

[ポスター講演] 階層的な復号を可能とするブロックスクランブル暗号化法

井澤 佑介[†] 今泉 祥子[†] 貴家 仁志^{††}

[†] 千葉大学 工学部 〒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: izawa@chiba-u.jp, imaizumi@chiba-u.jp, kiya@tmu.ac.jp

あらまし 本稿では、画像の特定領域のみを復号可能なブロックスクランブル暗号化法を提案する。提案法は、1枚の画像を複数領域に分割して暗号化処理を施す。これにより、暗号化された画像から特定の領域のみを、他の領域の暗号を解除することなく復号することができる。また、暗号化単位となるブロックのサイズを可変にすることにより、領域ごとの暗号化強度の制御が可能となる。

キーワード 画像暗号化, 階層性, 部分的復号, ブロック分割

A Block-Permutation-Based Image Encryption Allowing Hierarchical Decryption

Yusuke IZAWA[†], Shoko IMAIZUMI[†], and Hotoshi KIYA^{††}

[†] Faculty of Engineering, Chiba University

^{††} Faculty of System Design, Tokyo Metropolitan University

E-mail: izawa@chiba-u.jp, imaizumi@chiba-u.jp, kiya@tmu.ac.jp

Abstract This paper proposes a permutation-based image encryption scheme, which allows decrypting only a particular area in the encrypted image. We divide an image into multiple regions and configure the fixed-size blocks in each block. The initial encryption procedure is carried out within each region, and then the positional scrambling of the blocks is performed in the entire image. Consequently, the arbitrary region can be retrieved from the encrypted image without decrypting other regions. In addition, we can adequately control the encryption strength by using different block sizes.

Key words image encryption, hierarchy, partial decryption, block segmentation

1. ま え が き

近年、SNS やクラウドサービスが発達し、デジタル画像の共有や公開がますます増加している。これに伴い、画像の著作権、および、それに含まれるプライバシー情報の保護がより強く求められる。一方、画像解像度の増大により、画像は一般に、圧縮された形式で保存、伝送される。そのため、画像に対する暗号化の研究においては、暗号化の堅牢性と同時に、暗号化画像の圧縮効率を考慮することも重要となっている [1]。

現在、画像の提供者が、画像に暗号化を施した後で送信することにより、サービスプロバイダにセキュリティ上の問題が生じた場合にも画像の内容が保護される、Encryption-then-Compression (EtC) システムの研究が行われている [2-5]。この研究において、JPEG などの画像圧縮の国際標準方式に準拠した暗号化手法として、ブロックスクランブル暗号化法が提案されている [6-9]。ブロックスクランブル暗号化法は、画像全体

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、回転・反転、ネガポジ反転、色成分間スクランブルの四つの独立した処理を施すことで、暗号化画像を生成する。しかし、従来法は、画像全体に対する暗号鍵にもとづいて暗号化処理を施すため、暗号化画像から一部のみを復号することが困難である。

そこで、本研究では、画像の部分的な復号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。提案法は、はじめに、画像を複数領域に区分し、さらに各領域を一定サイズのブロックに分割する。次に、各領域において、ブロックの回転・反転、ネガポジ反転、色成分間スクランブルの三つの処理を施す。最後に、画像全体において、ブロック間の位置の入替えを行う。これにより、暗号化画像から特定領域のみを、他の領域の暗号化を解除することなく復号することが可能となる。また、提案法では、各領域に含まれる情報の重要度に応じて、ブロックサイズを設定することができる。これにより、圧縮効率の低下を抑制し、それぞれの領域に対して、柔軟な秘匿性を与えること

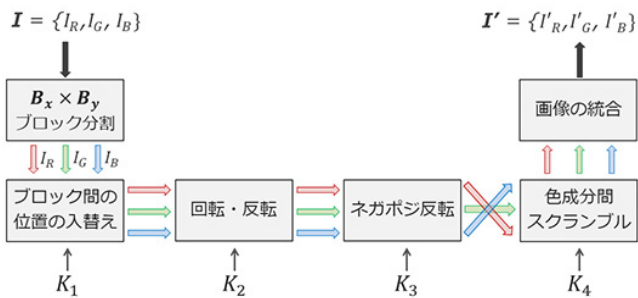


図 1: ブロックスクランブル暗号化法 [6] の処理手順

ができる。シミュレーションにより、提案法の暗号化処理と特定領域の復号処理において、それぞれ生成される画像の評価を行う。

2. 従来法 [6]

ここでは、従来のブロックスクランブル暗号化法 [6] について述べる。画像サイズ $M \times N$ 画素のカラー画像 $I = \{I_R, I_G, I_B\}$ に対する暗号化処理は図 1 の手順で施される。

- 手順 1: 原画像 I を $B_x \times B_y$ 画素のブロックに分割する。
- 手順 2: ブロック間の位置の入替えを行う。
- 手順 3: 回転・反転処理を施す。
- 手順 4: ネガポジ反転処理を施す。
- 手順 5: RGB の色成分間スクランブルを施す。
- 手順 6: ブロックを結合して暗号化画像 I' を生成する。

以下で四つの独立した暗号化処理について具体的に説明する。

- (1) ブロック間の位置の入替え
暗号鍵 K_1 に基づいて生成される疑似乱数に従って、ブロックの位置をランダムに置換する。
- (2) 回転・反転処理
暗号鍵 K_2 に基づいて生成される疑似乱数に従って、ブロックを $0^\circ, 90^\circ, 180^\circ, 270^\circ$ のいずれかの角度に回転、また、ブロックを垂直・水平方向にランダムに反転させる。
- (3) ネガポジ反転処理
暗号鍵 K_3 に基づいて生成される疑似乱数に従って、ブロックのネガポジ反転処理を施す。画素値 p の処理後の画素値 p' は次のように与えられる。

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

ここで、 $r(i)$ は i 番目のブロックに対する疑似乱数を示す。

- (4) 色成分間スクランブル
暗号鍵 K_4 に基づいて生成される疑似乱数に従って、表 1 に示すように RGB 成分の画素値を入れ替える。

なお、上記の四つの処理のうち、ブロック間の位置の入替え、

表 1: 色成分間スクランブルの例

疑似乱数	R	G	B
0	R	G	B
1	R	B	G
2	G	R	B
3	G	B	R
4	B	R	G
5	B	G	R

回転・反転、ネガポジ反転について、各処理を RGB 成分に対して同一、または独立に施すことを選択可能である。

このように、従来法は、画像を一定サイズのブロックに分割し、画像全体に対して共通の暗号鍵を用いて、ブロック単位の暗号化処理を行う。これにより、従来法は、すべての暗号化を解除して画像全体を復号することが必要であり、一部のみを復号することはできない。また、暗号化時のブロックサイズは、画像全体で一定であるため、プライバシーなどの重要情報が含まれていた場合、その領域に対してより小さいサイズのブロックを設定できるような柔軟性が考慮されていない。

3. 提案法

本章では、特定領域のみの復号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、図 2 に示すように、画像を複数の領域に区分した後、さらに各領域を分割してブロックを構成する。まず、領域ごとにブロックの回転・反転、ネガポジ反転、色成分間スクランブルを行い、ブロックを結合して暗号化領域を生成する。次に、すべての暗号化領域を同一サイズのブロックに再分割し、画像全体におけるブロック間の位置の入替えを行う。このとき、暗号鍵により、図 3 に示すようにそれぞれのブロックが移動する場所を指定する。これにより、画像の一部領域を復号するとき、該当領域のみを、他の領域の暗号を解除することなく復元することができる。提案法の暗号化処理手順、領域内のブロックサイズの制御、および、特定領域のみの復号処理手順について以下で説明する。

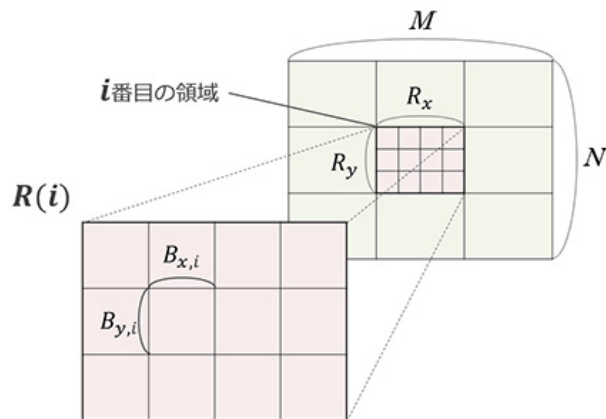


図 2: 提案法における領域・ブロック分割

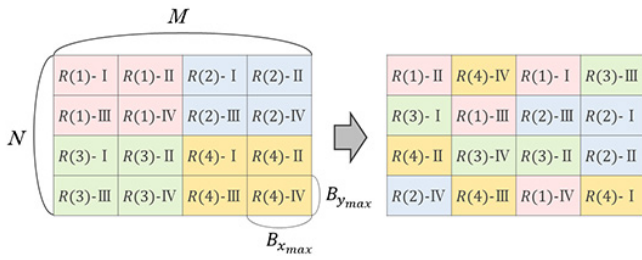


図 3: ブロックの移動位置の指定

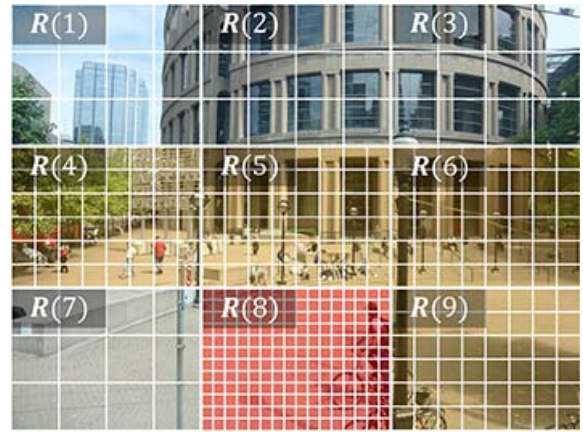


図 5: 各領域のブロック分割の例

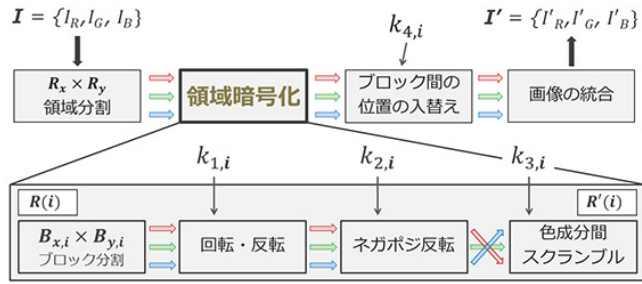


図 4: 提案法の暗号化手順

3.1 暗号化処理手順

暗号化処理は、図 4 の手順で施される。以下に、具体的な処理手順を述べる。

手順 1: 原画像 I を $R_x \times R_y$ 画素の N 個の領域に分割し、 i 番目 ($i=1,2,\dots,N$) の領域を $R(i)$ とする。

各領域 $R(i)$ について、

手順 2: $R(i)$ を $B_{x,i} \times B_{y,i}$ 画素のブロックに分割する。

手順 3: 暗号鍵 $k_{1,i}$ により、ブロックの回転・反転処理を施す。

手順 4: 暗号鍵 $k_{2,i}$ により、ネガポジ反転処理を施す。

手順 5: 暗号鍵 $k_{3,i}$ により、色成分間スクランブルを施す。

手順 6: ブロックを結合し、暗号化領域 $R'(i)$ を生成する。

すべての領域 $R(i)$ について手順 2~6 の操作を繰り返す。

手順 7: すべての暗号化領域を、ブロックの最大サイズ $B_{x,max} \times B_{y,max}$ 画素のブロックに再分割する。

手順 8: 図 3 のように、暗号鍵 $k_{4,i}$ を用いて、画像全体での位置を指定し、ブロックの入替え処理を施す。

手順 9: ブロックを結合して暗号化画像 I' を生成する。

3.2 領域内のブロックサイズの制御

提案法では、領域 $R(i)$ をブロック分割するとき、領域ごとに異なるブロックサイズ $B_{x,i} \times B_{y,i}$ 画素を設定することが可能である。これにより、各領域に対して柔軟な秘匿性を与えることができる。ブロックサイズの制御について、図 5 の例を用いて具体的に説明する。

はじめに、画像全体を 9 個の領域に分割する。次に、これらの領域を、重要情報が含まれる領域 (領域 I)、重要ではないが画像の特徴を表している領域 (領域 II)、および、その他の一般領域 (領域 III) に区分する。これに従い、 $R(8)$ に領域 I、 $R(4)$ 、 $R(5)$ 、 $R(6)$ 、 $R(9)$ に領域 II、 $R(1)$ 、 $R(2)$ 、 $R(3)$ 、 $R(7)$ に領域

III を割り当てる。ここで、領域 I を $B_{x,i} \times B_{y,i}$ 画素のブロックに分割すると仮定すると、領域 II は $2B_{x,i} \times 2B_{y,i}$ 画素のブロックに、領域 III は $4B_{x,i} \times 4B_{y,i}$ 画素のブロックにそれぞれ分割される。

これにより、各領域に対して柔軟な秘匿性を与えるとともに、圧縮効率の低下を抑制する。

3.3 特定領域の復号処理手順

特定領域の復号処理は、図 6 に示すように、暗号化画像 I' において、復号対象となる領域 $R(a)$ を指定し、その領域に対してのみ復号処理を行う。復号手順は次のとおりである。

手順 1: 暗号化画像 I' を、暗号化ブロックの最大サイズ $B_{x,max} \times B_{y,max}$ 画素のブロックに分割する。

手順 2: 暗号鍵 $k_{4,a}$ を用いて、領域 $R(a)$ を構成するブロックのみを抽出する。

手順 3: 抽出されたブロックを結合して暗号化領域 $R'(a)$ を生成する。

手順 4: 暗号化領域 $R'(a)$ を $B_{x,a} \times B_{y,a}$ 画素のブロックに再分割する。

手順 5: 暗号鍵 $k_{3,a}$ により、色成分間スクランブルの復号処理を施す。

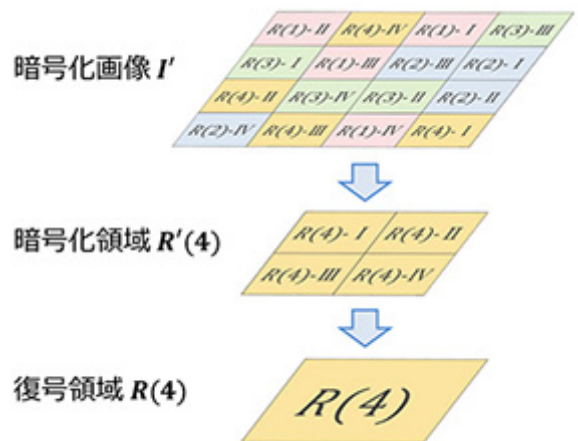


図 6: 領域 $R(4)$ のみ復号する場合の復号手法

表 2: ブロックサイズ別の領域数とブロック数

ブロックサイズ	提案法 (単一)	提案法 (複合)	従来法 [6]
96×96 画素	0 領域	1 領域	-
192×192 画素	9 領域	4 領域	全ブロック
384×384 画素	0 領域	4 領域	-
総ブロック数: 432 個			

手順 6: 暗号鍵 $k_{2,a}$ により, ネガポジ反転の復号処理を施す.

手順 7: 暗号鍵 $k_{1,a}$ により, 回転・反転の復号処理を施す.

手順 8: ブロックを結合して復号領域 $R(a)$ を取得する.

4. シミュレーション

ここでは, 提案法と従来法 [6] による, それぞれの暗号化画像の視認性と, 圧縮効率の評価を行う. 提案法は, 全領域で同一のブロックサイズを設定する単一ブロック暗号化と, 各領域で異なるブロックサイズを設定する複合ブロック暗号化に分けられる. これにより, 従来法 [6], 従来法と同一のブロック分割を施した単一ブロック暗号化, および, 3 種類のサイズを有する複合ブロック暗号化の三つの手法について評価を行う.

シミュレーションには, 図 7 を例とする, 6 種類の IHC 標準画像 (4,608×3,456 画素) [10] を使用した. また, 各画像につき 20 回の試行, すなわち, 20 枚の暗号化画像を生成し, JPEG-LS [11] を用いたロスレス圧縮を施した. なお, 本シミュレーションでは, すべての暗号化において, RGB 成分をそれぞれ独立に処理している.

各手法における, 画像または領域ごとのブロックサイズと総ブロック数を表 2 に示す. このとき, 提案法の単一ブロック暗号化手法と複合ブロック暗号化手法における領域・ブロック分割の構成例を図 8, 9 にそれぞれ示す.

4.1 視認性の評価

単一ブロック暗号化手法, 複合ブロック暗号化手法, および, 従来法 [6] により生成された暗号化画像を図 10~12 にそれぞれ示す.

図 10, 12 より, 単一ブロック暗号化手法による暗号化画像は, 従来法による暗号化画像と同一のブロックサイズで構成されており, スクランブルの程度も同様であることがわかる. しかしながら, 従来法では, 暗号化画像の一部のみを復号することができない.

一方, 複合ブロック暗号化手法による暗号化画像を図 11 に示す. 同図より, 暗号化画像は複数のブロックサイズで構成されていることがわかる. この手法では, 領域ごとに異なるブロックサイズを設定し, 秘匿性を制御することができる.

また, 図 13 は, 図 10 から一部の復号対象領域のブロックを抽出して, その他の領域のブロックから構成される暗号化画像を示している. 同図より, 一部のブロックが抽出された後も, 単一ブロック暗号化画像の秘匿性に大きな変化はないことがわかる.

表 3: JPEG-LS による暗号化画像の圧縮効率の比較 [bpp]

	提案法 (単一)	提案法 (複合)	従来法 [6]
Flower garden	11.67	11.66	11.67
Street view	9.96	9.75	9.96
Library	9.73	9.72	9.76
Port view	10.05	10.03	10.05
Bus	9.87	9.81	9.81
Flower pot	11.28	11.40	11.44

4.2 圧縮特性の評価

単一ブロック暗号化手法, 複合ブロック暗号化手法, および, 従来法 [6] により生成された暗号化画像 (図 10~12) に対して, JPEG-LS を用いてロスレス圧縮を施し, 圧縮効率を比較する. 表 3 に圧縮後の各ビットレート [bpp] を示す. なお, ビットレートは次式で与えられる.

$$\text{ビットレート (bpp)} = \frac{\text{画像のデータ量}}{\text{画像の画素数 (M} \times \text{N)}} \quad (2)$$

同表より, 提案法におけるいずれの手法についても, 従来法と比較して, 同等の圧縮効率を保持していることがわかる.

5. まとめ

本稿では, 画像の特定領域のみの復号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, まず, 画像を複数の領域に区分し, さらに各領域を一定サイズのブロックに分割する. 次に, 領域ごとにブロック単位の暗号化処理を施して暗号化領域を生成する. さらに, すべての暗号化領域を同一ブロックサイズに再分割し, 画像全体に対してブロック間の位置の入替え処理を施す. このとき, 暗号鍵を用いて, 各領域のブロックがどの位置に移動するかをあらかじめ割り当てる. これにより, 暗号化画像から, 一部の領域のみを, 他のブロックの暗号化を解除することなく復号可能となった. また, 提案法では, 領域ごとに異なるブロックサイズを設定することで, 秘匿性の制御を行うことができる. シミュレーションにより, 提案法によって生成される暗号化画像は, 従来法と比較して, 視認性と JPEG-LS による圧縮効率の観点から, 同等に維持できることを確認した.

文 献

- [1] 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, vol.117, no.201, pp.1-6, 2017.
- [2] M. Kumar and A. Vaish, “An Efficient Encryption-then-Compression Technique for Encrypted Images Using SVD,” Digital Signal Processing, vol.60, pp.81-89, 2017.
- [3] W. Liu, W. Dong, and Q. Yao, “Efficient Compression of Encrypted Grayscale Images,” IEEE Trans. Image Process., vol.19, no.4, pp.1097-1102, 2010.
- [4] J. Zhou, X. Liu, O.C. Au, and Y.Y. Tang, “Designing an Efficient Image Encryption-then-Compression System via Prediction Error Clustering and Random Permutation,” IEEE Trans. Inf. Forensics Secur., vol.9, no.1, pp.39-50, 2014.
- [5] K.G. Nimbokar, M.V. Sarode, and M.M. Ghonge, “A Survey Based on Designing an Efficient Image Encryption-then-Compression System,” in Proc. on IJCA National Level Technical Conference X-PLORE 2014, pp.6-8, 2014.



(a) Street view

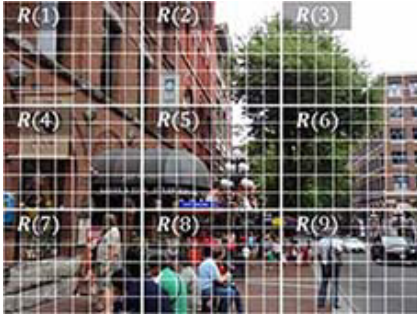


(b) Library

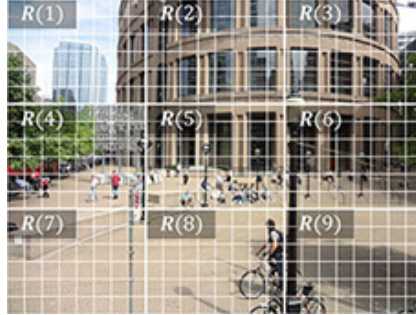


(c) Bus

図 7: 原画像 [10]



(a) Street view

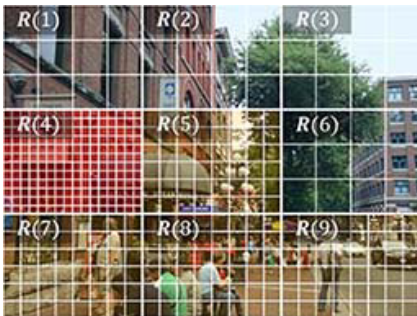


(b) Library

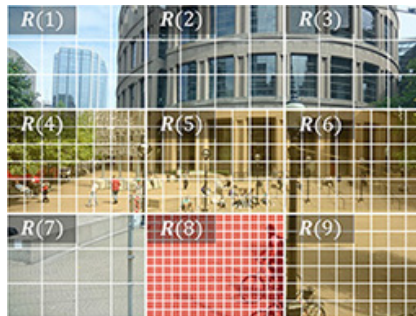


(c) Bus

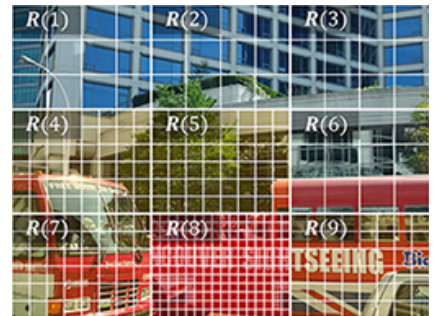
図 8: 単一ブロック暗号化における領域とブロックの構成例



(a) Street view



(b) Library



(c) Bus

$$B_{x,i} \times B_{y,i} = \begin{cases} 96 \times 96 \text{ 画素} & (i = 4) \\ 192 \times 192 \text{ 画素} & (i = 5, 7, 8, 9) \\ 384 \times 384 \text{ 画素} & (i = 1, 2, 3, 6) \end{cases}$$

$$B_{x,i} \times B_{y,i} = \begin{cases} 96 \times 96 \text{ 画素} & (i = 8) \\ 192 \times 192 \text{ 画素} & (i = 4, 5, 6, 9) \\ 384 \times 384 \text{ 画素} & (i = 1, 2, 3, 7) \end{cases}$$

$$B_{x,i} \times B_{y,i} = \begin{cases} 96 \times 96 \text{ 画素} & (i = 8) \\ 192 \times 192 \text{ 画素} & (i = 4, 5, 7, 9) \\ 384 \times 384 \text{ 画素} & (i = 1, 2, 3, 6) \end{cases}$$

図 9: 複合ブロック暗号化における領域とブロックの構成例

[6] K. Kurihara, M. Kikuchi, S. Imaizumi, S. Shiota, and H. Kiya, "An Encryption-then-Compression System for JPEG/Motion JPEG Standard," IEICE Trans. Fundamentals, vol.E98-A, no.11, pp.2238-2245, 2015.

[7] O. Watanabe, A. Uchida, T. Fukuhara, and H. Kiya, "An Encryption-then-Compression System for JPEG 2000 Standard," in Proc. on IEEE ICASSP, pp.1226-1230, 2015.

[8] K. Kurihara, S. Imaizumi, S. Shiota, and H. Kiya, "An Encryption-then-Compression System for Lossless Image Compression Standards," IEICE Trans. Inf. & Syst., vol.E100-D, no.1, pp.52-56, 2017.

[9] S. Imaizumi, T. Ogasawara, and H. Kiya, "Block-Permutation-Based Encryption Scheme with Enhanced Color Scrambling," in Proc. on Scandinavian Conference on Image Analysis, LNCS, vol.10269, pp.562-573, 2017.

[10] [Online] Available: <http://www.ieice.org/iss/emm/ihc/image/image.php>

[11] M.J. Weinberger, G. Seroussi, and G. Sapiro, "The LOCO-I Lossless Image Compression Algorithm: Principles and Standardization into JPEG-LS," IEEE Trans. Image Process., vol.9, no.8, pp.1309-1324, 2000.

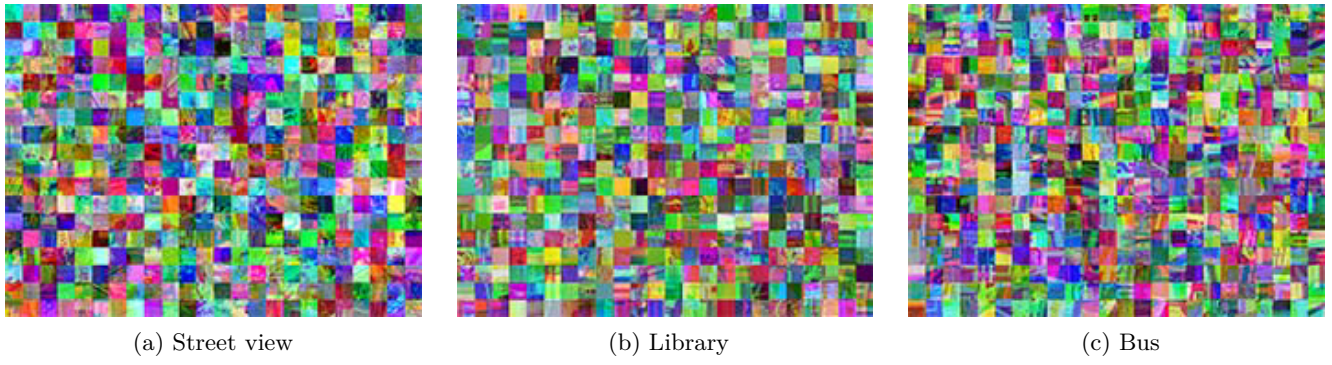


図 10: 単一ブロック暗号化手法による暗号化画像

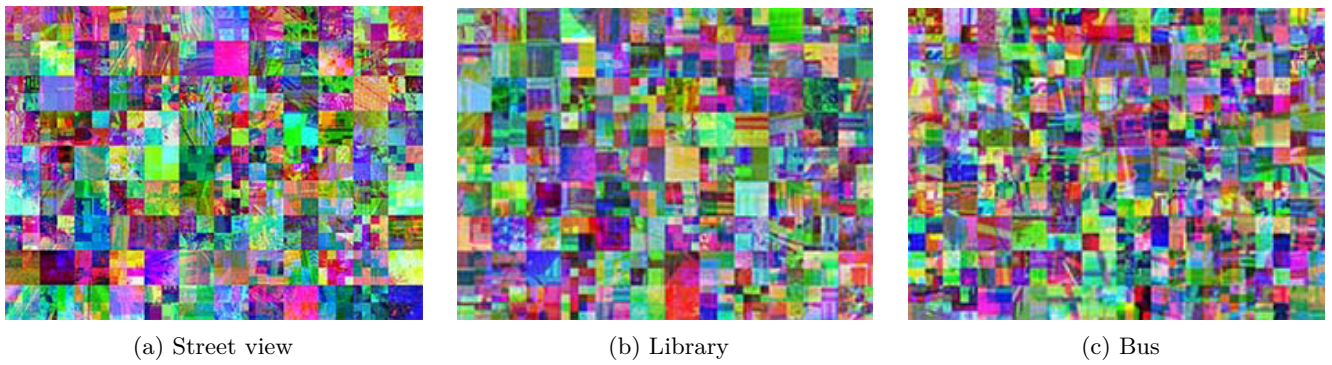


図 11: 複合ブロック暗号化手法による暗号化画像

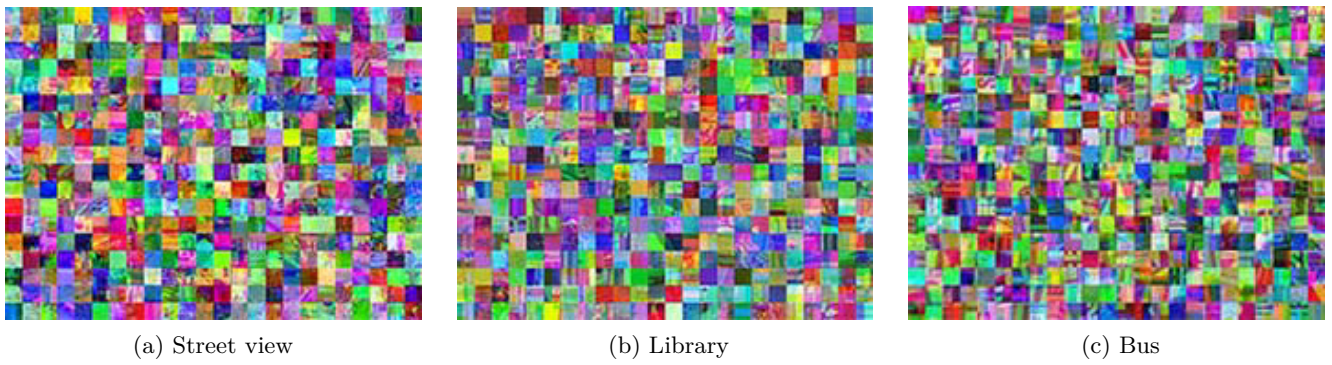


図 12: 従来法 [6] による暗号化画像

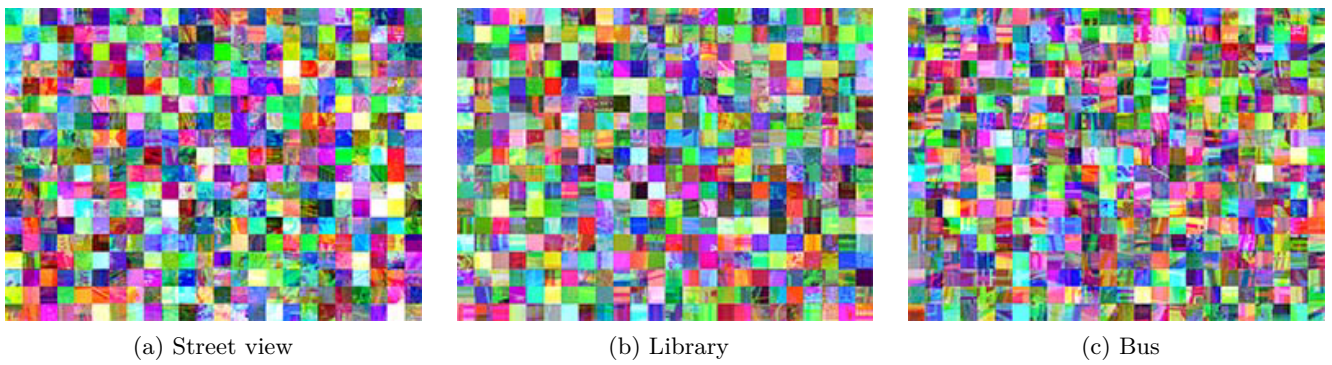


図 13: 図 10 から領域 $R(5)$ のブロックを抽出した後の暗号化画像