Journal of the Optical Society of Korea
Vol. 17, No. 5, October 2013, pp. 384-391
DOI: http://dx.doi.org/10.3807/JOSK.2013.17.5.384

Optical Image Split-encryption Based on Object Plane for Completely Removing the Silhouette Problem

Weina Li[1], Anh-Hoang Phan[1], Seok-Hee Jeon[2], and Nam Kim[1]*

[1]Department of Information & Communication Engineering, Chungbuk National University, 410 SungBong-ro, Heungduk-gu, Cheongju 361-763, Korea
[2]Department of Electronics Engineering, Incheon National University, 12-1 Songdo-dong, Yeonsu-gu, Incheon 406-772, Korea

(Received June 21, 2013 : revised September 9, 2013 : accepted September 24, 2013)

We propose a split-encryption scheme on converting original images to multiple ciphertexts. This conversion introduces one random phase-only function (POF) to influence phase distribution of the preliminary ciphertexts. In the encryption process, the original image is mathematically split into two POFs. Then, they are modulated on a spatial light modulator one after another. And subsequently two final ciphertexts are generated by utilizing two-step phase-shifting interferometry. In the decryption process, a high-quality reconstructed image with relative error $RE = 7.6061 \times 10^{-31}$ can be achieved only when the summation of the two ciphertexts is Fresnel-transformed to the reconstructed plane. During the verification process, any silhouette information was invisible in the two reconstructed images from different single ciphertexts. Both of the two single REs are more than 0.6, which is better than in previous research. Moreover, this proposed scheme works well with gray images.

Keywords : Split-encryption, Ciphertext, Silhouette problem, Phase-shifting interferometry
OCIS codes : (090.1995) Digital holography; (050.5080) Phase shift; (120.3180) Interferometry; (060.4785) Optical security and encryption

I. INTRODUCTION

With the development of computer calculations and network connections, more and more threats and attacks are generated in information communication systems. Optical information security has attracted a lot of attention, which offers primarily two types of benefits; the first is an inherent capability for parallel and rapid processing, and the second is a concealment in any of several dimensions, such as phase or spatial frequency [1]. Optical systems have an excellent capability to encode information. In general, there are three main classes of cryptography for implementing optical image encryption. The first is encrypting an image to one stationary white noise-like ciphertext utilizing an encryption key. The second is multiple-image encryption (MIE) which encrypts multiple images to one ciphertext by taking advantage of different encryption keys. The double random phase encoding (DRPE) method and the iterative phase-retrieval algorithm are extensively utilized in both of those encryption methods. In this paper we call the third one (encrypting one image into multiple ciphertexts) split-encryption (SE) for simplicity.

Encryption utilizing the DRPE method includes both symmetric and asymmetric cryptographic algorithms because the decryption key could be identical to or the conjugate with the encryption key. Two random phase-only functions (POFs) are utilized in this method. The first POF improves the signal of a charge-coupled device (CCD), and the second POF is the encryption key in the system [2]. However, when the complex conjugate of the information obtained in the frequency domain is considered as the ciphertext, the decryption key must be identical to the second random POF so-called symmetric cryptography. When the information obtained in the frequency domain is considered as the ciphertext, the decryption key has to be the conjugate of the second random POF-asymmetric cryptography. Indeed, the DRPE method is used in different

*Corresponding author: namkim@chungbuk.ac.kr
Color versions of one or more of the figures in this paper are available online.

interferometries and transforms to implement optical information security. Refregier and Javidi first suggested the DRPE method [3] that has been exhaustively developed in recent decades. As phase-shifting interferometry is developed, Lee and Gil applied the DRPE method to four-step phase-shifting interferometry for implementing optical encryption [4]. Shen *et al.* applied the DRPE method to three-step phase shifting interferometry to implement optical encryption [5]. Jeon and Gil applied DRPE to two-step phase-shifting interferometry to accomplish optical encryption [6]. Moreover, it is also employed in the information-hiding technique [7] and watermarking [8]. The encrypted optical field can be transmitted electronically. But DRPE cryptography is vulnerable to attack if the second phase-only function in the encrypted processing is obtained.

MIE encrypts several images into one single ciphertext. This encryption technique can hide more information, so it is more complicated. Meanwhile, most algorithms are time-consuming. The biggest problem is crosstalk, which means how to reconstruct every single image in high quality from the only one single ciphertext. Because of this, MIE is more suitable for binary images than gray images. Shi *et al.* employed cascade phase retrieval algorithms to hide three different images together in the Fresnel domain [9]. He *et al.* proposed an MIE scheme to encrypt two objects into one ciphertext by utilizing DRPE and phase-shifting methods [10]. The crosstalk problem was depressed by thresholding and binarization. Situ and Zhang introduced the wavelength multiplexing technique into a double random-phase encoding system to encrypt multiple images [11]. Liu and Liu proposed an encryption scheme, which simultaneously encrypts two images into a single image by fractional Fourier transform with different fractional orders [12]. Liu *et al.* proposed a novel MIE method to overcome the crosstalk problem, which is to abandon all high frequencies of the four ciphertexts and crop them to a quarter of the original size. They subsequently combined the four new quarter-size ciphertexts into one new original-size ciphertext by placing them into each quadrant [13]. Chang *et al.* proposed a novel wavelength-multiplexing algorithm based on the cascaded phase-only function architecture and that scheme significantly reduced the crosstalk problem [14].

Optical image split-encryption has been growing rapidly since Zhang and Wang suggested it for the first time [15]. The authors modulated the optical field in the Fresnel domain to two phase-only masks (POMs) to be allocated to two authorized users. In the decryption processing, if and only if the authorized users get together, the reconstructed image can be obtained by an inverse Fresnel transform. Unlike DRPE, the SE scheme does not need an explicit key for the ciphertext. In the SE scheme, one ciphertext also plays a role of the key of another ciphertext. Similarly, unlike MIE, the SE scheme does not introduce any time-consuming iterative phase-retrieval methods. Therefore, the SE scheme is more efficient and more convenient to manipulate. But there is a serious silhouette problem in the SE scheme. The silhouette information of the original image is visible (when reconstructed) in both of the two POMs. Addressing this issue, Wang and Zhao introduced a third random POM for effectively eliminating the silhouette problem [16], but this scheme only focused on removing the silhouette problem when reconstructing a single POM. If the product of two specific POMs is reconstructed, the silhouette information will become visible. Kumar *et al.* inserted a chaotic algorithm jigsaw transform to postprocessing of the two POMs [17], which can also effectively solve the silhouette problem. Even though the number of encrypted images is less than the last scheme, it also involves first inverse jigsaw transform and then inverse Fresnel transform in the decryption processing, which is the inverse manipulation of the encryption procedure, and both encryption and decryption require one extra transform. It is complicated and not distinctive. All of the above papers concentrated on the Fresnel domain. Jia *et al.* proposed cryptography based on the object plane to convert the original image to two phase-only functions via manipulation [18]. This can remove the silhouette problem as well. Nevertheless, it is only suitable for binary images, and cannot work on gray images.

In this paper, we propose an optical image split-encryption scheme to overcome the flaws enumerated in all the papers above. During the encryption process, the original image uses a random phase-only function introduced to influence phase distribution of the preliminary ciphertexts. Then we obtain a new complex original image and convert it to two phase-only functions that are the preliminary ciphertexts. Next, the optical fields of these two phase-only functions can be obtained by taking advantage of a two-step phase-shifting method. These two encrypted optical fields cooperate with each other to reconstruct the original image. This proposed scheme requires no extra iterative algorithms, chaotic algorithms and random POMs in the Fresnel domain. It can be applied not only to a binary image but also to a gray image. The most important characteristic is utilizing only two ciphertexts to completely eliminate the silhouette problem.

The principles of the proposed optical image split-encryption are introduced in Section 2. In Section 3, computer simulation is described to demonstrate the feasibility of the proposed SE scheme. Error analysis is described in Section 4. Concluding comments are shown in Section 5.

II. PRINCIPLES OF THE PROPOSED OPTICAL IMAGE SPLIT-ENCRYPTION

Fresnel transforms are based on Fourier transforms, and Fourier transforms obey the distributive law, so Fresnel transforms also obey the distributive law. This induces the proposed encryption scheme, whereby $f(x_0, y_0)$ is assumed to be the original image (real-valued data), which is

multiplied by a random phase-only function to obtain a new image $obj(x_0, y_0)$, represented mathematically as follows:

$$obj(x_0, y_0) = f(x_0, y_0) \times \exp(i \times 2\pi \times rand(M, N)). \quad (1)$$

where M and N are sampling numbers along the x-axis and y-axis of the original image. The purpose of $rand(M, N)$ is to generate an $M \times N$ random matrix distributed from 0 to 1. Throughout the remainder of this paper, the coordinates (x_0, y_0), (u, v) and (x, y) represent the object plane, frequency plane and reconstructed plane, respectively. The essential purpose of the random POF introduced in Eq. (1) is to widen the dynamic range of the phase in the two POFs, $P_1(x_0, y_0)$ and $P_2(x_0, y_0)$. The amplitudes of these two POFs are the constant 1. The rest of the required equations are as follows:

$$obj\_in(x_0, y_0) = abs(obj(x_0, y_0)), \quad (2)$$

$$obj\_phase(x_0, y_0) = \arg(obj(x_0, y_0)), \quad (3)$$

$$P_1(x_0, y_0) = \exp(i \times (obj\_phase(x_0, y_0) - \arccos(\frac{obj\_in(x_0, y_0)}{2}))), \quad (4)$$

$$P_2(x_0, y_0) = \exp(i \times (obj\_phase(x_0, y_0) + \arccos(\frac{obj\_in(x_0, y_0)}{2}))), \quad (5)$$

$$obj(x_0, y_0) = P_1(x_0, y_0) + P_2(x_0, y_0). \quad (6)$$

where $obj\_in(x_0, y_0)$, and $obj\_phase(x_0, y_0)$ denote the intensity and phase of $obj(x_0, y_0)$, respectively. $P_1(x_0, y_0)$ and $P_2(x_0, y_0)$ are essentially two split POFs that will be modulated on the spatial light modulator, and $abs()$ and $\arg()$ denote the modulus and phase, respectively, of the new image $obj(x_0, y_0)$. Therefore, the new image $obj(x_0, y_0)$ consists of $P_1(x_0, y_0)$ and $P_2(x_0, y_0)$.

The ideal encryption system can approach both encryption and decryption manipulations in an optical manner, but just one process could be implemented optically. Most researchers investigate decryption optically owing to restrictions such as component limitations and difficulty in optical setup configuration, etc. We adopt optical encryption to obtain the final ciphertexts $O\_P_1(u, v)$ and $O\_P_2(u, v)$ in this proposed scheme. Intensity-sensitive devices, such as CCD cameras, can only capture the intensity portion and cannot capture the phase portion of an optical field. Therefore, two-step phase-shifting interferometry is needed to calculate the phase portion and subsequently accomplish the encryption manipulation of the proposed scheme. The schematic diagram of the setup is depicted in Fig. 1.

The mathematical expressions of the encryption process are described as follows:

$$O\_P_1(u, v) = FrT\{P_1(x_0, y_0)\} = A_{P1} \times \exp(i\varphi_{P1}), \quad (7)$$

$$\begin{aligned} I_{P11} &= (O\_P_1(u, v) + r) \times (O\_P_1(u, v) + r)^* \\ &= A_{P1}^2 + R^2 + A_{P1} \times R \times [\exp(i(\varphi_r - \varphi_{P1})) \\ &\quad + \exp(-i(\varphi_r - \varphi_{P1}))] \\ &= A_{P1}^2 + R^2 + 2A_{P1} \times R \times \cos(\varphi_{P1}), \end{aligned} \quad (8)$$

$$I_{P12} = A_{P1}^2 + R^2 - 2A_{P1} \times R \times \sin(\varphi_{P1}), \quad (9)$$

$$O\_P_1(u, v) = (I_{P11} - DC_{P1}) + i \times (I_{P12} - DC_{P1}), \quad (10)$$

$$O\_P_2(u, v) = FrT\{P_2(x_0, y_0)\} = A_{P2} \exp(i\varphi_{P2}), \quad (11)$$

$$I_{P21} = A_{P2}^2 + R^2 + 2A_{P2} \times R \times \cos(\varphi_{P2}), \quad (12)$$

$$I_{P22} = A_{P2}^2 + R^2 - 2A_{P2} \times R \times \sin(\varphi_{P2}), \quad (13)$$

$$O\_P_2(u, v) = (I_{P21} - DC_{P2}) + i \times (I_{P22} - DC_{P2}). \quad (14)$$

where FrT denotes the Fresnel transform (Note: $*$ represents the complex conjugate). According to Euler's formula $\cos\theta = [\exp(i\theta) + \exp(-i\theta)]/2$, we can obtain the result of Eq. (8). In addition, the more mathematical information is introduced specifically by Goodman [19]. A_{P1}, A_{P2} and φ_{P1}, φ_{P2} are assumed to be amplitudes and phases of $O\_P_1(u, v)$ and $O\_P_2(u, v)$, respectively. Assume the reference beam $r = R \times \exp(i * \varphi_r)$, where R represents the constant amplitude and φ_r represents the constant phase. Then the quarter waveplate is tilted by $\pi/2$ and the second hologram I_{P12} is captured. According to Eq. (10) we can calculate $O\_P_1(u, v)$. DC_{P1} in Eq. (10) denotes the zero-order light of the hologram generated from $P_1(x_0, y_0)$, which consists of A_{P1}^2 and R^2 ($DC_{P1} = A_{P1}^2 + R^2$). DC_{P2} in Eq. (14) denotes the zero-order light of the hologram

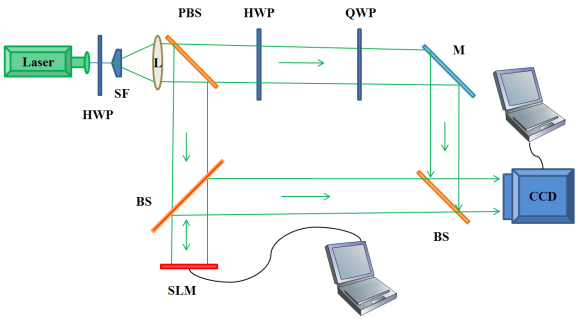


FIG. 1. Schematic diagram of the setup about two-step phase-shifting method. L: lens, M: mirror, SF: spatial filter, BS: beam splitter, PBS: polarizing beam splitter, HWP: half waveplate, QWP: quarter waveplate, SLM: spatial light modulator.

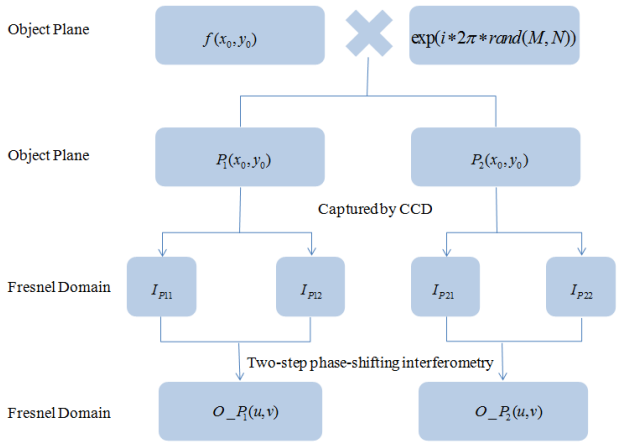


FIG. 2. Flow chart for the encryption procedure of the proposed method.

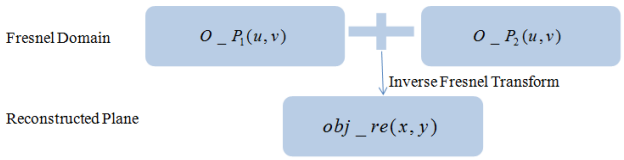


FIG. 3. Flow chart for decryption in the proposed method.

generated from $P_2(x_0,y_0)$, which is presented as $DC_{P2} = A_{P2}{}^2 + R^2$. It was introduced specifically by Shen *et al.* [5]. And $O\_P_2(u,v)$ generated from $P_2(x_0,y_0)$, can be calculated in the identical manner. For the sake of simplicity, we assume the phase of the reference beam in the Fresnel domain φ_r is 0. The encryption flow chart is depicted in Fig. 2.

Here, the optical fields $O\_P_1(u,v)$ and $O\_P_2(u,v)$ that are generated from POFs $P_1(x_0,y_0)$ and $P_2(x_0,y_0)$ can be obtained from the above process. Therefore,

$$obj\_re(x,y) = IFrT\{O\_P_1(u,v) + O\_P_2(u,v)\}. \quad (15)$$

where $IFrT$ denotes the inverse Fresnel transform. The intensity of $obj\_re(x,y)$ is technically the reconstructed image.

The decryption flow chart represented in Eq. (15) is depicted in Fig. 3.

III. COMPUTER SIMULATION WORK

The feasibility of the proposed scheme was verified with a 256×256 grayscale Baboon image (Fig. 4). The phase portions of the two POFs are depicted in Fig. 5(a) and Fig. 6(a), respectively.

No silhouette information of the original image can be seen in Fig. 5(c), which is the reconstructed image generated from $O\_P_1(u,v)$ in the analog. In addition, no silhouette information of the original image can be seen in Fig. 6(c),

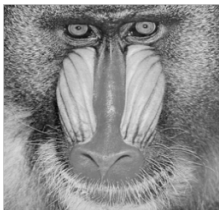
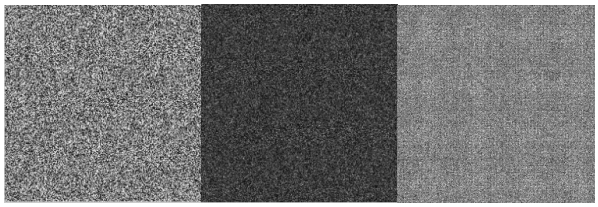
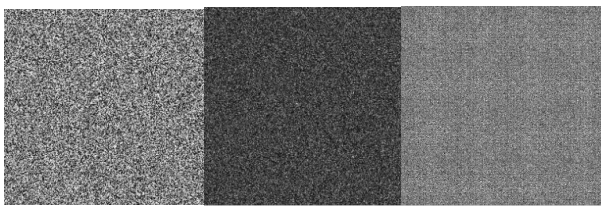


FIG. 4. Original Baboon image (256×256).



(a) (b) (c)

FIG. 5. (a) Phase of $P_1(x_0,y_0)$, (b) Single ciphertext $O\_P_1(u,v)$, and (c) Reconstructed image from single ciphertext $O\_P_1(u,v)$.



(a) (b) (c)

FIG. 6. (a) Phase of $P_2(x_0,y_0)$, (b) Single ciphertext $O\_P_2(u,v)$, and (c) Reconstructed image from single ciphertext $O\_P_2(u,v)$.

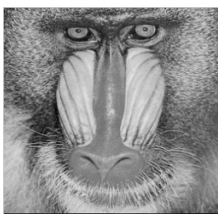


FIG. 7. Decrypted image from summation of Fig. 5(b) and Fig. 6(b).

which is generated from $O\_P_2(u,v)$ in the analog. If and only if optical fields of $O\_P_1(u,v)$ and $O\_P_2(u,v)$ are added together, can the original image be reconstructed. Fig. 7 shows the reconstructed image, decrypted correctly, looks nearly identical to the original image (shown in Fig. 4).

Relative error (RE) is introduced as the criterion of the reconstructed image's quality and is expressed as follows [15]:

$$RE = \frac{\sum_{m=1}^{M}\sum_{n=1}^{N}(R(m,n)-O(m,n))^2}{\sum_{m=1}^{M}\sum_{n=1}^{N}O(m,n)^2}. \quad (16)$$

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

FIG. 8. (a) Original Lena image (256×256), (b) Product of POF1 and POF3, (c) Reconstructed image from the product of POF1 and POF3, (d) Product of POF2 and POF3, (e) Reconstructed image from the product of POF2 and POF3.

where $R(m,n)$ denotes the intensity of the reconstructed image and $O(m,n)$ denotes the original image. We see that RE is smaller, and the gray-scale value of the reconstructed image is closer to the original image in terms of Eq. (16). This also means the higher the RE value of the single reconstructed image, the more irrelevant between the original image and the reconstructed image. However, when $RE > 0.2$, theoretically, one cannot distinguish the decrypted image with the naked eye [15].

The RE of the recovered image shown in Fig. 7 is 7.6061×10^{-31}. The recovered image generated from a single ciphertext is shown in Fig. 5(c) and 6(c). The RE values are both 0.6854. The two RE values are much more than 0.2, and the silhouette information is totally invisible.

For comparison, the method of Wang and Zhao [16] was simulated again for this paper. Some of the results are shown in Fig. 8.

They introduced a random POF to split the complex amplitude of the optical field into POF1, POF2 and POF3; the RE value of the three images reconstructed from those three POFs is around 0.4. Silhouette information is invisible in the three reconstructed images, which have RE values that are still lower than our RE values of the single ciphertext. And the silhouette problem appears when reconstructing the product of the specific two ciphertexts, as seen in Fig. 8(c) and (e). The RE values of Fig. 8(c) and (e) are 0.1567 and 0.1898, respectively, both of which are less than 0.2; therefore, the silhouette problem shows up.

IV. ERROR ANALYSIS

A digital hologram recorded on a CCD is quantized with 256 levels. So a gray-level error on CCD camera pixels can be generated due to a small intensity variation, which is the so-called quantization error [2]. If there is no error, the decryption equation expression should be like Eq. (7), Eq. (11) and Eq. (15). However, the error appears when the CCD camera captures the optical field $O\_P_1(u,v)$ and $O\_P_2(u,v)$. This will introduce two amplitude errors and two phase errors, which are mathematically presented in the following equations:

$$O\_P1_{real} = (A_{P1} + E_{P1}) \times \exp(i(\varphi_{P1} + e_{P1})), \tag{17}$$

$$O\_P2_{real} = (A_{P2} + E_{P2}) \times \exp(i(\varphi_{P2} + e_{P2})), \tag{18}$$

$$obj\_re_{real} = IFrT\{O\_P1_{real} + O\_P2_{real}\}. \tag{19}$$

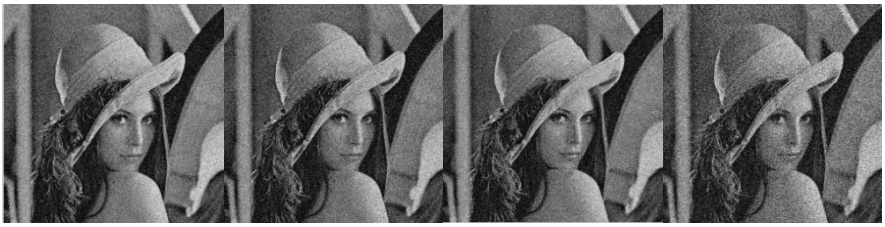
Where O_P1_{real} and O_P2_{real} denote the real calculated encrypted optical fields, respectively. E_{P1} stands for the amplitude error distributed from 0 to 255, and e_{P1} stands for the phase error distributed from $-\pi$ to π, which probably both appear in the encrypted optical field $O\_P_1(u,v)$. E_{P2} and e_{P2} are the amplitude error and the phase error, which appear in the encrypted optical field $O\_P_2(u,v)$. E_{P1}, e_{P1}, E_{P2}, and e_{P2} will introduce the white noise into the decrypted image. However, A_{P1} and A_{P2} are not distributed in the range [0, 255]; they should first be reset in [0,255].

The purpose of the error analysis is to calculate what amplitude error range (AER) and phase error range (PER) the reconstructed image can tolerate for the naked eye. First, a toleration criterion should be determined. The different RE value and the corresponding reconstructed images are depicted as follows, where we calculated many different images. The results of the 256×256 grayscale image Lena and the 256×256 grayscale image Baboon are depicted in this paper for the investigation of the tolerated boundary RE value.

All of the images depicted in Fig. 9 are the reconstructed images from the optical fields with amplitude errors or phase errors, or both. For example, the RE value is equivalent to 0.0116 in Fig. 9(a). The RE value is equivalent to 0.0811 in Fig. 9(h). The noise increases from Fig. 9(a) to (h). Still acceptable to the naked eye is Fig. 9(g), although the dimension of the noise has increased; the image quality worsens in Fig. 9(h). In addition, all of the attached images are 43% of the original size. Therefore, the noise in Fig. 9(h) cannot be tolerated.

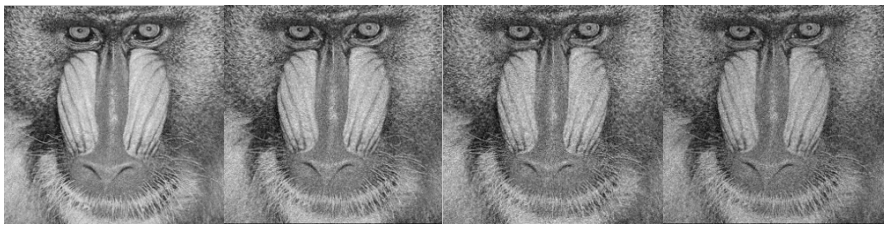
The results in Fig. 10 are similar to those in Fig. 9. The noise is acceptable to the naked eye from Fig. 10(a) to (f). However, the noise increases suddenly between Fig. 10(g) and (h), as seen in the nose of the Baboon images. Therefore, RE=0.07 is determined as a boundary criterion. The other

(a) $RE = 0.0116$ (b) $RE = 0.0208$ (c) $RE = 0.0330$ (d) $RE = 0.0400$

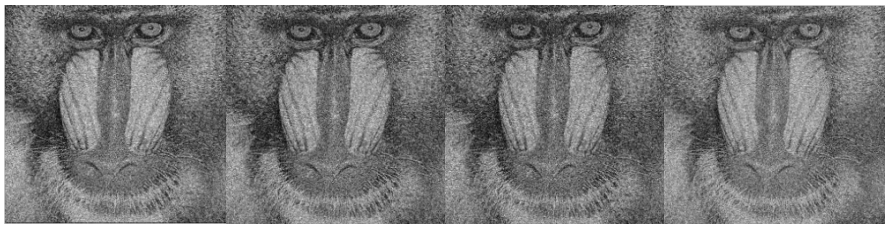


(e) $RE = 0.0503$ (f) $RE = 0.0637$ (g) $RE = 0.0693$ (h) $RE = 0.0811$

FIG. 9. Reconstructed Lena images with different RE values.



(a) $RE = 0.0084$ (b) $RE = 0.0199$ (c) $RE = 0.0317$ (d) $RE = 0.0423$



(e) $RE = 0.0508$ (f) $RE = 0.0601$ (g) $RE = 0.0730$ (h) $RE = 0.0848$

FIG. 10. Reconstructed Baboon images with different RE values.

verified images also give uniform results.

Here, the Lena and Baboon images are both utilized to analyze the AER and PER with $RE < 0.07$. However, only the curve graphs of the Baboon image are included in this paper.

In Fig. 11, the full black line represents the threshold line $RE = 0.07$. AE means amplitude error, and O_P1, O_P2 stand for single ciphertext $O\_P_1(u,v)$ and single ciphertext $O\_P_2(u,v)$, respectively. The red line with circles represents errors that only happened in the amplitude portion of $O\_P_1(u,v)$, which shows the tolerated AER is [-22.5, 22.5] with $RE < 0.07$. The blue line with dots represents errors that only happened in the amplitude portion of $O\_P_2(u,v)$, which shows the tolerated AER is [-24, 24] with $RE < 0.07$. The magenta line with asterisks represents errors that happened in the amplitude portion of

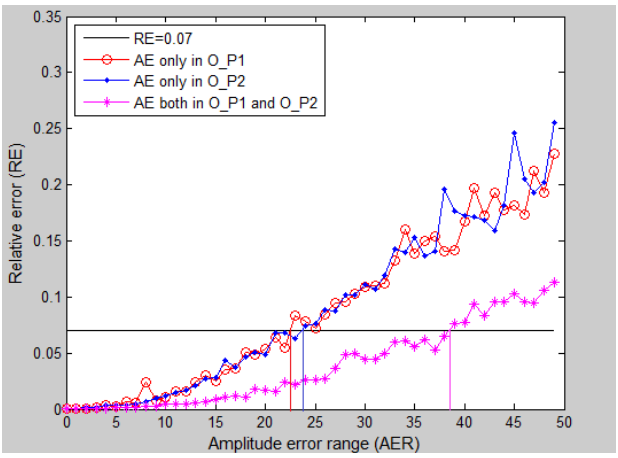


FIG. 11. RE curves along with the variations of AER in a single ciphertext or both of the two ciphertexts.

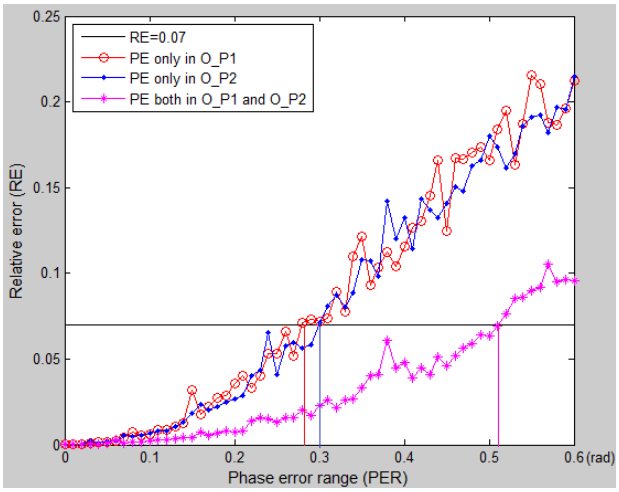


FIG. 12. RE curves along with the variations of PER in a single ciphertext or both of the two ciphertexts.

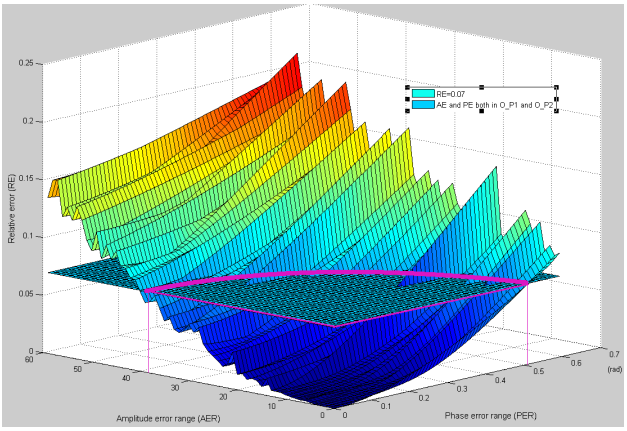


FIG. 13. RE curves along with the variations of AER and PER in both of the two ciphertexts.

both $O\_P_1(u,v)$ and $O\_P_2(u,v)$, which shows the tolerated AER extends to [-38, 38] with $RE < 0.07$.

In Fig. 12, the full black line represents the threshold line $RE = 0.07$. Phase error (PE) is in rads. O_P1, O_P2 represent single ciphertext $O\_P_1(u,v)$ and single ciphertext $O\_P_2(u,v)$, respectively. The red line with circles represents errors that only happened in the phase portion of $O\_P_1(u,v)$, which shows the tolerated PER is [-0.28, 0.28] with $RE < 0.07$. The blue line with dots represents errors that only happened in the phase portion of $O\_P_2(u,v)$, which shows the tolerated PER is [-0.3, 0.3] on condition $RE < 0.07$. The magenta line with asterisks represents errors that happened in both phase portions of $O\_P_1(u,v)$ and $O\_P_2(u,v)$, which shows the tolerated AER extends to [-0.52, 0.52] with $RE < 0.07$.

In Fig. 13, the plane represents the threshold plane $RE = 0.07$. The curved surface represent the PE and AE that happen in both $O\_P_1(u,v)$ and $O\_P_2(u,v)$. When these four kinds of errors happen at the same time, the tolerated PER and AER form a closed area surrounded by the closed magenta line.

TABLE 1. Tolerated AER and PER of the 256×256 grayscale Baboon image

Baboon256.bmp	PER of O_P1	PER of O_P2	AER of O_P1	AER of O_P2
RE<0.07	[-0.28, 0.28]	[-0.3, 0.3]	[-22.5, 22.5]	[-24, 24]
RE<0.07	[-0.52, 0.52]		[-38, 38]	
RE<0.07	[-0.51, 0.51][-38,38]			

TABLE 2. Tolerated PER and AER of the 256×256 grayscale image of Lena

Lena256.bmp	PER of O_P1	PER of O_P2	AER of O_P1	AER of O_P2
RE<0.07	[-0.24, 0.24]	[-0.25, 0.25]	[-18, 18]	[-17, 17]
RE<0.07	[-0.48, 0.48]		[-28, 28]	
RE<0.07	[-0.49, 0.49] [-28,28]			

The data in Table 1 illustrate Fig. 11, Fig. 12, and Fig. 13. It is worthwhile to note that the maximum AER and PER are taken from Fig. 13, assuming there is no influence from other different categories of errors. In these three figures, the last point not exceeding the black line is taken into account. In addition, although the RE curves increase tortuously as AER or PER expands, the shapes of the curves rise steadily in the long term.

We conducted the same process with the Lena image, and the results are depicted in Table 2. According to Table 1, Table 2 and other data not listed in this paper, different images have different tolerated PERs and AERs. However, if both of the phase errors of the optical field work together, the tolerated PER will increase to almost twice that seen when PE happens in a single optical field. If both of the amplitude errors (AEs) of the optical field work together, the tolerated AER will increase to almost twice when AE happens in single ciphertext. It means the PE in $O\_P_1(u,v)$ and PE in $O\_P_2(u,v)$ influence each other in a promotive way, as does AE in $O\_P_1(u,v)$ and AE in $O\_P_2(u,v)$. However, if the four kinds of errors happen at the same time, the phase error and the amplitude error influence each other antagonistically, as seen from the thick magenta line in Fig. 13.

V. CONCLUSION

The proposed optical image split-encryption scheme focuses on the optical information encryption for converting original plaintext to multiple ciphertexts. It requires no complicated iterative algorithms or chaotic transforms. Moreover, fewer phase-only functions need to be split. It can be applied to gray images, and introduces only one random POF for influencing subsequent encryption. The encryption procedure is to split the original image into two

POFs mathematically, subsequently obtain two authorized ciphertexts generated from those two POFs by taking advantage of a two-step phase-shifting method. The original image can be reconstructed with an extremely small relative error $RE = 7.6061 \times 10^{-31}$, if and only if these two ciphertexts are combined. During the verification process, no silhouette information can be seen with the naked eye in either reconstructed image generated from a single POF. In addition, both RE values of the reconstructed image generated from a single POF are around 0.68, which is much better than previous SE schemes. We also demonstrate that solo phase errors or amplitude errors in two ciphertexts can influence each other in a promotive way, but when the four kinds of errors happen at the same time, PE and AE influence each other antagonistically.

ACKNOWLEDGMENT

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MEST) (2012-0009225), and this work was also partly supported by the IT R&D program of MSIP/ MOTIE/KEIT. [10039169, Development of Core Technologies for Digital Holographic 3-D Display and Printing System]

REFERENCES

1. T. V. Vu, N. Kim, J. An, and S. Hong, "Experimental demonstration of kinogram-based single-phase decryption technique for information security," Appl. Opt. **46**, 7662-7669 (2007).
2. S. H. Jeon and S. K. Gil, "2-step phase-shifting digital holographic optical encryption and error analysis," J. Opt. Soc. Korea **15**, 244-251 (2011).
3. P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. **20**, 767-769 (1995).
4. H. J. Lee and S. K. Gil, "Error analysis for optical security by means of 4-step phase-shifting digital holography," J. Opt. Soc. Korea **10**, 118-123 (2006).
5. L. Shen, J. Li, and H. Chang, "Double-image encryption based on joint transform correlation and phase-shifting interferometry," Chinese Opt. Lett. **5**, 687-689 (2007).
6. J. P. Liu and T. C. Poon, "Two-step-only quadrature phase-shifting digital holography," Opt. Lett. **34**, 250-252 (2009).
7. S. Kishk and B. Javidi, "Information hiding technique with double phase encoding," Appl. Opt. **41**, 5462-5470 (2002).
8. S. Kishk and B. Javidi, "Watermarking of three-dimensional objects by digital holography," Opt. Lett. **28**, 167-169 (2003).
9. Y. Shi, G. Situ, and J. Zhang, "Multiple-image hiding in the Fresnel domain," Opt. Lett. **32**, 1914-1916 (2007).
10. M. Z. He, L. Z. Cai, Q. Liu, X. C. Wang, and X. F. Meng, "Multiple image encryption and watermarking by random phase matching," Opt. Commun. **247**, 29-37 (2005).
11. G. Situ and J. Zhang, "Multiple-image encryption by wavelength multiplexing," Opt. Lett. **30**, 1306-1308 (2005).
12. Z. Liu and S. Liu, "Double image encryption based on iterative fractional Fourier transform," Opt. Commun. **275**, 324-329 (2007).
13. Z. Liu, Y. Zhang, H. Zhao, M. A. Ahmad, and S. Liu, "Optical multi-image encryption based on frequency shift," Optik **122**, 1010-1013 (2011).
14. H. T. Chang, H. E. Hwang, C. L. Lee, and M. T. Lee, "Wavelength multiplexing multiple-image encryption using cascaded phase-only masks in the Fresnel transform domain," Appl. Opt. **50**, 710-716 (2011).
15. Y. Zhang and B. Wang, "Optical image encryption based on interference," Opt. Lett. **33**, 2443-2445 (2008).
16. X. Wang and D. Zhao, "Optical image hiding with silhouette removal based on the optical interference principle," Appl. Opt. **51**, 686-691 (2012).
17. P. Kumar, J. Joseph, and K. Singh, "Optical image encryption using a jigsaw transform for silhouette removal in interference-based methods and decryption with a single spatial light modulator," Appl. Opt. **50**, 1805-1811 (2011).
18. W. Jia, F. J. Wen, Y. T. Chow, and C. Zhou, "Binary image encryption based on interference of two phase-only masks," Appl. Opt. **51**, 5253-5258 (2012).
19. J. W. Goodman, *Introduction to Fourier Optics*, 2nd ed. (McGraw-Hill, San Francisco, CA, USA, 1996).