

可逆情報埋込の高速化のための埋込パラメータ決定法

葉山 書緯[†]藤吉 正明[†]貴家 仁志[†]

首都大学東京システムデザイン学部情報通信システム工学コース 〒191-0065 東京都日野市旭が丘 6-6

E-mail: {hayama-shoi@sd.,fujiyoshi-masaaki@,kiya@sd.}tmu.ac.jp

あらまし 本稿は、可逆情報埋込のために埋込パラメータ決定を高速化している。対象の可逆情報埋込法では、埋込パラメータの決定に、埋込処理時間の最大約7割を費やしている。提案法では、埋込パラメータの決定に要する時間を最大約1/250に低減し、可逆情報埋込の高速化に寄与している。

キーワード 可逆情報埋込, 電子透かし

An Embedding Parameter Decision for Speeding Up the Reversible Data Hiding Method

Shoi HAYAMA[†]Masaaki FUJIYOSHI[†]Hitoshi KIYA[†]

Dept. of Info. and Commun. Syst. Eng., Tokyo Metropolitan Univ. 6-6 Asahigaoka, Hino-shi, Tokyo, 191-0065 Japan

E-mail: {hayama-shoi@sd.,fujiyoshi-masaaki@,kiya@sd.}tmu.ac.jp

Abstract This paper proposes an embedding parameter decision for speeding up the reversible data hiding method. The reversible data hiding method focused in this paper spends up to 70% of the embedded processing time to determine an embedding parameter. The proposed method determines the embedding parameter up to 250 times faster than the conventional method, so the proposed method speeds up faster reversible data hiding.

Keyword Reversible Data Hiding, Digital Watermarking

1. はじめに

画像をわずかに歪ませることで、画像に別の情報を直接重畳する、画像情報埋込技術が広範囲に検討されている。中でも、歪んだ画像(ステゴ画像)から重畳した(埋めた)情報を抽出できるだけでなく、原画像も復元可能な可逆情報埋込法は、医用・軍用などを目的に研究が進んでいる [1]。

情報抽出に必要なパラメータを記憶不要な可逆情報埋込法 [2] は、可逆性を保証し、同時に、パラメータを記憶不要にするために、情報埋込に際して、画像ブロックの統計量に基づく埋込パラメータを決定する。この埋込パラメータの決定は、初期値からの反復処理によってなされるため、初期値とパラメータとの差が大きい場合、処理時間が増加し、埋め込み処理全体の約7割の時間を費やす場合もある。

そこで本稿では、埋込パラメータの決定を高速にすることで、処理時間を低減する手法を提案する。提案法は、埋込パラメータの初期値を再設定することで、埋込パラメータ決定までの反復回数を低減し、可逆情報埋込の高速化を図っている。

2. 準備

本節では、本稿が対象とする可逆情報埋込法 [2] について述べる。この従来法 [2] は、原画像を重複しないように分割し、分割した画像領域ごとに情報埋込(図1(a))、情報抽出・画像復元(図1(b))を行う。2.1, 2.2でそれぞれの処理について詳しく述べる。

以降では、原画像を $X \times Y$ 画素の濃淡画像とし、各画素は K ビッ

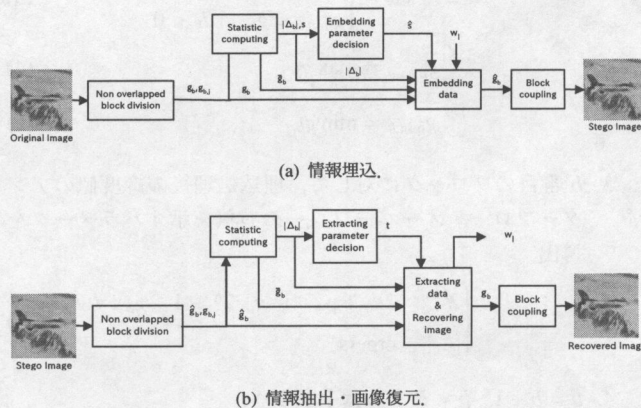
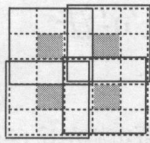


図1: 従来法 [2].

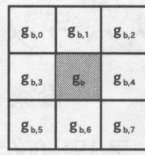
トで表されているものとする。なお、領域は $H_X \times H_Y$ 画素とし、原画像を分割しない場合は、 $H_X = X$, $H_Y = Y$ となる。また、埋める情報は長さ L の2値系列 $\mathbf{w} = \{w_l | w_l \in \{0, 1\}, l = 0, 1, \dots, L-1\}$ とする。

2.1. 情報埋込

この従来法 [2] では、領域をさらに、図2(a)に示すとおり、重複する 3×3 画素のブロック $B = \lfloor (H_X - 1)/2 \rfloor \lfloor (H_Y - 1)/2 \rfloor$ 個に分割する。ここで、 $\lfloor r \rfloor$ は実数 r を越えない最大整数である。ブロックごとに算出した統計量から、埋込情報量 L に応じた埋込パラメータを決定し、決定したパラメータを基に、埋込画素に1ビットの情報 $w_l \in \mathbf{w}$ を埋める。なお、埋込画素はブロックの



(a) ブロックの重複配置.



(b) 埋込ブロック.

図2: ブロック配置.

中央画素 g_b である (図 2 (b)). ただし, 埋込処理で輝度値がアンダーフローもしくはオーバーフローを引き起こすブロックでは, 可逆性が保証されない. そのようなブロックには情報を埋めなため, 埋込可能情報量 N は $0 \leq N \leq B$ となる. したがって, 埋める情報 w は $1 \leq L \leq N$ を満たす必要がある.

次節以降, 情報埋込のアルゴリズムについて詳説する.

2.1.1. 埋込パラメータ決定準備

埋込パラメータ決定に必要な統計量などを, 以下のアルゴリズムで導出する.

1. $b = 0$.
2. b 番目のブロックにおいて, 予測値 \bar{g}_b , 予測誤差 d_b , 最大絶対偏差様統計量 Δ_b を算出.

$$\bar{g}_b = \frac{1}{8} \left[\sum_{j=0}^7 g_{b,j} \right] \quad (1)$$

$$d_b = g_b - \bar{g}_b \quad (2)$$

$$\Delta_b = \begin{cases} g_{\max,b} - \bar{g}_b, & d_b \geq 0 \\ g_{\min,b} - \bar{g}_b, & d_b < 0 \end{cases} \quad (3)$$

$$g_{\max,b} = \max_j g_{b,j} \quad (4)$$

$$g_{\min,b} = \min_j g_{b,j} \quad (5)$$

3. b 番目のブロックに対して, 埋込処理後の輝度値のアンダーフロー・オーバーフローの有無を示すパラメータを導出.

$$s_b = \begin{cases} 2^k, & 2d_b + w_l \in [-g_b, 2^k - 1 - g_b], \forall w_l \\ |\Delta_b|, & \text{others} \end{cases} \quad (6)$$

4. $b = b + 1$. $b < B$ ならば手順 2 へ.
5. 式 (6) で求めた s_b の最小値を求める.

$$s = \min_b s_b \quad (7)$$

以上の手順によって, $|\Delta_b| < s$ を満たすブロックにおいて可逆性を保証する最大の s が求まる. この s を基に, 次節で述べるアルゴリズムによって, 埋込情報量 L に応じた埋込パラメータが決定される.

2.1.2. 埋込パラメータの決定

前節で導出した s を基に埋込情報量 L に適した埋込パラメータ \hat{s} を決定する.

1. 一時的なパラメータ値を $\sigma_0 = s$, $\sigma_1 = s$, $\sigma_2 = s$ とする.
2. $b = 0$, 推定埋込可能容量 $\beta = 0$ とする.

3. b 番目のブロックの最大絶対偏差様統計量が $|\Delta_b| < \sigma_0$ を満たす場合, $\beta = \beta + 1$.

4. $b = b + 1$. $b < B$ ならば手順 3 へ.

5. $\beta = L$ であれば, 手順 8 へ. その他の場合, $\sigma_2 = \sigma_1$, $\sigma_1 = \sigma_0$, $\sigma_0 = \sigma_0 + \text{sgn}(L - \beta)$. ここで, $\text{sgn}(r)$ は r の正負を表し, $+1$ もしくは -1 である.

6. $\sigma_0 > s$ ならば, $\sigma_0 = 0$ とし手順 8 へ. $\sigma_0 < 1$ ならば, $\sigma_0 = 1$ とし手順 8 へ. $\sigma_0 = \sigma_2$ ならば, 手順 8 へ.

7. 手順 2 へ.

8. $\hat{s} = \sigma_0$.

以上の手順によって, $\beta \geq L$ を満たす最小の \hat{s} を埋込パラメータとして決定する. 従来法 [2] は, この処理によって抽出パラメータの記憶を不要としている.

なお, $\hat{s} = 0$ の場合, この従来法 [2] では対象画像に L ビットの情報を埋めることができない. この場合, 可逆な前処理 [4] によって, 埋込可能情報量 N を増やすことが考えられる [2].

2.1.3. 情報埋込

前節で求めた埋込パラメータ \hat{s} に基づいて, 可逆性を保証できるブロックに情報ビット w_l を埋める.

1. $b = 0, l = 0$.

2. b 番目のブロックに対して, 最大絶対偏差様統計量 Δ_b と埋込パラメータ \hat{s} とを基に, 埋込み可能であれば 1 ビットの情報を埋める.

$$\hat{g}_b = \begin{cases} \bar{g}_b + 2d_b + w_l, & |\Delta_b| < \hat{s} \\ g_b, & |\Delta_b| \geq \hat{s} \end{cases} \quad (8)$$

3. $|\Delta_b| < \hat{s}$ ならば $l = l + 1$.

4. $b = b + 1$. $l < L$ なら手順 2 へ.

以上の手順によって, L ビットの情報 w を埋めたステゴ画像が生成される.

2.2. 情報抽出・原画像復元

この従来法 [2] ではまず, 情報埋込と同様にブロックごとの統計量を算出し, さらに抽出パラメータを決定する. その抽出パラメータに基づき情報を抽出し, 画像を復元する.

次節以降で情報抽出・画像復元の詳細なアルゴリズムについて述べる.

2.2.1. 抽出パラメータの決定

1. 抽出パラメータ t を, $t = 1$ で初期化する.

2. $b = 0$, 推定容量 $\hat{\beta} = 0$ とする.

3. 式 (9) を用いて最大絶対偏差様統計量 Δ_b を得る.

$$\Delta_b = \begin{cases} g_{\max,b} - \bar{g}_b, & \hat{g}_b - \bar{g}_b \geq 0 \\ g_{\min,b} - \bar{g}_b, & \hat{g}_b - \bar{g}_b < 0 \end{cases} \quad (9)$$

4. $|\Delta_b| < t$ ならば, $\hat{\beta} = \hat{\beta} + 1$.

5. $b = b + 1$. $b < B$ なら手順 3 へ.

6. $\hat{\beta} < L$ の場合, $t = t + 1$ とし, 手順 2 へ.

以上の手順によって, $\hat{\beta} \geq L$ を満たす最小の t を抽出パラメータとして決定する. ステゴ画像が編集されていなければ, $t = \hat{s}$ であり, したがって, この手法はパラメータの記憶が不要となっている.

2.2.2. 情報抽出・画像復元

前節で求めた抽出パラメータ t に基づいて, ブロックごとに埋められた情報 w_l を抽出し, また原画像を復元する.

1. $b = 0, l = 0$.

2. b 番目のブロックの最大絶対偏差様統計量 Δ_b と抽出パラメータ t とを基に, 情報抽出・画像復元を行う.

$$w_l = (\hat{g}_b - \bar{g}_b) \bmod 2, \quad |\Delta_b| < t \quad (10)$$

$$g_b = \begin{cases} \frac{\hat{g}_b + \bar{g}_b - w_b}{2}, & |\Delta_b| < t \\ \hat{g}_b, & |\Delta_b| \geq t \end{cases} \quad (11)$$

3. $|\Delta_b| < t$ ならば, $l = l + 1$.

4. $b = b + 1$. $l < L$ ならば手順 2 へ.

以上の手順によって, L ビットの情報 w が抽出され, また, 原画像が復元される.

2.3. 問題点

この従来法 [2] では, 抽出パラメータの記憶を不要とするために, 埋込情報量 L に適した埋込パラメータ \hat{s} を決める. 2.1.2 で述べたアルゴリズムでは, \hat{s} が s から反復的に求められる. ここで, s と \hat{s} とが大きく異なる場合, 反復回数が多く処理に時間を要することになる. 予備実験においても, 全てのブロックが埋込み可能である場合, 2.1.2 のアルゴリズムの実行時間が埋込処理全体の約 7 割に達する事を確認している.

ここで次節では, 埋込パラメータを再初期化することで反復回数を低減する, 高速な埋込パラメータ決定法を提案する.

3. 提案法

提案法は, 埋込パラメータ \hat{s} の決定に要する処理時間を短縮することで, 埋込み処理全体の高速化を図る. 以下では, \hat{s} 決定に用いられる最大絶対偏差様統計量 Δ_b について考察し, その結果に基づき, 新たな埋込パラメータ決定アルゴリズムを提案する.

3.1. Δ_b に関する考察

2.1.2 で述べた従来法 [2] の埋込パラメータ決定アルゴリズムでは, 手順 2~4 で $|\Delta_b|$ がパラメータよりも小さいブロックの個数を推定埋込可能容量 β として求めている. ここで, パラメータの変化による β の変化を考察する. これは, $|\Delta_b|$ に対するブロック数の累積頻度を求めることに他ならない.

512×512 画素の 8 ビット濃淡画像 7 枚 [3] を対象とした, $|\Delta_b|$ に対するブロック数の累積頻度を図 3 に示す. ただし, 可逆性の保証を前提としているため, $|\Delta_b| < s$ の範囲に限定されている. 図 3 から分かる通り, $|\Delta_b|$ の増加に伴い, β が急激に増加していることが分かる. したがって, L の広い範囲に対して \hat{s} は小さい値となり得る. また, 一方向性ハッシュ値を埋める [2] 用途の

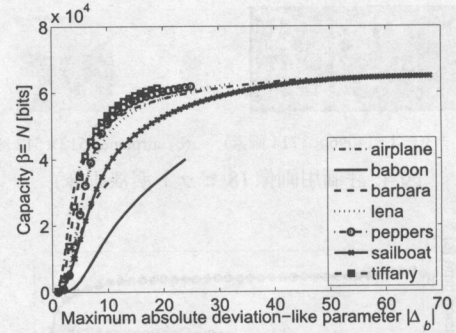


図 3: $|\Delta_b| < s$ での $|\Delta_b|$ に対するブロック数の累積頻度.

場合, 例えば, $L = 512$ [bits] であり, 対応する $|\Delta_b|$ は極めて小さい.

いずれの場合においても, s からの反復減少によって埋込パラメータ \hat{s} を求めるためには, 著しい反復回数を必要とする. その結果, \hat{s} 決定に要する時間が大きくなる事が分かる.

3.2. 埋込パラメータ決定アルゴリズム

前節の考察に基づき, 新たなアルゴリズムを提案する.

1. $s' = \min_b |\Delta_b| + 1$. $\sigma_0 = s'$, $\sigma_1 = s'$, $\sigma_2 = s'$.

2. $b = 0, \beta = 0$.

3. b 番目のブロックが $|\Delta_b| < \sigma_0$ を満たす場合, $\beta = \beta + 1$.

4. $b = b + 1$. $b < B$ の場合, 手順 3 へ.

5. $\beta = L$ であれば, 手順 8 へ. その他の場合, $\sigma_2 = \sigma_1$, $\sigma_1 = \sigma_0$, $\sigma_0 = \sigma_0 + \text{sgn}(L - \beta)$.

6. $\sigma_0 > s$ ならば, $\sigma_0 = 0$ とし手順 8 へ. $\sigma_0 < 1$ ならば, $\sigma_0 = 1$ とし手順 8 へ. $\sigma_0 = \sigma_2$ ならば, $\sigma_0 = \sigma_0 + 1$ とし手順 8 へ.

7. 手順 2 へ.

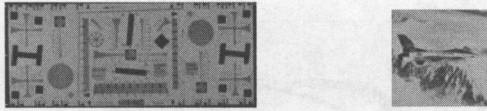
8. $\hat{s} = \sigma_0$.

以上のように, 提案するアルゴリズムでは, $s' = \min_b |\Delta_b| + 1$ で再初期化する. これにより手順 2~4 の反復回数が低減され, 埋込パラメータ決定に要する時間を短縮することが可能となっている.

なお上述のアルゴリズムでは, 手順 1 において $s' = \min_b |\Delta_b| + 1$ で再初期化しているが, 他の値で再初期化するアルゴリズムも考えられる. 上記のアルゴリズムを提案法 1 とし, 手順 1 において, $s' = 1$ とするアルゴリズムを提案法 2 として比較する.

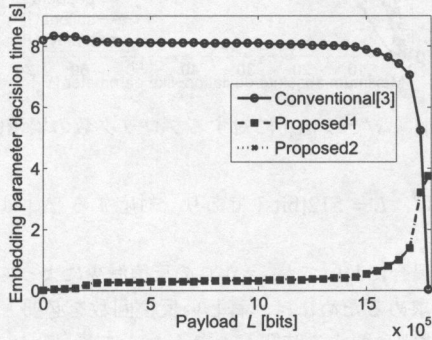
4. 数値実験

図 4 に示す 2 種類の濃淡画像を用いて提案法を評価する. 図 4 (a) は, 各画素が 8 ビットで量子化されている 4094×1714 画素の画像, すなわち, $K = 8, X = 4096, Y = 1714$ である. 同画像は, 埋込不可ブロックを有していない. 一方, 図 4 (b) は各画素が 8 ビットで量子化されている 512×512 画素の画像, すなわち, $K = 8, X = Y = 512$ である. 同画像は, 埋込不可ブロックを有する画像である. なお, 実験環境は Intel(R) Core(TM)2

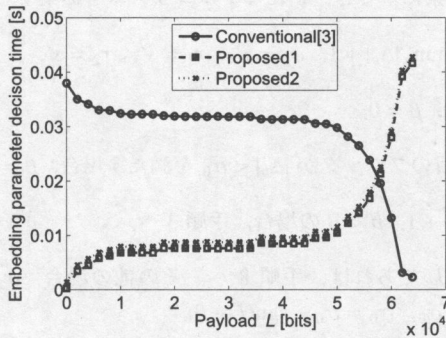


(a) テストチャート (4096×1714 画素). (b) airplane (512×512 画素) [3].

図 4: 評価用画像 (8 ビット濃淡画像).



(a) テストチャート.



(b) airplane.

図 5: 埋込情報量 L に対する埋込パラメータ決定時間.

CPU 2.4GHz, 2.0GiB RAM, Linux 2.6.32-37-generic, MATLAB version 7.5 である.

従来法 [2], 提案法 1, 提案法 2 の 3 つの方法で, 埋込情報量 L に応じた埋込パラメータ \hat{s} の決定に要する処理時間を計測した. 5 回の試行の平均を図 5 に示す. なお, 原画像は領域分割されておらず ($H_X = X, H_Y = Y$), また, 埋込情報量は 1 ビットから埋込可能情報量 N ビットまでとする. 図 5 から, 提案法は L の広い範囲において, 従来法 [2] よりも埋込パラメータを高速に決定していることが分かる. 特に, L が小さい場合, $s = 2^K$ となる図 4(a) では約 250 倍の, $s = \min_b s_b$ となる図 4(b) の画像でも約 30 倍の, 高速化がなされている. なお, L が N に近い場合, 埋込パラメータ \hat{s} は s と近い値をとるため, 従来法 [2] の反復回数が少なくなっている. 以上のことは図 3 に示された $|\Delta_b|$ に対するブロック数の累積頻度の傾向から導かれる結論と一致する.

次に図 4(b) の画像を図 6 のように 64×64 画素, すなわち, $H_X = H_Y = 64$ である領域に分割して評価を行う. 分割された 64 の領域において, 埋込可能情報量 N の最小値は 886 ビットである. そこで, 各領域に $1 \sim 886$ ビットの情報を埋める条件で, 埋込パラメータ \hat{s} の決定時間を計測する. 処理時間のブロック平



図 6: 領域分割 (airplane 画像, 64×64 画素領域).

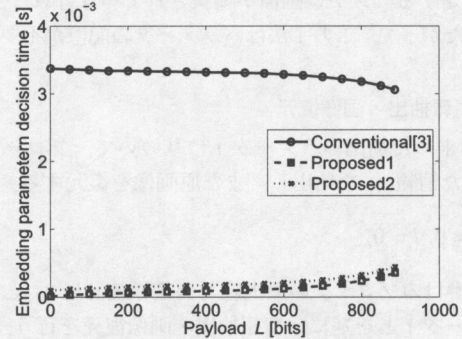


図 7: 画像 airplane, 64 分割時の 1 領域あたりのパラメータ決定平均時間.

均を図 7 に示す. 図 7 から, 提案法は図 4(b) の時よりも高速に (最大約 40 倍) 動作することが分かる. これは, 領域分割時, ブロックで埋込可能となる領域が複数生じ, 従来法 [2] では, 図 4(a) の画像同様 $s = 2^K$ から反復処理を施す回数が増えるためである.

なお, いずれの場合においても, $s' = 1$ で再初期化する提案法 2 よりも, $s' = \min_b |\Delta_b| + 1$ で再初期化する提案法 1 の方が高速であった. これは図 3 に示されているとおり, $|\Delta_b|$ が 1 のように極端に小さい場合 β も極めて小さく, その結果, 従来法 2 では反復回数が増えるためである.

5. おわりに

本稿では, 可逆情報埋込法 [2] に対して, 埋込パラメータを高速に決定する方法を提案した. 従来法 [2] では, 取りうる最大のパラメータ値から, 反復減少によって, 埋込情報量に応じた埋込パラメータを決定する. 一方, パラメータ決定に用いる統計量について考察した結果を踏まえ, 提案法は小さいパラメータ値から反復増加によって埋込パラメータを決定する. これにより, 従来法 [2] の埋込処理時間の最大約 7 割を占める埋込パラメータ決定処理に対して, 提案法は最大約 250 倍の高速化を達した.

文 献

- [1] R. Caldelli, F. Filippini, and R. Becarelli, "Reversible watermarking techniques: an overview and a classification," EURASIP J. Inf. Security, vol.2010, May 2010.
- [2] S. Han, M. Fujiyoshi, and H. Kiya, "A reversible image authentication method without memorization of hiding parameters," IEICE Trans. Fundamentals., vol.E92-A, no.10, pp.2572–2579, Oct. 2009.
- [3] Centre for Image Processing, Rensselaer Polytechnic Institute, "Still image and sequenes," <http://www.cipr.rpi.edu/>
- [4] H.L. Jin, Y. Choe, and H. Kiya, "Reversible Data Hiding Based On Adaptive Modulation Of Statistics Invertibility," IEICE Trans. Fundamentals, vol.E93-A, no.2, pp.565–569, Feb. 2010.