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

信学技報
TECHNICAL REPORT OF IEICE.

ジグソーパズル解法に対するブロックスクランブル画像暗号化法の評価

中満　達也† 　栗原　健太† 　貴家　仁志†

† 首都大学東京大学院 システムデザイン研究科　〒 191–0065 東京都日野市旭ヶ丘 6–6
E-mail: †{chuman-tatsuya,kurihara-kenta}@ed.tmu.ac.jp, ††kiya@tmu.ac.jp

あらまし　ブロックスクランブル画像暗号化法は，圧縮可能であること，雑音に対してロバストであるなど，DES や AES に代表される暗号化法にはない優れた特徴を持つ．一方，その安全性に対しては他の暗号化法とは異なる観点から考察する必要がある．本稿では，ジグソーパズル解法に基づく攻撃に対して，ブロックスクランブル画像暗号化法の安全性を検討する．従来，ブロックスクランブル画像暗号化法に対して，総当たり攻撃の仮定の下で，総当り数と鍵空間の大きさの観点から安全性が議論されてきた．しかし，ブロックベースで暗号化が行われているため，ブロック内の相関は暗号前とほぼ等しく，その相関を糸口にする攻撃が想定される．本稿では, ブロックをパズルのピースに例え，安全性をジグソーパズル解法から考察する．また，JPEG 圧縮され量子化雑音が重複した暗号化画像に対して，攻撃耐性と雑音の関係についても実験的に評価する．
キーワード　ETC システム，画像暗号化，JPEG，ジグソーパズル解法

Safety Evaluation for Permutation-Based Image Encryption Schemes against Jigsaw Puzzle Solvers

Tatsuya CHUMAN†, Kenta KURIHARA†, and Hitoshi KIYA†

† Graduate School of System Design, Tokyo Metropolitan University　6–6 Asahigaoka, Hino-shi, Tokyo, 191–0065 Japan
E-mail: †{chuman-tatsuya,kurihara-kenta}@ed.tmu.ac.jp, ††kiya@tmu.ac.jp

Abstract　Block-based scrambled image encryption schemes have superior features that are compressible and against to noises to number theory-based encryption methods such as RSA and DES. On the other hand, it needs to be considered from different viewpoints from conventional ones. In this paper, we discuss the security of the block-based scrambled schemes against jigsaw-puzzle solvers. Block-based scrambled image encryption schemes are conventionally verified secure because the key space is large enough to be against a brute-force attack. The encrypted image has the same each correlation blocks between the original ones despite the encryption. We compare divided blocks to jigsaw-puzzle pieces to verify the security of permutation-based image encryption schemes. Moreover, we conduct experiments with quantization noises image to evaluate the relation between security and noises.
Key words　ETC syestem，JPEG，image encryption，jigsaw puzzle

1. ま え が き

近年，カメラやビデオの普及によって膨大な画像データが日々生成されると同時に，画像は SNS やインターネット，クラウドコンピューティングの中心コンテンツとして不可欠なものとなっている．一方，画像は多くの場合で監視カメラ映像に代表されるように個人情報を含み，また著作物でもある．さらに，データ量の膨大さから，データ圧縮が施された形式で保存や伝送されることが一般的に行われている．このような背景から，セキュアに画像検索や画像同定を行う研究や，暗号化技術と画像圧縮技術との融合研究に関する研究が盛んに行われている [1,2].

安全性が確立されないチャネル上で，コンテンツを安全に通信するために，一般に DES や AES などの暗号化法が適用される．一方，これらの暗号化法が持つ制約を緩和するために，近年画像視覚情報を認識困難にする暗号化（視覚暗号化，知覚暗号化と呼ばれる）が数多く研究されている．それらの目的は，暗号化に伴う計算量の低減，雑音やデータ誤りに対するロバストの向上，暗号化後も画像データを維持することによってデータを安全に保護すると同時に既存システムとの互換性の維持，

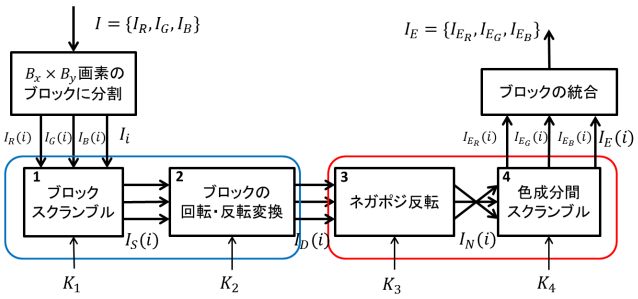


図 1　ブロックスクランブル画像暗号化の手順

暗号化の後にデータ圧縮を可能にし暗号化と圧縮の処理手順の自由度向上などがある [3]．また既存の AES などと組み合わせで使用することができ，互いの欠点を補う使用法も可能である．本稿では，知覚暗号化の一つである，画像をブロック分割し，そのブロック間の想定的関係とブロック内の操作によって暗号化を施す，ブロックスクランブル画像暗号法に対して安全性の考察を行う．

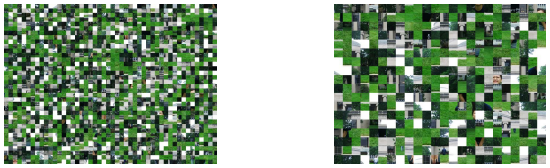
ブロックスクランブル画像暗号法は，JPEG などの画像圧縮の国際標準規格に適用可能な画像暗号化法として提案された [4–7]．従来その安全性は，総当り攻撃を想定して鍵空間の広さに基づき議論されている [4,5]．また，総当り攻撃の高速化という観点からも研究されており，総ブロック数が重要なパラメータとなっている [8–10]．一方，暗号化とは独立にジグゾーパズル解法という分野があり，大きなブロック数を持つパズルの復元報告がある [11–18]．本稿では，暗号化のためブロックをパズルのピースに見立て，ジグゾーパズル解法をブロックスクランブル暗号化の攻撃として想定し，暗号化の安全性を評価する．

本稿では，まずブロックスクランブル暗号化法を簡単に要約する．次に，最先端のジグソーパズル解法を紹介し，それに基づく攻撃を提案する．最後に代表的ジグソーパズル解法による攻撃を暗号化画像に適用し，暗号化法の安全性を評価する．総ブロック数，ブロックサイズ，暗号化手法をパラメータとした場合は，十分な鍵空間を持つとされた暗号化画像でも，最先端のジグソーパズル解法によって復元されることが確認された．一方，ブロックサイズや暗号化法の適切な選択が，画像の復元を困難にすることが示される．さらに，JPEG 圧縮を暗号化画像に適用し，量子化雑音と復元の困難性の関係についても考察している．

2. 準　　備

2.1 ブロックスクランブル画像暗号化法

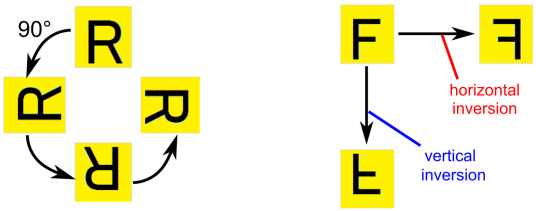
ここでは，画像の視認性を困難にして，かつ圧縮可能な暗号化画像を生成可能なブロックスクランブル画像暗号化法を要約する．この暗号化法は画像通信において，送信者自身が画像に暗号化を施し，第三者であるネットワークプロバイダが圧縮を行う ETC(Encryption-then-Compression) システムの実現のために提案された [4–7]．送信者自身が暗号化を行うことで，ネットワークプロバイダにデータを開示する必要がないため，機密性の保持が可能となる．



(a) スクランブル画像
($L = 864$, $B_x \times B_y = 14$)

(b) スクランブル画像
($L = 432$, $B_x \times B_y = 28$)

図 2　ブロックスクランブルされた画像



(a) ブロックの回転

(b) ブロックの反転

図 3　ブロックの回転，反転のイメージ

このブロックスクランブル画像暗号化法は図 1 に示すように，4 つのステップにより実行される．サイズ $M \times N$ のカラー画像 $I = \{I_R, I_G, I_B\}$ の，RGB 成分は共通なサイズ $B_x \times B_y$ のブロックに分割され，ブロックベースで処理が施される．このブロックを単位として暗号化を行った場合，総ブロック数 L は

$$L = \lfloor \frac{M}{B_x} \rfloor \times \lfloor \frac{N}{B_y} \rfloor \tag{1}$$

と与えられる．ここで，$\lfloor\rfloor$ は小数点以下での切り捨て処理を意味する．各ステップの詳細を以下に示す．

A. ブロックスクランブル

ブロックスクランブルは，分割されたブロック $I(i) = \{I_R(i), I_G(i), I_B(i)\}$ を鍵 K_1 によって生成される乱数を用いてランダムに置換する．ただし，RGB の各ブロック $I_R(i), I_G(i), I_B(i)$ は共通の鍵を使用して置換されるものとする．ブロック毎の位置関係をスクランブルすることで，元画像の視認性を制御することを可能とする．ここで，ブロックサイズ $B_x \times B_y$ の違いによる視認性を図 2 に例示する．図 2 からわかるように，ブロックサイズを小さくすることで元画像の特定が困難になり，秘匿性が向上することがわかる．また，総ブロック数 L が増加する．

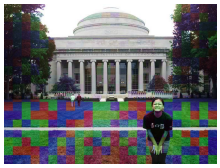
B. 回転，反転変換

ブロックの回転変換は，ブロックの位置関係を変化させずに，図 3 に示すように，ブロックを 0°，90°，180°，270° のいずれかの角度だけ RGB 成分を共通に回転する．回転変換を行う場合，正方形ブロックを扱う必要があるので，ブロックサイズ $B_x \times B_y$ がブロックサイズ $B_x = B_y$ の場合のみを考えることとする．ブロックの反転変換は回転変換と同様に位置関係を変化させずに，図 3 に示すように，RGB 成分を共通にブロックを水平・垂直方向に鍵 K_2 によってランダムで反転させる．反転を行わない，もしくは水平・垂直方向どちらにも反転するといったことも起こり得る．

C. ネガポジ反転

i 番目のブロック $I_D(i) = \{I_{D_R}(i), I_{D_G}(i), I_{D_B}(i)\}$ は画素の乱数に基づき，RGB 成分共通，かつブロック単位でネガポ

(a) ネガポジ反転



(b) 色成分間スクランブル

図 4　色変換によるブロックスクランブル画像暗号化
($L = 432$, $B_x \times B_y = 28$)

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

ジ反転が選択される．ネガポジ反転を施した画像を図 4(a) に示す．ブロック内の画素を p，鍵 K_3 による乱数を $r(i)$ としたとき，次式によりブロックにネガポジ反転を行う．

$$\begin{cases} p' = p & (r(i) = 0) \\ p = 255 - p & (r(i) = 1) \end{cases} \tag{2}$$

RGB 成分にブロックスクランブル，回転，反転変換を行った場合，RGB 成分の各ヒストグラムは元画像と同一であるが，ネガポジ反転を施すことによって，ヒストグラムが異なるので秘匿性を増すことができる．

D. 色成分間スクランブル

色成分間スクランブルは，ブロックごとに RGB 成分間の画素値を入れ替える．ブロックごとに生成した乱数を表 1 の成分間の対応に従い色成分間スクランブルを鍵 K_4 の制御によって施す．色成分間スクランブルを施した画像を図 4(b) に示す．

2.2　鍵空間による安全性評価

ここでは，鍵空間の観点からブロックスクランブル画像暗号化法の安全性について要約する．ブロックスクランブル画像暗号化法は，元画像をブロックに分割してブロックベースの暗号化を施しているため，ブロックの総数 L が鍵空間に関係するパラメータである．すべての通りの鍵を用いて総当り攻撃が行われる場合を想定し，ブロックスクランブル画像暗号化法の評価が行われてきた．

ブロックスクランブルで暗号化を施す場合，ブロックの置換の総数がブロックスクランブルにおける鍵空間の大きさ N_B となる．これは総ブロック数 L を用いて $L!$ と表すことができるため，

$$N_B = L! \tag{3}$$

となる．サイズ 672 × 504 の画像をサイズ 28 × 28 のブロックに分割した場合を考える．式 (1) より，総ブロック数 L は $\lfloor 672/28 \rfloor \times \lfloor 504/28 \rfloor = 432$ となるため，鍵空間の大きさは 432! となる．$2^{256} < 432!$ であることから，256 ビットの鍵を使用する暗号よりも大きい鍵空間を持つことがわかる．

ブロックの回転変換を施す場合，各ブロックの回転方向は，回転しない場合を含む 4 通りから選ぶことができる．また，ブロックの反転変換においても，各ブロックにつき水平・垂直方向それぞれに反転するか選ぶことができる．回転変換，反転変換をそれぞれ施した場合の鍵空間の大きさを N_R，N_I とすると，

$$N_R = 4^L,\ N_I = 4^L \tag{4}$$

となる，回転，反転変換を両方施した場合の鍵空間の大きさを N_D とすると，270°回転したブロックと水平・垂直方向に反転したブロックは等しいので

$$N_D = 8^L \tag{5}$$

となる．ネガポジ反転を施した場合，RGB 成分共通，かつブロック単位でネガポジ反転を行うので，鍵空間の大きさを N_N とすると，

$$N_N = 2^L \tag{6}$$

となる．同様に色成分間スクランブルを施した場合は，表 1 から分かるように 6 通りの RGB 成分間の入れ替えが考えられるので，鍵空間の大きさを N_E とすると，

$$N_E = 6^L \tag{7}$$

となる．上記の暗号化法はそれぞれ独立な処理であることから，組み合わせて用いた場合に生成され得る暗号化画像の総数は，各暗号化により生成され得る暗号化画像の総数の積で表される．すなわち，暗号化画像の総数 N_A は，

$$N_A = L! \cdot 8^L \cdot 2^L \cdot 6^L \tag{8}$$

により計算されることとなる．サイズ 672 × 504 の画像をサイズ 28 × 28 のブロックに分割し全ての暗号化を施した場合，総ブロック数 $L = 432$ なので，暗号化画像は $N_A = 432! \times 8^{432} \times 2^{432} \times 6^{432}$ の鍵空間を有する．$2^{256} \ll N_A$ であるから，鍵空間の観点からすると総当り攻撃に対しては安全であると言える．

表 2　ジグソーパズル解法の分類と成果 (✓:ピースの回転を考慮)

組み立て手法	著者	回転	発行年	ピース数
局所探索	Pomeranz [12]		2011	3300
	Gallagher [14]	✓	2012	9600
	Son [15]	✓	2014	9801
大域探索	Cho [11]		2010	432
	Andalo [13]		2012	3300
	Sholomon [16]	✓	2014	22755
	Sholomon [18]		2016	30745
ハイブリッド探索	Rui [17]	✓	2015	3300

3.　ジグソーパズル解法による攻撃

ジグソーパズル解法では，ジグソーパズルのピース間の相関を利用し，パズルの組み立てを行う．ブロックスクランブル画像暗号化はブロックベースで暗号化が行われるため，ジグソーパズルのピースを画像のブロック $B_x \times B_y$ として例えることができる．そのため，画像の暗号化にブロックスクランブル画像暗号化法が用いられていた場合，ジグソーパズル解法に基づく攻撃が想定される．

3.1　ジグソーパズル解法の従来研究

ジグソーパズル解法では，初期状態から局所最適解を見つけ

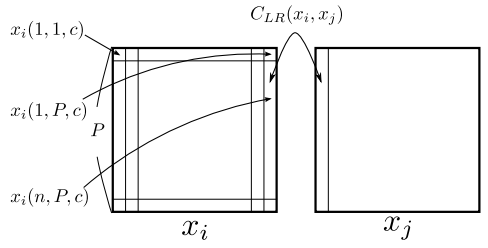


図 5　ピース x_i, x_j の位置関係と適応度 $C_{LR}(x_i, x_j)$

徐々にパズルを組み立てていく局所探索（greedy method）と，予めパズルを組み立てておき，直接大域最適解を求める大域探索（global method），局所探索と大域探索を組み合わせたハイブリッド探索（hybrid method）の 3 種類に分類される [17]．表 2 に代表的なジグソーパズル解法を示す．大域探索の例としては，遺伝的アルゴリズムを応用してジグソーパズルを組み立てる解法 [18] が挙げられ，30745 ピースからなる巨大ジグソーパズルを元画像と全て同じ位置に復元することに成功している．また，2012 年に初めてピースの位置情報に加えて方向情報 (回転) が不明のジグソーパズル組み立てに成功している [14]．以上のように鍵空間の観点からすると，十分な広さのピース数を持つ画像に対しても，ジグソーパズル解法はすでに復元に成功している．

3.2　MGC 解法

ジグソーパズル解法は最初にピース間の適応度（compatibility）を求め，求めた適応度を元にジグソーパズルを組み立てていく手法が主流である．代表的な適応度の計算に，テンプレートマッチングで用いられている SSD(Sum of Squared Difference) に基づく RGB SSD がある．RGB SSD は隣接している 2 つのピースの画素の差を RGB 成分ごとに求め，これらの二乗を足し合わせた値を適応度としている．RGB 成分間の差の二乗を全て等しい重みで和をとっているので，適切なピースの組み合わせを見つけるのが困難である．そこで，RGB 成分毎の重みを考慮する計算方法である MGC(Mahalanobis Gradient Compatibility) が提案された [14]．MGC は局所探索だけでなく，ハイブリッド探索でピース間の適応度を求める際にも使用され，多くの論文から有用性が確認されている [15,17]．以上の理由から，本実験では MGC に基づく局所探索法を例にして，ブロックスクランブル暗号化画像の安全性を考察する．以下に適応度を求め，パズルの組み立てを行う手法を簡単に要約する．

総ピース数を L，ブロックスクランブル画像暗号化が施された画像のピースを $x_i (i = 1, 2, \ldots, L)$ とする．ただし，回転変換が行われたピースからジグソーパズル組み立てを行うので，ピースサイズを $P \times P$ の正方形ピースとする．

(1) ピース間の適応度計算

MGC を用いて i 番目のピース x_i の右側と，j 番目のピース x_j の左側の適応度 $C_{LR}(x_i, x_j)$ を求める場合を考える (図 5 参照)．

ピース x_i の画素値を $x_i(n, m, c)$,$n, m \in \{1, 2, \ldots, P\}$,$c \in \{R, G, B\}$ とすると，変数 n を用いて右端の画素は $x_i(n, P, c)$ と表すことができる．ピース x_i の各 R,G,B 成分での右側の勾配 $G_{iL}(n, c)$ を次式とする．

$$G_{iL}(n, c) = x_i(n, P, c) - x_i(n, P-1, c) \tag{9}$$

また，その勾配の平均 $\mu_{iL}(c)$ を，

$$\mu_{iL}(c) = \frac{1}{P} \sum_{n=1}^{P} G_{iL}(n, c) \tag{10}$$

と与える．さらに x_i の右側と x_j の左側の勾配 $G_{ijLR}(n, c)$ を，

$$G_{ijLR}(n, c) = x_j(n, 1, c) - x_i(n, P, c) \tag{11}$$

と表す．次に，これらの R,G,B 成分を要素とするベクトル $\boldsymbol{G_{ijLR}}(n)$ を次式により定義する．

$$\boldsymbol{G_{ijLR}}(n) = [G_{ijLR}(n, R) - \mu_{iL}(R), \\ G_{ijLR}(n, G) - \mu_{iL}(G), G_{ijLR}(n, B) - \mu_{iL}(B)]^{\mathrm{T}} \tag{12}$$

式 (12) から，次に x_i から x_j に対する部分適応度 $D_{LR}(x_i, x_j)$ が定義される．

$$D_{LR}(x_i, x_j) = \sum_{n=1}^{P} \boldsymbol{G_{ijLR}}(n)^{\mathrm{T}} \boldsymbol{S_{iL}^{-1}} \boldsymbol{G_{ijLR}}(n) \tag{13}$$

ここで，$\boldsymbol{S_{iL}}$ は式 (9) から求めた各 R,G,B 成分の勾配 G_{iL} の 3×3 の共分散行列である．式 (13) の x_i から x_j に対応する部分適応度 $D_{LR}(x_i, x_j)$ と同様に，x_j から x_i に対する部分適応度 $D_{RL}(x_j, x_i)$ を計算し，x_i と x_j の適応度 $C_{RL}(x_i, x_j)$ を以下のように求める．

$$C_{LR}(x_i, x_j) = D_{LR}(x_i, x_j) + D_{RL}(x_j, x_i) \tag{14}$$

上記の手順にしたがい，全てのピース間の適応度を求める．したがって，ブロックスクランブルのみが施された暗号化画像では $2L \times (L-1)$ 回の適応度計算が必要となる．一方，ブロックスクランブルに加え回転変換が施された場合は $8L \times (L-1)$ 回の適応度計算が必要となる．

(2) 適応度に基づくピースの組み立て

求めた適応度を元に最小全域木（Minimum Spanning Tree）を利用し，ジグソーパズルを組み立てる．最小全域木を求めるアルゴリズムとして，制限付きのクラスカル法を利用する [19]．単純なクラスカル法は一般に適応度（重み）が最小の辺が選択されるので，ジグソーパズルの組み立てに応用した場合，ピース間で重複が起こる可能性がある．一方，制限付きクラスカル法は，制限を付けることで，このピース間で重複が起こる問題を解決している．仮に木構造による組み立てで元画像のサイズ $M \times N$ に収まらなかった場合，外側にあるピースはトリミングが行われる．トリミングが行われたピースをサイズ $M \times N$ 内の空いているピースに当てはめることで，ジグソーパズル組み立てが完成する．また，複数のピースにトリミングが行われた場合，全てのトリミング行われたピースと，空いているピースに隣接してるピースとの適応度の和を求め，適応度が小さい順に当てはめる．

4.　実　　験

本実験では，いくつかの画像にブロックスクランブル画像暗号化法を施し，ジグソーパズル解法を適用し，その安全性を評価する．

表 3　ブロックスクランブル暗号化法の評価 ($M \times N = 672 \times 504$, 使用画像枚数 20)

暗号化方式	A. ブロックスクランブル			A+回転変換		A+反転変換		A+ネガポジ反転		A+色成分間スクランブル	
ブロックサイズ P	7	14	28	14	28	14	28	14	28	14	28
ブロック総数 L	1728	864	432	864	432	864	432	864	432	864	432
$Dc(I,J)$(平均値)	—*	0.670	0.953	0.373	0.822	0.019	0.018	0.017	0.039	0.025	0.018
$Nc(I,J)$(平均値)	—*	0.805	0.951	0.549	0.904	0.024	0.028	0.132	0.191	0.026	0.028
$Lc(I,J)$(平均値)	—*	0.704	0.953	0.477	0.889	0.020	0.017	0.033	0.093	0.024	0.022
$Pc(I,J)$(総数)	0	2	12	0	9	0	0	0	0	0	0

* ジグソーパズル解法による復元画像の生成不可

4.1　評 価 基 準

暗号化を施す前の元画像とジグソーパズル解法により復元された画像の関係を評価するため，以下の 4 つの評価尺度 [14] [11] を用いる．

第 1 の尺度は Direct comparison(Dc) であり，組み立てられた画像のピースが正しい位置に復元できた割合を表す．暗号化を施し，鍵を用いて復元した画像 I とジグソーパズル解法により復元した画像 J の i 番目のブロックをそれぞれ $I(i)$, $J(i)(i = 1, 2, \ldots, L)$ と置き，それらの値には I のブロック番号を対応させる．すなわち，$I(i) = i, J(i) \in \{1, 2 \ldots, L\}$ となる．このとき，$Dc(I,J)$ を次式より定義する．

$$Dc(I,J) = \frac{1}{L}\sum_{i=1}^{L} d(i),\ d(i) = \begin{cases} 1, & (I(i) = J(i)) \\ 0, & (I(i) \neq J(i)) \end{cases} \tag{15}$$

全てのピースが正しい位置に復元されたとき，$Dc(I,J) = 1$ となり，全て異なった位置に復元された場合は $Dc(I,J) = 0$ となる．

第 2 の尺度は Neighbor comparison(Nc) であり，各ブロックに隣接しているピースの正しい割合を表す．隣接しているブロックの総境界数を B とし，各ブロックの境界を $l_k(k = 1.2 \ldots B)$ とする．$Nc(I,J)$ を次式より定義する．

$$Nc(I,J) = \frac{1}{B}\sum_{k=1}^{B} n(k) \tag{16}$$

ただし，

$$n(k) = \begin{cases} 1, & (\text{画像 } J \text{ の } l_k \text{が正しく隣接している}) \\ 0, & (othereise) \end{cases} \tag{17}$$

全てのピースが正しく復元されたとき，$Nc(I,J) = 1$ となり，隣接しているピースが全て異なる場合 $Nc(I,J) = 0$ となる．

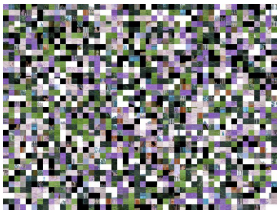
第 3 の尺度は Largest component(Lc) である．ピースの位置に関わらず，連結的に正しく復元できたピースが多いとき，大きな値となる尺度である．複数のピースからなる連結関係として正しい領域を，部分復元領域と呼ぶ．ジグソーパズル解法によって復元された画像 J の i 番目のブロックを含む部分復元領域を $K(I,J,i)$ と表すと，$Lc(I,J)$ は以下のように定義される．

$$Lc(I,J) = \frac{1}{L}\max_{i}\{K(I,J,i)\} \tag{18}$$

$Lc(I,J)$ の値が大きいほど部分的ではあるが，暗号化を施す前の元画像の特定が容易となる．

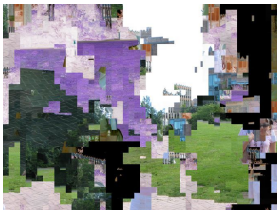
第 4 の尺度は Perfect(Pc) であり，I と J のピースが完全に一致したときの値とし，次式より定義される．

元画像



暗号画像 (ブロックスクランブル +ネガポジ反転)

復元画像 (ブロックスクランブル) $DC(I,J) = 0.670$



復元画像 (ブロックスクランブル +ネガポジ反転)$DC(I,J) = 0.017$

図 6　ジグソーパズル解法による復元画像例 ($P = 14, L = 864$)

$$Pc(I,J) = \begin{cases} 1, & (Dc(I,J) = 1) \\ 0, & (Dc(I,J) \neq 1) \end{cases} \tag{19}$$

上述の各式は，単純なブロックスクランブルの場合の評価式である．さらに，回転変換などが加わった場合には，ピースの方向情報等を考慮し，拡張される必要がある．

4.2　実 験 条 件

MIT データベース [11] の 20 枚の画像 ($M \times N = 672 \times 504$, RGB カラー画像) をブロックサイズ $P = 7, 14, 28$ に分割して実験を行った．使用した JPEG 圧縮のプログラムは，IJG(Independent JPEG Group) [20] である．使用したジグソーパズル解法は MGC 解法である [14].

攻撃者が複数回ジグソーパズル解法を用いて復元を試みる場合を考慮しなければならない．したがって，実験では，各画像および各暗号化条件下において，異なる鍵によって 5 枚の暗号化画像をそれぞれ生成し，復元された画像の $Dc(I,J), Nc(I,J), Lc(I,J)$ の和が最大となる画像 1 枚を評価画像として使用した．これらの条件下で，20 枚の画像に試行を実行して，その平均値を評価値とした．

4.3　実 験 結 果

A. JPEG 圧縮なし

まず，JPEG 圧縮を行わずに，ジグソーパズル解法によって復元された画像と元画像を評価した結果を表 3 に示す．暗号化の方式は 5 種類を準備した．A. ブロックスクランブルのみ，A とブロック回転，A と反転変換，A とネガポジ反転，A と色成分間スクランブルである．表 3 の結果から，ブロックサイズが小さくなるにつれて，復元が困難となっていることがわかる．

表 4　JPEG 圧縮を行った暗号化画像の評価 (ブロック回転なし)
($M \times N = 672 \times 504$, 使用画像枚数 20)

暗号化方式	ブロックスクランブル					
ブロックサイズ P	14			28		
Quality factor	85	90	95	85	90	95
$Dc(I,J)$(平均値)	0	0	0.003	0	0.042	0.606
$Nc(I,J)$(平均値)	0.033	0.054	0.169	0.127	0.357	0.714
$Lc(I,J)$(平均値)	0	0	0.043	0.005	0.231	0.697
$Pc(I,J)$(総数)	0	0	0	0	0	1

表 5　JPEG 圧縮を行った暗号化画像の評価 (ブロック回転あり)
($M \times N = 672 \times 504$, 使用画像枚数 20)

暗号化方式	ブロックスクランブル+回転変換					
ブロックサイズ P	14			28		
Quality factor	85	90	95	85	90	95
$Dc(I,J)$(平均値)	0	0	0	0	0	0.264
$Nc(I,J)$(平均値)	0.012	0.016	0.040	0.069	0.072	0.435
$Lc(I,J)$(平均値)	0	0.009	0.015	0.044	0.047	0.389
$Pc(I,J)$(総数)	0	0	0	0	0	0

このことから，ブロックサイズの適切な選択が安全性のために重要であることがわかる．また，反転変換などの処理が追加されると，ジグソーパズル解法では，より復元が困難であることがわかる．これは，ジグソーパズル解法がそれらの処理を想定していないからである．図 6 に表中のいくつかの処理画像例を示す．

B. JPEG 圧縮あり

ブロックスクランブルを施した暗号化画像に JPEG 圧縮を行い，暗号化に用いた鍵を使用して復元した画像とジグソーパズル解法によって復元した画像 を評価した結果を表 4 に示す．表 5 はブロックスクランブルとブロック回転を同時に施した暗号化画像を評価した結果である．表 3 の結果と同様に，回転処理の追加が，復元の困難性の向上に寄与することがわかる．表 3 との比較から，圧縮により発生する量子化雑音が，画像の復元を困難にすることがわかる．このことは，Q 値が小さい，すわなち量子化が大きほど顕著になる．

5. むすび

ブロックスクランブル画像暗号化の安全性を、ジクソーパズル解法による復元を攻撃と想定し、評価を行った。従来の鍵空間に広さでの安全性議論では、十分な場合においても復元される場合があることが確認された。ブロック内の相関精度を低下させる適切なブロックサイズの選択、ジクソーパズル解法ではまだ想定されていない処理（反転、ネガポジ、色変換）の追加が攻撃耐性向上に有効であることが示された。また、圧縮による量子化誤差が、ジクソーパズル解法による解法を困難にすることが確認された。

文　献

[1] C.T. Huang, L. Huang, Z. Qin, H. Yuan, L. Zhou, V. Varadharajan, and C. C. J. Kuo, “Survey on securing data storage in the cloud,” APSIPA Transactions on Signal and Information Processing, vol.3, e7, 2014.

[2] R. L. Lagendijk, Z. Erkin, and M. Barni, “Encrypted signal processing for privacy protection: Conveying the utility of homomorphic encryption and multiparty computation,” IEEE Signal Processing Mag., vol.30, no.1, pp. 82-105, 2013.

[3] 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. Forens. Security, vol.9, no.1, pp.39-50, 2014.

[4] Kenta KURIHARA, Osamu WATANABE, and Hitoshi KIYA, “AnEncryption-then-Compression System for JPEG XR Standard,” Proc. IEEE International Symposium on Broadband Multimedia Systems and Broadcasting, 2016.

[5] Kenta KURIHARA, Masanori KIKUCHI, Shoko IMAIZUMI, Sayaka SHIOTA, and Hitoshi KIYA, “An Encryption-then-Compression System for JPEG / Motion JPEG Standard,” IEICE Trans. Fundamentals, vol.E98-A, no.11, pp.2238-2245, 2015.

[6] O. Watanabe, A. Uchida, T. Fukuhara, and H. Kiya, “An Encryption-then-Compression system for JPEG 2000 standard,” Acoustics, Speech, and Signal Processing (ICASSP), 2015 IEEE International Conference on, pp.1226-1230, 2015.

[7] K. Kurihara, S. Shiota, and H. Kiya, “An Encryption-then-Compression system for JPEG standard,” In Proceedings of Picture Coding Symposium 2015, pp.119-123, 2015.

[8] S. Li, C. Li, G. Chen, N. G. Bourbakis, and K.-T. Lo, “A general quan-titative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks,” Image Commun., vol. 23, no. 3, pp. 212-223, 2008.

[9] C. Li and K.-T. Lo, “Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks,” Signal Process., vol. 91, no. 4, pp. 949-954, 2011

[10] A. Jolfaei, X.-W. Wu, V. Muthukkumarasamy, “On the security of permutation-only image encryption schemes, “IEEE Transactions on Infor-mation Forensics and Security, Vol.11, No.2, 2016.

[11] T. Cho, S. Avidan and W. Freeman, “A probabilistic image jigsaw puzzle solver, “Computer Vision and Pattern Recognition(CVPR), 2010 IEEE Conference on,pp.183-190, 2010.

[12] D. Pomeranz, M. Shemesh and O. Ben-Shahar, “A fully automated greedy square jigsaw puzzle solver, “Computer Vision and Pattern Recognition(CVPR), 2011 IEEE Conference on, pp.9-16, 2011.

[13] F.A. Andalo, G. Taubin, and S. Goldenstein, “Solving image puzzles with a simple quadratic programming formulation, “Graphics, Patterns and Images(SIBGRAPI), 2012 25th SIBGRAPI Conference on, pp.63-70, 2012.

[14] A.C. Gallagher, “Jigsaw puzzles with pieces of unknown orientation, “ Computer Vision and Pattern Recognition(CVPR) 2012 IEEE Conference on, pp.382-389, 2012.

[15] K. Son, J. Hays, and D.B. Cooper, “Solving square jigsaw puzzles with loop constraints, “ European Conference on Computer Vision(ECCV), Springer, LNCS, 8694, pp.32-46, 2014.

[16] D. Pomeranz, M. Shemesh and O. Ben-Shahar, “A Generalized Genetic Algorithm-Based Solver for Very Large Jigsaw Puzzles of Complex Types, “National Conference on Artificial Intelligence(AAAI2014), pp2839-2845, 2014.

[17] R. Yu, C. Russell, and L. Agapito, “Solving Jigsaw Puzzles with Linear Programming, “[online] arXiv:1511.04472 [cs.CV], 2015.

[18] D. Pomeranz, M. Shemesh and O. Ben-Shahar, “A Genetic Algorithm-Based Solver for Very Large Jigsaw Puzzles, “Genetic Programming and Evolvable Machines, 2016.

[19] J. B. Kruskal, “On the Shortest Spanning Subtree of a Graph and the Traveling Salesman Problem,” Proceedings of the American Mathematical Society, Vol.7, No.1, pp.48-50, 1956.

[20] Independent JPEG Group, http://www.ijg.org/