

# 可逆情報埋込みと画像スクランブルの順序可換な協調手法

A Collaborative Method for Reversible Data Hiding and Image Scrambling

劉審川  
Shenchuan LIU

藤吉正明  
Masaaki FUJIYOSHI

貴家仁志  
Hihoshi KIYA

首都大学東京大学院システムデザイン研究科情報通信システム学域  
Department of Information and Communications Systems, Tokyo Metropolitan University

## 1 まえがき

本稿では、可逆情報埋込みと画像スクランブルとが協調する手法を提案する。画像へ情報を埋める情報埋込みと画像のスクランブルとは、併用すると互いが干渉していた。一方、各々の適用箇所を分けることで、互いに干渉しない協調手法も提案されている [1, 2]。この従来法 [1, 2] は符号化画像を対象としており、復号後の画像に対して埋めた情報の抽出やスクランブルの解除を正しく実行できない。また、原画像を復元できない非可逆な情報埋込みである。そこで、空間領域で情報埋込みと画像スクランブルとを施す可逆な手法を提案する。

## 2 従来法

図 1 に協調手法の概念を示す。情報埋込みと画像スクランブルとが互いに干渉せず、図 1 のとおり処理順序を問わない。従来法は、符号化画像の DCT 係数の振幅に情報を埋め、正負符号でスクランブルする [1]、もしくは、ある周波数の係数に情報を埋め、別の周波数の係数でスクランブルする [2]。従来法は復号後の画像に対して、情報抽出やスクランブル解除を正しく実行できず、また、原画像を復元できない非可逆情報埋込みである。次節では、空間領域で処理する可逆な手法を提案する。

## 3 提案法

提案法は画像を非重複ブロックに分割し、ブロック内の画素を情報埋込み用とスクランブル用とに分ける。また、情報を埋めなかったブロックでは情報埋込み用画素もスクランブルする。以下では  $M \times N$  個の  $5 \times 5$  画素のブロック  $B_{m,n}$  に分割し、各ブロック 3 画素 ( $a_{m,n}, g_{m,n}, b_{m,n}$ ) を情報埋込みに用いるものとする。以下、パラメタ導出、情報埋込み、スクランブルの順で説明する。

### 3.1 パラメタ導出

以下で求められるパラメタ  $p$  を情報埋込み、抽出に用いる。

$$\tilde{g}_{m,n} = \lfloor (a_{m,n} + b_{m,n}) / 2 \rfloor \quad d_{m,n} = |a_{m,n} - b_{m,n}| \quad (1)$$

$$\tilde{g}_{m,n} = 2g_{m,n} - \tilde{g}_{m,n} \quad (2)$$

$$s_{m,n} = \begin{cases} d_{m,n}, & \tilde{g}_{m,n} < 0 \text{ or } \tilde{g}_{m,n} > 254 \\ \infty, & \text{others} \end{cases} \quad (3)$$

$$S = \min_{m,n} s_{m,n} \quad D = \max_{m,n} d_{m,n} \quad (4)$$

$$p = \min(255 - D, S) \quad (5)$$

### 3.2 情報埋込み

パラメタ  $p$  を用いて、1 ビット情報  $w_l$  を  $B_{m,n}$  に埋込み可能か判断する。 $d_{m,n}$  は埋込みによって変化しないため、抽出時も  $d_{m,n} < p$  によって情報が埋められているか判別

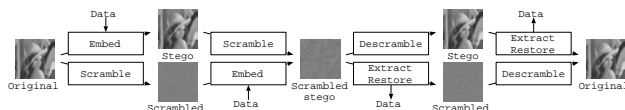


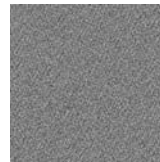
図 1 情報埋込み・画像スクランブル協調手法の概念。



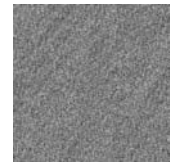
(a) 原画像。



(b) ステゴ画像 (633 ビット埋込, PSNR: 62.5 dB).



(c) スクランブル画像 (PSNR: 9.609 dB).



(d) スクランブルステゴ画像 (633 ビット埋込, PSNR: 9.605 dB).

図 2 シミュレーション結果。

可能である。 $w_l$  は  $\text{mod}(\hat{g}_{m,n} + \tilde{g}_{m,n}, 2)$  で抽出され、その後、式 (6) の逆処理によって原画像が復元される。

$$\hat{g}_{m,n} = \begin{cases} \tilde{g}_{m,n} + w_l, & d_{m,n} < p \\ g_{m,n}, & \text{others} \end{cases} \quad (6)$$

### 3.3 画像スクランブル

0~255 の乱数  $5 \times 5$  個からなる行列  $R_1, R_2$  とを用いて  $B_{m,n}$  をスクランブルする。ただし、 $R_1, R_2$  の  $a_{m,n}, g_{m,n}, b_{m,n}$  に相当する要素は 0 である。スクランブル解除は  $R_1, R_2$  を用いて可能である。

$$B'_{m,n} = \text{mod}(B_{m,n} + mR_1 + nR_2, 256) \quad (7)$$

さらに、情報が埋められていない  $B_{m,n}$  の  $a_{i,j}, g_{i,j}, b_{i,j}$  を、0~255 の乱数  $M \times N$  個からなる行列  $Q$  でスクランブルする。ここで、 $d_{m,n} \geq p$  であれば  $|a_{m,n} - b_{m,n}| = |a'_{m,n} - b'_{m,n}|$  であるので、スクランブル後も  $d_{m,n} \geq p$  によって情報が埋められていないことを判別可能である。

$$a'_{m,n} = \text{mod}(a_{m,n} + mQ_{m,n}, 256) \quad (8)$$

$$b'_{m,n} = \text{mod}(b_{m,n} + mQ_{m,n}, 256) \quad (9)$$

$$g'_{m,n} = \text{mod}(g_{m,n} + nQ_{m,n}, 256) \quad (10)$$

## 4 シミュレーション

512 × 512 画素、256 階調濃淡画像 Lena に提案法を適用した結果を図 2 に示す。スクランブル後の画像から原画像を推定できないことがわかる。なお、図 1 に示すとおり、処理順序を問わないことも確認している。

### 参考文献

- [1] 阿部剛仁, 藤井寛, 串間和彦, 櫻井紀彦, “個別情報埋め込みにより管理機能を強化した画像流通方式,” 信学論 (A), vol.J82-A, no.9, pp.1474–1482, Sept. 1999.
- [2] 若色宏明, 姜錫, 坂本雄児, “半開示スクランブル動画の不正な再利用のための電子透かし技法” 信学 MIH 研資料, pp.53–58, Jun. 2010.