一般社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report
EMM2020-65(2021-01)

暗号化画像に対するMSB予測型可逆情報埋込み法の拡張

平澤　凌一†　今泉　祥子††　貴家　仁志†††

† 千葉大学大学院 融合理工学府　〒263–8522 千葉市稲毛区弥生町 1–33
†† 千葉大学大学院 工学研究院　〒263–8522 千葉市稲毛区弥生町 1–33
††† 首都大学東京 システムデザイン学部　〒191–0065 東京都日野市旭ヶ丘 6–6
E-mail: †ryoichi0616@chiba-u.jp, ††imaizumi@chiba-u.jp, †††kiya@tmu.ac.jp

あらまし　本稿では，暗号化画像を対象として大容量かつ可逆性を保証するMSB予測型情報埋込み法を提案する．提案法では，MSB予測における条件を正確に与えるとともに，埋込み処理の前処理として，埋込み情報と暗号化画像に対してマーカとフラグをそれぞれ設定する．これらの処理により，提案法は，高い埋込み容量を実現するとともに，十分な可逆性を保証することができる．シミュレーションにより，可逆性と埋込み容量の観点から評価を行い，提案法の有効性を確認する．

キーワード　可逆情報埋込み，画像暗号化，可逆性，埋込み容量，MSB予測

An Extension of MSB Prediction-Based Method for Reversible Data Hiding in Encrypted Images

Ryoichi HIRASAWA†, Shoko IMAIZUMI††, and Hitoshi KIYA†††

† Graduate School of Science and Engineering, Chiba University　Yayoicho 1–33, Inage-ku, Chiba, 263–8522
†† Graduate School of Engineering, Chiba University　Yayoicho 1–33, Inage-ku, Chiba, 263–8522
††† Faculty of System Desing, Tokyo Metropolitan University　Asahigaoka 6–6, Hino-shi, Tokyo, 191–0065
E-mail: †ryoichi0616@chiba-u.jp, ††imaizumi@chiba-u.jp, †††kiya@tmu.ac.jp

Abstract　In this paper, we propose a high capacity MSB prediction-based method with sufficient reversibility for data hiding in encrypted images. First, as preprocessing of data hiding, the proposed method introduces markers and flags to the payload and encrypted image, respectively. Additionally, by defining precise conditions for MSB prediction, our method can guarantee the perfect reversibility. Experimental results show the effectiveness of the proposed method in terms of reversibility and hiding capacity.

Key words　Reversible data hiding, image encryption, reversibility, hiding capacity, MSB prediction

1. まえがき

近年，クラウドサービスやSNSの一般化により，外部のサーバやサービスを介した画像の公開および共有の機会が増加している．これに伴い，画像に含まれるプライバシ情報や著作権情報の保護がより強く求められる．画像保護技術の一つである可逆情報埋込みは，画像に埋め込まれた情報を抽出した後，原画像を完全に復元できるため，多くの研究が進められている [1–4]．可逆情報埋込みは，一般的に，原画像に対して埋込み処理を施すものであるが，暗号化画像を対象とする手法も提案されている [5–9]．これらの手法は，あらかじめ所有者により暗号化された画像に対して，システム管理者などの第三者が，追加の情報，例えば，画像の注釈や認証情報などを埋め込むことを想定している．

Maらの手法 [6] では，暗号化処理を施す前に原画像を空間領域で二分割し，一方の領域のLSBを他方の領域に可逆に埋め込む．その後，画像全体に対してXOR演算による暗号化を施す．これらの処理により，暗号化された画像において前者の領域のLSBが埋込み可能領域となる．この手法の特徴は，埋め込まれた情報を抽出しなくとも暗号を解除するだけで，あらかじめ埋め込まれたLSBの情報から原画像を復元することができる点にある．しかし，この手法では，最大で0.5bpp程度しか埋め込むことができない．

Puteauxら [8] は，暗号化画像に対する可逆情報埋込みにおいて，多くの従来手法が用いているLSB置換に代わりMSB置換を適用し，複雑な処理を必要とせず大容量な手法を提案

This article is a technical report without peer review, and its polished and/or extended version may be published elsewhere.
Copyright ©2021 by IEICE

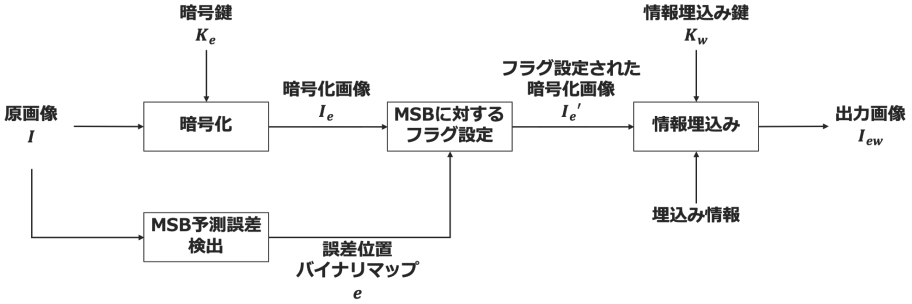
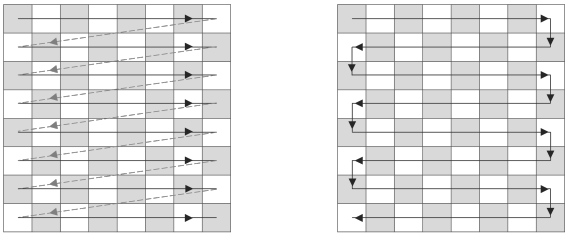


図 1: 提案法の処理手順



(a) Raster 走査　　(b) Serpentine 走査

図 2: 走査順序

した．さらに，Dragoi ら [9] は，この手法の MSB に対する処理を改良し，安全性を向上させた．しかしながら，上述の二つの手法では，いずれも複数の点において可逆性が十分に保証されていない．

そこで，本稿では，MSB 予測を用いて大容量かつ可逆性を保証する，暗号化画像に対する情報埋込み法を提案する．提案法では，埋込み情報と暗号化された画像に対して可逆性を保持するためのマーカとフラグをそれぞれ設定する．さらに，MSB 予測において，その条件を整理し正確に与えることで十分な可逆性を保証する．シミュレーションでは，提案法の可逆性を確認するとともに，埋込み容量について評価を行う．

2. 提　案　法

本章では，暗号化画像に対する大容量な MSB 予測型可逆情報埋込み法を提案する．提案法では，情報埋込み法として，MSB 置換を用いており，LSB よりも容易に予測可能な MSB を情報埋込み領域とすることで，可逆かつ大容量な手法を実現する．また，埋込み情報や暗号化画像に対して前処理を施すことで，可逆性を十分に保証することができる．

図 1 に，提案法における処理手順を示す．まず，原画像から MSB 予測誤差を検出し，画像を暗号化する．暗号化画像において，埋込み可能／不可能な画素を区別するためのフラグを設定し，埋込み可能な画素に対して MSB 置換により情報を埋め込む．以下では，提案法の処理手順，および，先行研究 [8] の可逆性における課題について説明する．

2.1 情報埋込み・暗号化処理手順

ここでは，図 1 に従い，情報埋込みと暗号化の処理について具体的な手順を述べる．なお，以下では，原画像のサイズを $M \times N$ 画素とする．

2.1.1 MSB 予測誤差検出

提案法は，MSB 置換により情報を埋め込む．そのため，埋込み前の MSB の値が埋込み処理により失われる．そこで，以下の手順により，復元時に正しく MSB を予測できるよう，隣接画素を用いて予測誤差の検出を行い，誤差が検出された箇所を記録するための誤差位置バイナリマップ e を生成する．

処理 1-1: 原画像のすべての画素 $p(i,j)$ について式 (1) を用いて，MSB が反転された画素値 $inv(i,j)$ を得る．

$$inv(i,j) = (p(i,j) + 128) \bmod 256 \tag{1}$$

ここで，i,j は座標を示しており，$0 \leqq i < M$，$0 \leqq j < N$ である．

処理 1-2: 現在の $p(i,j)$ の一つ前に走査された隣接画素を，復元時の予測値算出に用いる画素（以降，参照画素と呼ぶ）$pred(i,j)$ とする．このとき，走査順序は，Raster 走査（図 2(a)）および Serpentine 走査（図 2(b)）を，水平方向（左から右），垂直方向（上から下）にそれぞれ適用し，これらのうち予測誤差の発生数が最も少ない走査／方向を採用する．なお，図 2 はいずれも水平方向での走査順序を示している．

処理 1-3: 次式より，$pred(i,j)$ と $p(i,j)$，および，$pred(i,j)$ と $inv(i,j)$ の絶対差 Δ，Δ^{inv} を算出する．

$$\begin{cases} \Delta = |pred(i,j) - p(i,j)| \\ \Delta^{inv} = |pred(i,j) - inv(i,j)| \end{cases} \tag{2}$$

処理 1-4: 式 (3) に従い，誤差位置バイナリマップ e を生成する．

$$e(i,j) = \begin{cases} 0, & \text{if} \Delta < \Delta^{inv} \\ 0, & \text{if} \Delta = \Delta^{inv} \text{かつ } p(i,j) \bmod 128 = 0 \\ 1, & \text{if} \Delta = \Delta^{inv} \text{かつ } p(i,j) \bmod 128 = 1 \\ 1, & \text{if} \Delta > \Delta^{inv} \end{cases} \tag{3}$$

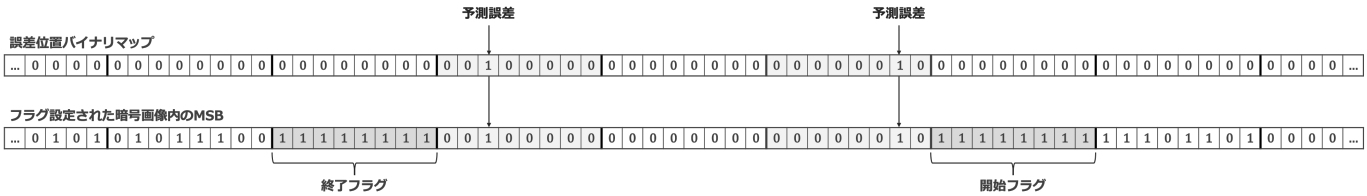


図 3: 暗号化画像の MSB に対するフラグ設定

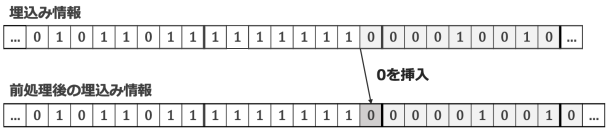


図 4: 埋込み情報に対する前処理

これにより，$\Delta = \Delta^{inv}$ の場合，もとの MSB が格納される．

2.1.2 画像暗号化

提案法において，暗号化は XOR 演算によって行われる．ただし，提案法では XOR 演算を用いるが，任意のストリーム暗号を用いることができる．

処理 2: 暗号鍵 K_e により生成された $8 \times M \times N$ ビットの疑似乱数列 s を用いて，XOR 演算により暗号化を行う．

$$p_e(i,j) = s(i,j) \oplus p(i,j) \qquad (4)$$

ここで，$p_e(i,j)$ は暗号化後の各画素，$s(i,j)$ は $p(i,j)$ と演算される 8 ビットの s の要素をそれぞれ表す．これにより，暗号化画像 I_e が生成される．

なお，この暗号化処理により，次節で述べるフラグが発生する可能性が生じる．これは後述する処理 3-2 により回避することができる．

2.1.3 暗号化画像に対するフラグ設定

提案法において，情報埋込みは画像を分割したブロックごとに施される．ここでは，情報埋込み時に，埋込み可能／不可能なブロックを区別することができるよう，暗号化画像に対してフラグを設定する．

処理 3-1: 暗号化された画像 I_e と誤差位置バイナリマップ e を，それぞれ 8×1 画素のブロックに分割する．

処理 3-2: 暗号化画像 I_e において，各ブロックの MSB を確認し，ブロック内の MSB がすべて 1 である場合，そのブロックの MSB を修正する．ただし，修正においては，すべて 1 とならない限り任意に可能である．

処理 3-3: 誤差位置バイナリマップ e より，ブロック内に少なくとも一つの予測誤差が含まれていた場合，図 3 に示すように，暗号化画像 I_e 内の対応するブロックの MSB を e で置換する．

処理 3-4: 誤差位置バイナリマップ e より，予測誤差のないブロックが三つ以上連続した場合，これらのブロックは埋込み可能ブロックとなる．この一連の埋込み可能ブロックを埋込み可能領域と呼ぶ．暗号化画像 I_e において，埋込み可能領域を特定するため，この領域内の両端のブロックに対して MSB をすべて 1 に置き換えることによりフラグを設定し，暗号化画像 I'_e を生成する．

以上の手順により，フラグに囲まれたブロックは埋込み可能領域と判断され，次節で述べる情報埋込みに使用される．一方，フラグの外にあるブロックは，埋込み処理から除外される．

2.1.4 情報埋込み

埋込み可能領域に対して，情報埋込みを行い，出力画像 I_{ew} を生成する．以下に手順を述べる．

処理 4-1: 埋込み情報 b を 8 ビットごとに区切る．各 8 ビットにおいて，図 4 に示すように，先頭の 7 ビットに 1 が連続して出現した場合，8 ビット目の値に関わらず，7 ビット目と 8 ビット目の間に 0 を挿入する．この処理を b 全体に対して行い，埋込み情報 b' を得る．

処理 4-2: フラグが設定された暗号化画像 I'_e の埋込み可能領域において，フラグとなる両端ブロックを除く各ブロック内の画素の MSB を埋込み情報 b' で置換する．

$$p_{ew}(i,j) = b'_k \times 128 + (p_e(i,j) \bmod 128) \qquad (5)$$

ここで，b'_k は k ビット目の埋込み情報を示す．

処理 4-3: 情報埋込み鍵 K_w を用いて，MSB 全体を暗号化し，I_{ew} を生成する．

ここで，処理 4-1 では埋込み情報に対して前処理を行っている．ある埋込み情報内に 1 が 8 ビット以上連続して現れ，埋込み可能ブロックの MSB がすべて 1 に置換された場合，抽出処理でフラグと誤って認識される．これを回避するため，あらかじめ埋込み情報に 1 が 7 ビット連続して出現した際，8 ビット目にマーカとして 0 を挿入している．これにより，提案法は，埋込み情報の特性に関わらず可逆性を保証することができる．

2.2 情報抽出・復元処理手順

ここでは，図 5 に従い，情報抽出と復元の処理について具体的な手順を述べる．

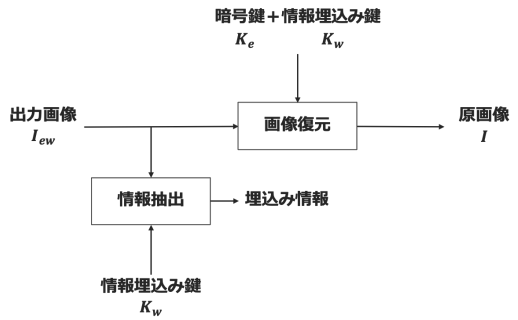


図 5: 提案法の情報抽出・復元処理手順

2.2.1 情 報 抽 出

まず，埋込み情報 b' を抽出する．手順は以下のとおりである．

処理 5-1: 情報埋込み鍵 K_w を用いて，出力画像 I_{ew} の MSB を復号する．

処理 5-2: 処理 3-3 で設定されたフラグから埋込み可能領域を特定し，フラグとなる両端ブロックを除く各ブロック内の画素の MSB に対して，式 (6) により情報を抽出する．

$$b'_k = p_{ew}(i,j)/128 \tag{6}$$

処理 5-3: 抽出された情報 b' を 8 ビットごとに区切る．各 8 ビットにおいて，先頭の 7 ビットに 1 が連続して出現した場合，8 ビット目の 0 を削除する．この処理を b' 全体に対して行い，埋込み情報 b を得る．

2.2.2 画 像 復 元

提案法は，情報を抽出後，もとの MSB を正確に予測することで，原画像を復元できる．

処理 6-1: 出力画像 I_{ew} の下位 7 ビットに対して，暗号鍵 K_e により生成された $8 \times M \times N$ ビットの疑似乱数列 s の対応するビット列を用いて，XOR 演算を施す．

$$\tilde{p}(i,j) = s(i,j) \oplus p_{ew}(i,j) \tag{7}$$

処理 6-2: 出力画像 I_{ew} の MSB より，設定されたフラグに従い，誤差位置バイナリマップ e を得る．

処理 6-3: 現在の $\tilde{p}(i,j)$ の一つ前に復元された隣接画素を参照画素 $pred(i,j)$ とする．次式より，MSB を 0 とした場合の値 $\tilde{p}(i,j)^{MSB=0}$ と $pred(i,j)$，および，1 とした場合の値 $\tilde{p}(i,j)^{MSB=1}$ と $pred(i,j)$ の絶対差 Δ^0 と Δ^1 を計算する．

$$\begin{cases} \Delta^0 = |pred(i,j) - \tilde{p}(i,j)^{MSB=0}| \\ \Delta^1 = |pred(i,j) - \tilde{p}(i,j)^{MSB=1}| \end{cases} \tag{8}$$

処理 6-4: 式 (9) に従い，もとの MSB を予測し，原画像 I を得る．

$$\tilde{p}(i,j) = \begin{cases} \tilde{p}(i,j)^{MSB=0}, & \text{if} \Delta^0 < \Delta^1 \text{かつ } e(i,j) = 0 \\ \tilde{p}(i,j)^{MSB=1}, & \text{if} \Delta^0 < \Delta^1 \text{かつ } e(i,j) = 1 \\ \tilde{p}(i,j)^{MSB=0}, & \text{if} \Delta^0 = \Delta^1 \text{かつ } e(i,j) = 0 \\ \tilde{p}(i,j)^{MSB=1}, & \text{if} \Delta^0 = \Delta^1 \text{かつ } e(i,j) = 1 \\ \tilde{p}(i,j)^{MSB=1}, & \text{if} \Delta^0 > \Delta^1 \text{かつ } e(i,j) = 0 \\ \tilde{p}(i,j)^{MSB=0}, & \text{if} \Delta^0 > \Delta^1 \text{かつ } e(i,j) = 1 \end{cases} \tag{9}$$

提案法では，埋込み情報自体の暗号化を指定していないため，原画像の復元が可能なユーザは埋込み情報も取得可能となる．これを回避するため，別の暗号鍵を導入し，処理 4-1 の前に埋込み情報をあらかじめ暗号化しておくことも有効である．これにより，原画像の復元が可能なユーザは埋込み情報の抽出ができる一方，抽出した情報の内容を知ることはできない．

2.3 先行研究 [8] の課題

Puteaux ら [8] は，MSB 予測を用いた暗号化画像に対する可逆情報埋込み法を提案した．この手法は，低演算量で 1bpp の大容量を達成する手法である．しかし，この手法は，複数の点において可逆性が保証されず，情報抽出・暗号解除が行われても完全には原画像を復元することができない．以下では，これらの問題点について具体的に説明する．

2.3.1 埋込み情報

先行研究では，暗号化画像に対するフラグ設定において，提案法と同様に暗号化画像と誤差位置バイナリマップを 8×1 画素のブロックに分割する．その後，誤差位置バイナリマップより，ブロック内に少なくとも一つの予測誤差が含まれていた場合，そのブロックの前後に隣接するブロック内の MSB をすべて 1 に置換する．これにより，前後のブロックは埋込み不可能なブロックを特定するフラグとして機能する．そのため，埋込み情報に 1 が 8 ビット以上連続して現れ，それらがある埋込み可能ブロックのすべての MSB に置換された場合，そのブロックは誤ってフラグと判断され，正しい情報抽出と画像復元を妨げる．

一方，提案法では，一定の条件下で，埋込み情報にマーカとして 0 を挿入する前処理を施す．このため，上述のように，情報埋込みによって誤ったフラグが生成されることなく，情報の抽出と原画像の復元が正しく行われる．

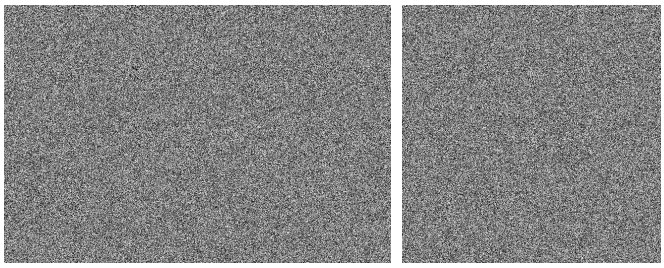
2.3.2 誤差位置バイナリマップの生成

提案法では，誤差位置バイナリマップの生成に式 (3)，画像復元処理に式 (9) を用いているが，先行研究ではこれらの式がそれぞれ式 (10)，(11) に置き換えられる．

$$e(i,j) = \begin{cases} 0, & \text{if} \Delta < \Delta^{inv} \\ 1, & \text{if} \Delta \geqq \Delta^{inv} \end{cases} \tag{10}$$

(a) 画像 23　　(b) 画像 31

図 6: 原画像



(a) 画像 23　　(b) 画像 31

図 7: 提案法による出力画像

$$\tilde{p}(i,j) = \begin{cases} \tilde{p}(i,j)^{MSB=0}, & \text{if} \Delta^0 < \Delta^1 \text{かつ } e(i,j) = 0 \\ \tilde{p}(i,j)^{MSB=1}, & \text{if} \Delta^0 < \Delta^1 \text{かつ } e(i,j) = 1 \\ \tilde{p}(i,j)^{MSB=1}, & \text{if} \Delta^0 \geqq \Delta^1 \text{かつ } e(i,j) = 0 \\ \tilde{p}(i,j)^{MSB=0}, & \text{if} \Delta^0 \geqq \Delta^1 \text{かつ } e(i,j) = 1 \end{cases} \quad (11)$$

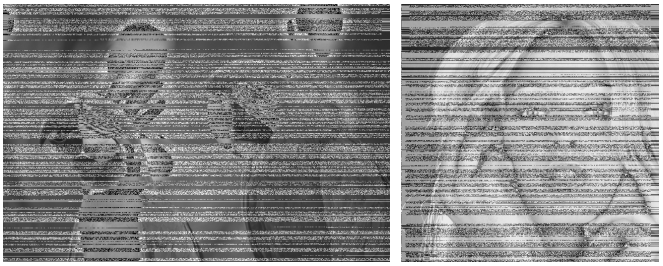
まず，誤差位置バイナリマップの生成時，式 (10) より，絶対差 $\Delta = \Delta^{inv}$，すなわち，$\Delta^0 = \Delta^1$ のとき，$e(i,j) = 1$ となる．一方，画像復元処理の際，式 (11) に従うと，$\Delta^0 = \Delta^1$ かつ $e(i,j) = 1$ の場合，MSB $= 0$ と指定されているため，もとの MSB が 1 であった場合，正しく復元されない．

これに対して，提案法では，絶対差 $\Delta = \Delta^{inv}$ の場合，式 (3) に従いもとの MSB を $e(i,j)$ に格納し，式 (9) により正しい MSB が復元される．

2.3.3　暗号化画像の MSB に対するフラグ設定

先行研究では，2.3.1 で述べたとおり，予測誤差を含むブロックの前後に隣接するブロックをフラグとして埋込み不可能なブロックを特定する．そのため，最初，もしくは，最後のブロックが予測誤差を含む場合，これらのブロックの前もしくは後に隣接するブロックが存在せず，フラグを設定することができない．その結果，予測誤差を含む最初と最後のブロックも埋込み可能なブロックと判断され，MSB 置換が行われてしまい，もとの画素値を正確に予測できない．

提案法では，埋込み不可能なブロックではなく，埋込み可能なブロック，すなわち，埋込み可能領域を特定する．したがって，最初，もしくは，最後のブロックが予測誤差を含む場合でも，これらのブロックはフラグで囲まれる必要がなく，フラグの外のブロック，すなわち，埋込み不可能なブロックとして判断される．



(a) 画像 23　　(b) 画像 31

図 8: 先行研究 [8] による復元画像

3.　シミュレーション

提案法において，可逆性と埋込み容量の観点からそれぞれ評価を行う．シミュレーションには，画像データベース [10,11] より 32 枚の試験画像を使用した．ただし，本研究では，各画像をグレースケールに変換しており，画像データベース [10] の画像については 1/4 に縮小している．したがって，画像サイズは，$512 \times 768/768 \times 512$ 画素 [10] および 512×512 画素 [11] となる．図 6 に試験画像の例を，図 7 に提案法を用いて図 6 の原画像から生成された出力画像の例をぞれぞれ示す．

3.1　可逆性の評価

ここでは，提案法と先行研究 [8] により生成された出力画像に対して，情報抽出および復元処理を行った際，原画像が復元可能であるかを確認する．結果を表 1 に示す．同表において，①は埋込み情報に対するマーカ挿入（2.3.1），②は $\Delta = \Delta^{inv}$ のときの MSB 予測条件（2.3.2），③は埋込み可能領域特定のためのフラグの導入（2.3.3）をそれぞれ意味する．これより，提案法は，すべての画像において原画像を復元可能で，埋込み情報と画像の特性に関わらず，可逆性が保証されていることがわかる．これに対して，先行研究では，図 8 に示すように，多くの場合に原画像を復元することができない．なお，②または③のみを適用した場合，提案法も先行研究と同様にいずれの画像についても原画像を復元できなかった．したがって，①，②，③のすべての特徴を保持することが可逆性の保証に必要となる．

3.2　埋込み容量の評価

表 2 に，すべての画像における提案法と先行研究の埋込み容量を示す．同表より，提案法は先行研究 [8] と同等の埋込み容量を保持していることがわかる．また，従来の暗号化画像に対する可逆情報埋込み法では，埋込み容量は最大でも 0.5bpp 程度である [6]．このことから，提案法は 2 倍程度の大きい埋込み容量を実現している．

提案法では，可逆性を保証するために埋込み情報にマーカとして 0 を挿入する前処理を施す．したがって，埋込み可能領域に対する実際の埋込み情報の割合は先行研究と比較して減少する．一方で，誤差位置バイナリマップの生成において，提案法は先行研究とは異なり，絶対差 Δ と Δ^{inv} が等しい場合に，もとの MSB を誤差位置バイナリマップに格納する．これにより，先行研究と比較して予測誤差の発生数は減少し，ま

表 1: 情報抽出・復元処理後に原画像へ復元可能

画像番号	提案法			先行研究	画像番号	提案法			先行研究
	①のみ	①+②	①+②+③	[8]		①のみ	①+②	①+②+③	[8]
01	×	✓	✓	×	17	×	✓	✓	×
02	×	✓	✓	×	18	×	✓	✓	×
03	×	✓	✓	×	19	×	✓	✓	×
04	✓	✓	✓	×	20	×	✓	✓	×
05	×	✓	✓	×	21	×	✓	✓	×
06	×	✓	✓	×	22	×	✓	✓	×
07	✓	✓	✓	×	23	×	✓	✓	×
08	×	✓	✓	×	24	×	✓	✓	×
09	×	✓	✓	×	25	×	×	✓	×
10	×	✓	✓	×	26	×	✓	✓	×
11	×	✓	✓	×	27	×	×	✓	×
12	×	✓	✓	×	28	×	✓	✓	×
13	×	✓	✓	×	29	×	✓	✓	×
14	×	✓	✓	×	30	×	×	✓	×
15	×	✓	✓	×	31	×	×	✓	×
16	×	✓	✓	×	32	×	×	✓	×
原画像へ復元可能な画像 [枚]						2	27	32	0

表 2: 埋込み容量

画像番号	埋込み容量 [bpp]		画像番号	埋込み容量 [bpp]	
	提案法	先行研究 [8]		提案法	先行研究 [8]
01	0.9465	0.9469	17	0.9883	0.9894
02	0.9944	0.9955	18	**0.9694**	0.9560
03	0.9948	0.9952	19	0.9587	0.9587
04	0.9948	0.9958	20	**0.9593**	0.9574
05	0.9314	0.9324	21	0.9804	0.9805
06	**0.9774**	0.9762	22	**0.9816**	0.9765
07	0.9955	0.9966	23	**0.9940**	0.9911
08	**0.8591**	0.8582	24	**0.9369**	0.9269
09	0.9875	0.9885	25	**0.9404**	0.9080
10	0.9871	0.9881	26	**0.9897**	0.9864
11	0.9802	0.9812	27	**0.8595**	0.8557
12	0.9937	0.9946	28	**0.9390**	0.9211
13	0.9235	0.9242	29	**0.9314**	0.9216
14	0.9764	0.9764	30	**0.9879**	0.9691
15	0.9906	0.9912	31	**0.9807**	0.9738
16	0.9977	0.9985	32	**0.9535**	0.9399
平均 [bpp]				**0.9650**	0.9610

た，Serpentine 走査を採用することで，より予測誤差の発生数が少ない走査／方向が選択可能となる．上記の理由から，提案法は可逆性を保証しながらも先行研究と同等の埋込み容量を保持する．

4. ま と め

本稿では，暗号化画像を対象とし，MSB 予測を用いることにより，大容量かつ可逆性を保証する情報埋込み法を提案した．提案法の特徴は，埋込み情報と暗号化後の画像に対してマーカやフラグを設定し，さらに，MSB 予測における条件を正確に与えることで可逆性を十分に保証する点にある．シミュレーションにより，すべての試験画像に対して可逆性を確認し，埋込み容量についても 0.965bpp 程度と高い結果を得た．今後は，予測誤差の算出方法について改善し，埋込み容量のさらなる向上を図る．

文 献

[1] J. Tian, “Reversible data embedding using a difference expansion,” IEEE Trans. Circuits Syst. Video Technol., vol.13, no.8, pp.890–896, 2003.

[2] D. M. Thodi and J. J. Rodriguez, “Prediction-error based reversible watermarking,” in Proc. IEEE Int. Conf. Image Process., vol.3, pp.1549–1552, 2004.

[3] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, “Reversible data hiding,” IEEE Trans. Circuits Syst. Video Technol., vol.16, no.3, pp.354–362, 2006.

[4] Y. Q. Shi, X. Li, X. Zhang, H. T. Wu, and B. Ma, “Reversible data hiding: Advances in the past two decades,” IEEE Access., vol.4, pp.3210–3237, 2016.

[5] X. Zhang, “Reversible data hiding in encrypted image,” IEEE Signal Process. Lett., vol.18, no.4, pp.255-258, 2011.

[6] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, “Reversible data hiding in encrypted images by reserving room before encryption,” IEEE Trans. Inf. Forensics Security, vol.8, no.3, pp.553–562, 2013.

[7] S. Imaizumi, Y. Izawa, R. Hirasawa, and H. Kiya, “A Reversible Data Hiding Method in Compressible Encrypted Images,” IEICE Trans. Fundamentals, vol.E103-A, no.12, pp.1579–1588, 2020.

[8] P. Puteaux and W. Puech, “An Efficient MSB Prediction-Based Method for High-Capacity Reversible Data Hiding in Encrypted Images,” IEEE Trans. Inf. Forensics Security, vol.13, no.7, pp.1670–1681, 2018.

[9] I. C. Dragoi and D. Coltuc, “On the Security of Reversible Data Hiding in Encrypted Images by MSB Prediction,” IEEE Trans. Inf. Forensics Security, vol.16, 2021.

[10] [Online] Available: http://www.math.purdue.edu/~lucier/PHOTO_CD/D65_TIFF_IMAGES/

[11] [Online] Available: http://sipi.usc.edu/database/database.php