圧縮効率を考慮したカラー画像のための知覚暗号化法

菊池 真徳† 栗原 健太† 塩田 さやか† 貴家 仁志†

†首都大学東京大学院
191-0065 東京都日野市旭が丘 6-6
{kikuchi-masanori, kurihara-kenta}@ed.tmu.ac.jp
{sayaka, kiya}@tmu.ac.jp

あらまし
本稿では，圧縮を前提としたカラー画像における新しい知覚的暗号化法を提案する．知覚暗号化は画像を視覚的に認識困難にする暗号化であり，整数論的な暗号化に比べ，暗号化後に画像圧縮が可能であるなどの高い処理自由度を持つ．提案法はブロック分割した領域で色成分間の値をランダムに入れ替えることで，原画像と比べ色を変化させる方式であり，圧縮に対して影響が少ないという特徴を持つ．さらに，その方法とブロックスクランブル法との組み合わせを考察し，提案法の有効性の評価および適切なブロックサイズについて検討を行う．

A Comprssion-friendly Perceptual Encryption Method for Color Images

Masanori Kikuchi† Kenta Kurihara† Sayaka Shiota† Hitoshi Kiya†

†Tokyo Metropolitan University.
6-6, Asahigaoka, Hino-shi, Tokyo 191-0065, JAPAN
{kikuchi-masanori, kurihara-kenta}@ed.tmu.ac.jp
{sayaka, kiya}@tmu.ac.jp

Abstract
In this paper, a new compression-friendly perceptual encryption method is proposed for color images. Perceptual encryption is an encryption which makes images difficult to recognize visually. Compared to number theory-based encryption methods, perceptual encryption has high flexibility for some image processing. For example, it is able to compress encrypted images. Permutating values among R, G and B components in each divided block is proposed to change the color of an image from the original one and to compress the encrypted image effectively. Furthermore, we propose to combine with the bock scramble scheme in each color component. We discuss how to choose the block size and evaluate the effectiveness of the proposed method.

1 まえがき

近年，クラウドコンピューティングや分散処理などの広まりに伴い，セキュリティの観点から暗号化データの圧縮に関する研究が多く行われている [1–7]．それらの環境では，コンテンツの通信及びコンテンツに対する処理は，帯域制限があり，かつ安全性の確立できない通信チャネルを用いている．そのため，通信時の安全性

を高めるために，コンテンツの暗号化が必要となる．

一般的に，セキュリティを考慮した画像コンテンツの通信は最初に画像の圧縮を行い，その後，圧縮データに対して暗号化を行う．その際，コンテンツ提供者がネットワークプロバイダに画像を送信し，ネットワークプロバイダが暗号化処理を施すことが多い．圧縮データの暗号化には，一般に AES や DES など [8] の数論変換に基づく暗号化方式を用いる．ネットワークプロバイダは暗号化データを受信者に送信し，受信者は復号と伸長を行うことで画像を得る．しかし，このモデルではネットワークプロバイダに画像を開示しなければならないという問題がある．また，数論変換に基づく暗号化の使用下では，一般的に暗号化データの誤りを許容しないため，伝送路上で誤りが生じた場合には暗号化データの復元が困難となるという問題がある．

上記の問題を解決するために，画像に暗号化を施した後に，暗号化データを圧縮するモデルがある．一般的に，数論変換に基づく暗号化の使用下では，画像データの圧縮効果は期待できない．そのため，このモデルでは，数論変換に基づく暗号化方式ではなく，画像圧縮が可能な知覚的暗号化法を用いる．知覚暗号化法は視覚的に認識困難にする暗号化方式である．

暗号化の前処理を伴う画像の圧縮に関する研究は，ロスレス圧縮とロッシー圧縮に分類される．本稿では，ロッシー圧縮，ロスレス圧縮両方の使用を前提とした知覚的暗号化法を考察する．画像圧縮を前提とした知覚的暗号化法として，空間領域でのピクセルスクランブル [2] やブロックスクランブル [3]，位相スクランブル [4] などが存在する．しかしながら，上記の先行研究では，圧縮方式として国際標準方式の使用を前提としていない．従って，暗号化なしの場合に比べ，JPEG 方式などの使用においては，圧縮効率が大きく低下してしまう．一方，国際標準方式を前提とした先行研究 [5, 6] は，カラー画像について考慮されていない．

本稿では，国際標準規格である JPEG，JPEG 2000 [9]，JPEG-LS [10, 11] 圧縮方式を前提とし，かつカラー画像について考慮された提案法は，ブロック分割をベースとした JPEG 圧縮方式と親和性の高いブロックベースの知覚的暗号化法である．提案する知覚的暗号化法はカラー画像においてブロック分割した領域で色成分間の値をランダムに入れ替え，その後ブロックスクランブルを施す．評価実験から，提案法は原画像に対して圧縮効率の低下が少ないことが確認される．

2 準備

一般的に，セキュリティを考慮した画像通信は最初に画像の圧縮を行い，その後，圧縮されたデータに対して暗号化を行う．しかし，いくつかのアプリケーションでは，暗号化と圧縮の順序を逆転されたモデルが考えられており，本稿ではそのモデルを想定している．

2.1 知覚暗号化

はじめに，最初に画像圧縮を行い，その後，暗号化を行うモデルを概説する．ここでは，コンテンツ提供者とネットワークプロバイダは別々な要素とする．

コンテンツ提供者は画像をネットワークプロバイダに送信する．ネットワークプロバイダは画像に対して圧縮を行い，その後，AES や DES などの数論変換に基づく暗号化方式を用いて圧縮されたデータの暗号化を行う．暗号化されたデータは送信され，受信者は鍵を用いて，復号と伸長を行うことで画像を得ることができる．しかし，上記のモデルには以下のような課題が指摘されている．

- 画像の内容をネットワークプロバイダに開示しなければならない (ネットワークプロバイダの安全性を仮定)．
- 伝送路上で誤りが生じた場合，数論変換の使用下では暗号化データの復元が困難である．

本稿では，画像を暗号化した後に，暗号化されたデータを圧縮するモデルを想定する．このモデルで用いられる暗号化方式では，数論変換に基づく暗号化方式ではなく，知覚暗号化法を用いる．画像知覚暗号化法は以下のような性質を持つ．

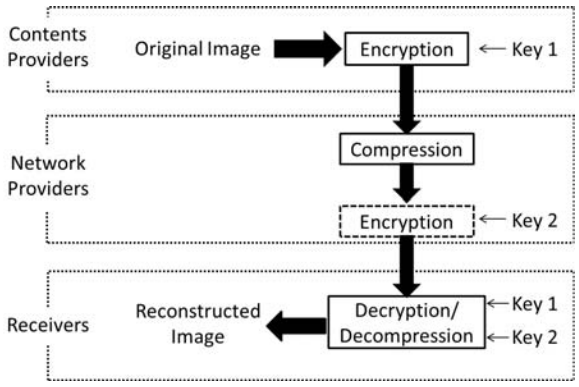


図 1: 知覚暗号化方式の通信モデル.

- 画像を視覚的に認識困難な状態にする.
- 暗号化されたデータの一部が誤った場合でも，データの復号が可能.

本稿で用いる知覚暗号化方式は上記の特性に加えて画像圧縮が可能である．さらに，提案法は，JPEG，Motion JPEG に加え，JPEG 2000 や JPEG-LS といった国際標準の圧縮法が適用可能である．一方，数論変換に基づく暗号化の使用では，伝送路上で誤りが生じた場合，暗号化データの復元が困難である．さらに，数論変換に基づく暗号化は一般的に圧縮することはできない.

図 1 に知覚暗号化方式を用いた画像通信モデルを示す．コンテンツ提供者はネットワークプロバイダに情報を秘密にしたままで，受信者に画像を送りたいとする．コンテンツ提供者はまず知覚暗号化方式を用いてデータを暗号化する．その知覚暗号化されたデータをネットワークプロバイダが圧縮した後，受信者に送信する．受信者は鍵を用いて，知覚暗号化されたデータの復号と伸長を行うことで，画像を得ることができる．このモデルでは，コンテンツ提供者は画像を秘密にしたまま，ネットワークプロバイダが任意のレートでデータを圧縮することができる.

2.2 ブロックベース知覚暗号化

代表的な画像の知覚暗号化法として，画像をブロック分割し，そのブロックを単位とする方法が数多く研究されている [12].

グレースケール画像に対して，ブロックベースの知覚暗号化法の一例を以下に示す (図 2 参照).

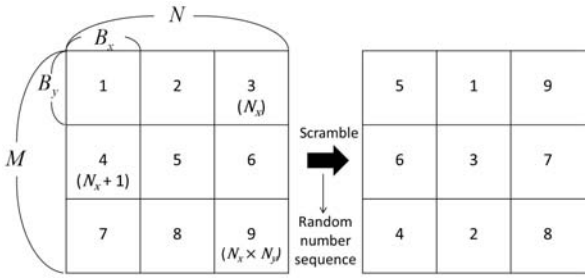


図 2: ブロックスクランブルの例 (ブロック数 $N_x \times N_y = 9$ の場合).

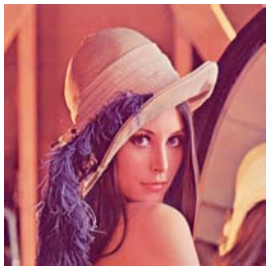
1. $N \times M$ サイズの入力画像を $B_x \times B_y$ サイズのブロックに分割する．このとき，$N_x = \lfloor N/B_x \rfloor$，$N_y = \lfloor M/B_y \rfloor$ より，ブロック数は $N_x \times N_y$ となる．ここで，$\lfloor x \rfloor$ は値 x の小数点以下の切り捨てを示している.
2. シード σ を入力とした疑似乱数生成器によって，1〜$N_x \times N_y$ の乱数列を生成.
3. ブロックは左上から右下へ水平方向にスキャニングを行い，乱数列を用いてブロック交換を行う.

本稿では，上記の知覚暗号化法を特にブロックスクランブルと呼ぶこととする．このとき，復号のために乱数列を保持する必要がある．ブロックベースの知覚暗号化法には，ブロックスクランブル以外の方法も存在する.

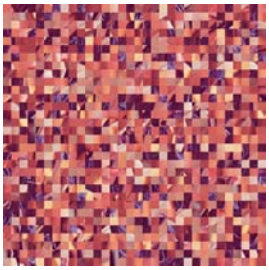
JPEG 圧縮はブロック分割による圧縮であるため，ブロックベースの知覚暗号化法と親和性が高い．しかし，ブロックスクランブルをカラー画像に拡張する場合，以下の点が課題となる.

- R，G，B 成分に同一の乱数列を用いブロックスクランブルを施す場合，原画像と同じ色の画像が生成される (図 3(b))．さらに，R，G，B 成分の各ヒストグラムは，原画像と同一である.
- R，G，B 成分毎に独立な乱数列を用いてブロックスクランブルを施す場合，色の変更は可能となるが，圧縮効率が大きく低下する (図 3(c))．さらに，R，G，B 成分の各ヒストグラムは，原画像と同一である.

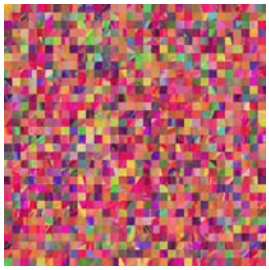
図 3 は，上述の方法を例示している．また，知覚暗号化は，画像の一部に適用することもでき



(a) 原画像.



(b) R，G，B 成分に同一の乱数列を用いた場合.



(c) R，G，B 成分毎に独立な乱数列を用いた場合.

(d) 特定領域のスクランブル.

図 3: 原画像とスクランブル画像 ($B_x = B_y = 16$).

る (図 3(d)).

2.3 画像圧縮

本稿では，ロッシー符号化として JPEG 圧縮方式，ロスレス圧縮として JPEG 2000，JPEG-LS 圧縮方式をそれぞれ用いて提案法を評価する．ここでは，JPEG 圧縮方式の実行手順について概説する．

1. 原画像に $\mathrm{YC_bC_r}$ 色変換を施す.
2. $\mathrm{C_b}, \mathrm{C_r}$ 成分に対してサンプリングを行う．サンプリング比は [4 : 2 : 0]，[4 : 2 : 2]，[4 : 4 : 4] の 3 種類がある．サンプリング比 [4 : 2 : 0] では，$\mathrm{C_b}, \mathrm{C_r}$ 成分は水平方向，垂直方向がそれぞれ 1/2 に間引かれる．[4 : 2 : 2] では，$\mathrm{C_b}, \mathrm{C_r}$ 成分が水平方向のみ 1/2 に間引かれる．[4 : 4 : 4] では，間引き処理が実行されない.
3. $\mathrm{Y}, \mathrm{C_b}, \mathrm{C_r}$ の各成分の値が -128〜127 の範囲になるようにレベルシフトを行う．さらに，8×8 サイズにブロック分割を行う.
4. ブロックごとに DCT 変換を施す.
5. 量子化テーブルにより，量子化を施す.
6. DC 係数は，隣接するブロック間で差分値をとり，ハフマン符号によってエントロピー符号化する．AC 係数はブロック内のジグザグスキャンにより，スキャニングをし，ハフマン符号によってエントロピー符号化する.

上記のように JPEG 圧縮は 8×8 サイズのブロック分割が用いられている．このことが考慮されて，ブロックベースの知覚暗号化法が次に提案される.

3 カラー画像の知覚暗号化

圧縮効率と視覚的な情報保護の観点から，カラー画像のための知覚暗号化法を考察する.

3.1 ブロックサイズの検討

ここでは，ブロックベースの知覚暗号化法を圧縮に適したものにするために，ブロックサイズの検討を行う.

はじめに，ブロック分割を用いた圧縮である JPEG 圧縮方式について検討する．2.3 の JPEG 圧縮方式の実行手順において上述したように，JPEG 圧縮方式の処理は，直流成分の予測を除けば，8×8 サイズのブロックごとに閉じている．ただし，入力がカラー画像である場合，$\mathrm{C_b}, \mathrm{C_r}$ 成分に対して最大で 1/2 の間引きが施される．このことを考慮すると，1/2 の間引きをする場合，色差成分で 8×8 サイズのブロックを作るためには，16×16 サイズのブロックが必要となる．したがって，JPEG 圧縮を前提とした場合，$16k \times 16l$ サイズ (ここで，k, l は自然数とする) のブロックで暗号化を行うことで，直流成分以外の DCT 係数をブロック前と同じ状態に保持することが可能となる．本稿では，ブロックサイズとして $16k \times 16l$ を選択することを提案する.

次に，圧縮時にブロック分割を用いない JPEG 2000，JPEG-LS 圧縮方式について検討する．これらの圧縮方式では，一般にブロック分割することが圧縮効率に影響を与える．ブロックサイズが小さい場合，圧縮効率が低下し，ブロック

表 1: 色成分間スクランブルにおける乱数と成分間の対応表

乱数	R 成分	G 成分	B 成分
0	R	G	B
1	G	R	B
2	R	B	G
3	B	G	R
4	B	R	G
5	G	B	R

サイズが大きいほど，圧縮効率の低下が軽減される．また，JPEG 2000 では，その解像度スケーラビリティ機能を維持するためにブロックサイズを 2 のべき乗に選択する必要がある．

上述のように，ブロックベースの知覚暗号化法におけるブロックサイズの選択は，暗号化画像の視認性や鍵空間の問題だけでなく，圧縮効率にも影響を与えるため，重要な課題となる．

3.2 色成分間のブロックスクランブル

RGB 色空間におけるブロックベースの色成分間のブロックスクランブルを提案する．以下に提案法の手順を示す．

1. $N \times M$ サイズの入力画像を $C_x \times C_y$ サイズのブロックに分割する．このとき，$M_x = \lfloor N/C_x \rfloor$，$M_y = \lfloor M/C_y \rfloor$ より，ブロック数は $M_x \times M_y$ となる．
2. シード σ を入力とした疑似乱数生成器によって，0〜5 の整数をブロック数 $M_x \times M_y$ だけ生成する．
3. 2. で生成した乱数列と表 1 の成分間の対応に従って，ブロックごとに R，G，B 成分間の画素値を入れ替える．

本稿では，上記の知覚暗号化法を特に色成分間のブロックスクランブルと呼ぶ．このとき，この処理によって，原画像と異なる色が生成され，かつヒストグラムも変形される．

一方，RGB 色空間内における成分毎に独立なブロックスクランブルは，圧縮効率を大きく低下させることに注意する．スクランブルによって輝度を変化させないため，RGB 色空間から

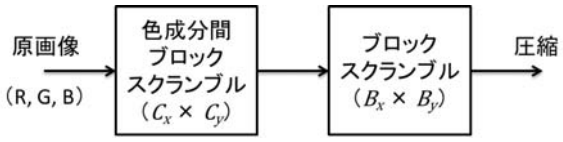


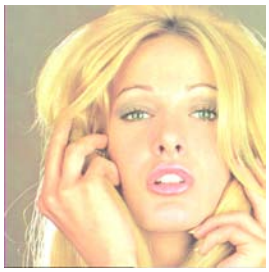
図 4: 混合スクランブルの処理手順．

YC_bC_r 色空間に変換し，Y, C_b, C_r 成分毎に独立な乱数列を用いてスクランブルを施す方法も考えられる．しかし，スクランブル後に，スクランブル画像を RGB 色空間に逆変換する際，一般に RGB 色空間の値域を超えてしまうために，復元画像の画質劣化を生じさせる．その結果，この方法でも，課題の解決にはならない．

3.3 混合スクランブル

3.2 で述べた色成分間のブロックスクランブルによって，原画像とは異なる色を持つスクランブル画像を生成することができる．しかし，後述するように視覚的には画像の内容を認知することは容易である．そこで，ここでは，ブロックスクランブルと色成分間のスクランブルを併用した知覚的暗号化法を提案する．以下に提案法の手順を示す．

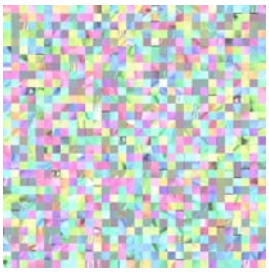
1. $N \times M$ サイズの入力画像を $C_x \times C_y$ サイズのブロックに分割する．このとき，$M_x = \lfloor N/C_x \rfloor$，$M_y = \lfloor M/C_y \rfloor$ より，ブロック数は $M_x \times M_y$ となる．
2. シード σ_1 を入力とした疑似乱数生成器によって，0〜5 の整数をブロック数 $M_x \times M_y$ だけ生成する．
3. 2. で生成した乱数列と表 1 の成分間の対応に従って，ブロックごとに R，G，B 成分間の画素値を入れ替える．
4. $N \times M$ サイズの入力画像を $B_x \times B_y$ サイズのブロックに分割する．このとき，$N_x = \lfloor N/B_x \rfloor$，$N_y = \lfloor M/B_y \rfloor$ より，ブロック数は $N_x \times N_y$ となる．
5. シード σ_2 を入力とした疑似乱数生成器によって，$1 \sim N_x \times N_y$ の乱数列を生成する．
6. ブロックは左上から右下へ水平方向にスキャニングを行い，R，G，B 成分に 5. で生成



(a) 原画像.

(b) 色成分間スクランブル ($C_x = C_y = 128$).

(c) 色成分間スクランブル ($C_x = C_y = 16$).



(d) 混合スクランブル ($B_x = B_y = 16$, $C_x = C_y = 16$).

図 5: 原画像とスクランブル画像.

した同一の乱数列を用いてブロック交換を行う.

上記の手順 1.〜3. は色成分間のブロックスクランブルに相当し，手順 4.〜6. はブロックスクランブルに対応する (図 4 参照)．本稿では，上記の知覚暗号化法を特に混合スクランブルと呼ぶこととする.

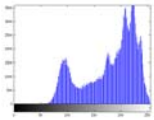
4 評価実験

ブロックスクランブルを用いた知覚暗号化法について視認性と圧縮効率の観点から評価を行う．画像圧縮は，ロッシー (JPEG) とロスレス (JPEG 2000，JPEG-LS) の両方から評価を行う.

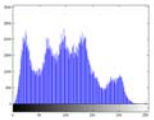
4.1 視認性の確認

知覚暗号化を施した画像の視認性を確認する．色成分間ブロックスクランブルと混合スクランブルを施した画像を図 5 に示す.

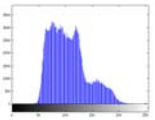
図 5(b)，(c) から，色成分間ブロックスクランブルのみの場合，暗号化画像において原画像の情報が視認できるため画像の知覚暗号化に不十分であることが分かる．一方，混合スクランブルの場合，視覚的に原画像の情報は確認できない.



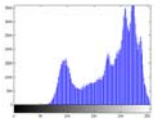
(a) 原画像 (R 成分).



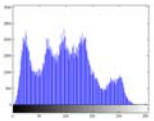
(b) 原画像 (G 成分).



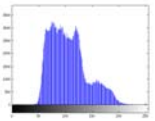
(c) 原画像 (B 成分).



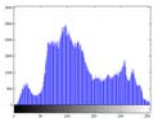
(d) ブロックスクランブル (R 成分).



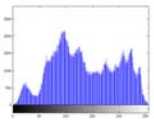
(e) ブロックスクランブル (G 成分).



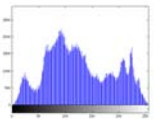
(f) ブロックスクランブル (B 成分).



(d) 混合スクランブル (R 成分).



(e) 混合スクランブル (G 成分).



(f) 混合スクランブル (B 成分).

図 6: 原画像とスクランブル画像の各成分のヒストグラム.

また，図 5(b)，(c) から分かるように，ブロックベースの知覚暗号化法による暗号化画像の視認性はブロックサイズに依存する．そのため，ブロックサイズは適切なものを選択する必要がある.

さらに，原画像 (Lenna)，R，G，B 成分毎に独立な乱数列を用いたブロックスクランブル画像，混合スクランブル画像，3 種類の R，G，B 成分それぞれのヒストグラムを図 6 に示す．ブロックスクランブルでは，原画像のヒストグラムと変化がないこと分かる．一方，混合スクランブルでは，R，G，B 全ての成分でヒストグラムが変化していることが分かる.

4.2 JPEG 符号化での評価

ここでは，ロッシー圧縮である JPEG 圧縮方式を用いて知覚暗号化法の圧縮効率について評

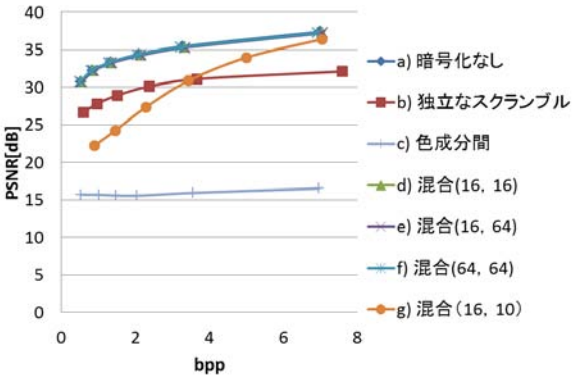


図 7: JPEG 圧縮における実験結果（[4 : 2 : 0]）.

価を行う．圧縮処理の前処理の違いによって，以下の 7 つの条件を使用した．

a) 暗号化なし．

b) R，G，B 成分毎に独立な乱数列を用いたブロックスクランブル ($B_x = B_y = 16$).

c) 色成分間のブロックスクランブル ($C_x = C_y = 1$).

d) 混合スクランブル ($B_x = B_y = 16$，$C_x = C_y = 16$).

e) 混合スクランブル ($B_x = B_y = 16$，$C_x = C_y = 64$).

f) 混合スクランブル ($B_x = B_y = 64$，$C_x = C_y = 64$).

g) 混合スクランブル ($B_x = B_y = 16$，$C_x = C_y = 10$).

上記 7 つの方法を Lenna 画像 (サイズ:512×512，ビット深度:RGB 各 8 ビット) に対して用いた場合の圧縮時における bpp と復号画像との PSNR の関係を図 7 に示す．ただし，JPEG 圧縮のサンプリング比は [4 : 2 : 0] である．

c) および g) の条件で，図 7 の結果から，ブロックサイズを $16k \times 16l$ と選択しなかった場合，圧縮効率が大きく低下していることが分かり，3.1 での検討の妥当性が確認される．また，b) の成分毎に独立な乱数列を用いた場合では，ブロックサイズを $16k \times 16l$ と選んだ場合でも，圧縮効率が大きく低下していることが分かる．

表 2: 実験条件

画像	標準画像
画像数	5 枚
画像サイズ ($N \times M$)	512×512
ビット深度 (R, G, B)	8 ビット × 3 成分

表 3: JPEG-LS によるロスレス圧縮

方法	bpp
a) 暗号化なし	13.25
b) 独立なスクランブル ($B_x = 16$)	13.84
c) 色成分間 ($C_x = 1$)	21.38
d) 混合 ($B_x = 16, C_x = 16$)	13.86
e) 混合 ($B_x = 16, C_x = 64$)	13.86
f) 混合 ($B_x = 64, C_x = 64$)	13.43
g) 混合 ($B_x = 16, C_x = 10$)	14.44

一方，提案法である混合スクランブルの場合，グラフは暗号化なしの場合とほぼ一致しており，圧縮効率の低下を防いでいることが分かる．さらに，e)，f) のように混合スクランブルにおけるブロックサイズを大きく選択した場合においても，圧縮効率に大きな変化は見られない．視認性と鍵空間を考慮するとブロックサイズは 16×16 の選択が JPEG 圧縮方式において妥当であると考えられる．

4.3 ロスレス符号化での評価

ここでは，ロスレス圧縮である JPEG 2000，JPEG-LS 圧縮方式を用いて知覚暗号化法の圧縮効率について評価を行う．4.2 での 7 つの条件について比較を行う．その他の実験条件は，表 2 にまとめる．以下の実験結果における bpp は画像 5 枚の平均を示している．

JPEG-LS 圧縮方式による結果を表 3 に示す．JPEG-LS 圧縮方式は空間領域で処理が行われるため，d) の混合スクランブルの圧縮効率は，b) の独立な乱数列を用いたブロックスクランブルと同程度の圧縮効率となっている．また，d) ～f) の結果より，混合スクランブルの圧縮効率は，色成分間のブロックスクランブルにおけるブロックサイズ ($C_x \times C_y$) による影響よりも，ブロックスクランブルにおけるブロックサイズ ($B_x \times B_y$) による影響が大きいことが分かる．

表 4: JPEG 2000 によるロスレス圧縮

方法	bpp
a) 暗号化なし	13.78
b) 独立なスクランブル ($B_x = 16$)	16.57
c) 色成分間 ($C_x = 1$)	21.32
d) 混合 ($B_x = 16, C_x = 16$)	15.41
e) 混合 ($B_x = 16, C_x = 64$)	15.40
f) 混合 ($B_x = 64, C_x = 64$)	14.21
g) 混合 ($B_x = 16, C_x = 10$)	16.74

このとき，ブロックサイズ ($B_x \times B_y$) が大きいほど圧縮効率の低下を防ぐ．

次に，JPEG 2000 圧縮方式による結果を表 4 に示す．JPEG 2000 圧縮方式は，ウェーブレット変換により変換領域において処理が行われるため，ブロック分割の影響を JPEG-LS に比べ受ける．その結果，ブロックサイズが大きいほど，その影響は小さい．

5 まとめ

本稿では，カラー画像における圧縮効率を考慮した知覚的暗号化法を提案した．提案法はブロック分割した領域で色成分間の値を入れ替えることで，原画像と比べ色を変化させ，かつ圧縮に対して影響の少ない知覚的暗号化を実現する．実験結果は，他の方法に比べ提案法の圧縮への影響が少ないことを示した．

参考文献

[1] Liu, W., Wenjun, Z., Dong, X. and Yao, Q.: Efficient Compression of Encrypted Grayscale Images, IEEE Trans. Image Processing, Vol.19, No.4, pp.1097-1102 (2010).

[2] Zhang, X.: Lossy Compression and Iterative Reconstruction for Encrypted Image, IEEE Trans. Information Forensics and Security, Vol.6, No.1, pp.53-58 (2010).

[3] Hu, R., Li, X. and Yang, B.: A new lossy compression scheme for encrypted gray-scale images, *Proc. IEEE ICASSP*, pp.7387-7390 (2014).

[4] Ito, I. and Kiya, H.: One-Time Key Based Phase Scrambling for Phase-Only Correlation between Visually Protected Images, EURASIP Journal on Information Security, Vol.2009, no.841045 (2009).

[5] 内田輝，貴家仁志：JPEG 2000 圧縮のための画像の知覚暗号化法，信学技報，Vol.114, No.124, SIP2014-44, pp.117-122 (2014).

[6] 栗原健太，斉藤裕子，今泉祥子，塩田さやか，貴家仁志：JPEG/モーション JPEG 画像のための知覚暗号化とその効率的鍵管理法，信学技報，SIS (2014 発表予定).

[7] El-Samie, F.E.A., Ahmed, H.E.H., Elshry, I.F., Shahieen, M.H., Faragallah, O.S., El-Rabaie, E.S.M., Alshebeili, S.A.: Image Encryption: A Communication Perspective, CRC Press(2013).

[8] Daemen, J. and Rijmen, V.: The Design of Rijndael – AES – The Advanced Encryption Standard, *Information Security and Cryptography. Springer* (2002).

[9] *Information technology — JPEG 2000 image coding system – Part 1: Core coding system.* Int. Std. ISO/IEC IS-15444-1 (2000).

[10] *Information technology — Lossless and near-lossless compression of continuous-tone still image — Baseline.* Int. Std. ISO/IEC IS-14495-1 (1994).

[11] *Information technology — Lossless and near-lossless compression of continuous-tone still image: Extensions.* Int. Std. ISO/IEC IS-14495-2 (2003).

[12] Tang, Z., Zhang, X. and Lan W.: Efficient image encryption with block shuffling and chaotic map, *Multimedia Tools and Applications. Springer* (2014).