https://doi.org/10.7840/kics.2024.49.8.1132

Sub-Block-Based Compressible Perceptual Encryption Algorithm with Chroma Subsampling

Ijaz Ahmad[◆], Seokjoo Shin[°]

ABSTRACT

Perceptual Encryption (PE) provides an efficient solution to the requirement of cipher images format-compatibility of photo-storage and photo-sharing applications. They deliver a desired level of security while preserving image intrinsic properties necessary to enable image processing such as image compression, in the encrypted domain. PE methods implement blockwise geometric and color transformation functions wherein the choice of block size results in a tradeoff relationship between encryption efficiency and compression savings. Nonetheless PE methods that incorporate sub-block level processing alongside block level processing can better manage this tradeoff. However, such methods have a compatibility issue with the JPEG lossy standard as the recovered images have subsampling distortions. Specifically, it cannot avoid the blur distortion resulted from the subsampling of the luminance component that is shuffled with the chroma component of the image during encryption. To address this limitation, we propose a color transformation function for the sub-block-based PE algorithms that integrates the image component shuffling step of encryption with the chroma subsampling function of compression. The simulation analyses show that the images are decoded without any visible artifacts and distortions. In addition, the proposed function reduces the datarate difference by 87% at maximum and 18% at minimum for different sub-block sizes.

Key Words : perceptual encryption, JPEG, image compression, image encryption, chroma subsampling

Ⅰ. Introduction

Compression and encryption are the two requirements for efficient and secure image data transmission and/or storage. Both of these processes aim to reduce the redundancy present in the image data[1]. The compression eliminates this undesirable redundancy to give a compact representation to the data thus efficiently utilizes the available limited bandwidth and storage capacities. The encryption removes this redundancy to make the data random and unintelligible thereby protects it from unauthorized access. Compression can be carried out either in lossless mode where higher image quality is preserved, or in lossy mode where image quality is traded for better compression savings. Encryption algorithms can be classified as symmetric-key algorithm which uses the same key for encryption and decryption, or asymmetric-key algorithm which uses two different keys during encryption and decryption. Regardless of their mode of operation, compression and encryption have competing requirements and the order in which they are coupled together affects the overall performance of the target application system[2]. In general, compression is completed prior to encryption or else there is less or no redundancy left in the cipher images to

※ This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government. (MSIT) (RS-2023-00278294).

◆ First Author : Chosun University Department of Computer Engineering, ahmadijaz@chosun.kr, 학생회원

° Corresponding Author : Chosun University Department of Computer Engineering, sjshin@chosun.ac.kr, 종신회원

논문번호 : 202403-043-0-SE, Received February 26, 2024; Revised April 13, 2024; Accepted April 23, 2024

be exploited by the compression process[2]. However, applications such as photo-storage or photo-sharing services, where format-compatibility is a requirement then it is necessary to reverse this order. Though the traditional number theory and chaos theory -based image encryption algorithms are the most secure options, they do not cater to this requirement. Towards this perceptual encryption (PE) algorithms have been proposed that adds randomness to the image data in such a way that its redundancy remains intact, which makes their cipher images compressible[3]. The output of a PE algorithm is an image which can be encoded with image compression standards such as the JPEG algorithm[4]. In addition, PE has an advantage of low computational cost which makes them suitable for data protection in resource-constrained devices[5] and for real-time multimedia applications[6].

In general, a PE algorithm performs geometric and color transformations on a block level in such a way that the human perceivable information in the image is protected while its intrinsic characteristics are preserved. In PE methods, the choice of block size results in a tradeoff relationship between security efficiency and compression savings. Usually, a larger number of blocks is required for better security, which can be achieved by choosing smaller block size. However, to avoid any adverse impact of compression, an encryption algorithm should adhere to the JPEG standard recommendations for this choice of block size. Therefore, for the color and grayscale image encryption block sizes 16 × 16 and 8 × 8 should be used, respectively. Nonetheless, as opposed to reducing the block size during encryption, several other practices have been proposed that efficiently manage this tradeoff. For example, a larger number of blocks can be achieved by processing each color component independently[7] or by representing an input true color image as a pseudo grayscale image to exploit the 8 × 8 block size for color image encryption [8]. Alternatively, sub-block-level processing can enable the use of smaller block size than the JPEG specifications in selected encryption steps [5], [9]. For a detail description, we recommend the comprehensive analysis and review presented in [6], [10], [11], [12], [13]. For example, [10] implements these best practices of the PE algorithms and provides a perspective on their compression and encryption efficiencies. In addition, [6] provides an overview of PE methods, [13] analyzes their encryption efficiency while [12] analyzes their robustness against various communication impairments, and [11] summarizes their privacy-preserving applications.

Despite the aforementioned improvements in PE methods, there is a prerequisite of an input color image for security efficiency in [7] and [8], and there is a compatibility issue with the JPEG lossy standard in [9]. In the latter case, performing compression with the chroma subsampling results in block artifacts and blur distortion. Towards this we propose a subsampling function that can be integrated with the PE methods based on sub-block processing. Specifically, this function is implemented in the component shuffling step of the PE algorithm. The current work is an extension of [14] and its main contributions are summarized as following: (1) The encryption efficiency is improved with a new set of rules for the image components shuffling step. (2) The compression performance is analyzed for a wide range of the JPEG quality factors implemented with both luminance and chrominance quantization tables. (3) The encryption and compression efficiencies are analyzed for three different sub-block sizes. (4) The compression savings and image quality are measured using Bjøntegaard delta (BD) metrics[15].

Ⅱ. Proposed Method

2.1 Motivation

Block artifacts and blur distortion can appear in the recovered images when the JPEG chroma subsampling and quantization steps are mishandled. The JPEG chroma subsampling is a block-based operation that down samples a 16 × 16 chroma block to an 8 × 8 block size. To recover the original image resolution, the JPEG decoder performs interpolation in the down sampled blocks. The implementation of permutation and negative-positive transformation steps of PE algorithm on a block size less than 16 × 16 results in pixels having low correlation; therefore, the JPEG decoder recovers images with block artifacts. On the

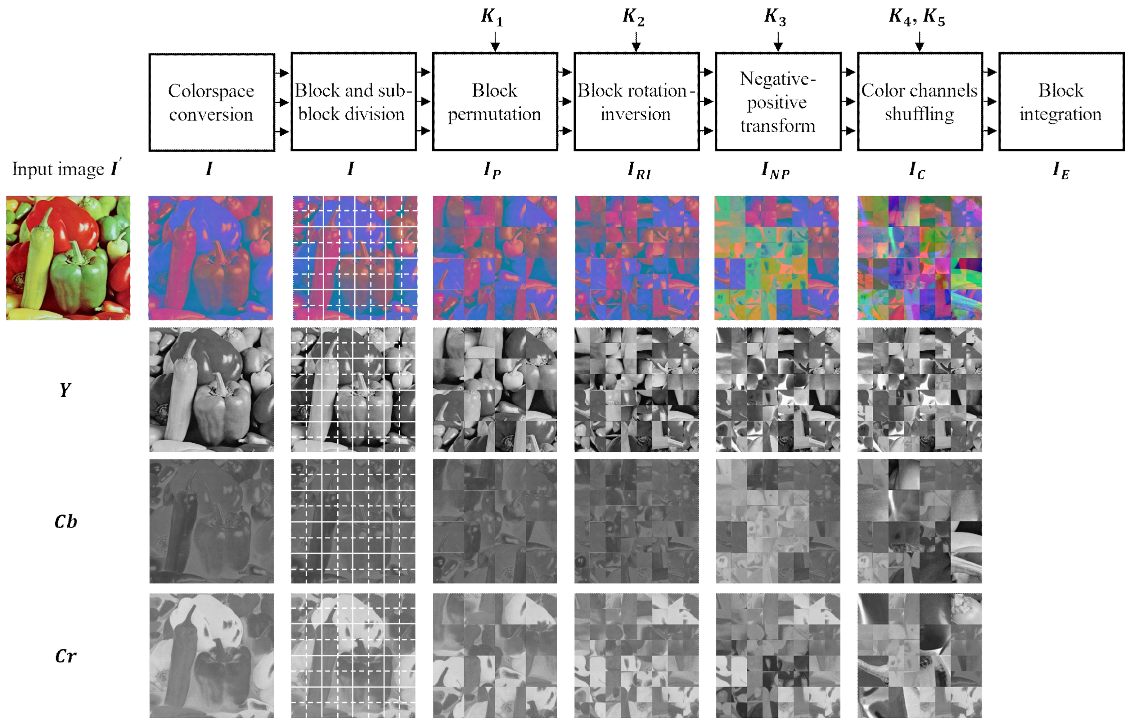


Fig. 1. An illustration of our proposed PE method. I_P is the permutation, I_{RI} is the rotation-inversion, I_{NP} is the negative-positive transformation, and I_C is the color channels shuffling steps performed on the image I.

other hand, the color channel shuffling step of PE algorithm invalidates the JPEG colorspace conversion and quantization functions. This conversion is necessary to separate luminance and chrominance components of the image for the JPEG sub-sampling step. A simple solution to this is to perform the colorspace conversion prior to encryption. However, when the luminance component is mixed up with either of the chrominance components in the shuffling step of PE algorithm, then it is subjected to sub-sampling during compression, which later results in the blur distortion. The methods that incorporate sub-block processing to exploit smaller block size only for inside-out transformation can avoid the block artifacts; however, they cannot completely eliminate the blur distortion. To address this issue, we present our proposed method in the following subsections.

2.2 Proposed Perceptual Encryption

For an image $I^{H\times W\times C}$, whose dimensions are specified as H rows, W columns, and C color channels, our proposed PE algorithm is illustrated in Fig.1. and consists of the following steps:

Step 1) Separate the luminance component ($\boldsymbol{Y}$) from the chrominance components ($\boldsymbol{Cb}$ and $\boldsymbol{Cr}$) of the image by performing colorspace conversion as

$$\begin{aligned}\boldsymbol{Y} &= (0.3\times\boldsymbol{R})+(0.59\times\boldsymbol{G})+(0.11\times\boldsymbol{B})\\ \boldsymbol{Cb} &= 128-(0.17\times\boldsymbol{R})+(0.33\times\boldsymbol{G})+(0.5\times\boldsymbol{B})\\ \boldsymbol{Cr} &= 128+(0.5\times\boldsymbol{R})+(0.42\times\boldsymbol{G})+(0.08\times\boldsymbol{B}).\end{aligned} \tag{1}$$

Step 2) Divide $I^{H\times W\times C}$ into $L\times M$ nonoverlapping blocks where $L = H/B$ and $M = W/B$. Each block has B^2 pixels and C channels.

Step 3) Scramble the block positions in the image using a randomly generated key $\boldsymbol{K_1}$.

Step 4) Apply the inside-out transformation proposed in [9] by using key $\boldsymbol{K_2}$ to change each block orientation in the shuffled image. Each entry of this key represents an axis of rotation and inversion.

Step 5) Apply the negative-positive transformation proposed in [3] to randomly chosen blocks by using key $\boldsymbol{K_3}$. The modified value of a pixel $p_{x,y}$ positioned at *x*, *y* in a block is obtained as:

$$\acute{p}_{x,y} = \begin{cases} p_{x,y} & \boldsymbol{K}_3(i) = 0 \\ 255 - p_{x,y} & \boldsymbol{K}_3(i) = 1, \end{cases} \tag{2}$$

where i = 0, 1, 2, ⋯, $L \times M$ is the i^{th} key element. *Step 6)* Shuffle the luminance and chrominance components in each block using a random key $\boldsymbol{K}_4$. The key $\boldsymbol{K}_4$ elements and their associated shuffle actions are described in Table 1. An additional key $\boldsymbol{K}_5$ is used to randomly choose sub-blocks from the $\boldsymbol{Y}$ component. This color transformation function is further explained in the subsection 2.3.

In its basic form, PE methods process each color component with the same key. However, for a larger key space these methods can be extended: to process each color component independently [7], to introduce sub-block-level processing [9], and to represent an input as a pseudo grayscale image [8]. To preserve the spatial information of an image, which is necessary for privacy-preserving computation applications, we considered sub-block-level processing in Step 4 and adopted inside-out transformation function as proposed in [9]. Though this sub-block processing avoids block artifacts by preserving the correlation among the neighboring pixels within a block, it cannot avoid the blur distortion resulted from the subsampling of the luminance component that is shuffled with the chroma component of the image during encryption. To mitigate the subsampling distortions, we proposed the following color transformation function.

Table 1. Key rules for proposed color transformation function.

K_4	Y	Cb	Cr
0	$Y_{\mathcal{A}}$	Cr	Cb
1	$Y_{\mathcal{A}}\dot{Cb}$	$\ddot{Y}_{\mathcal{B}}$	Cr
2	$Y_{\mathcal{A}}\dot{Cb}$	Cr	$\ddot{Y}_{\mathcal{C}}$
3	$Y_{\mathcal{A}}\dot{Cr}$	$\ddot{Y}_{\mathcal{B}}$	Cb
4	$Y_{\mathcal{A}}\dot{Cr}$	Cb	$\ddot{Y}_{\mathcal{C}}$
5	$Y_{\mathcal{A}}\dot{Cb}\dot{Cr}$	$\ddot{Y}_{\mathcal{B}}$	$\ddot{Y}_{\mathcal{C}}$

$\mathcal{A}, \mathcal{B}, \mathcal{C} \subseteq \mathcal{S}$, where $\mathcal{A}, \mathcal{B}, \mathcal{C}$ are mutually exclusive and $\mathcal{S}$ consists of all sub-blocks of Y; $\dot{\mathbf{x}}$ and $\ddot{\mathbf{x}}$ denote sub- and up-sampling of $\mathbf{x}$, respectively.

2.3 Proposed Color Transformation Function

Firstly, proposed method represents an input image in YCbCr colorspace prior to encryption; thus, avoids invalid calculation of luma and chroma components during compression. Secondly, chroma subsampling is integrated into the color channel shuffling step as shown in Fig. 2. For a randomly chosen block, the proposed method modifies Step 6 according to the luma and chroma components as:

1. To shuffle the luma component with either of the chrominance components, luminance sub-blocks are randomly chosen (two sub-blocks can be shuffled at maximum), and up-sampled to 16 × 16 block size.
2. Conversely, to shuffle either of the chrominance components of a block with the luminance component, the chroma block is down-sampled to 8 × 8 block size.

The block sizes 16 × 16 and 8 × 8, and the chroma sub- and up-sampling functions are chosen according to the JPEG standard requirements.

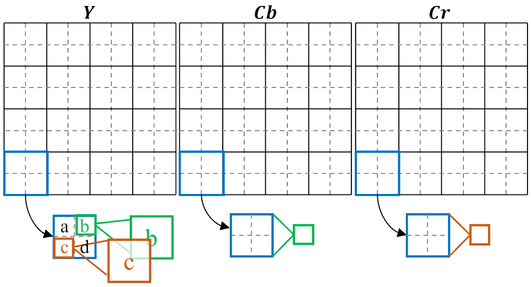


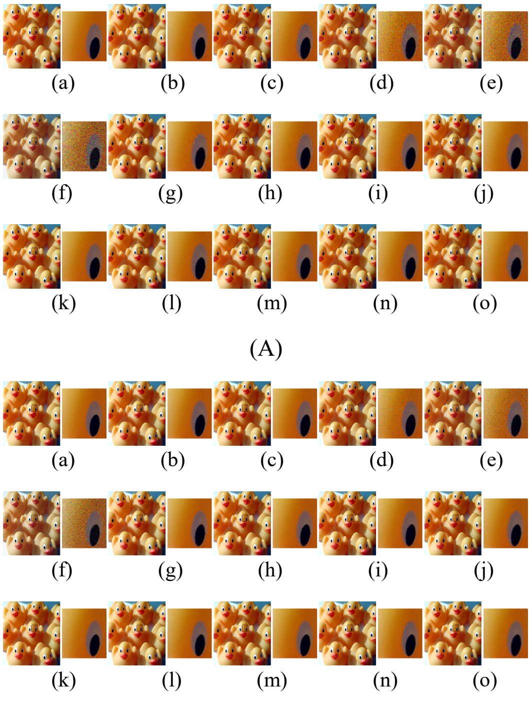
Fig. 2. An illustration of our proposed color transformation function that combines image-component shuffling step of encryption with the chroma subsampling function of compression. The sub-blocks labeled as ‘b’ and ‘c’ in $\boldsymbol{Y}$ are up-sampled before shuffling them with the ‘*Cb*’ and ‘*Cr*’ components, respectively. Here, $\boldsymbol{K}_4$ = 5.

Ⅲ. Results

In the simulations, we have used Tecnick sampling dataset [16] that consists of 120 true color images of size 1200 × 1200. The JPEG quality factor $Q_f \in$ {71, 72, 73, ⋯, 99, 100}, the chroma sub-sampling ratio {4:2:0} and the standard luminance and chrominance quantization tables were used. The block size was set to be 16×16 with sub-block sizes {8 × 8, 4 × 4, 2 × 2} for the inside-out transformation and 8 × 8 for the channel shuffling step. The image quality was measured using the log transformed value of Multiscale Structural Similarity Index Measure (MS-SSIM)[17].

3.1 Visual Analysis

For visual quality analysis of the recovered images, an example image is shown in Fig. 3. The image was compressed with the JPEG standard implemented with the chroma subsampling of ratio 4:2:0 and standard quantization tables. For better inspection, a boxed region in each image is zoomed in and shown on the right of its corresponding image. It can be observed that the block artifact is avoided in Color-CPE method proposed in [3] for block size 16 × 16 and in IIB-CPE method proposed in [9] for all sub-block sizes as the correlation among the neighboring pixels within a block has been preserved. However, due to the erroneous calculation of the colorspace conversion function in both methods, regardless of the block size, the blur distortion appears in regions where there is an abrupt change in the intensity values. This blur distortion is reduced when the JPEG quality factor is set to a higher value, as shown in Fig. 3. (B). In addition, images recovered from Color-CPE cipher images where block sizes smaller than 16 × 16 were used have both block artifacts and blur distortions. On the other hand, no block artifacts and blur distortions are visible in the images recovered from our proposed method. The block artifacts were avoided by incorporating sub-block processing to preserve the pixel correlation, while the blur distortions were avoided by performing colorspace conversion and the chroma subsampling prior to the image component shuffling step. Since, proposed method used a single quantization table; therefore, for chrominance table, the edges in the recovered images are smudged for smaller block sizes. For a quantitative analysis and better understanding, the following subsection presents image quality and datarate differences using BD-measures.



(a) (b) (c) (d) (e)

(f) (g) (h) (i) (j)

(k) (l) (m) (n) (o)

(A)

(a) (b) (c) (d) (e)

(f) (g) (h) (i) (j)

(k) (l) (m) (n) (o)

(B)

Fig. 3. Visual quality analysis of images recovered from PE methods. (a) The original image. (b) Image recovered from the plain image. (c-f) Images recovered from the Color-CPE method with block sizes (16 × 16, 8 × 8, 4 × 4, and 2 × 2), respectively. (g-i) Images recovered from IIB-CPE method. (j-l) and (m-o) are images recovered from proposed method implemented with luminance and chrominance tables, respectively. The sub-block sizes (8 × 8, 4 × 4, and 2 × 2) were used in (g, j, m), (h, k, n) and (i, l, o), respectively. The boxed region in each image is zoomed in and shown on its right side. The JPEG quality factor is 70 in (A) and 100 in (B).

3.2 Compression Analysis

For compression performance analysis of our proposed method, Fig. 4. plots the rate distortion (RD) curves for compression savings calculated as bitrate and the MS-SSIM quality of the recovered images. The RD curves were computed for the JPEG quality factor in the range of [70, 100] and standard quantization tables were used. The chroma subsampling ratio was set to 4:2:0. The 'JPEG-Only' curve is the JPEG compression of plain images, 'IIB-CPE' implements the baseline PE method proposed in [9] that incorporates sub-block processing, and 'Proposed_Lum' and 'Proposed_Chr' implement our proposed method with luminance and chrominance quantization tables, respectively. During encryption, the block size used was (16 × 16) and sub-block sizes used were (8 × 8), (4 × 4) and (2 × 2) for the IIB-CPE and proposed

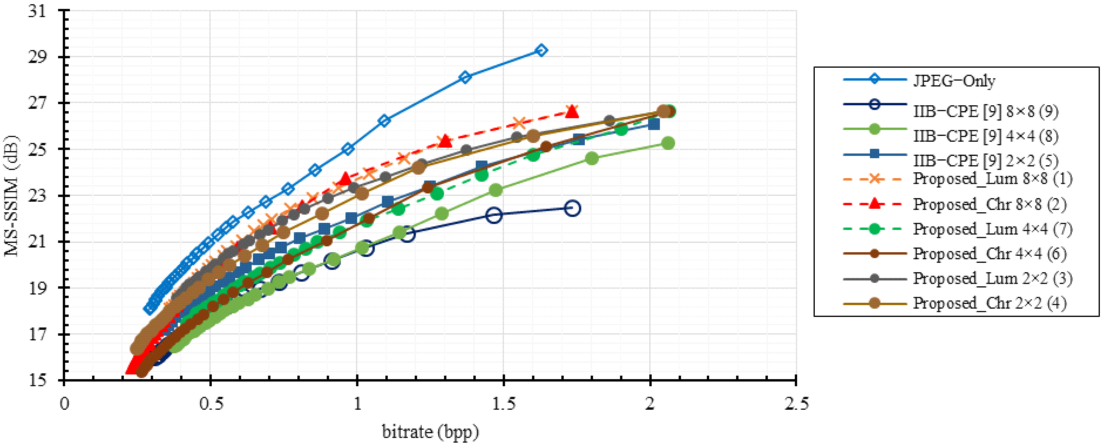


Fig. 4. Rate distortion curves for the compression performance analysis. Each method is ranked based on BD-measures presented in Fig. 5. The rank is given in the legend as a number enclosed in brackets.

methods.

Fig. 5. quantitatively compares the RD curves by using the BD difference metrics that is, rate and quality differences. The BD rate measures a percentage difference between two bitrates for an equivalent image quality, while the BD quality measures an average quality difference (dB) between two RD curves for the equivalent bandwidth. The MS-SSIM values for nearly identical quality images lie closer on the curve; therefore, the MS-SSIM (M) score is $-10\log_{10}(1-M)$, as suggested in [9]. Compared to IIB-CPE method, the proposed method reduced the datarate difference by 87% at maximum (Proposed_Lum 8 × 8) and 18% at minimum (Proposed_Chr 2 × 2). In addition, the choice of quantization table has a negligible effect on the compression savings of proposed method implemented with larger sub-block sizes; however, for smaller sub-block size (2 × 2) compression with the luminance quantization table offered 8% better datarate than the chrominance quantization table.

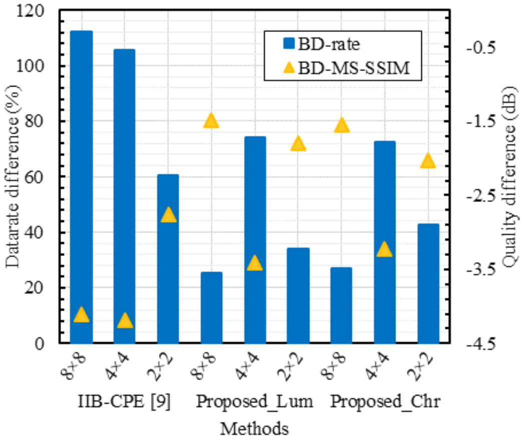


Fig. 5. Performance of the JPEG compression standard on PE methods implemented with different block sizes in terms of BD measures. The rate differences are for the equivalent quality relative to the JPEG under MS-SSIM for RD curves plotted in Fig. 4.

Besides comparison with IIB-CPE technique in Fig. 5., we compared our proposed scheme with the PE techniques proposed in [3] and [8] in-terms of BD rate differences. Though these schemes preserve the JPEG compression savings for larger block sizes (such as 16 × 16 in [3] and 8 × 8 in [8]), their performances drastically degrade on smaller block sizes. For smaller block sizes, the PE scheme proposed in [3] cannot satisfy the bitrate requirements to deliver the same quality image as that of the plain image while [8]'s scheme requires 352% and 549% more bitrate than the compression of plain images for block sizes 4 × 4 and 2 × 2, respectively.

3.3 Encryption Analysis

PE belongs to a class of symmetric key algorithm and consists of four secret keys as: permutation key K_1, rotation-inversion transformation key K_2, negative‐positive transformation key K_3, and color-component shuffling key K_4. For a PE algorithm, the key-space $\mathcal{K} = \{K_1, K_2, K_3, K_4\}$ is the set of all aforementioned keys whose size depends on the chosen block size. The number of blocks N in a color image $I^{H\times W\times C}$, where $H\times W$ pixels in C color channels is the image size, is given by

$$N=\frac{W}{B}\times\frac{H}{B}, \tag{3}$$

where B is the chosen block size. For the sub-block processing, the number of sub-blocks n in a block $B^{B\times B\times C}$ of size $B^2\times C$ pixels are given by

$$n=\frac{B}{b}\times\frac{B}{b}, \tag{4}$$

where b is the chosen sub-block size. The missing term C in (3) and (4) shows that a common key is used to process the color components in blocks and sub-blocks, respectively. The keyspace $\mathcal{K}_{[3]}$ of Color-CPE scheme is given as

$$\begin{gathered}\mathcal{K}_{[3]}=\{\boldsymbol{K}_{1,[3]},\boldsymbol{K}_{2,[3]},\boldsymbol{K}_{3,[3]},\boldsymbol{K}_{4,[3]}\},\\ |\mathcal{K}_{[3]}|=N!\cdot 8^N\cdot 2^N\cdot 6^N.\end{gathered} \tag{5}$$

The keyspace $\mathcal{K}_{[9]}$ of IIB - CPE scheme is given as

$$\begin{gathered}\mathcal{K}_{[9]}=\{\boldsymbol{K}_{1,[9]},\boldsymbol{K}_{2,[9]},\boldsymbol{K}_{3,[9]},\boldsymbol{K}_{4,[9]}\},\\ |\mathcal{K}_{[9]}|=N!\cdot(8^N\cdot 8^n)\cdot 2^N\cdot 6^N.\end{gathered} \tag{6}$$

The keyspace $\mathcal{K}_{pro}$ for proposed method can be derived as

$$\begin{gathered}\mathcal{K}_{pro}=\{\boldsymbol{K}_{1,pro},\boldsymbol{K}_{2,pro},\boldsymbol{K}_{3,pro},\mathcal{K}_{4,pro}\},\\ |\mathcal{K}_{pro}|=N!\cdot(8^N\cdot 8^n)\cdot 2^N\cdot(6^N\cdot 4^N).\end{gathered} \tag{7}$$

When the sub-block processing is incorporated as in (6) and (7) then the key size is increased by a factor of 8^f compared to $\mathcal{K}_{[3]}$, which processes an entire block during encryption. This increment depends on the chosen sub-block size as $n\in\{8^2, 4^2, 2^2\}$ the factor becomes $8^f\in\{8^{4n}, 8^{16n}, 8^{64n}\}$, respectively. In addition, $\mathcal{K}_4$ in (7) is the set of two keys: color shuffling key and the luminance component sub-block selection key. Therefore, the key size of proposed method is increased by a factor of 4^N compared to [9].

Table 2. Analysis of PE techniques robustness against the jigsaw puzzle solver attack.

PE Methods	**D$_c$**	**N$_c$**	**L$_c$**
[3] (16 × 16)	0.01	0.11	0.12
[8] (8 × 8)	0.001	0.001	0.002
[9] (8 × 8)	0.01	0.08	0.02
[9] (4 × 4)	0.01	0.05	0.02
[9] (2 × 2)	0.01	0.06	0.02
Proposed (8 × 8)	0.01	0.08	0.02
Proposed (4 × 4)	0.01	0.05	0.02
Proposed (2 × 2)	0.01	0.06	0.02

D$_c$: direct comparison, **N$_c$**: neighbor comparison, and **L$_c$**: largest component comparison.

Block-based PE methods are vulnerable against a ciphertext-only attack known as jigsaw puzzle solver (JPS) attack, which treats each block of the cipher image as a jigsaw puzzle piece and tries to reconstruct the original image as a whole or partially. The robustness of a PE method against JPS attack can be quantified in-terms of three measures [9]: direct comparison (**D$_c$**) measure that gives the ratio of blocks in the correct position, neighbor comparison (**N$_c$**) measure that gives the ratio of correctly joined pairwise blocks and largest component comparison (**L$_c$**) measure that gives the ratio of the largest joined blocks that have correct neighbors in a component. A smaller value of each metric indicates better robustness of a PE scheme against the JPS attack. Table 2. summarizes robustness analysis of our proposed scheme against JPS attack in comparison with the conventional PE techniques. It can be seen that techniques that use smaller block size have better resistance against the JPS attack because they reduce the efficiency of the JPS compatibility function.

3.4 Discussion

The proposed method mitigated the compatibility issue with the JPEG lossy standard of the conventional sub-block-based PE method [9]. However, the main limitation of our proposed method is the associated computational cost with performing chroma up- and sub-sampling twice. For example, in our proposed color transformation function, a luminance component that is shuffled with either of the chrominance components is up-sampled which undergoes sub-sampling during compression as explained in subsection 2.3. Therefore, this incurred an additional cost of performing color sampling twice.

Ⅳ. Conclusions and Future Work

In this paper, we proposed a color transformation function for PE methods that jointly performed image component shuffling and chroma subsampling functions. The proposed method adopts sub-block level processing to change the orientation of a block for better security and to preserve the correlation among adjacent pixels. The main advantage of our scheme is a better tradeoff between compression savings and encryption efficiency for photo-storage and photo-sharing applications.

The notable application of the conventional PE methods is privacy-preserving deep learning. Therefore, implementing our proposed method for such an application could be an interesting research direction.

References

[1] I. Ahmad and S. Shin, “A novel hybrid image encryption-compression scheme by combining chaos theory and number theory,” *Signal Process. Image Commun.*, vol. 98, p. 116418, Oct. 2021. (http://dx.doi.org/10.1016/j.image.2021.116418)

[2] B. Carpentieri, “Efficient compression and encryption for digital data transmission,” *Secur. Commun. Netw.*, vol. 2018, pp. 1-9, 2018. (http://dx.doi.org/10.1155/2018/9591768)

[3] K. Kurihara, S. Shiota, and H. Kiya, “An encryption-then-compression system for JPEG standard,” in *2015 IEEE Picture Coding Symp. (PCS)*, pp. 119-123, Cairns, Australia, May 2015. (http://dx.doi.org/10.1109/PCS.2015.7170059)

[4] G. K. Wallace, “The JPEG still picture compression standard,” *IEEE Trans. Consum. Electron.*, vol. 38, no. 1, pp. xviii-xxxiv, Feb. 1992. (http://dx.doi.org/10.1109/30.125072)

[5] I. Ahmad and S. Shin, “Perceptual encryption-based privacy-preserving deep learning in internet of things applications,” in *2022 IEEE 13th Int. Conf. ICTC*, pp. 1817-1822, Jeju Island, Korea, Oct. 2022. (http://dx.doi.org/10.1109/ICTC55196.2022.9952589)

[6] H. Kiya, A. P. M. Maung, Y. Kinoshita, S. Imaizumi, and S. Shiota, “An overview of compressible and learnable image transformation with secret key and its applications,” *APSIPA Trans. Signal Inf. Process.*, vol. 11, no. 1, 2022. (http://dx.doi.org/10.1561/116.00000048)

[7] S. Imaizumi and H. Kiya, “A block-permutation-based encryption scheme with independent processing of RGB components,” *IEICE Trans. Inf. Syst.*, vol. E101.D, no. 12, pp. 3150-3157, Dec. 2018. (http://dx.doi.org/10.1587/transinf.2018EDT0002)

[8] W. Sirichotedumrong and H. Kiya, “Grayscale-based block scrambling image encryption using YCbCr color space for encryption-then-compression systems,” *APSIPA Trans. Signal Inf. Process.*, vol. 8, no. 1, 2019. (http://dx.doi.org/10.1017/ATSIP.2018.33)

[9] I. Ahmad and S. Shin, “IIB–CPE: Inter and intra block processing-based compressible perceptual encryption method for privacy-preserving deep learning,” *Sensors*, vol. 22, no. 20, p. 8074, Oct. 2022. (http://dx.doi.org/10.3390/s22208074)

[10] I. Ahmad, W. Choi, and S. Shin, “Comprehensive analysis of compressible perceptual encryption methods–compression and encryption perspectives,” *Sensors*, vol. 23, no. 8, p. 4057, Apr. 2023. (http://dx.doi.org/10.3390/s23084057)

[11] R. El Saj, E. Sedgh Gooya, A. Alfalou, and M. Khalil, “Privacy-preserving deep neural network methods: Computational and perceptual methods–An overview,” *Electr.*, vol. 10, no. 11, p. 1367, Jun. 2021.

(http://dx.doi.org/10.3390/electronics10111367)

[12] I. Ahmad and S. Shin, "Perceptual image encryption: A communication perspective," in *2024 IEEE ICOIN*, pp. 660-663, Ho Chi Minh, Vietnam, Jan. 2024.

[13] P. Li and K. Lo, "Survey on JPEG compatible joint image compression and encryption algorithms," *IET Signal Process.*, vol. 14, no. 8, pp. 475-488, Oct. 2020. (http://dx.doi.org/10.1049/iet-spr.2019.0276)

[14] I. Ahmad and S. Shin, "Chroma subsampling for sub-block-based perceptual encryption algorithms," in *Proc. Symp. KICS*, pp. 852-853, 2023. [Online] Available: http://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE11667552

[15] G. Bjøntegaard, "Calculation of average PSNR differences between RD-curves," *Comput. Sci., Eng.,* 2001.

[16] N. Asuni and A. Giachetti, "TESTIMAGES: A large-scale archive for testing visual devices and basic image processing algorithms," *Smart Tools Apps Graph.-Eurographics Ital. Chapter Conf.*, p. 8, 2014. (http://dx.doi.org/10.2312/STAG.20141242)

[17] Z. Wang, E. P. Simoncelli, and A. C. Bovik, "Multiscale structural similarity for image quality assessment," in *IEEE The Thrity-Seventh Asilomar Conf. Signals, Syst. & Comput., 2003*, pp. 1398-1402, Pacific Grove, CA, USA, 2003. (http://dx.doi.org/10.1109/ACSSC.2003.1292216)

Ijaz Ahmad

Aug. 2018 : M.S. degree, Chosun University

Aug. 2023 : Ph.D. degree, Chosun University

Jan. 2024~Current : Postdoctoral Researcher, Korea University

<Research Interests> Image encryption and compression, Privacy-preserving deep learning

[ORCID:0000-0002-6022-7413]

Seokjoo Shin

1999 : M.S. degree, Gwangju Institute of Science and Technology

2002 : Ph.D. degree, Gwangju Institute of Science and Technology

2003~Current : Professor, Chosun University

<Research Interests> Wireless communication systems, AI for communication, privacy-preserving machine learning, and network security and privacy

[ORCID:0000-0003-2092-1336]