GRAYSCALE-BASED BLOCK SCRAMBLING IMAGE ENCRYPTION FOR SOCIAL NETWORKING SERVICES

Warit Sirichotedumrong, Tatsuya Chuman*, Shoko Imaizumi† and Hitoshi Kiya**

*Tokyo Metropolitan University, Asahigaoka, Hino-shi, Tokyo, 191-0065, Japan
†Chiba University, Chiba, 263-8522, Japan

ABSTRACT

This paper proposes a new block scrambling encryption scheme that enhances the security of encryption-then-compression (EtC) systems for JPEG images, which are used, for example, to securely transmit images through an untrusted channel provider. The proposed method allows the use of a smaller block size and a larger number of blocks than the conventional ones. Moreover, images encrypted using proposed scheme include less color information due to the use of grayscale even when the original image has three color channels. These features enhance security against various attacks such as jigsaw puzzle solver and brute-force attacks. The results of an experiment in which encrypted images were uploaded to and then downloaded from Twitter and Facebook demonstrated the effectiveness of the proposed scheme for EtC systems.

Index Terms— Encryption, EtC system, social media

1. INTRODUCTION

The rapid growth of the Internet and multimedia systems causes the increment of using images and video especially in Social Networking Service (SNS). To securely transmit images through an untrusted channel provider such as SNS, encryption has to be performed. There are many encryption schemes which have been studied for securing an image [1–3]. The most secure option is to fully encrypt the whole image using the famous cryptosystems, such as RSA and AES. However, security is not the only requirement that cryptosystems should satisfy. Low processing cost and the format compliance have to be considered for using in many applications. A lot of perceptual encryption schemes has been proposed to satisfy the requirements by trading-off the security of encryption schemes [4–9].

This paper focuses on encrypting images before compression process which is called Encryption-then-Compression (EtC) systems [3, 10, 11]. For transmitting the encrypted images over the internet via many platforms, the format of encrypted image has to be compatible with the international image compression standards. The previously proposed EtC systems [3, 12–15] is not compatible with with the international standards. Consequently, the encryption schemes for EtC systems with format compliance to international standards have been proposed [16–20]. Furthermore, the security of conventional EtC systems against jigsaw puzzle and brute-force attacks have been discussed and evaluated [21, 22].

Considering the applicability of EtC systems to SNS, it has been confirmed that the conventional EtC is applicable to SNS. However, color components of images with the conventional scheme can be affected by JPEG compression. Due to the limitation, the color image must be split into 16×16-blocks. Because of such a situation, this paper proposes a new encryption scheme to improve format compliance, robustness against SNS recompression, and the security against several attacks. The contributions of this work are:

- We propose a new block scrambling encryption scheme for EtC systems which enhances the security by dividing the image into smaller block size, having a large number of blocks, and containing less color information.
- We discuss the important characteristics of the image recompression manipulated by SNS provider and elaborately consider this characteristic for designing the encryption scheme which is appropriate for SNS.
- We evaluate the security and downloaded image quality of the proposed scheme and compare them with the conventional EtC encryption scheme.

The rest of paper is organized as follows. Section 2 introduces the EtC systems for image encryption which describe block scrambling-based encryption procedures, the security of EtC systems, and application to SNS. Section 3 elaborates the grayscale-based block scrambling encryption scheme, starting from the grayscale encryption processes followed by describing how the proposed scheme enhances the security and avoids image manipulation process by SNS providers. We evaluate and discuss the performance in Section 4. Concluding remarks are in Section 5.

2. PREPARATION

In this section, after the conventional block scrambling-based image encryption [17–20] is summarized, the security

This work was partially supported by Grant-in-Aid for Scientific Research(B), No.17H03267, from the Japan Society for the Promotion Science.

978-1-5386-1737-3/18/$31.00 ©2018 IEEE

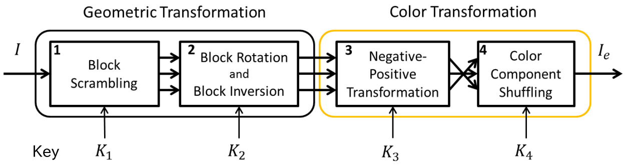
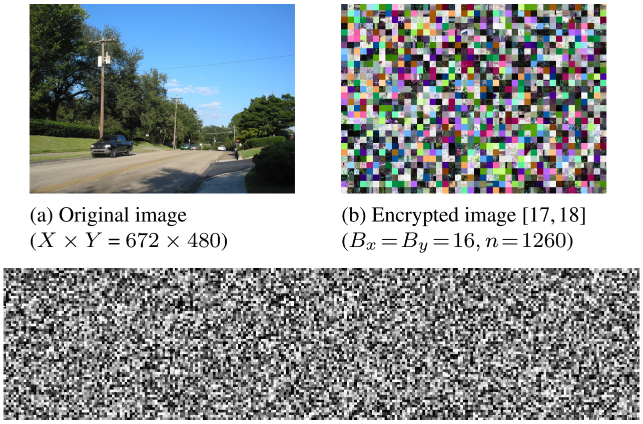

Geometric Transformation
Color Transformation
I
1 Block Scrambling
2 Block Rotation and Block Inversion
3 Negative-Positive Transformation
4 Color Component Shuffling
I_e
Key
K_1
K_2
K_3
K_4

Fig. 1: Block scrambling-based processing steps [21,22]



(a) Original image ($X \times Y$ = 672 × 480)

(b) Encrypted image [17,18] ($B_x = B_y = 16, n = 1260$)

(c) Encrypted image using proposed scheme ($B_x = B_y = 8, n = 15120$)

Fig. 2: Examples of encrypted images

of the scheme against ciphertext-only attacks is addressed. Then, the application of EtC systems for SNS is discussed.

2.1. Block scrambling-based image encryption

According to the block scrambling-based image encryption scheme for EtC systems [16–20], an image with $M \times N$ pixels is divided into non-overlapping blocks each with $B_x \times B_y$ pixels. The number of divided blocks, n, is expressed by

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

where $\lfloor \cdot \rfloor$ is the round down function to the nearest integer.

In order to generate an encrypted image (I_e), each divided block is processed using the following four block scrambling-based steps (See Fig. 1).

Step1: Divide an image with $M \times N$ pixels (I) into blocks with $B_x \times B_y$ pixels, and permute the divided blocks randomly based on the random integer which is generated by a secret key K_1.

Step2: Randomize the integer using a secret key K_2, then rotate and invert each block according to the previously randomized integer.

Step3: Apply the negative-positive transformation to each block using a random binary integer generated by a secret key K_3. A transformed pixel of ith block is represented by p' and computed as

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

where $r(i)$ is a random binary integer generated by K_3 and p is the pixel value of an original image with L bits per pixel.

Step4: The three color components in each block are shuffled using a senary integer generated by the fourth secret key K_4.

Note that the secret keys, K_1, K_2, and K_3, are commonly used for all color components.

According to the block scrambling-based encryption scheme, the above four steps construct I_e that provides a compatibility with the JPEG standard and almost preserves the compression efficiency at the same level as the original JPEG image. In JPEG compression, color sub-sampling is usually done for reducing the color components of a color image. In order to make 8 × 8-blocks for color sub-sampling process, the color image must be split into Minimum Coded Unit (MCU) which corresponds to 16 × 16-blocks. Therefore, the possible smallest block size of block scrambling-based encryption is 16 × 16. When the block size is smaller than 16 × 16, the block scrambling process affects the color sub-sampling of JPEG compression. An example of an encrypted image ($B_x = B_y = 16$) is illustrated in Fig. 2(b) where Fig. 2(a) is the original one.

2.2. Security analysis

Along with the encryption scheme, robustness and security against the attacks have to be considered in terms of key space as explained in [18]. The key space of the scheme is generally large enough against the brute-force attacks as ciphertext-only attack. However, regarding the blocks of an encrypted image as pieces of a jigsaw puzzle, jigsaw puzzle solver attacks based on the correlation can be assumed [23–28]. For example, the jigsaw puzzle solver [25] completely succeeded in assembling large puzzles which consist of 30745 pieces with the size of 28 × 28. Besides, even when the number of blocks in an encrypted image is larger than 22755, there is a possibility that the image is completely decrypted if the piece size is large [24]. There are three conditions making assembling encrypted images more difficult as indicated below.

- The number of blocks is large.
- Block size is small.
- Encrypted images include JPEG distortion [29].

Moreover, as most of jigsaw puzzle solvers utilize the color information to assemble the encrypted images, reducing the color components makes the assembling process more difficult.

Table 1: Relationship between uploaded JPEG files and downloaded ones in terms of sub-sampling ratios [30]

SNS provider	Uploaded JPEG file		Downloaded JPEG file	
	Sub-sampling ratio	Q_f	Sub-sampling ratio	Q_f
Twitter (Up to 4096×4096 pixels)	4:4:4	low	No recompression	
		high	4:2:0	85
	4:2:0	1,2,... 84	No recompression	
		85,86,... 100	4:2:0	85
Facebook (HQ, Up to 2048×2048 pixels)	4:4:4	1,2,... 100	4:2:0	71,72,... 85
Facebook (LQ, Up to 960×960 pixels)	4:2:0			

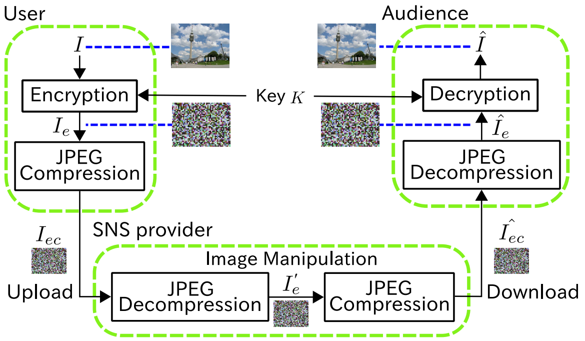


Fig. 3: EtC system [21, 22]

2.3. Application to SNS

It has been confirmed that EtC systems can be applied to SNS [30]. Figure 3 illustrates the application of EtC systems for SNS, where a user wants to securely transmit image I to an audience, via a SNS provider. As the user does not give the secret key K to the SNS provider, the privacy of shared image is controlled by the user, even if the SNS provider decompresses image I. Therefore, the user is able to protect the privacy by him/herself. Although encrypted images saved in the SNS servers are leaked by malicious users, the third party and general audiences could not see these images visually unless they have the secret keys.

Meanwhile, it is known that almost all SNS providers manipulate images uploaded by users, e.g., rescaling image resolution and recompressing with different parameters, for decreasing the data size of images [30–32]. As a result, the quality of images recompressed by SNS providers is reduced by image manipulation on social media.

This paper proposes a new encryption scheme for the EtC system, which avoids some effects of recompression by SNS providers. As a result, using the proposed scheme enables us to secure the privacy of the image and keep higher quality than the conventional one, even when recompression is carried out by SNS providers.

3. PROPOSED SCHEME

In this section, the proposed block scrambling-based image encryption scheme is described, and then the security of the scheme is discussed.

3.1. Encryption procedure

Three steps to encrypt a color image with $M \times N$ pixels are carried out as follows.

Step1: The RGB color components of the full-color image are separated into three individual channels. The scheme considers each channel as an individual image, and red, green, and blue channels can be respectively represented by i_r, i_g, and i_b.

Step2: i_r, i_g, and i_b are combined as a new image in grayscale (I_{gray}). For example, this combination process can be done vertically and horizontally, so size of the new image is equal to $M \times 3N$ or $3M \times N$.

Step3: Step 1 to step 3 of block scrambling-based encryption described in Section 2.1 is performed over I_{gray}.

After three steps above, the grayscale encrypted image is produced and can be represented by $I_{e_{gray}}$. Note that the color components shuffling in the conventional scheme are neglected.

3.2. Smaller block size with less chroma component

Since the JPEG standard downsamples chroma components by splitting a color image into MCU, the possible smallest block size of conventional scheme is $B_x = B_y = 16$. As a grayscale image contains only one color channel per pixel, it is not sub-sampled by JPEG compression. Hence, the smallest block size of the proposed scheme is decreased to $B_x = B_y = 8$ which causes fourfold rising to the number of blocks. As a result, as shown in Fig. 2(c), the size of encrypted image is $3(M \times N)$, the number of block is totally 12 times larger than that with the conventional one. Summarily, the proposed scheme enhances the security by utilizing less color information, block size reduction, and larger number of blocks.

3.3. Image manipulation on SNS

The proposed scheme also has some advantages over the SNS platform. This paper focuses on the JPEG compression as one of compression methods because the JPEG standard is the most widely used image compression standards, and most of SNS providers support the JPEG standard [30].

Generally, the JPEG standard encodes color images by transforming the color components from RGB space to

YCbCr space, then the color components, Cb and Cr, are downsampled to reduce the spatial resolution. Besides, when an image is uploaded to SNS, the image will be recompressed again by providers as shown in Table 1 [30]. The image recompression of SNS providers is concluded as follows.

- **Twitter** decides whether an uploaded image has to be manipulated or not based on uploaded image compression properties as shown in Table 1. When the quality factor (Q_f) of an uploaded JPEG image is higher than 84, Twitter transcodes it into the new image. Q_f of transcoded image is equal to 85, and the color components of transcoded image are distorted using 4:2:0 color sub-sampling. Otherwise, Twitter does not recompress the uploaded image.

- **Facebook** always recompresses an uploaded images regardless of sub-sampling ratio and Q_f. Every image is recompressed with 4:2:0 color sub-sampling, and there are many possible Q_f using in Facebook recompression process. Depending on Facebook compression algorithm [30], Q_f is selected from the specific range ($71 \leqq Q_f \leqq 85$).

According to [30], it has been confirmed that the conventional block scrambling scheme is also applicable to SNS while other encryption schemes, such as AES, cannot be applied to SNS. Moreover, the proposed scheme can reduce influence of the color sub-sampling, caused by SNS providers.

4. EXPERIMENTAL RESULTS

4.1. Experimental set-up

In order to evaluate some performances of the encryption schemes, we employed two datasets as below.

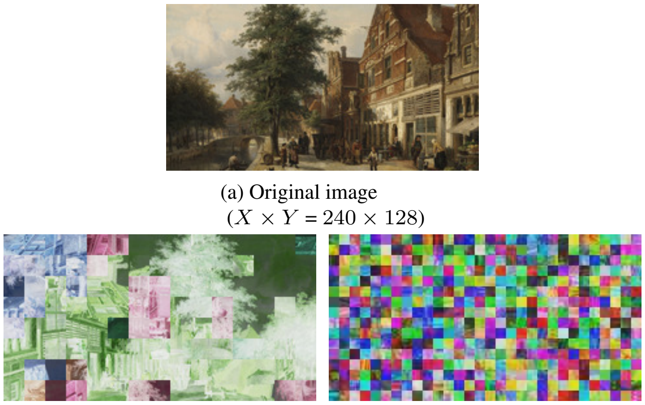
(a) 20 images from MIT dataset (672 × 480) [33].

(b) 20 images from resized Ultra-Eye dataset (240 × 128) [34].

All images in both datasets were encrypted using the conventional scheme ($B_x = B_y = 16$ and $B_x = B_y = 8$) and the proposed scheme ($B_x = B_y = 8$). We also compressed the images using the JPEG standard from Independent JPEG Group (IJG) software [35] with specific range of quality factors, $Q_f \in [70, 100]$. We focused on Twitter and Facebook because these SNS providers always recompress if images uploaded by users meet the conditions. The encrypted and non-encrypted JPEG files with 4:4:4 sampling from dataset (a) were uploaded to Twitter and Facebook while the encrypted and non-encrypted images from dataset (b) were utilized for evaluating the robustness against jigsaw puzzle solver attacks [21, 22, 26, 33, 36].

4.2. Results and discussions

The performances of the encryption scheme are shown in two aspects: security, and quality of downloaded images.



(a) Original image
($X \times Y$ = 240 × 128)

(b) Assembled image
(Conventional scheme,
$B_x = B_y = 16$,
$D_c = 0.25, N_c = 0.26, L_c = 0.24$)

(c) Assembled image
(Proposed scheme,
$B_x = B_y = 8$,
$D_c = 0, N_c = 0.002, L_c = 0.002$)

Fig. 4: Examples of assembled images

4.2.1. Security

The security of the encryption schemes was evaluated by the robustness against jigsaw puzzle solvers attack [21, 22, 26, 33, 36]. This paper used the extended jigsaw puzzle solver [21, 22] for assembling encrypted images. There are three metrics [33, 36] using for determining the robustness against the extended solvers which are described as follows.

- **Direct comparison(D_c)** is the ratio between the number of pieces which are placed in the correct position and the total number of pieces.

- **Neighbor comparison (N_c)** expresses the ratio of the number of pieces that are joined with the correct pattern and the total number of pieces.

- **Largest components(L_c)** refers to the ratio between the number of the largest joined blocks that are correctly adjacent and the number of pieces.

In the measures, D_c, N_c, $L_c \in [0, 1]$, a larger value means a higher compatibility as illustrated in Fig. 4. Thirty different encrypted images from dataset (b) were generated by random keys from one ordinary image. The assembled image which has the highest sum of D_c, N_c, and L_c in those of thirty images was chosen. We performed these procedures for each original image independently, and the average score of 20 images for each metric was calculated.

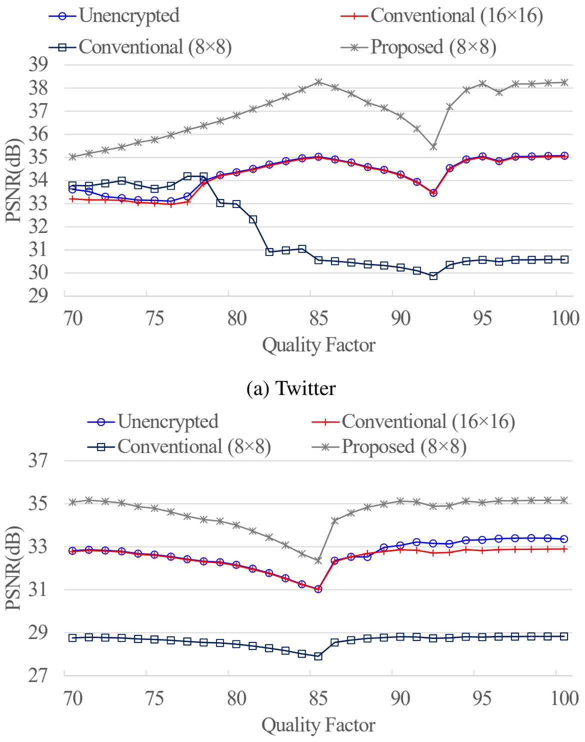
As shown in table 2, the average D_c, N_c, and L_c of images with the proposed scheme are respectively equal to 0.002, 0.003, and 0.003 which are lower than those with the conventional scheme. Summarily, encrypting images using the proposed scheme provides more robustness against the extended jigsaw puzzle solver attack in addition to larger key space.

4.2.2. Quality of downloaded images

To evaluate the effectiveness of the proposed scheme, we uploaded images encrypted using the proposed scheme as well

Table 2: Evaluation of the conventional and proposed scheme

Encryption types	Conventional scheme[17,18]	Proposed scheme
Color channel	RGB	Gray scale
Block size $B_x \times B_y$	16 × 16	8 × 8
Number of blocks n	120	1440
D_c (Average)	0.189	0.002
N_c (Average)	0.255	0.003
L_c (Average)	0.310	0.003



(a) Twitter

(b) Facebook

Fig. 5: The result of PSNR versus Q_f

as the conventional scheme [17, 18] to Twitter and Facebook respectively. The images encrypted using the conventional scheme and the non-encrypted ones were compressed with a 4:4:4 sub-sampling ratio and Q_f = 70,71,...,100. Then, downloading uploaded images from the SNS providers, decoding the downloaded images, and decrypting the encrypted images were carried out respectively.

Figure 5 shows the performance for JPEG compressed images without encryption, with the conventional scheme, and with the proposed scheme. The arithmetic mean PSNR of 20 images from dataset (a) per quality factor uploaded to Twitter and Facebook were plotted in Fig. 5(a) and Fig. 5(b) respectively.

Twitter recompresses uploaded images that were compressed with high quality factor ($Q_f \geqq 85$), using Q_f = 85 as shown in table 1 [30]. Otherwise, uploaded JPEG images are not recompressed. In contrast, Facebook recompresses every uploaded JPEG image regardless of quality factor based on its compression algorithm with 4:2:0 sampling.

As shown in Fig. 5, the proposed scheme offered higher image quality than the conventional scheme even if image JPEG recompression was carried out by Twitter and Facebook. When encrypting images using conventional scheme with the same block size as the proposed scheme ($B_x = B_y = 8$), the quality of downloaded images is strongly affected by the color sub-sampling operation, while the proposed scheme can avoid this influence even in case of using $B_x = B_y = 8$. Moreover, the PSNR values of decrypted images with the proposed scheme were higher than unencrypted images in both providers due to avoiding the effect of color sub-sampling. These results show that the proposed scheme allows us to download higher quality images than unencrypted ones.

5. CONCLUSION

This paper presented the new image encryption scheme that can be applied to SNS called grayscale-based block scrambling image encryption. The proposed encryption scheme can avoid the influence of color sub-sampling from JPEG compression. Compared to the conventional scheme, the proposed scheme has less color information, smaller block size, and larger number of blocks which enhance the security and robustness against attacks. The experiment was conducted by uploading the encrypted and unencrypted images to the SNS providers: Twitter and Facebook. Moreover, the robustnesses against jigsaw puzzle solver attacks were evaluated. The results proved that the proposed scheme offers the better security and higher image quality than the conventional scheme.

6. REFERENCES

[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. Lagendijk, Z. Erkin, and M. Barni, "Encrypted signal processing for privacy protection: Conveying the utility of homomorphic encryption and multiparty computation," *IEEE Signal Processing Magazine*, 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 transactions on information forensics and security*, vol. 9, no. 1, pp. 39–50, 2014.

[4] W. Zeng and S. Lei, "Efficient frequency domain selective scrambling of digital video," *IEEE Transactions on Multimedia*, vol. 5, no. 1, pp. 118–129, 2003.

[5] I. Ito and H. Kiya, "A new class of image registration for guaranteeing secure data management," in *IEEE International Conference on Image Processing (ICIP)*, 2008, pp. 269–272.

[6] H. Kiya and I. Ito, "Image matching between scrambled images for secure data management," in *16th European Signal Processing Conference (EUSIPCO)*, 2008, pp. 1–5.

[7] I. Ito and H. Kiya, "One-time key based phase scrambling for phase-only correlation between visually protected images,"

EURASIP Journal on Information Security, vol. 2009, no. 841045, pp. 1–11, 2010.

[8] Z. Tang, X. Zhang, and W. Lan, "Efficient image encryption with block shuffling and chaotic map," *Multimedia Tools Applications*, vol. 74, no. 15, pp. 5429–5448, 2015.

[9] C. Li, D. Lin, and J. L, "Cryptanalyzing an image-scrambling encryption algorithm of pixel bits," *IEEE Transactions on Multimedia*, vol. 24, no. 3, pp. 64–71, 2017.

[10] Z. Erkin, A.Piva, S. Katzenbeisser, R. L. Lagendijk, J. Shokrollahi, G. Neven, and M. Barni, "Protection and retrieval of encrypted multimedia content: When cryptography meets signal processing," *EURASIP Journal on Information Security*, vol. 2007, no. 78943, pp. 1–20, 2007.

[11] N. Nimbokar G. and S. Sarode V., "Article: A survey based on designing an efficient image Encryption-then-Compression system," *IJCA Proceedings on National Level Technical Conference X-PLORE 2014*, vol. XPLORE2014, pp. 6–8, 2014.

[12] M. Johnson, P. Ishwar, V. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," *IEEE Transactions on Signal Processing*, vol. 52, no. 10, pp. 2992–3006, 2004.

[13] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," *IEEE Transactions on Image Processing*, vol. 19, no. 4, pp. 1097–1102, 2010.

[14] X. Zhang, "Lossy compression and iterative reconstruction for encrypted image," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 1, pp. 53–58, 2011.

[15] R. Hu, X. Li, and B. Yang, "A new lossy compression scheme for encrypted gray-scale images," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2014, pp. 7387–7390.

[16] O. Watanabe, A. Uchida, T. Fukuhara, and H. Kiya, "An encryption-then-compression system for jpeg 2000 standard," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2015, pp. 1226–1230.

[17] K. Kurihara, S. Shiota, and H. Kiya, "An encryption-then-compression system for jpeg standard," in *Picture Coding Symposium (PCS)*, 2015, pp. 119–123.

[18] K. Kurihara, M. Kikuchi, S. Imaizumi, S. Shiota, and H. Kiya, "An encryption-then-compression system for jpeg/motion jpeg standard," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 98, no. 11, pp. 2238–2245, 2015.

[19] K. Kurihara, O. Watanabe, and H. Kiya, "An encryption-then-compression system for jpeg xr standard," in *IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB)*, 2016, pp. 1–5.

[20] K. Kurihara, S. Imaizumi, S. Shiota, and H. Kiya, "An encryption-then-compression system for lossless image compression standards," *IEICE transactions on information and systems*, vol. E100-D, no. 1, pp. 52–56, 2017.

[21] T. Chuman, K. Kurihara, and H. Kiya, "On the security of block scrambling-based etc systems against jigsaw puzzle solver attacks," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2017, pp. 2157–2161.

[22] T. Chuman, K. Kurihara, and H. Kiya, "Security evaluation for block scrambling-based etc systems against extended jigsaw puzzle solver attacks," in *IEEE International Conference on Multimedia and Expo (ICME)*, 2017, pp. 229–234.

[23] K. Son, J. Hays, and D. B. Cooper, "Solving square jigsaw puzzles with loop constraints," in *European Conference on Computer Vision (ECCV)*, 2014, pp. 32–46.

[24] G. Paikin and A. Tal, "Solving multiple square jigsaw puzzles with missing pieces," in *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2015, pp. 4832–4839.

[25] 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.

[26] K. Son, D. Moreno, J. Hays, and D. B. Cooper, "Solving small-piece jigsaw puzzles by growing consensus," in *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2016, pp. 1193–1201.

[27] D. Sholomon, O. E. David, and N. S. Netanyahu, "A generalized genetic algorithm-based solver for very large jigsaw puzzles of complex types," in *National Conference on Artificial Intelligence (AAAI)*, 2014, pp. 2839–2845.

[28] F. A. Andalo, G. Taubin, and S. Goldenstein, "Psqp: Puzzle solving by quadratic programming," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 39, no. 2, pp. 385–396, 2017.

[29] T. Chuman and H. Kiya, "On the security of block scrambling-based image encryption including jpeg distorsion against jigsaw puzzle solver attacks," in *IEEE International Workshop on Signal Design and its Applications in Communications (IWSDA)*, 2017, pp. 64–68.

[30] T. Chuman, K. Iida, and H. Kiya, "Image manipulation on social media for encryption-then-compression systems," in *2017 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)*, 2017, pp. 858–863.

[31] O. Giudice, A. Paratore, M. Moltisanti, and S. Battiato, "A classification engine for image ballistics of social data," *arXiv preprint arXiv:1610.06347*, 2016.

[32] M. Moltisanti, A. Paratore, S. Battiato, and L. Saravo, "Image manipulation on facebook for forensics evidence," in *International Conference on Image Analysis and Processing (ICIAP) 2015*, 2015, pp. 506–517.

[33] T. Cho, S. Avidan, and W. Freeman, "A probabilistic image jigsaw puzzle solver," in *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2010, pp. 183–190.

[34] H. Nemoto, P. Hanhart, P. Korshunov, and T. Ebrahimi, "Ultra-eye: Uhd and hd images eye tracking dataset," in *Sixth International Workshop on Quality of Multimedia Experience (QoMEX)*, 2014, pp. 39–40.

[35] "Independent jpeg group," http://www.ijg.org/.

[36] A. Gallagher, "Jigsaw puzzles with pieces of unknown orientation," in *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2012, pp. 382–389.