 (PSNR) が 40.000[dB] となるように，埋め込み強度 α を設定した．漸化式によって求めたアダマール行列 $\boldsymbol{H}_N$ を初期鍵（Default key）とし，SA を用いて鍵系列の設計を行った．ただし，冷却率 γ を 0.99，総処理時間 t を 5000 とし，初期温度 100 のもとで $T(t+1) = \gamma T(t)$ と変化させてシミュレーションを行った．図 1 は本手法における k に対する s_k の値を示している．設計鍵を用いた場合には，初期鍵と比較して s_k が大きい値を示している．図 2 に JPEG Quality 値に対する透かしの検出率を示す．設計鍵により JPEG 圧縮に対する耐性がおおむね向上していることがわかる．

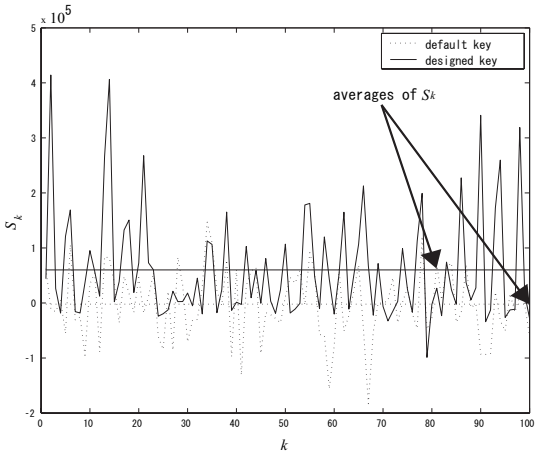

図 1: s_k の各値とその平均値

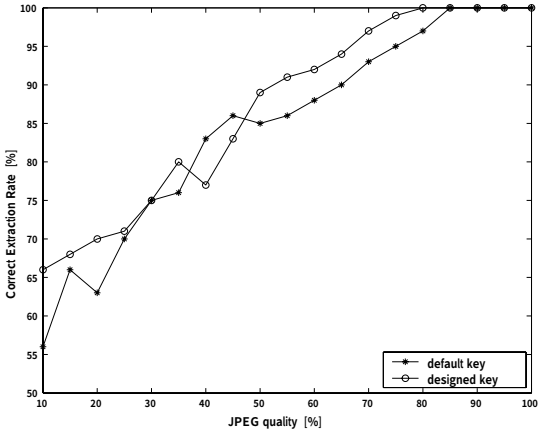

図 2: JPEG 圧縮に対する耐性

5 むすび

本論文では，アダマール変換を用いた画像電子透かし法を提案した．変換核であるアダマール行列を鍵系列として保持することにより，画像の著作権保護に利用することができる．さらに，攻撃に対する耐性を向上させるためのアダマール行列（鍵系列）の設計法を示した．また，シミュレーションによって JPEG 圧縮に対する耐性を示し，その有効性を確認した．

参考文献

[1] 松井甲子雄，電子透かしの基礎－マルチメディアのニュープロテクト技術－，森北出版，1998.

[2] S.M.Sait and H.Youssef，(白石洋一訳)，最適化アルゴリズムの最新手法，丸善株式会社，2002 年

[3] 谷萩隆嗣，高速アルゴリズムと並列信号処理，コロナ社，2000 年

[4] 木野，和田，信学論 (A), vol.J86-A, no.2, pp.160-167, Feb 2003.