Perceptual Image Encryption: A Communication Perspective

Ijaz Ahmad
Dept. of Computer Engineering
Chosun University
Gwangju, 61452, Korea
ahmadijaz@chosun.kr

Seokjoo Shin
Dept. of Computer Engineering
Chosun University
Gwangju, 61452, Korea
sjshin@chosun.ac.kr (Corresponding author)

***Abstract*—Due to the popularity of cloud services, privacy sensitive image data is outsourced to avail of third-party owned computation and/or storage resources. In this regard, image encryption is necessary not only to protect identifiable information in them that can lead to privacy concerns, but to protect the data ownership as well. Different from the conventional full image encryption techniques, Perceptual Encryption (PE) algorithm protects only perceivable image contents while leaving its intrinsic characteristics intact to cater for the requirements of multimedia applications. Several techniques (such as the pseudo grayscale representation, processing of each color channel independently, and sub-block processing) have been proposed to achieve an efficient tradeoff between security efficiency and the multimedia application's performance. This study integrates PE algorithms into the source coding block of an orthogonal frequency-division multiplexing (OFDM) system and analyze their performance in terms of the recovered image quality. Specifically, we have considered four PE schemes, and four modulation schemes and two channel models in the OFDM system. Our analyses have shown that PE methods are robust against wireless communication impairments with a slight difference between the quality of recovered images from plain and PE cipher images over a Rayleigh fading channel.**

Keywords—perceptual encryption, OFDM, cloud services, image encryption

I. Introduction

When image data is outsourced to avail third-party owned computational and/or storage services, it is necessary to protect the data not only during transmission but during storage and computation as well. Encryption is a process of obfuscating the data by adding randomness to it to protect the data form unauthorized access. The conventional number theory and chaos theory-based image encryption techniques are proven to be the most secure options; however, in multimedia applications such as privacy-preserving computation or photo storage services, where format-compatibility is a requirement, these methods are inadequate. In this regard, Perceptual Encryption (PE) schemes have been proposed that protect human perceivable image contents while preserving image intrinsic properties. These schemes trade security to enable other requirements of multimedia applications such as format-compatibility and low computational complexity. A comprehensive survey on PE methods can be found in [1], [2], their best practices have been implemented in [3] and their privacy-preserving applications are summarized in [4].

The core idea of PE algorithms is to partition an image into nonoverlapping blocks, and to protect the image global contents, perform some color and geometric transformations on these blocks. Such block transformation functions protect an image perceivable information while preserving image intrinsic characteristics within a block, for example, spatial correlation among the adjacent pixels. These characteristics can be exploited to enable several applications such as, format-compatible compression for photo sharing/archiving, reversible data-hiding systems, content-based image retrieval and privacy-preserving deep learning. PE schemes belong to a symmetric-key algorithms thus, requires the same secret key during the decryption of cipher-images that have been used in the encryption of plain-images. In general, PE methods have a tradeoff between compression savings and encryption efficiency due to the choice of block size, and there are several practices that have been proposed to efficiently manage this tradeoff [3]. For example, for larger size keyspace, process each color channel independently or perform sub-block-level processing, and to allow smaller block size during encryption represent an input true color image as pseudo grayscale image.

In this paper, we adopt four PE methods in the source coding block of an orthogonal frequency-division multiplexing (OFDM) -based system and discuss the robustness of PE methods against wireless communication impairments. Specifically, we have considered four PE methods, and four modulation schemes and two channel models in the OFDM system. A related work to current study is presented in [5] that deals with the performance of conventional number theory and chaos theory-based full image encryption techniques under the influence of wireless communication impairments. Several studies have investigated image transmission over OFDM communication systems under various factors, such as different modulation schemes, channel models, modes of OFDM and varying number of antennas as summarized in [6]. However, they do not consider encryption in the source coding. In [7], the authors have investigated a pixel-based PE method in machine learning-based image communication system.

The rest of the paper is summarized as follows: Section 2 provides an overview and preliminary details of the PE methods, Section 3 discusses their performance analysis and Section 4 concludes the paper.

II. Perceptual Image Encryption

In PE schemes, there are two geometric transformation functions: *block permutation* that shuffles block positions, and *block rotation-inversion* function that changes block orientations; and two-color transformation functions: *color channel shuffling,* and *negative-positive transformation* functions that modify pixel values and alter image intensity distribution. The secret key of a PE scheme is the set of all these randomly generated keys that controls each of these

979-8-3503-3094-6/24/$31.00 ©2024 IEEE

transformation functions. The size of this key depends on the chosen block and/or sub-block size, and whether a common key is used to process each of the color components. PE belongs to a class of symmetric-key algorithms and the same secret key is used for the encryption and decryption of plain and cipher images, respectively.

For an image $\boldsymbol{I}^{H,W,C}$, whose dimensions are specified as H rows, W columns, and C color channels, a block-based PE algorithm consists of the following steps:

1. Divide the image $\boldsymbol{I}^{H,W,C}$ into $L \times M$ blocks where $L = H/N$ and $M = W/N$. Each block has N^2 pixels and C color components.
2. Scramble the block locations in the image using a randomly generated key $\boldsymbol{\mathcal{K}}_1$. Each entry of the key represents a new location of a block in the shuffled image.
3. Change each block orientation in the scrambled image using key $\boldsymbol{\mathcal{K}}_2$. Each entry of the key represents rotation and inversion axis.
4. Apply negative–positive transformation to randomly chosen blocks using a uniformly distributed binary key $\boldsymbol{\mathcal{K}}_3$. The modified value of pixel $p_{j,k}$ in the i^{th} block is given as:

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

here $\acute{p}_{j,k}$ $(j, k = 1, \ldots, N)$ is the modified value of pixel $p_{j,k}$ and $\boldsymbol{\mathcal{K}}_3(i)$ is the i^{th} element of the key.

5. Shuffle color channel in each block using a key K_4. The entries in this key K_4 represents a unique permutation of the image color components.

The PE methods can be categorized based on their input representation technique: methods that represent the input as a true color image and methods that represent the input as a pseudo grayscale image. In the first category, Color-PE methods [8] use the same key to process each color component as, $\boldsymbol{\mathcal{K}}_i = \{\boldsymbol{K}_i^R, \boldsymbol{K}_i^G, \boldsymbol{K}_i^B\}$, where $\boldsymbol{K}_i^R = \boldsymbol{K}_i^G = \boldsymbol{K}_i^B$ and $i = \{1,2,3\}$ encryption step, and R is the red, G is the green and B is the blue color channels. A straightforward extension of Color-PE methods is Extended-PE [9] methods that process each color component independently by using a different key for each one of them, such as $\boldsymbol{\mathcal{K}}_i = \{\boldsymbol{K}_i^R, \boldsymbol{K}_i^G, \boldsymbol{K}_i^B\}$ where $\boldsymbol{K}_i^R \neq \boldsymbol{K}_i^G \neq \boldsymbol{K}_i^B$. This processing alters the spatial information within and across each color channel efficiently; however, this results in format-compatibility issues. An alternative approach is IIB-PE [10], that adopts sub-block-level processing in one or more than one steps of the encryption while processing each color component in a similar way. For sub-block processing, a block $\boldsymbol{B}^{N,N}$ where $N = P \times Q$ denotes the number of rows and columns, can be further divided into P^2 sub–blocks and each with $SN \times SN$ pixels. When sub-block processing is integrated in Step 3 then the correlation is preserved; however, they are incompatible with the JPEG lossy standard.

In the second category, PGS-PE methods [11] deals with the format-compatibility and color sub-sampling issues in the first category. The core idea is to transform an input true color image into a pseudo grayscale image representation by concatenating the chroma components either in vertical or horizontal direction. For an input image $\boldsymbol{I}^{H,W,C}$, its three components $\boldsymbol{R}^{H,W}$, $\boldsymbol{G}^{H,W}$, and $\boldsymbol{B}^{H,W}$ are concatenated either in vertical direction to create an image $\boldsymbol{I}^{(H\times C),W}$ or in horizontal direction to create an image $\boldsymbol{I}^{H,(W\times C)}$. The main advantages of these schemes are that the chroma subsampling can be completed prior to encryption and since the image is represented in grayscale, a small block size can be used during encryption for improved security. Similar to grayscale image encryption, the final step of color channel shuffling is omitted in the PGS-PE scheme.

In a basic form, PE methods process each color channel with the same key. However, when more security is desirable (for example, a larger key space and/or to disrupt the color information), then these schemes can be extended: *to process each color component independently (Extended-PE)* [9], *introduce sub-block-level processing (IIB-PE)* [10], and *represent an input as a pseudo grayscale image (PGS-PE)* [11]. Based on the requirements of an application a suitable PE method can be adopted [3]. For example, PGS-PE can be used in format-compatible image compression for photo storage/sharing services, Extended-PE is suitable for reversible data-hiding applications, and Color-PE and IIB-PE are viable schemes for image processing applications in the encrypted domain, examples include content-based image retrieval and privacy-preserving machine learning.

For a PE algorithm, the number of blocks in an image is $B = L \times M \times C$, and when a block $\boldsymbol{B}$ is divided into sub-blocks for sub-block-level processing, the number of sub blocks $SB = P^2 \times B \times C$. The keyspace for each PE method, which depends on the number of blocks, can be derived as:

For Color-PE, the key size is

$$\boldsymbol{\mathcal{K}}_{C-PE} = (B/3)! \cdot 8^{B/3} \cdot 2^{B/3} \cdot 6^{B/3}. \tag{2}$$

Similarly, for Extended-PE, the key size is

$$\boldsymbol{\mathcal{K}}_{E-PE} = B! \cdot 8^{B} \cdot 2^{B} \cdot 6^{B}. \tag{3}$$

For IIB-PE, the key size is

$$\boldsymbol{\mathcal{K}}_{I-PE} = (B/3)! \cdot \left(8^{B/3} \cdot 8^{SB/3}\right) \cdot 2^{B/3} \cdot 6^{B/3}. \tag{4}$$

Finally, for PGS-PE, the key size is

$$\boldsymbol{\mathcal{K}}_{P-PE} = 4B! \cdot 8^{4B} \cdot 2^{4B}. \tag{5}$$

The $B/3$ term in (2) and (4) shows that the color components were processed with the same key, the $8^{SB/3}$ term in (4) shows that sub-block processing was integrated in Step 3, and the term $4B$ in (5) shows that a block size of (8 × 8) was used instead of (16 × 16). Overall, the key size relation of PE methods is $\boldsymbol{\mathcal{K}}_{P-PE} \gg \boldsymbol{\mathcal{K}}_{E-PE} \gg \boldsymbol{\mathcal{K}}_{I-PE} > \boldsymbol{\mathcal{K}}_{C-PE}$.

III. Results and Discussion

This section presents robustness analysis of PE methods against communication impairments. In the simulations, we have used the color images of resolution 512 × 512 from the

TABLE I. Summary the simulation parameters used in the communication system.

Parameters	Values
Modulation techniques	BPSK, QPSK, 8PSK, 32QAM
Transform	FFT
Channel Model	AWGN, Rayleigh fading
Channel estimation	Least Square Error
IFFT/FFT length	64
CP length	16 samples

USC–SIPI Miscellaneous dataset [12]. The simulation parameters for the wireless image communication system are summarized in Table 1. In our analysis, the image quality was compared using peak signal-to-noise ratio (PSNR) and multiscale structural similarity index measure (MS-SSIM) [13]. The block size used was 16×16 in Color-PE and Extended-PE methods, and 8×8 in the PGS-PE method. For IIB-PE, the block size used was 16×16 and sub-block processing with block size 8×8 was implemented in Step 3.

A. Image Visual Quality Analysis

Fig. 1. shows an example plain image and its cipher images along with their corresponding decrypted images obtained from different PE methods discussed in Section 2. Here, decryption was applied in the original cipher images without being transmitted. Since, the encryption process itself is lossless the images are recovered without any degradations. Examples for visual inspection of plain-images recovered from their corresponding cipher images transmitted over different communication systems are shown in Fig. 2. for AWGN channel and Fig. 3. for Rayleigh fading channel. For both channel models, it can be observed that the image quality degrades with the modulation order because in higher order schemes, the distance between the constellation points decreases thus the error margin increases.

B. Image Quality Analysis

In general, a bit error ratio is used to quantify the quality of the received signal regardless of its contents; however, it does not provide an indication of the image quality. Therefore, in our analysis, the image quality was quantified using PSNR and MS-SSIM. The MS-SSIM value M was transformed as $-10 \times \log_{10}(1-M)$. For the AWGN channel in Fig. 4. (a) and (b) there is no difference between images recovered from plain and cipher images in terms of the PSNR and MS-SSIM, respectively. On the other hand, when the cipher images were transmitted over a Rayleigh fading channel then there is a slight difference between the images recovered from plain and cipher images as shown in Fig. 4. (c) and (d).

IV. Conclusion

In this study, we analyzed the performance of a class of image encryption algorithms called perceptual encryption methods under the influence of a wireless communication system's impairments. The main advantages of PE-based image encryption algorithms are the format compatibility and low computational overhead while providing a necessary level of security. Our analyses showed that the images recovered from plain and cipher-images have the same quality when transmitted over AWGN channel while there is a slight difference in quality when transmitted over Rayleigh fading channel. The robustness of PE methods against the communication impairments can be attributed to the lack of diffusion mechanism in them.

Acknowledgment

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

References

[1] 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, doi: 10.1561/116.00000048.

[2] 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, doi: 10.1049/iet-spr.2019.0276.

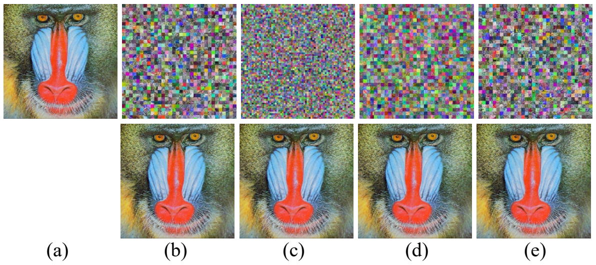

Fig.1. Image encryption and decryption using PE schemes. (a) is a plain image and (b) – (e) are cipher images (top row) along with decrypted images (bottom row) obtained from Color-PE, PGS-PE, Extended-PE and IIB-PE schemes, respectively. In (c) the cipher-image of PGS-PE method is generated by transforming the pseudo grayscale image to color image.

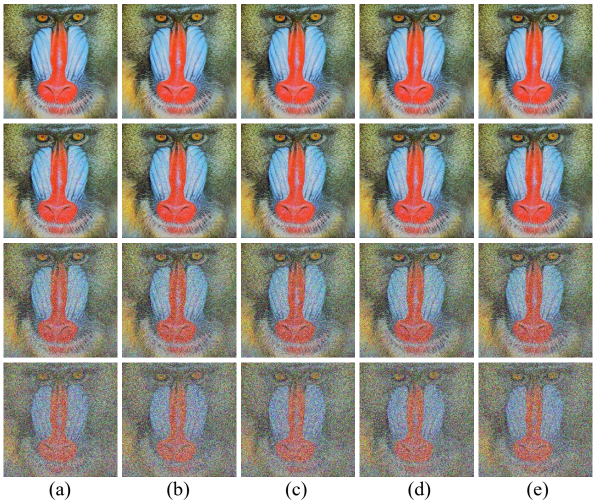

Fig.2. An example image transmitted over the AWGN channel with SNR=5 dB. The modulation schemes used are BPSK (1st row), QPSK (2nd row), 8-PSK (3rd row) and 32-QAM (4th row). The images in (a) – (e) are recovered from the images in the top row of Fig. 1. (a) – (e), respectively.

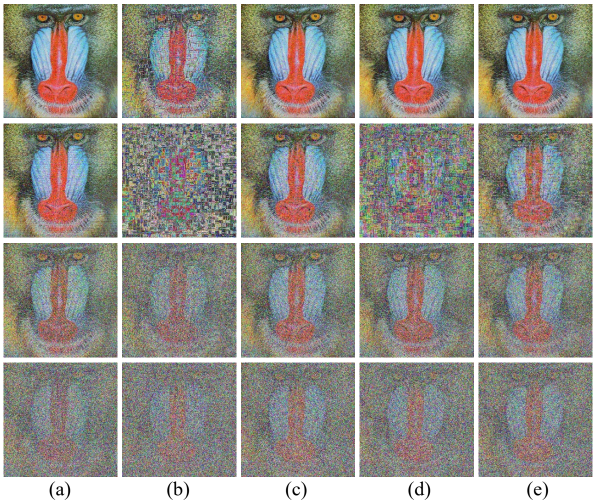

Fig.3. An example image transmitted over Rayleigh fading channel with SNR=5 dB. The modulation schemes used are BPSK (1st row), QPSK (2nd row), 8-PSK (3rd row) and 32-QAM (4th row). The images in (a) – (e) are recovered from the images in the top row of Fig. 1. (a) – (e), respectively.

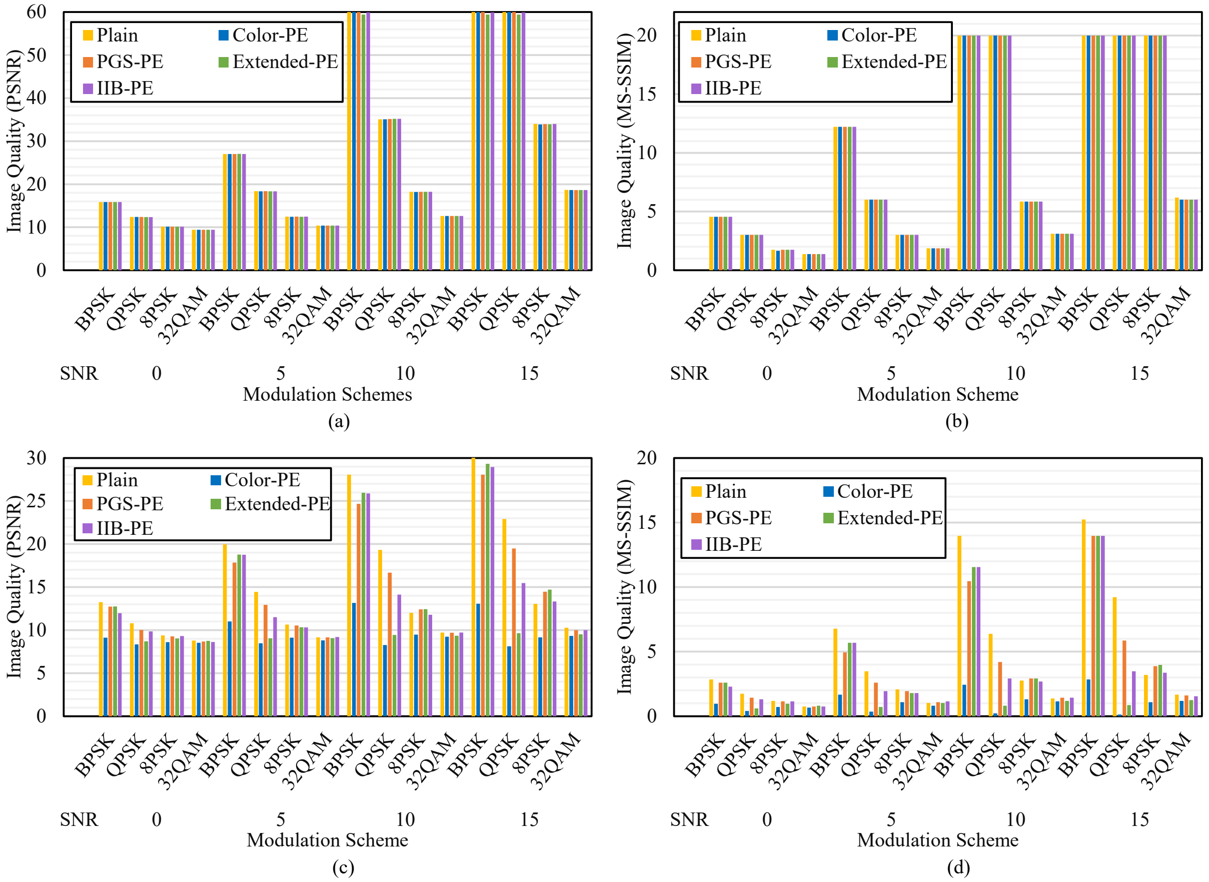

Fig. 4. Recovered image quality analysis with respect to different image quality metrics. In (a) and (b) images are transmitted over AWGN channel, while in (c) and (d) images are transmitted over Rayleigh fading channel.

[3] 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, doi: 10.3390/s23084057.

[4] R. El Saj, E. Sedgh Gooya, A. Alfalou, and M. Khalil, "Privacy-Preserving Deep Neural Network Methods: Computational and Perceptual Methods—An Overview," *Electronics*, vol. 10, no. 11, p. 1367, Jun. 2021, doi: 10.3390/electronics10111367.

[5] F. E. Abd el-Samie *et al.*, *Image encryption a communication perspective*. Boca Raton [Florida: CRC Press, 2014.

[6] L. Kansal, S. Berra, M. Mounir, R. Miglani, R. Dinis, and K. Rabie, "Performance Analysis of Massive MIMO-OFDM System Incorporated with Various Transforms for Image Communication in 5G Systems," *Electronics*, vol. 11, no. 4, p. 621, Feb. 2022, doi: 10.3390/electronics11040621.

[7] J. Xu, B. Ai, W. Chen, A. Yang, and P. Sun, "Image Encryption Methods in Deep Joint Source Channel Coding: A Review and Performance Evaluation," in *2021 7th International Conference on Computer and Communications (ICCC)*, Chengdu, China: IEEE, Dec. 2021, pp. 240–244. doi: 10.1109/ICCC54389.2021.9674532.

[8] K. Kurihara, S. Shiota, and H. Kiya, "An encryption-then-compression system for JPEG standard," in *2015 Picture Coding Symposium (PCS)*, Cairns, Australia: IEEE, May 2015, pp. 119–123. doi: 10.1109/PCS.2015.7170059.

[9] 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, doi: 10.1587/transinf.2018EDT0002.

[10] 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, doi: 10.3390/s22208074.

[11] T. Chuman, W. Sirichotedumrong, and H. Kiya, "Encryption-Then-Compression Systems Using Grayscale-Based Image Encryption for JPEG Images," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 6, pp. 1515–1525, Jun. 2019, doi: 10.1109/TIFS.2018.2881677.

[12] "SIPI Image Database - Misc." Accessed: Jul. 04, 2022. [Online]. Available: https://sipi.usc.edu/database/database.php?volume=misc

[13] Z. Wang, E. P. Simoncelli, and A. C. Bovik, "Multiscale structural similarity for image quality assessment," in *The Thrity-Seventh Asilomar Conference on Signals, Systems & Computers, 2003*, Pacific Grove, CA, USA: IEEE, 2003, pp. 1398–1402. doi: 10.1109/ACSSC.2003.1292216.