

アクセス制御を可能とするブロックスクランブル暗号化法

菊池敦史*, 今泉祥子 (千葉大学), 貴家仁志 (首都大学東京)

A Block-Permutation-Based Encryption Scheme with Access Control

Tsutoshi Kikuchi, Shoko Imaizumi (Chiba University)

Hitoshi Kiya (Tokyo Metropolitan University)

Abstract

This paper proposes a permutation-based image encryption scheme, which allows access control according to user's authority. We first concatenate several images that have been encrypted individually. In the concatenated image, all the blocks would be permuted depending on the assigned positions. Consequently, the arbitrary image/images can be retrieved from the entire encrypted image without decrypting other images.

キーワード: 画像暗号化, ブロックスクランブル暗号化, アクセス制御, ジグソーパズル解法
(Image encryption, block-permutation-based encryption, access control, jigsaw puzzle solver)

1. はじめに

近年, スマートフォンやタブレットの普及により, Social Networking Service (以降, SNS と呼ぶ) やクラウドサービスを介して画像をやり取りする機会が増加している. SNS で画像を送信する場合, 画像の提供者は, その内容を公開したまま SNS プロバイダに送信する. 一般に, 画像は個人情報を含む場合が多いため, SNS プロバイダ上でセキュリティ上の問題が発生した場合, 画像に含まれている個人情報漏洩する危険性がある. そのため, 提供者が送信する画像に対して事前に暗号化を施してから SNS プロバイダに送信し, 情報を公開したい相手にも暗号鍵を提供することで, 画像の情報を取得できるシステムが求められている.

一方, 近年, 画像のデータ量は膨大なため, Facebook や Twitter などの SNS プロバイダは, 提供者から受信した画像に, JPEG によるデータ圧縮を施し, 保存や伝送を行っている [1]. そのため, AES のような整数論的な暗号化法が施された画像に対しては, 圧縮率を保持することができず, データ量を削減することが困難である.

このような背景から, 画像の提供者が, 送信する画像に対して暗号化を施した後に, 暗号化画像に対して圧縮を行う Encryption-then-Compression (以降, EtC と呼ぶ) システム [2, 3] の研究が盛んに行われている. EtC システムに有効な暗号化手法として, ブロックスクランブル暗号化法 [4-6] が提案されている. ブロックスクランブル暗号化は, 画像をブロックに分割し, 各ブロック間の位置の入替え, ブロック単位での回転・反転, ネガポジ反転, RGB 色成分間の入替えの各処理を施すことで暗号化画像を生成する.

ブロックスクランブル暗号化画像の安全性の一部は, 総当たり攻撃を想定した鍵空間の広さに基づいて議論されている. 鍵空間の広さは, 暗号化画像の分割ブロック数に依存しており, ブロック数が多いほど鍵空間が広がる. しかし, ブロックをパズルのピースに例え, ブロックの相関を利用して画像を復元する, ジグソーパズル解法 (以降, JPS

と呼ぶ) に基づく攻撃に対しては, 鍵空間の広さが十分であっても脆弱な場合があることが報告されている. これに対して, 文献 [8] では, 既存のジグソーパズル解法では, 暗号化画像の色成分の変換が施された場合や, 分割ブロック数が増加した場合, 画像の復元率が低下することを示している.

暗号化画像のスクランブル度合いを改善し, 総当たり攻撃やジグソーパズル解法に対する攻撃耐性を向上させるため, 複数枚の画像を結合してブロックスクランブル暗号化を施す手法 [9] が提案された. この手法では, 分割ブロック数を増加させることが可能となることに加え, 複数枚の画像情報が 1 枚の画像中に混在し, もとのブロック間の相関が低下するため, 上述の攻撃に対する攻撃耐性が向上する. しかし, この手法では, 結合により生成された暗号化画像から, 任意の画像のみを抽出して暗号化を解除することができず, すべての画像の暗号化を同時に解除しなければならない.

そこで, 本稿では, 複数枚の画像を結合して生成した暗号化画像から, 任意の画像のみを取り出すことが可能なブロックスクランブル暗号化法を提案する. 提案法では, 個別に暗号化を施した複数枚の画像を結合し, 再度, 画像全体の位置のスクランブルを施す. このとき, 暗号鍵により各画像のブロックが移動する位置を割り当てる. これにより, 暗号化画像から任意の画像のみを, 他の画像の暗号化を解除することなく抽出し, 復号することが可能となる. シミュレーションにより, 提案法の有効性を確認する.

2. 準備

〈2・1〉 ブロックスクランブル暗号化法 [4]

ここでは, 従来のブロックスクランブル暗号化法 [4] の概要を説明する. 従来法では, 図 1 に示すように, 画像を一定サイズのブロックに分割し, ブロック間の位置の入替え, ブロック単位での回転・反転, ネガポジ反転, RGB 色成分間の入替えの各処理を施すことで暗号化画像を生成し

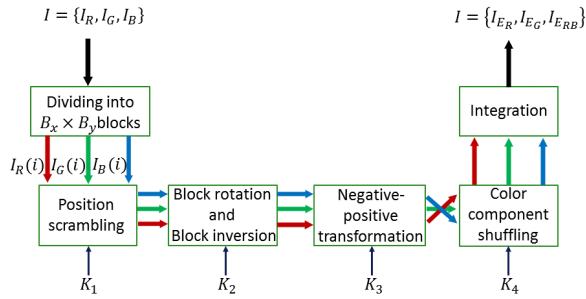


図 1 ブロックスクランブル画像暗号化の手順

Fig. 1. Procedure of block-permutation-based encryption

ている．従来のブロックスクランブル暗号化法の処理手順を以下に示す．

- 処理 1:** $M \times N$ 画素のカラー画像 $I = \{I_R, I_G, I_B\}$ を、任意の $B_x \times B_y$ 画素のブロックに分割する．ここで、 I_R, I_G, I_B は、 I の R, G, B 成分をそれぞれ表す．
- 処理 2:** 分割されたブロックの位置を入れ替える．
- 処理 3:** 各ブロックの回転と反転を行う．
- 処理 4:** 各ブロックの RGB 成分に対してネガポジ反転を行う．
- 処理 5:** 各ブロックの RGB 成分を入れ替える．
- 処理 6:** 分割されたブロックを結合し、暗号化画像 $I_E = \{I_{ER}, I_{EG}, I_{EB}\}$ を生成する．

ここで、処理 2~4 について、RGB 成分に対してそれぞれ同一の処理が施される．上述の処理のうち、処理 2~5 について以下で詳しく述べる．

〈2・1・1〉 ブロック間の位置の入替え

暗号鍵 K_1 により生成された疑似乱数に応じて、分割されたブロックの位置を入れ替える．

〈2・1・2〉 回転・反転

暗号鍵 K_2 により生成された疑似乱数に応じて、図 2 に示すように、各ブロックを回転・反転させる．

〈2・1・3〉 ネガポジ反転

暗号鍵 K_3 により生成された疑似乱数に応じて、各ブロックの画素値を反転させる．画素値の反転は、以下の式で与えられる．

$$\begin{cases} p' = p & (r(i) = 0) \\ p' = 255 - p & (r(i) = 1) \end{cases} \quad (1)$$

ここで、 p はもとの画素値、 p' は処理後の画素値、 $r(i)$ は i 番目のブロックに対する疑似乱数をそれぞれ表す．

〈2・1・4〉 色成分間スクランブル

暗号鍵 K_4 により生成された疑似乱数に応じて、表 1 に示すような RGB 成分の入替えを行う．

ブロックスクランブル暗号化法では、ブロックをパズル

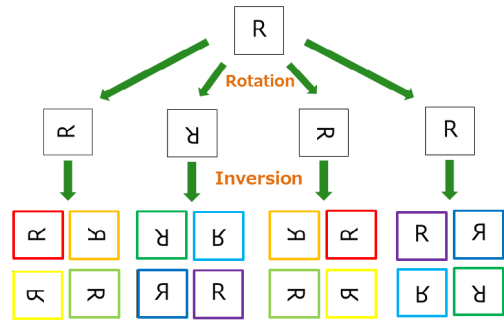


図 2 ブロックの回転・反転

Fig. 2. Block rotation and inversion

表 1 色成分間スクランブル

Table 1. Color component shuffling

Random number	R	G	B
0	R	B	G
1	B	R	G
2	B	G	R
3	G	R	B
4	G	B	R
5	R	G	B

のピースに例え、JPS による攻撃 [7] が想定される．既存の JPS は、分割ブロック数が増加した場合や、ブロック間の色の相関が低下した場合に画像の復元率が低下することが示されている [8]．次節で述べる手法は、ブロック分割数を増加させると同時にブロック間の色の相関を低下させることで、JPS 解法に対する耐性を向上させる．提案法はこの手法に基づき、JPS に高い耐性を考慮している．

〈2・2〉 結合画像を用いたブロックスクランブル暗号化法 [9]

従来法 [9] は、画像データベースの中から複数枚の画像を組み合わせ、結合した画像に対してブロックスクランブル暗号化を施す手法である．以下に手順を説明する．まず、図 3 に示すように、 $M \times N$ 画素の S 枚の画像を含む画像データベースの中から、鍵 K_S を用いて、例えば 4 枚を 1 組として、選択・結合し、 $2M \times 2N$ 画素の結合画像を P 枚 ($P = \frac{S}{4}$) 生成する．

- 処理 1:** $2M \times 2N$ 画素の結合画像 $I_c = \{I_{cR}, I_{cG}, I_{cB}\}$ を、任意の $B_x \times B_y$ 画素のブロックに分割する．ここで、 I_{cR}, I_{cG}, I_{cB} は、 I_c の R, G, B 成分をそれぞれ表す．
- 処理 2:** 分割されたブロックの位置を入れ替える．
- 処理 3:** 各ブロックの回転と反転を行う．
- 処理 4:** 各ブロックの RGB 成分に対してネガポジ反転を行う．
- 処理 5:** 各ブロックの RGB 成分を入れ替える．

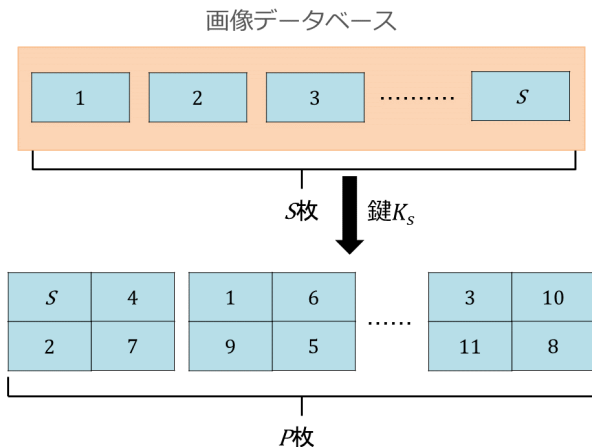


図3 データベースからの画像の選択・結合 [9]

Fig. 3. Concatenation of multiple images in database

処理 6: 分割されたブロックを結合し、暗号化画像 $I_{CE} = \{I_{CE.R}, I_{CE.G}, I_{CE.B}\}$ を生成する。

処理 7: 処理 1～処理 6 までを、 P 枚の結合画像に対して繰り返すことで、 P 枚の暗号化画像を生成する。

このように、従来法 [9] は、画像の結合により、画像サイズが拡大されたため、ブロック分割サイズを保持したまま、ブロックの総数を増加させることができる。また、複数枚の画像情報が 1 枚の画像中に混在するため、ブロック間の相関を低下させることが可能である。これにより、JPS に対する攻撃耐性が向上する。しかし、この手法では、任意の画像に対してのみ暗号化解除を施すことができず、すべての画像の暗号化を同時に解除しなければならない。次章で提案する手法は、複数枚の画像を結合して生成した暗号化画像から、任意の画像を選択し、他の画像の暗号化を解除することなく、復元することを可能とする。

3. 提案法

本章では、ユーザ権限に応じたアクセス制御を可能とするブロックスクランブル暗号化法を提案する。提案法では、画像データベースの中から複数枚の画像選択し、個別にブロックスクランブル暗号化を施した後、それらを結合し、再度、画像全体のブロックの位置に対してスクランブルを施す。この手法では、画像全体のスクランブルを施す際、暗号鍵により、各ブロックが移動する場所を割り当てる。これにより、アクセス制御が可能となり、結合された暗号化画像から、任意の画像のみを、他の画像の暗号化を解除することなく取り出すことができる。以下では、例として、データベースの中から 4 枚の画像を選択し、暗号化を施す場合の処理手順を説明する。

処理 1: 4 枚の $M \times N$ 画素のカラー画像 $I =$

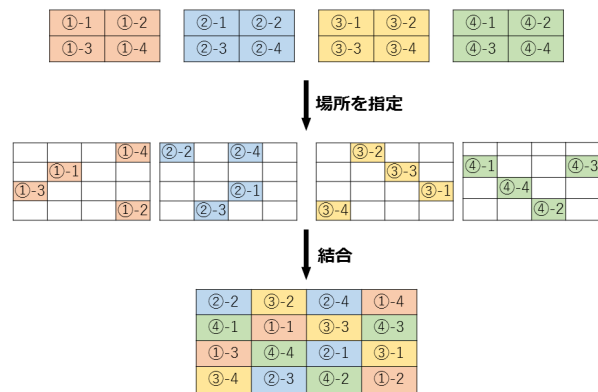


図4 提案法による画像の結合

Fig. 4. Concatenation of multiple images using proposed method

$\{I_R, I_G, I_B\}$ に対して、ブロックスクランブル暗号化法 [4] をそれぞれ適用し、暗号化画像 $I_{E1}, I_{E2}, I_{E3}, I_{E4}$ を生成する。

処理 2: 暗号鍵によって生成された疑似乱数を用いて、4 枚の暗号化画像の各ブロックが移動する位置を図 4 のように割り当てる。

処理 3: 4 枚の暗号化画像を結合し、 $2M \times 2N$ 画素の暗号化画像 $I_{EC} = \{I_{EC.R}, I_{EC.G}, I_{EC.B}\}$ を生成する。

上述のように提案法では、画像の結合により、画像サイズが拡大されるため、ブロック分割サイズを保持したまま、画像中のブロック数を増加させることができる。また、複数枚の画像情報が一枚の画像中に混在するため、ブロック間の相関が低下する。これにより、総当たり攻撃や JPS に対する攻撃耐性が向上する。攻撃耐性を向上させた従来のブロックスクランブル暗号化法 [9] では、生成した暗号化画像から、任意の画像のみを抽出し、復元することができず、すべての画像の暗号化を同時に解除する必要があった。しかし、提案法では、画像全体のスクランブルを施す際、暗号鍵を用いて、それぞれの画像のブロックの移動する位置を指定している。これにより、 $2M \times 2N$ 画素の暗号化画像から復元したい画像のブロックのみを抽出し、他の画像のブロックを残したまま、抽出したブロックから対象画像を復元することが可能である。

4. シミュレーション

提案法を用いて生成された暗号化画像について、スクランブルの度合いを確認するため、評価を行う。シミュレーションには、画像データベースの Content-based image retrieval database [10] から 4 枚ずつの画像（各 768×512 画素、24 ビットカラー）を合計 8 組使用する。ここで、ブロック分



図 5 使用した 4 枚の画像
Fig. 5. Original images

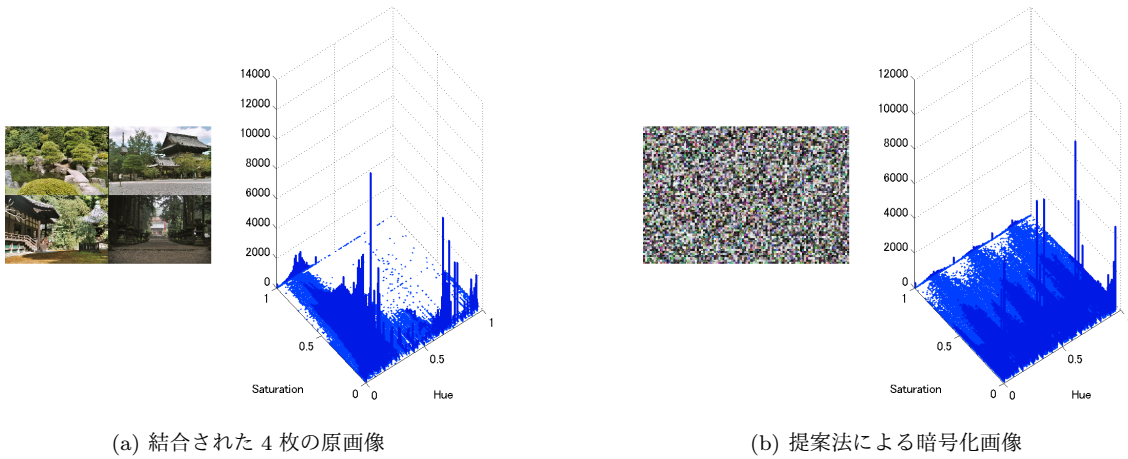


図 6 原画像と暗号化画像のヒストグラムの比較
Fig. 6. Comparison of histograms of original and encrypted images

割サイズはいずれも 16×16 画素である。シミュレーションに用いた 4 枚の原画像の例を図 5 に示す。

〈4・1〉 ヒストグラムを用いた色情報の分布

暗号化画像および暗号化画像から任意の画像を復元した後の暗号化画像の色情報の偏りについて、ヒストグラムを用いて評価を行った。各画像を RGB から HSV に色変換し、H (色相) と S (彩度) に関するヒストグラムを生成した。図 5 に示す 4 枚の原画像を結合した画像とその暗号化画像、およびそれぞれのヒストグラムについて、図 6 に示す。同図より、提案法による暗号化画像の H と S の分布は、原画像と比較して広範囲に分布していることから、色情報の偏りが低減されていることが確認できる。また、暗号化画像から、任意の 1 枚の画像を復元した際のヒストグラムを図 7 に、任意の 2 枚の画像を復元した際のヒストグラムを図 8 にそれぞれ示す。暗号化画像から任意の画像を復元した場合も、原画像と比較して、H と S が広範囲に分布していることがわかる。

〈4・2〉 エントロピーによる評価

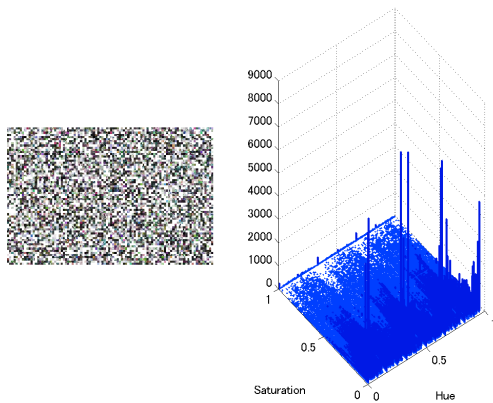
エントロピーについて評価をする。エントロピー $H(A)$ は、情報の無秩序さを表す尺度であり、ある事象系 A を $A = \{a_1, a_2, \dots, a_n\}$ とし、ある事象の生起確率 $p(\{a_i\})$ とした場合、

表 2 エントロピーの比較
Table 2. Comparison of entropies

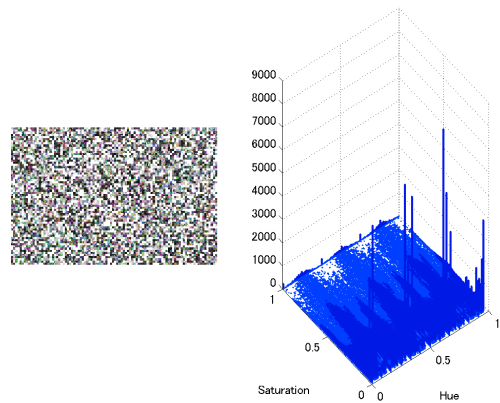
	原画像	従来法 [4]	提案法
画像 1	16.246	17.923	-
画像 2	14.287	16.222	-
画像 3	15.930	17.400	-
画像 4	11.912	14.492	-
結合画像	15.763	-	17.970

$$H(A) = - \sum_{i=1}^n p(a_i) \log_2 p(a_i) \quad (2)$$

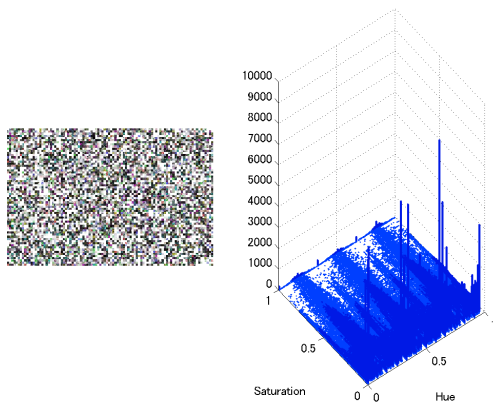
と表すことができる。エントロピーの値は、事象の生起確率の偏りが小さいほど大きく、偏りが大きいほど小さい値となる。表 2 に、図 5 の 4 枚の原画像、4 枚の原画像を結合した画像、従来法 [4] によって暗号化された 4 枚の個別画像、および、提案法により暗号化された結合画像の各エントロピーを比較した結果を示す。同表より、提案法のエントロピーの値が、従来法 [4] と原画像の値よりも高くなっており、色情報の偏りが小さくなっていることがわかる。また、暗号化画像から、任意の画像を抽出したときのエントロピーの値を表 3 に示す。同表より、各エントロピーの値が、表 2 の原画像より高くなっており、任意の画像を抽出した場合でも、色情報の偏りは、原画像と比べて



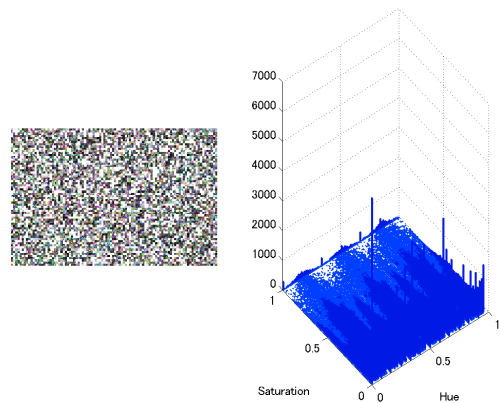
(a) 暗号化画像から画像 1 を復号した暗号化画像



(b) 暗号化画像から画像 2 を復号した暗号化画像



(c) 暗号化画像から画像 3 を復号した暗号化画像



(d) 暗号化画像から画像 4 を復号した暗号化画像

図 7 暗号化画像から任意の 1 枚の画像を復号したときのヒストグラムの比較

Fig. 7. Comparison of histograms of encrypted images after restoration of one arbitrary image

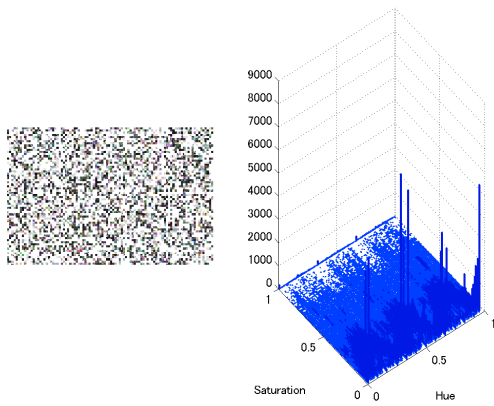
十分小さくなっていることがわかる。以上より、提案法による暗号化は、スクランブルの度合いが向上していることから、総当たり攻撃や JPS に対する耐性の観点からも有効であるといえる。

5. まとめ

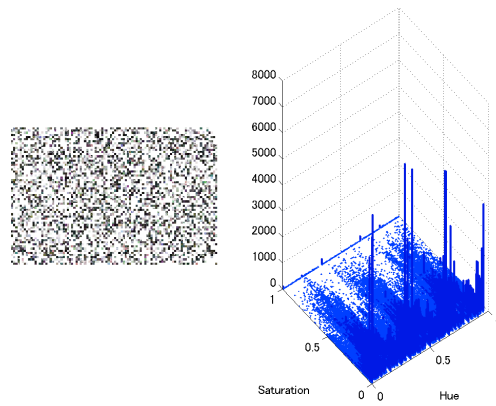
本稿では、ユーザ権限に応じたアクセス制御を可能とするブロックスクランブル暗号化法を提案した。提案法では、画像データベースの中から複数枚の画像を選択し、個別に暗号化を施した後で結合し、再度、全体のブロックの位置に対してスクランブル処理を施す。このとき、各画像のそれぞれのブロックが移動する位置を暗号鍵を用いて割り当てる。これにより、結合された暗号化画像から、任意の画像のみを、他の画像の暗号化を解除することなく取り出すことが可能となった。また、シミュレーションより、提案法によって生成された暗号化画像のスクランブルの度合いが、従来法よりも向上していることを確認した。

参考文献

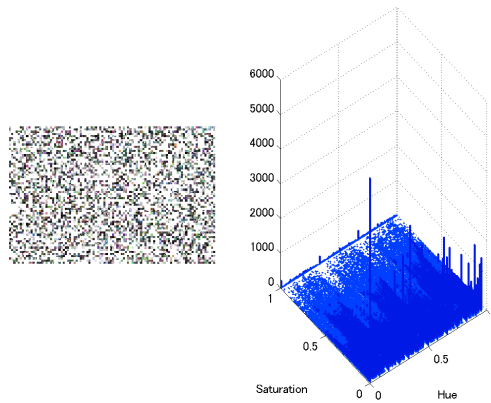
- (1) T.Chuman, K.Iida and H.Kiya: "Image Manipulation Analysis on Social Networking Service for Encryption-then-Compression Systems", Proc. IEICE Technical Report, Vol.117, No.201, pp.1-6 (2017-9) (in Japanese) 中満達也, 飯田健太, 貴家仁志: "Encryption-then-Compression システムのための SNS における画像加工解析", 信学技報, **117**, 201, pp.1-6 (2017-9)
- (2) K.G. Nimbokar, M.V, Sarode and M.N. Chonge: "A Survey based on Designing an Efficient Image Encryption-then-Compression System", Proc. IJCA National Level Technical Conference X-PLORE 2014, pp.6-8 (2014-5)
- (3) O.Watanabe, A.Uchida, T.Fukuhara and H.Kiya: "An Encryption-then-Compression System for JPEG 2000 Standard", Proc. IEEE ICASSP, No.IVMSP-L4.1, pp.1226-1230 (2015-4)
- (4) K.Kurihara, M.Kikuchi, S.Imaizumi, S.Shiota and H.Kiya: "An Encryption-then-Compression System for



(a) 暗号化画像から画像 1 と 2 を復号した暗号化画像



(b) 暗号化画像から画像 1 と 3 を復号した暗号化画像



(c) 暗号化画像から画像 1 と 4 を復号した暗号化画像

図 8 暗号化画像から任意の 2 枚の画像を復号したときのヒストグラムの比較

Fig. 8. Comparison of histograms of encrypted images after restoration of two arbitrary images

表 3 暗号化画像から任意の画像を復号したときのエントロピーの比較

Table 3. Comparison of entropies of encrypted images after restoration of arbitrary image/images

復元する画像	画像 1	画像 2	画像 3	画像 4	画像 1 と 2	画像 1 と 3	画像 1 と 4
エントロピーの値	17.155	17.862	17.434	18.381	16.706	16.058	17.562

JPEG/Motion JPEG Standard”, IEICE Trans. Fundamentals, Vol.E98-A, No.11, pp.2238-2245 (2015-11)

- (5) S.Imaizumi, T.Ogasawara and H.Kiya: “Block-Permutation-Based Encryption Scheme with Enhanced Color Scrambling”, Proc. Scandinavian Conference on Image Analysis, LNCS, Vol.10269, pp.562-573 (2017-6)
- (6) K.Kurihara, S.Imaizumi, S.Shiota and H.Kiya: “An Encryption-then-Compression System for Lossless Image Compression Standards”, IEICE Trans. Inf. & Sys., Vol.E100-D, No.1, pp.52-56 (2017-1)
- (7) D.Sholomon, O.E. David and N.S. Netanyahu: “An Automatic Solver for Very Large Jigsaw Puzzles Using Genetic Algorithms”, Genetic Programming and Evolvable Machines, Vol.17, No.3, pp.291-313 (2016-9)

- (8) T.Chuman, K.Kurihara and H.Kiya: “On The Security of Block Scrambling-based ETC System Against Jigsaw Puzzle Solver Attacks”, Proc. IEEE ICASSP, pp.2157-2161 (2017-3)
- (9) T.Ogasawara, S.Imaizumi and H.Kiya: “A Permutation-Based Image Encryption Scheme with Resistance against Some Attacks and Its Key Management”, Proc. IEICE Technical Report, Vol.116, No.501, pp.31-36 (2017-3) (in Japanese) 小笠原剛史, 今泉祥子, 貴家仁志, “攻撃耐性向上のためのブロックスクランブル暗号化法とその鍵管理”, 信学技報, **116**, 501, pp.31-36 (2017-3)
- (10) Available: <http://imagedatabase.cs.washington.edu/groundtruth>