K-022

誤り訂正符号利用型電子透かしによる改ざん画像修復法
A Digital Watermarking Method for Restoration of Tampered Images Using Error Correcting Codes

青森 祐人† 篠田 一馬† 長谷川 まどか†
Yuto Aomori Kazuma Shinoda Madoka Hasegawa

1. はじめに

ディジタル画像は，複製や編集等の操作が容易であることから，痕跡を残さない巧妙な改ざんが可能であるという問題がある．これに対して，電子透かしを用いたディジタル画像の改ざん検知・修復に関する研究が行われている．

電子透かしによる改ざん画像修復法の一つとして，Niu らは誤り訂正符号を用いた手法を提案している[1]．この手法では，画素の下位ビットに透かしを埋め込むことを前提としており，透かしは修復情報と改ざん検知情報からなる．修復情報は，画素の上位ビットを情報記号とし，これを誤り訂正符号の一種である最大距離分離符号で符号化して得られる検査記号のビット列である．改ざん検知情報は，矩形ブロックごとに，ブロック番号，ブロック内の画素および修復情報から算出されるハッシュ値である．抽出の際は，改ざん検知情報による改ざんブロックの特定をした後，画素値の上位ビットを情報記号とみなし，下位ビットから抽出される検査記号と連接した系列に対して消失訂正を施すことで改ざんブロックを修復する．

Niu らの手法における改ざん修復は，最大距離分離符号の消失訂正能力に依存する．したがって，改ざんが訂正上限を超えた場合は修復できない．訂正上限を向上させるには，情報記号数を削減する，あるいは検査記号数を増加させることが必要となる．従来手法では，情報記号数は画素の上位ビットの情報量，検査記号数は埋め込み容量で決定される．つまり，画素の上位ビットの情報量を削減すると，それらに対して割り当てられる情報記号数が減少するため，結果的に訂正能力の向上が期待できる．本稿では，画像を矩形ブロックに分割し，上位ビットプレーンに対して画像圧縮を施すことで情報記号数を削減し，修復画像の画質を維持しつつ訂正能力の向上を図ったので報告する．

2. 提案手法

2.1 透かし埋め込み処理

透かしの生成と埋め込みの流れを図 1 に示す．提案手法では，従来手法の誤り訂正符号化部の前に，画像中の矩形ブロックごとに画像圧縮を施す．提案手法における透かしは，圧縮情報に対する誤り訂正符号化によって生成される検査記号と各ブロックの圧縮情報量から構成される修復情報，および改ざん検知情報からなる．まず，修復情報生成では，原画像の画素の下位 3 ビットを切り捨てた後，画像を $w\times h$[pixel]のブロック $\boldsymbol{B}_i$ (i=1,2,...,N)に分割し，ブロックごとに画像圧縮を施す．次に，各ブロックの圧縮情報 $\boldsymbol{c}_i$ を連結したものを情報記号とし，$GF(2^p)$の元に対応させ，最大距離分離符号を用いた誤り訂正符号化を施し，検査記号を得る．この検査記号を N 個に等分した $\boldsymbol{p}_i$ を $\boldsymbol{B}_i$ にそれぞれ埋め込む．ここで，各ブロックに施す画像圧縮のパラメータが異なると，圧縮情報 $\boldsymbol{c}_i$ の情報量(ビット長)はそれぞれ異なる．つまり，情報記号で占める割合もブロックごとに異なってしまうため，改ざん後に誤り訂正符号語を再構成するには $\boldsymbol{c}_i$ の情報量 l_i が必要となる．そこで，l_i をそれぞれ固定長で表し，抽出側との共有秘密鍵 K を用いて画像中からランダムに選んだ複数のブロックに埋め込みを行う．改ざん検知情報は，ラスタスキャン順のブロック番号 i，ブロック内の画素の上位 5 ビットおよび $\boldsymbol{p}_i$ を入力として算出されるハッシュ値 $\boldsymbol{H}_i$ であり，これを $\boldsymbol{B}_i$ に埋め込む．図 2 は，$\boldsymbol{B}_i$ に埋め込まれる透かしの構成である．透かしは，検査記号の一部である $\boldsymbol{p}_i$，別のブロック $\boldsymbol{B}_x$～$\boldsymbol{B}_y$の圧縮情報量 l_x～l_y，およびブロックごとのハッシュ値 $\boldsymbol{H}_i$ から構成される．なお，修復情報と改ざん検知情報の埋め込みは，いずれも画素の下位 3 ビットプレーンの置き換えにより行うものとし，情報量はそれぞれ 2.5[bpp]，0.5[bpp]とする．これらは従来手法[1]と同じ値である．

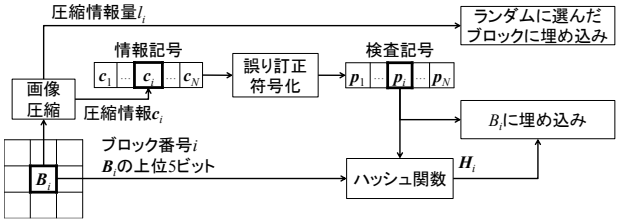


図 1 透かし生成・埋め込みの流れ

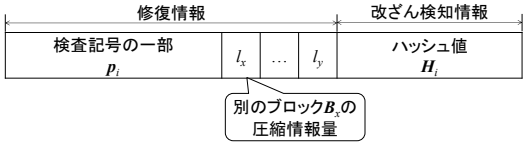


図 2 ブロック $\boldsymbol{B}_i$ に埋め込まれる透かしの構成

2.2 改ざん画像の修復

改ざん検知では，まず，画素の下位 3 ビットプレーンから $\boldsymbol{p}_i$'，$\boldsymbol{H}_i$'を抽出する．次に，ブロック番号 i，ブロック内の画素の上位 5 ビット，および $\boldsymbol{p}_i$'からハッシュ値を再計算し，抽出した $\boldsymbol{H}_i$'と比較する．両者が不一致の場合，改ざんブロックと判定する．画像中に改ざんブロックが存在する場合，共有鍵 K を用いて非改ざんブロックから抽出した l_i をもとに，画像を再圧縮することで情報記号を生成し，誤り訂正符号語を再構成する．ここで，改ざんブロックの総数を N_E とすると，$\boldsymbol{p}_i$ は改ざんによって消失する $\boldsymbol{p}_{e(s)}$ (s=1,2,...,N_E)と，非改ざんブロックから透かしとして抽出可能な $\boldsymbol{p}_{r(t)}$ (t=1,2,...,$N-N_E$)に分類できる．$\boldsymbol{c}_i$ も同様に，改ざんブロックの圧縮情報 $\boldsymbol{c}_{e(s)}$ と，非改ざんブロックの圧縮情報 $\boldsymbol{c}_{r(t)}$ に分けられる．そこで，$\boldsymbol{p}_{r(t)}$ と $\boldsymbol{c}_{r(t)}$ を真値，他を消失記号とし，訂正を試みる．消失訂正の結果，得られた $\boldsymbol{c}_{e(s)}$ を復号することで修復に用いる画素を得る．

2.3 改ざん修復能力

提案手法における，符号長 $n(n\leq 2^p-1)$，情報記号数 k，検査記号数 m は次式で算出される．

†宇都宮大学大学院工学研究科
Graduate School of Engineering, Utsunomiya University

$$n = k + m \quad (1)$$
$$k = \lceil C_L / p \rceil \quad (2)$$
$$m = \lceil V / p \rceil \quad (3)$$

ここで，C_L は圧縮情報 $\boldsymbol{c}_1$ から $\boldsymbol{c}_N$ までの情報量の総和[bit]，V は検査記号の埋め込み容量[bit]をそれぞれ示す．このとき，最大距離分離符号では，m 個までの記号が消失訂正可能となる．したがって，符号語に対して，訂正可能な消失記号の割合 R は次式で与えられる．

$$R = \frac{m}{n} \times 100 \ [\%] \quad (4)$$

したがって，圧縮情報量 C_L が小さい，あるいは検査記号の埋め込み容量 V が大きいほど r は大きくなる．

3. 実験結果

実験には，図 3 で示す 512×512[pixel]のグレイスケール画像 barbara，home，lake を用いた．ブロックサイズは 16×16[pixel]とし，圧縮には JPEG2000 可逆圧縮(kakadu ver7.4)を用いた．可逆圧縮を使用するのは，Niu らの手法[1]と同様に画素の上位 5 ビットの正確な修復を行いつつ，改ざん割合を増大させたときの修復結果を比較するためである．また，l_i は 8[bit]で表し，各ブロックに均等に 6 回(=48[bit])埋め込みを行った．誤り訂正符号には，$GF(2^{16})$上の Reed-Solomon 符号を用いた．符号長 n が 2^{16-1} を上回った場合は，各ブロックの圧縮情報を複数個に等分し，生成する符号語数を増加させた．

各画像の画素の上位 5 ビットに対し，16×16[pixel]のブロックごとに JPEG2000 可逆圧縮したときの情報量を表 1 に示す．なお，表 1 は，圧縮パラメータを含むヘッダを除いた情報量を示している．本実験では，ヘッダは埋め込み側と抽出側との共有情報とし，画像への埋め込みは行わなかった．ただし，ヘッダは全ブロック共通であるため，修復情報や改ざん検知情報に比べて微量で済む．次に，各手法における，訂正可能な消失記号の割合を表 2 に示す．従来手法では，画素の上位 5 ビットを情報記号としているので，画像による違いは生じない．一方，提案手法では，圧縮情報を情報記号とみなすので，画像の圧縮効率によって訂正可能な割合は変化する．

両手法とも埋め込みは画素の下位 3 ビット置き換えによるものであり，埋め込むビット列の'0'，1'の出現確率はほぼ等確率であったので，透かし埋め込み画像の PSNR はともに約 37.9[dB]となった．透かし埋め込み画像に対し，図 4 に示す領域編集を施し，各手法による修復結果を比較した．図 4 の括弧内は画像中の改ざん画素の割合を示す．各改ざん画像の改ざん検知結果を図 5 に示す．また，従来手法による修復結果を図 6，提案手法による修復結果を図 7 にそれぞれ示す．図 6，図 7 の括弧内は，図 4(a)～(c)の改ざんによって消失した記号の割合を示す．従来手法では，図 4(c)の改ざんは修復できたが，図 4(a)(b)では消失記号の割合が上限を超えたため修復ができなかった．これに対し，提案手法では，上限 R が向上したため，いずれの改ざんに対しても画素の上位 5 ビットの正確な修復が確認できた．ただし，従来手法と提案手法ともに，改ざん検知・修復はブロック単位である．したがって，改ざんが画像中に分散して発生する場合には，両手法ともに修復能力は低下すると考えられる．

(a)barbara (b)home (c)lake

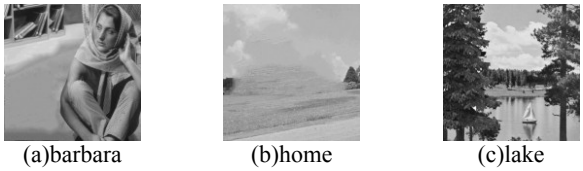
図 3　実験画像

表 1　JPEG2000 可逆圧縮後の情報記号の情報量[bpp]

画像	barbara	home	lake
情報量	3.85	3.03	3.95

表 2　訂正可能な消失記号の割合[%]

画像	barbara	home	lake
従来手法[1]	33.3	33.3	33.3
提案手法	37.5	42.5	36.9

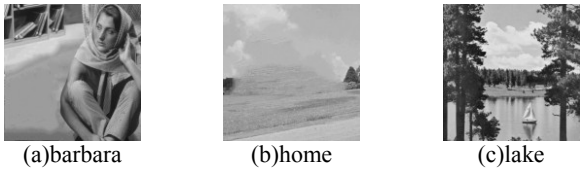


(a)barbara (改ざん割合:32.3%) (b)home (改ざん割合:31.3%) (c)lake (改ざん割合:30.2%)

図 4　改ざん画像

(a)barbara (b)home (c)lake

図 5　改ざん検知結果



(a)barbara (消失記号:34.1%) (b)home (消失記号:33.6%) (c)lake (消失記号:32.5%)

図 6　従来手法[1]による修復結果

(a)barbara (消失記号:34.0%) (b)home (消失記号:40.8%) (c)lake (消失記号:35.3%)

図 7　提案手法による修復結果

4. おわりに

本稿では，誤り訂正符号利用型電子透かしによる改ざん画像修復法における，誤り訂正符号化部の前処理として画像圧縮の導入を提案した．実験の結果，従来手法と比較して，広範囲の領域編集を伴う改ざんの修復に有効であることが確認できた．今後の課題として，画像中に改ざん領域が分散した場合における性能評価と有効な修復法の検討が挙げられる．

参考文献

[1] D. Niu, H. Wang, M. Cheng, L. Zhou, “Self-Embedding Watermarking Scheme Based on MDS Codes,” Lecture Notes in Computer Science, vol.9569, pp. 250-258 (2016).