Current Optics and Photonics
Vol. 2, No. 4, August 2018, pp. 368-377

ISSN: 2508-7266(Print) / ISSN: 2508-7274(Online)
DOI: https://doi.org/10.3807/COPP.2018.2.4.368

Avalanche and Bit Independence Properties of Photon-counting Double Random Phase Encoding in Gyrator Domain

Jieun Lee[1], Nishat Sultana[2], Faliu Yi[3], and Inkyu Moon[4]*

[1]*Division of IT Convergence Engineering, Hansung University, Seoul 02876, Korea*
[2]*Department of Computer Engineering, Chosun University, Gwangju 61452, Korea*
[3]*Department of Clinical Science, University of Texas Southwestern Medical Center, Dallas 75390, USA*
[4]*Department of Robotics Engineering, DGIST, Daegu 42988, Korea*

(Received May 1, 2018 : revised July 2, 2018 : accepted July 4, 2018)

In this paper, we evaluate cryptographic properties of a double random phase encoding (DRPE) scheme in the discrete Gyrator domain with avalanche and bit independence criterions. DRPE in the discrete Gyrator domain is reported to have higher security than traditional DRPE in the Fourier domain because the rotation angle involved in the Gyrator transform is viewed as additional secret keys. However, our numerical experimental results demonstrate that the DRPE in the discrete Gyrator domain has an excellent bit independence feature but does not possess a good avalanche effect property and hence needs to be improved to satisfy with acceptable avalanche effect that would be robust against statistical-based cryptanalysis. We compare our results with the avalanche and bit independence criterion (BIC) performances of the conventional DRPE scheme, and improve the avalanche effect of DRPE in the discrete Gyrator domain by integrating a photon counting imaging technique. Although the Gyrator transform-based image cryptosystem has been studied, to the best of our knowledge, this is the first report on a cryptographic evaluation of discrete Gyrator transform with avalanche and bit independence criterions.

Keywords : Double random phase encoding, Discrete Gyrator transform, Optical security, Photon counting imaging, Avalanche and bit independence criterion
OCIS codes : (200.3050) Information processing; (060.4785) Optical security and encryption; (100.4998) Pattern recognition, optical security and encryption

I. INTRODUCTION

Development of reliable encryption techniques or cryptosystems is of great interest among scientists to help restore some trust to digital images by converting plaintext into ciphertext before transmitting the data through an insecure communication channel [1, 2]. Among many of these techniques, data encryption standard (DES), advanced encryption standard (AES), Rivest-Shamir-Adelman (RSA) and elliptic curve cryptosystems (ECC) are the most commonly used platforms. Concurrently, to analyze the encryption algorithms, several cryptographic attack methods have been contrived. For example, brute force attacks, meet-in-the-middle attacks, linear cryptanalysis and differential cryptanalysis. The former two focus on the length of the key. In contrast, the linear cryptanalysis and differential cryptanalysis depends on the statistical analysis of the plaintext and the encryption key. To make the cipher algorithm robust against the statistical attacks, avalanche effect and bit independence criterion are the two most important properties to take into account first. Avalanche effect is a characteristic in which a slight change in an input produces significant change in the output. A cryptanalyst can make predictions about the input, being given only the output if a cipher algorithm does not show good avalanche effect. Bit independence criterion is a test of randomness of a cryptographic encryption algorithm. It is not possible to infer one value in the sequence from the others if it is

*Corresponding author: inkyu.moon@dgist.ac.kr, ORCID 0000-0003-0882-8585
Color versions of one or more of the figures in this paper are available online.

produced by an algorithm that achieves an excellent bit independence criterion. Although digital forgeries may leave no visual traces of tampering, however, such modifications usually perturb the underlying statistics of the original image [1]. Therefore, we can analyze the avalanche and bit independence properties to construct robust image cryptography algorithms because a slight modification in the image would introduce a huge difference in the new message digest. The above-mentioned digital encryption algorithms have acceptable avalanche and bit independence properties [3]. The investigation of these properties in encryption algorithms can be very useful for evaluation of further cryptographic performance.

The optical encryption techniques have a significant role in the image cryptography field as they offer high-speed parallel processing ability, multiple keys and multiple degrees of freedom. The double random phase encoding (DRPE) scheme is a widely used optical encryption technique such that it is useful for image encryption, authentication, information hiding and watermarking [3-8]. It has been implemented in different domains like Fourier, Fresnel, Gyrator domains, and so on [9-11]. Among all these domains, avalanche and bit independence properties were tested for Fourier and Fresnel domains in [12]. As an extension of work [12], we evaluate the avalanche and bit independence properties of the DRPE in the discrete Gyrator domain. Gyrator transform-based image encryption has been widely implemented for single image, double image, multi-image and color [13-18] image encryption. In this domain, a secret image is encrypted applying random operations in image Gyrator transform domains. The DRPE in the Gyrator domain is considered to be more secure than the traditional DRPE technique in the Fourier domain because the rotation angle in the Gyrator transform has greatly increased the key space [19]. Recently, the expression for the Gyrator transform (GT) has been rewritten by using a convolution operation, which is known as discrete Gyrator transform (DGT). In this expression, conventional GT can be expressed using phase-only filtering, Fourier transform and inverse Fourier transform. This expression is regarded as the fast algorithm of discrete Gyrator transform and simple to implement [14, 20]. It has been claimed in [19] that based on the periodicity of the Gyrator transform, the rotation angle in a single Gyrator transform can possibly be obtained approximately by applying exhaustive search with a known-plaintext attack. However, since Gyrator transform is continuous, it is very time consuming to apply thus exhaustive search techniques. Even though there exists some security analysis research about DRPE in the Gyrator domain [6, 21], there is no research about its avalanche effect and bit independence criterion features which are desirable properties of cryptographic algorithms. Therefore, we introduce these properties into an optical encryption algorithm [12] and measure the avalanche and bit independence for DRPE in the Gyrator domain in this paper. Moreover, a photon counting imaging (PCI) technique [22, 23] is integrated into the system of DRPE in the Gyrator domain to improve the avalanche effect characteristic of DRPE in the Gyrator domain, which can enhance the security of the system.

This paper is organized as follows. First, we give an overview of the double random phase encoding in Section 2. Then we show the mathematical modeling of a fast algorithm of discrete Gyrator transform with double random phase masks in Section 3. In Section 4, we shed light on the concept of photon counting imaging. We then describe what the avalanche and bit independence criterion is, in Section 5. In Section 6, we show and discuss our experimental results. Finally, we conclude our discussion in Section 7.

II. DOUBLE RANDOM PHASE ENCODING (DRPE)

Since double random phase encoding (DRPE) was proposed in 1995, it has been studied and implemented vastly in the information security aspect [24, 25]. It was found robust to different types of noise and distortion [3]. The encoded image resulting from two random phase masks is a complex function consisting of phase and amplitude. The pixel values in real and imaginary parts of this complex function are independent stationary white noise data. The phases of the statistically independent

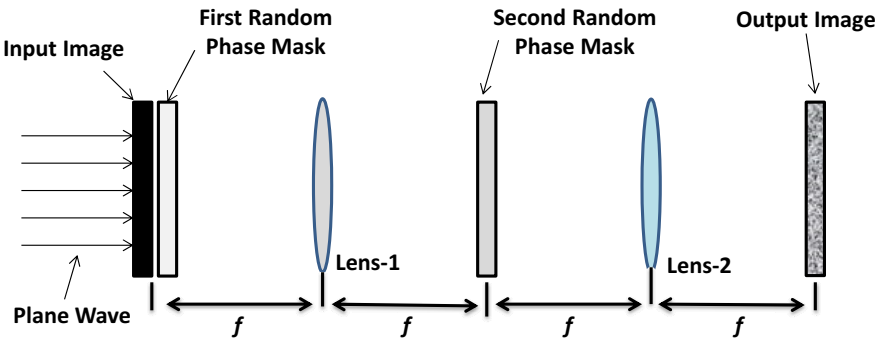

FIG. 1. Schematic diagram of the DRPE in Fourier domain (*f* is the focal length of the lens).

random masks (keys) in the spatial and frequency domains are expressed as exp[$i2\pi n(x, y)$] and exp[$i2\pi b(\mu, v)$] where the random functions $n(x, y)$ and $b(\mu, v)$ are uniformly distributed in the range of [0,1]. The encryption process can be shown with the following equation:

$$f_c(x,y) = \Im^{-1}\left[\Im\left[f(x,y)\exp[i2\pi n(x,y)]\right]\exp[i2\pi b(\mu,v)]\right], \tag{1}$$

where $\Im$ and $\Im^{-1}$ are 2D Fourier and inverse Fourier transforms. The procedure is reversed for the decryption. Figure 1 shows the DRPE schematic in the Fourier domain.

Since DRPE in the Fourier domain has been reported as vulnerable to chosen ciphertext, ciphertext only and known plaintext-ciphertext attacks, many improvements in the conventional DRPE system have taken place afterwards [26-28]. For example, the DRPE system integrated with a photon counting imaging (PCI) technique was proposed by Pérez-Cabré to improve the cryptographic performance of the DRPE system where the photon counting DRPE scheme introduces an additional layer of protection and thus makes the cryptosystem more secured [22, 23].

III. MATHEMATICAL MODELING OF DRPE IN GYRATOR DOMAIN

The Gyrator transform (GT) belongs to the orthosymplectic class of linear canonical transforms as well as to the fractional Fourier transforms, and produces the rotation in twisted position-spatial frequency planes of phase space [29, 30]. For the large range of rotation angles α, GT domain can be constructed with only three generalized lenses with a fixed distance between them [30]. GT expression of a two dimensional function $f_i(\vec{g}_i)$, having rotation angle α, can be defined as:

$$f_o(\vec{g}_o) = G^{\alpha}[f_i(\vec{g}_i)](\vec{g}_o) = \iint f_i(x_i,y_i)K_{\alpha}(x_i,y_i;x_o,y_o)dx_i dy_i = \frac{1}{|\sin\alpha|}\times \iint f_i(x_i,y_i)\left\{\exp\left[i2\pi\frac{(x_o y_o + x_i y_i)\cos\alpha - (x_i y_o + x_o y_i)}{\sin\alpha}\right]\right\}dx_i dy_i, \tag{2}$$

$$K_{\alpha}(x_i,y_i;x_o,y_o) = \frac{1}{|\sin\alpha|}\times\exp\left[i2\pi\frac{(x_o y_o + x_i y_i)\cos\alpha - (x_i y_o + x_o y_i)}{\sin\alpha}\right], \tag{3}$$

where $\alpha = pp/2$, $0 \le \alpha < 2p$, and $0 \le p < 4$. GT is expressed as G^a. $\vec{g}_i$ and $\vec{g}_o$ represents the input and output plane coordinates. In the equation, $K_{\alpha}(x_i,y_i;x_o,y_o)$ is the kernel function of the GT. The Gyrator transform is periodic with $2p$ [17]. For $p = 0$ ($\alpha = 0$), the transform is an identity transform. At $p = 1$ ($\alpha = p/2$), the direct Fourier transform with rotation of the coordinate at $p/2$ is obtained. When $p = 2$ ($\alpha = p$), it corresponds to the reverse transform. For $p = 3$ ($\alpha = 3p/2$), the system resembles the inverse Fourier transform with a rotation of the coordinate by $p/2$. The inverse Gyrator transform corresponds to a Gyrator transform at a rotation angle $-\alpha$ [19, 31].

The Fresnel diffraction integral in the free space under paraxial approximation can be used to calculate the discrete GT. However, if we think about the computational scheme, the computational load would be heavier. The fact that a fast algorithm of discrete GT obtained by simulating the convolution expression of fractional Fourier transform accelerates the application and the validity of the aforementioned algorithm has been proved by numerical simulation in [20]. If we want to construct an image cipher, a fast algorithm is more preferred. Therefore, we follow a fast algorithm of discrete Gyrator transform to design our algorithm. Using the trigonometric equation, $\cot\alpha = -\tan[\frac{\alpha}{2}] + 1\Big/\sin\alpha$, Eq. (3) can be expressed as follows:

$$K_{\alpha}(x_i,y_i;x_o,y_o) = \frac{\exp\left[-i2\pi(x_i y_i + x_o y_o)\tan\frac{\alpha}{2}\right]}{|\sin\alpha|} \times\exp\left[i2\pi\frac{(x_i - x_o)(y_i - y_o)}{\sin\alpha}\right]. \tag{4}$$

Combining Eqs. (2) and (4), the convolution equation of GT can be constructed as follows:

$$f_o(x_o,y_o) = f_g = p_1(x_o,y_o)\left\{\left[f_i(x_i,y_i)\,p_1(x_i,y_i)\right] * p_2(x_i,y_i)\right\}, \tag{5}$$

where the symbol '*' represents the convolution operation. p_1 and p_2 are two phase only masks, which are equal to

$$p_1(x,y) = e^{-i2\pi xy\tan\frac{\alpha}{2}}, \tag{6}$$

$$p_2(x,y) = \frac{e^{i2\pi xy\csc\alpha}}{|\sin\alpha|}. \tag{7}$$

Since we are using two random phase masks $RP1$ and $RP2$ and two different angles α_1 and α_2 as additional phase keys, our new phase masks in the discrete Gyrator domain are as follows:

$$p_1'(x,y) = e^{-i2\pi RP1(x,y)\tan\frac{\alpha_1}{2}}, \tag{8}$$

$$p_2'(x,y) = \frac{e^{i2\pi RP2(x,y)\csc\alpha_2}}{|\sin\alpha_2|}. \tag{9}$$

According to the convolution property of Fourier transforms, Eq. (5) can be written as:

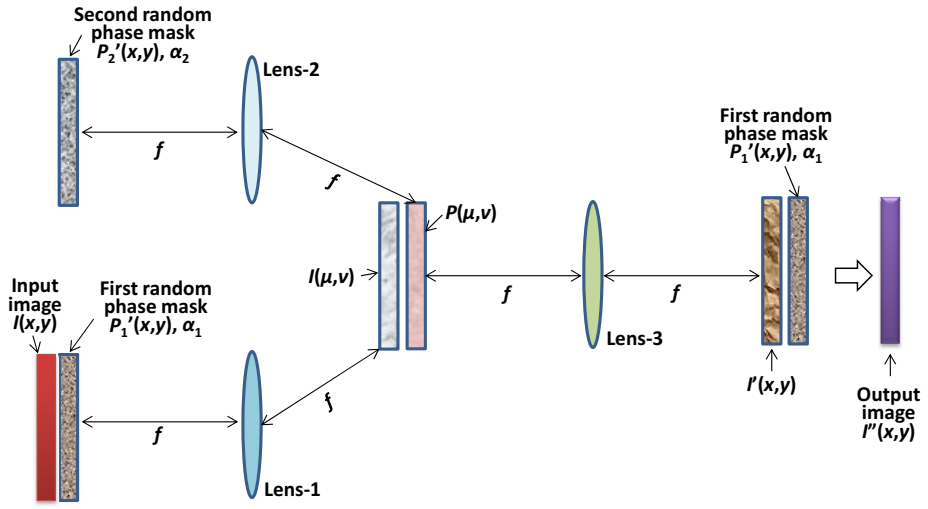

FIG. 2. Schematic diagram of the DRPE in Gyrator domain (f is the focal length of the lens).

$$f_g = p_1'\Im^{-1}\left[\Im\left[p_1' f_i\right]\Im\left[p_2'\right]\right]. \tag{10}$$

We substitute $\Im\left[p_2'\right]$ with P in Eq. (10) and get our final equation of discrete Gyrator transform as follows:

$$f_g = p_1'\Im^{-1}\left[\Im\left[p_1' f_i\right]P\right]. \tag{11}$$

Discrete Gyration transform can be implemented by applying the FFT algorithm twice. Thus the computational speed is much increased [14, 20]. The simple schematic diagram of DRPE in the Gyrator domain is illustrated in Fig. 2. As shown in Fig. 2, the lenses are Fourier optics lenses. $P(\mu,\nu)$ and $I(\mu,\nu)$ denote P and $\Im\left[p_1' f_i\right]$ in Eq. (11), respectively. $I'(\mu,\nu)$ represents $\Im^{-1}\left[\Im\left[p_1' f_i\right]P\right]$ in Eq. (11) and the two plans together in Fig. 2 means the pixel-wise multiplication.

IV. PHOTON COUNTING IMAGING

The photon counting imaging (PCI) technique was invented for low light levels or night vision, situations in which only a limited number of photons can reach the image sensors [5, 22, 23]. PCI has the advantage that, in the entire scene, the number of photons can be limited by controlling the expected number of incident photons. A photon limited image carries less information than that of the original counterpart and hardly reveals the original appearance of the primary image. Thus, such a system improves information authentication robustness against intruder attacks. By generating a sparse encrypted data, it generates a distribution with fewer photons than conventional imaging techniques and also provides a substantial bandwidth reduction [22, 23, 32].

The PCI simulation has the assumption that the probability of counting photons at any arbitrary pixel in a captured image follows a Possion distribution [5]. The Poisson distribution of the probability of counting l_j photons at pixel j is shown by the following equation:

$$Poisson(l_j;\lambda_j) = \frac{[\lambda_j]^{l_j} e^{-\lambda_j}}{l_j!},\ l_j = 0,1,2..., \tag{12}$$

where l_j is the Poisson parameter defined by:

$$\lambda_j = N_p x_j, \tag{13}$$

where N_p is the expected number of incident photons, x_j is the normalized irradiance at pixel j, such that $\sum_{j=1}^{N} x_j = 1$, and N is the total number of pixels in the scene [5].

It has been proved that photon-limited encrypted distributions have sufficient information for successful authentication and retrieval of the signal [22, 23]. Although the signal can be retrieved after decryption, it remains a visually unrecognizable noise-like signal to the receiver because of the sparse representation of the encrypted image. Even though intruders may try to get some information from the decrypted image, they cannot recognize the image by visual inspection [22, 23]. We can draw some conclusions from the previous discussion that the integration of PCI can make the system one-way as the decrypted image will not be visually recognizable and will be useful for image verifications. Therefore, usually the sparse distributed photon limited image obtained by applying PCI is not intended for visualization of the original primary image. Rather, it is intended for the verification of the authenticity of the original image by means of optical correlation.

V. AVALANCHE AND BIT INDEPENDENCE CRITERIONS

The avalanche and bit independence criterions are good cryptographic properties and widely used to design the cryptographic algorithms, especially the block ciphers [33]. When the security of cryptographic systems is analyzed, it is necessary to measure whether the system reaches a certain optimum level of security or not. Cryptographic test methods such as avalanche, strict avalanche and bit independence criteria are of great interest to measure the degree of security of the designed cryptographic networks [34] because the statistical-based cryptanalysis such as linear and differential cryptanalysis are related to these criterions [35]. Therefore, we introduce the avalanche and bit independence properties into an optical domain-based encryption algorithm. If the designed optical encryption algorithms achieve a satisfactory bit independence and avalanche effect, they would be robust against statistical-based cryptanalysis [12] as in the case of block ciphers.

5.1. Avalanche and Strict Avalanche Criterions

In cryptographic function design, avalanche effect is a very well-known heuristic. Although the name of this criterion was first coined by Feistel, the original idea links back to Shannon's notion of diffusion [36]. From the view of an encryption algorithm, an avalanche effect is evident if a small change in the plaintext or key brings a drastically large change in the cipher-text. For encryption, it is a characteristic in which a small change in the message produces a large change in the message digest [37]. The avalanche effect intuitively reflects the idea of high-nonlinearity [38]. If a substantial degree of avalanche effect is not exhibited during the avalanche test, then the designed algorithm has a poor randomization, which would allow a cryptanalyst to make predictions about the input, only from the given output. This weakness of the algorithm may partially or completely break the algorithm [39].

Webster and Tavares proposed the combination of completeness and the avalanche effect as a new criterion called strict avalanche criterion (SAC). It is a generalization of the avalanche effect. The SAC can be satisfied when an average of 50% of the output bits exhibit a change with the change in one input bit [39].

Suppose an encryption process E is represented as $Y = E(X, K)$, where X is the plaintext, K is the encryption key and Y is the ciphertext. If we change the plaintext into X', then after encryption, we obtain the new ciphertext $Y' = E(X', K)$. If we change the key into K', then the ciphertext becomes $Y'' = E(X, K')$. If we consider the Hamming distance between the original ciphertext Y and the ciphertext Y' (which we obtain by encrypting after changing some bits of the original plaintext) is $H(Y, Y')$, then the avalanche effect can be calculated from the following equation:

$$Avalanche = \frac{H(Y, Y')}{Num(Y)}, \tag{14}$$

where $Num(Y)$ denotes the total number of binary bits of the ciphertext. Similarly, the avalanche equation for some big change in the key (K') can be represented by the following equation:

$$Avalanche = \frac{H(Y, Y'')}{Num(Y)}, \tag{15}$$

where $H(Y, Y'')$ is the Hamming distance between the original ciphertext Y and the ciphertext Y'' (with some bits changed in the key).

5.2. Bit Independence Criterion

Bit independence criterion (BIC) was introduced by Webster and Tavares as another property for S-box security. It is a test of randomness of a cryptographic encryption algorithm [38]. If the bit independence criterion is satisfied, then it is not possible to infer one value in the sequence from the others [37]. We measure the degree of independence between a pair of avalanche variables by calculating the correlation coefficient. BIC is satisfied if any change in the single input bit i in the plaintext or in the encryption key results in a change in a way that any two output bits j and k in the ciphertext are changed independently of each other. Suppose there are total N bits in the plaintext and according to BIC, the plaintext can be changed N times when only one bit is flipped at a time. The bit independence (BI) between bits j and k in the ciphertext can be defined using the absolute correlation coefficient as follows:

$$BI\left(C\left(b_j\right), C\left(b_k\right)\right) = \left| corr\left(\left(b_j^1 \ldots, b_j^i \ldots, b_j^N\right), \left(b_k^1 \ldots, b_k^i \ldots, b_k^N\right)\right)\right|, \tag{16}$$

where $C(b_j)$ and $C(b_k)$ connote the j_{th} and k_{th} bits in the ciphertext, and b_j^i and b_k^i denote the values of the j_{th} and k_{th} bits in the ciphertext with change in the i_{th} bit in the plaintext. If the resulting value of Eq. (16) is close to 1, then it reveals strong correlation between two bits. The bit independence criterion implies that each pair of bits in the ciphertext for a given crypto algorithm should be bit independent. Accordingly, the bit independence criterion (BIC) for an encryption algorithm can be demonstrated with the following equation:

$$BIC(E(X, Y)) = \max_{\substack{1 \le j,k \le N \\ j \ne k}} BI\left(C\left(b_j\right), C\left(b_k\right)\right), \tag{17}$$

where $E(X, K)$ connotes the encryption algorithm. If $BIC(E(X, K))$ is far from 1, it demonstrates that the algorithm

satisfies bit independence criterion very well. Conversely, the $BIC(E(X, K))$ value close to 1 means some bit pairs are dependent on each other in the encrypted image [38].

VI. EXPERIMENTAL RESULTS AND ANALYSIS

In this paper, all experiments were performed under the following environment: 1) Computer: Intel® Core™ i5-2500, 2) CPU: 3.30 GHz, 3) RAM: 4 GB, 4) OS: Windows 7, 5) Matlab: R2014a.

Moreover, all resulting data were digitally recorded and stored in the computer without optical configuration. In the simulation part of our experiment, a grayscale image of size 50×50 is used to test the avalanche criterion. The avalanche effect and bit independence values of a good encryption algorithm should be independent of the size of input image. Similar results are obtained when input images with different sizes are used in this paper. An illustration of the used image is shown in Fig. 3(a). We converted the amplitude value of the image encrypted by the DRPE in discrete Gyrator domain into binary representation whenever we analyzed our proposed method for bit units. We used IEEE 754 double precision floating point format for binary representation and only considered the fractional portion consisting of 52 bits of significant digits. The values of this portion were only altered when even one bit was flipped. In contrast, the value in the sign and exponent portions were similar for the majority of the amplitude values with double formats. Therefore, we only concentrated on the 52 bits of the significant digits to carry the experiment without loss of generality. 100 simulation results were averaged to calculate the avalanche values. To calculate the avalanche effect, we conducted the experiment changing plaintext, first phase key, second phase key and rotation angle independently. The rotation angles were randomly chosen and kept fixed at $\alpha 1 = 0.32$ and $\alpha 2 = 0.75$ (in radian) to calculate these properties when bits in plaintext, first phase key and second phase key are altered. We measured the results in both bit unit and pixel unit. In bit unit, all of the pixel values are denoted and compared in bit. The ideal value of avalanche effect is 50% in bit unit because there are only two possible values (0 and 1) in bit space and 50% makes the most difficulty for the cryptanalyst to make a prediction. In pixel unit, pixels are compared using the pixel intensity value directly. In this case, the avalanche effect of 100% is the ideal value because the value space in pixel unit is much higher and 100% brings the most difficulty for the cryptanalyst to do an inference. Figure 4 presents the avalanche effect values obtained by varying the number of bits in the plaintext, Fig. 5 presents the avalanche effect values obtained by varying number of bits in the first phase key, and Fig. 6 presents the avalanche values obtained by varying number of bits in the second phase key for DRPE in the Fourier and Gyrator domains.

In all of the figures, the resulting avalanche values are shown in terms of the avalanche effect of DRPE in bit unit. Furthermore, the avalanche effect in pixel unit is also

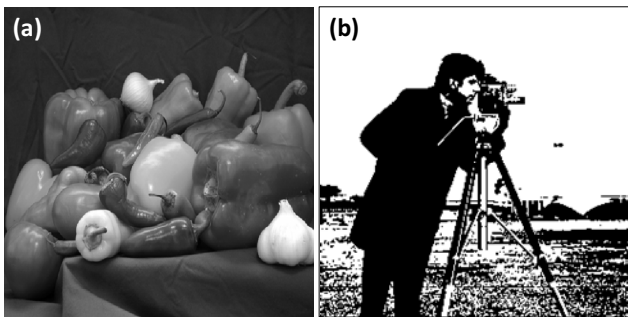

FIG. 3. Illustration of (a) the gray scale image used for testing avalanche criterion and (b) the binary image used for testing bit independence criterion.

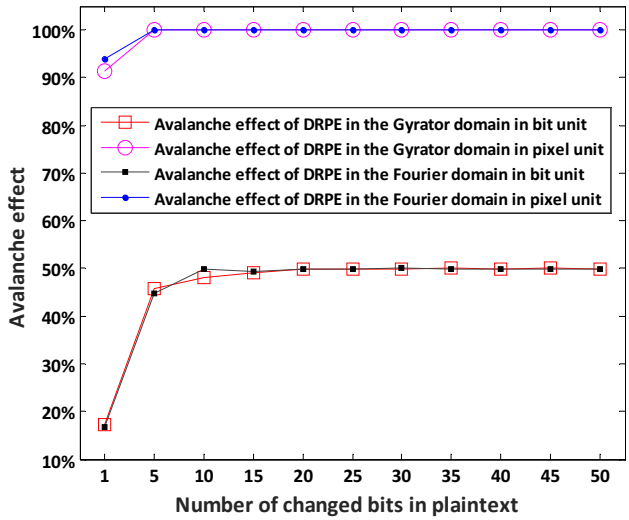

FIG. 4. Avalanche effect with some bits in the plaintext inverted.

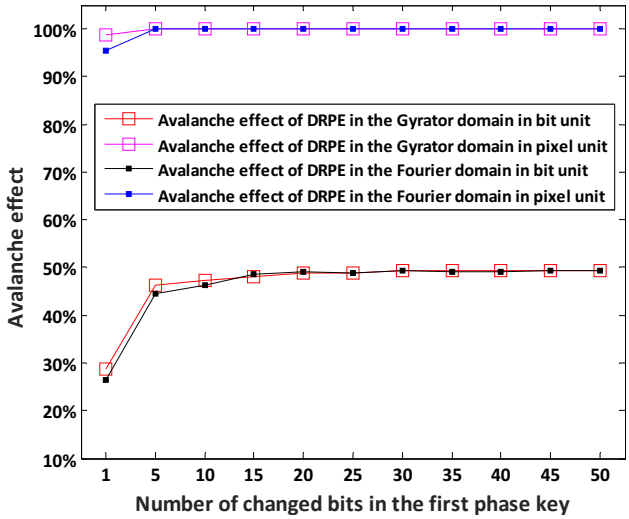

FIG. 5. Avalanche effect with some bits in the first phase key inverted.

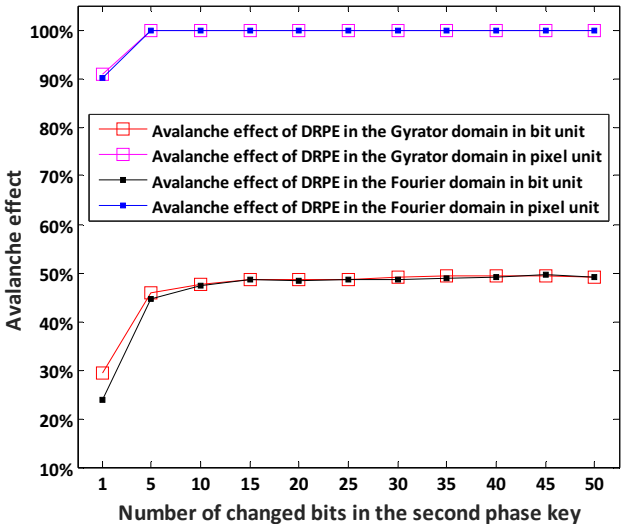

FIG. 6. Avalanche effect with some bits in the second phase key inverted.

calculated and shown in all of the figures, which is labeled as DRPE in pixel unit. It is evident from the Figs. 4~6 that the DRPE in discrete Gyrator domain shows similar avalanche effect as compared to that of Fourier domain when 50% and 100% are regarded as ideal values for avalanche effect in bit and pixel unit, respectively. All avalanche values obtained by varying the number of bits in the plaintext, first phase key, and second phase key of the DPRE in discrete Gyrator domain tend to be close to 50% as the increase of number of flipped bits. In brief, when the number of bits changed is less than 10 bits in the plaintext, less than 15 bits in the first and second phase key of the DRPE in both Fourier and Gyrator domain, the avalanche effect was not satisfactory as it was not close to 50% in bit unit. When more than 5 bits are changed in the plaintext, first or second phase key, the avalanche effects in pixel unit reach 100% for DRPE in both Fourier and Gyrator domain. Even if one bit is changed, the avalanche effects in pixel unit are larger than 90% for DRPE in both Fourier and Gyrator domains, which means that one-bit change affects most of the output values.

In the next step, we also check the avalanche effect of the two rotation angles. The rotation angles for the a_1 and a_2 are set to be 40 degree and are used as reference in this experiment. Then, the avalanche effect values are measured by changing the rotation angle. The resulting avalanche values are shown in Table 1. From Table 1, it is observed that the resulting avalanche effects in bit unit are all nearly 50% when some degrees are changed. It is also measured that all the avalanche effects in pixel unit are 1 which means all of the output values are changed when the input rotation angles are changed. Any change in the rotation angle results in a drastic change in all of the bits and pixel, which proves the great potential of the rotation angle as a key.

TABLE 1. Avalanche effect for DRPE in discrete gyrator with rotation angle changed

Rotation angle α_1 (in degree)	Avalanche effect in bit unit	Rotation angle α_2 (in degree)	Avalanche effect in bit unit
45	0.4899	45	0.4990
60	0.5008	60	0.4986
90	0.4978	90	0.5011
120	0.4994	120	0.5019
135	0.5015	135	0.4993
150	0.4990	150	0.5003
210	0.5011	210	0.4988
225	0.5006	225	0.4995
240	0.4988	240	0.5010
270	0.4995	270	0.5009
300	0.5000	300	0.4989
315	0.4994	315	0.5007
330	0.5010	330	0.4997

Based on the previous simulation results, we try to integrate the photon counting imaging (PCI) technique into DRPE in Gyrator domain to improve the avalanche effect. PCI is designed for low light levels (photon starved conditions) or night vision. Logically, the fewer photons it contains, the less information it has to interpret visually since the scene becomes more sparse due to fewer photons arriving at each pixel. Figures 7~9 show the avalanche effect values by flipping some number of bits in the plaintext, first and second phase key of DRPE in the Gyrator domain. Here, the number of photons Np is set to

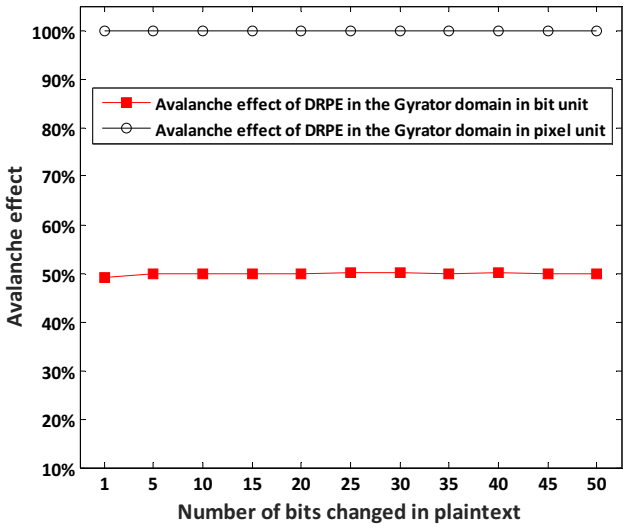

FIG. 7. Avalanche effect with some bits in the plaintext inverted for DRPE in the Gyrator domain integrated with PCI ($N_p = 10^5$).

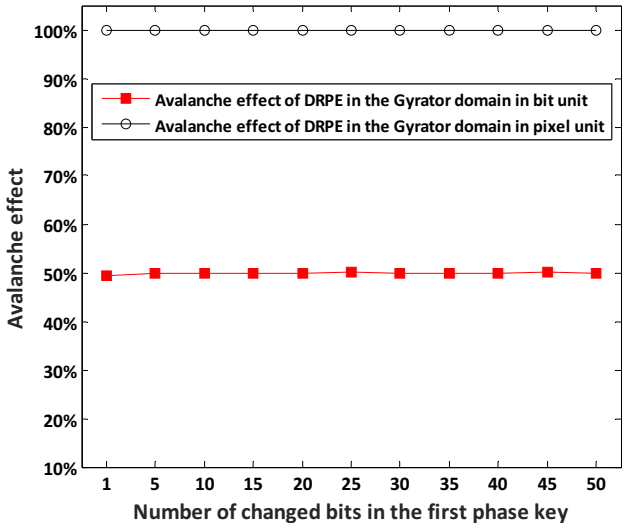

FIG. 8. Avalanche effect with some bits in the first phase key inverted for DRPE in the Gyrator domain integrated with PCI ($N_p = 10^5$).

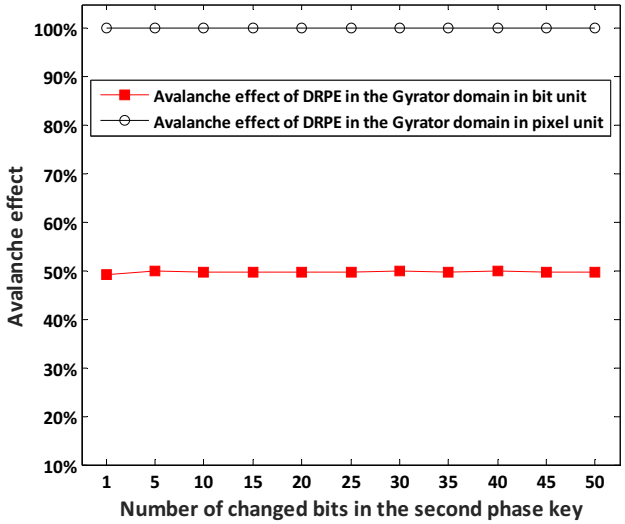

FIG. 9. Avalanche effect with some bits in the second phase key inverted for DRPE in the Gyrator domain integrated with PCI ($N_p = 10^5$).

be 105 and the two rotation angles are given as $\alpha 1 = 0.32$ and $\alpha 2 = 0.75$ (in radians) respectively. It is noted from Figs. 7~9 that all of the avalanche effect values in bit unit are very close to 50% and avalanche effect in pixel unit are almost 100% which means excellent avalanche effect is achieved when the PCI technique is introduced into DRPE in the Gyrator domain. In the view of cryptanalysis, the combination of DRPE in the Gyrator domain and PCI can enhance the system security because it has substantial avalanche effect, which is one of the primary design objectives.

In order to visually observe the effect of these algorithms, the encrypted and decrypted images for Fig. 3(a) using

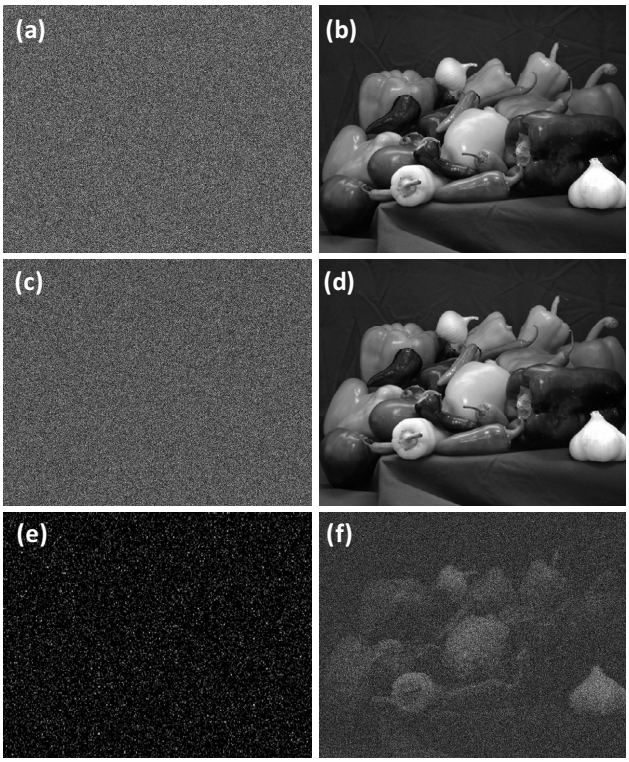

FIG. 10. Encrypted and decrypted images from (a)-(b): DRPE in the Fourier domain, (c)-(d): DRPE in the Gyrator domain, (e)-(f): photon-counting DRPE in the Gyrator domain with PCI ($N_p = 10^5$).

TABLE 2. Bit independence criterion for DRPE in the Fourier and discrete Gyrator domains

Repeatedly changing bits in	Bit independence criterion	
	Discrete Gyrator domain	Fourier domain
Plaintext	0.2606	0.2820
First random key	0.4381	0.4809
Second random key	0.3936	0.5638

DRPE in the Fourier domain, the Gyrator domain, and the photon-counting DRPE in the Gyrator domain are given in Fig. 10. The average processing times for DRPE in the Fourier and Gyrator domains are 0.2536 s and 0.4548 s, respectively while it is 0.5517 s for the photon-counting DRPE in the Gyrator domain.

After evaluating avalanche effect criterion, we tested bit independence criterion (BIC) of the DRPE systems in both the Fourier and Gyrator domains. To test the BIC, a binary cameraman image was utilized. The binary image used for this purpose is shown in Fig. 3(b). All of the bit independence values were measured taking an average of 100 numerical simulations. A correlation value obtained from Eq. (16) shows satisfactory bit independence criterion if it is not close to 1. Table 2 is a comparison table

TABLE 3. Bit independence criterion for DRPE in the discrete Gyrator domains integrated with PCI

Repeatedly changing bits in	Photon counting DRPE in discrete Gyrator domain
Plaintext	0.2393
First random key	0.2049
Second random key	0.1867

showing bit independence values for the DPRE in the discrete Gyrator domain and the DRPE in the Fourier domain. It can be seen from Table 2 that the BIC for DRPE in both Fourier and Gyrator domains are good because there is no value that is close to 1, which means there are no strong correlations between any pair of bits. Therefore, it is difficult to predict one bit from other bits and make the cryptanalysis difficult.

Moreover, Table 3 shows the bit independence values for the photon counting DPRE in the discrete Gyrator domain. Here, the rotation angles were randomly chosen as $\alpha 1 = 0.35$ and $\alpha 2 = 0.75$ (in radians) and the photon number is given as 105. It is noted from Table 3 that excellent BIC values are achieved for photon counting DRPE in the Gyrator domain.

Avalanche and bit independence properties signify the robustness against statistical analysis. Verification of these properties has paramount importance in designing of the cryptographic algorithms, especially for block cipher designing. Gyrator domain has been widely implemented in image encryption recently. Therefore, analysis of avalanche and bit independence properties of encryption systems in the Gyrator domain is important to investigate the feasibility of using it in the secure image authentication systems based on DRPE. Image encryption algorithms in the Fourier domain have weaknesses which might lead to easy statistical analysis of it. Our study shows that the DRPE encryption system in the discrete Gyrator domain has a very similar avalanche effect to that in the Fourier domain, which indicates potential risk from statistical analysis. On the other hand, it is verified that the photon counting DRPE in the Gyrator domain can greatly improve the avalanche effects and can enhance the security of the system since excellent avalanche effects can have the system be robust against statistical attacks.

VII. CONCLUSION

In this study, we have evaluated the avalanche and bit independence characteristics of a double random phase encoding scheme in the discrete Gyrator domain. It is found that the DRPE in the Gyrator domain has a good bit independence property but does not possess excellent avalanche effects and would bring potential statistical attack risk to the encryption system. On the other hand, our experiment shows that the change of rotation angle in the discrete Gyrator domain can produce total different output that means the rotation angle can be viewed as an additional key and provides an additional layer of system security. Moreover, we have integrated the photon counting imaging technique into double random phase encoding in the Gyrator domain and it is verified that the photon counting imaging can improve the avalanche effect of DRPE in the Gyrator domain because the combined system achieves excellent avalanche effects. The analysis of avalanche effect and bit independence properties of the cryptosystems in the virtual optical domain can be regarded as an effective tool for the future design of the robust cryptosystems in computational optical domain instead of conventional digital block ciphers.

ACKNOWLEDGMENT

This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF), funded by the Ministry of Science, ICT, & Future Planning (NRF-2015R1A2A1A10052566) for Inkyu Moon. Also, this research was financially supported by Hansung University for Jieun Lee.

REFERENCES

1. H. Farid, "Image forgery detection," IEEE Signal Process. Mag. **26**, 16-25 (2009).
2. M. Stamp, *Information Security: Principles and Practice* (Wiley, 2011).
3. S. Kishk and B. Javidi, "3D object watermarking by a 3D hidden object," Opt. Express **11**, 874-888 (2003)
4. Y. Sheng, Z. Xin, M. Alam, L. Xin, and L. Xiao-Feng, "Information hiding based on double random-phase encoding and public-key cryptography," Opt. Express **17**, 3270-3284 (2009).
5. F. Yi, I. Moon, and Y. Lee, "A multispectral photon-counting double random phase encoding scheme for image authentication," Sensors **14**, 8877-8894 (2014).
6. H. Singh, A. K. Yadav, S. Vashisth, and K. Singh, "Double phase-image encryption using gyrator transforms, and structured phase mask in the frequency plane," Opt. Lasers Eng. **67**, 145-156 (2015).
7. T. Zhao, Q. Ran, L. Yuan, Y. Chi, and J. Ma, "Information verification cryptosystem using one-time keys based on double random phase encoding and public-key cryptography," Opt. Lasers Eng. **83**, 48-58 (2016).
8. X. Wang, W. Chen, and X. Chen, "Optical information authentication using compressed double-random-phase-encoded images and quick-response codes," Opt. Express **23**, 6239-6253 (2015).
9. P. Réfrégier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. **20**, 767-769 (1995).

10. G. Situ and J. Zhang, "Double random-phase encoding in the Fresnel domain," Opt. Lett. **29**, 1584-1586 (2004).
11. N. Singh and A. Sinha, "Gyrator transform-based optical image encryption, using chaos," Opt. Lasers Eng. **47**, 539-546 (2009).
12. I. Moon, F. Yi, Y. H. Lee, and B. Javidi, "Avalanche and bit independence characteristics of double random phase encoding in the fourier and fresnel domains," J. Opt. Soc. Am. A **31**, 1104-1111 (2014).
13. Z. Liu, X. Lie, C. Lin, J. Dai, and S. Liu, "Image encryption scheme by using iterative random phase encoding in gyrator transform domains," Opt. Lasers Eng. **49**, 542-546 (2011).
14. S. Daza, F. Vega, L. Matos, C. Moreno, M. Diaz, and Y. Daza, "Image encryption based on convolution operation in the gyrator transform domain," in *Proc. IECON 2012 - 38th Annual Conference on IEEE Industrial Electronics Society* (Canada, Oct. 2012), pp. 1527-1529.
15. Z. Liu, Y. Zhang, S. Li, W. Liu, W. Liu, Y. Wang, and S. Liu, "Double image encryption scheme by using random phase encoding and pixel exchanging in the gyrator transform domains," Opt. Lasers Technol. **47**, 152-158 (2013).
16. Q. Wang, Q. Guo, and L. Lei, "Multiple-image encryption system using cascaded phase mask encoding and a modified Gerchberg-Saxton algorithm in gyrator domain," Opt. Commun. **320**, 12-21 (2012).
17. M. Abuturab, "Color image security system using double random-structured phase encoding in gyrator transform domain," Appl. Opt. **51**, 3006-3016 (2012).
18. M. Abuturab, "An asymmetric color image cryptosystem based on Schur decomposition in gyrator transform domain," Opt. Lasers Eng. **58**, 39-47 (2014).
19. J. Sang, J. Zhao, Z. Xiang, B. Cai, and H. Xiang, "Security analysis of image encryption based on gyrator transform by searching the rotation angle with improved PSO algorithm," Sensors **15**, 19199-19211 (2015).
20. Z. Liu, D. Chen, J. Ma, S. Wei, Y. Zhang, J. Dai, and S. Liu, "Fast algorithm of discrete gyrator transform based on convolution operation," Optik - Int. J. Light Electron Opt. **122**, 864-867 (2011).
21. J. Chen, Z. Zhu, C. Fu, L. Zhang, and H. Yu, "Analysis and improvement of a double-image encryption scheme using pixel scrambling technique in gyrator domains," Opt. Lasers Eng. **66**, 1-9 (2015).
22. E. Pérez-Cabré, C. Héctor, S María, and B. Javidi, "Photon-counting double-random-phase encoding for secure image verification and retrieval," J. Opt. **14**, 094001 (2012).
23. E. Pérez-Cabré, M. Cho, and B. Javidi, "Information authentication using photon-counting double-random-phase encrypted images," Opt. Lett. **36**, 22-24 (2010).
24. Z. Xin, D. Lai, S. Yuan, D. Li, and J. Hu, "A method for hiding information utilizing double-random phase-encoding technique," Opt. Lasers Technol. **39**, 1360-1363 (2007).
25. G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," Opt. Lett. **25**, 887-889 (2000).
26. G. Li, W. Yang, D. Li, and G. Situ, "Cyphertext-only attack on the double random-phase encryption: Experimental demonstration," Opt. Express **25**, 8690-8697 (2017).
27. X. Liu, J. Wu, W. He, M. Liao, C. Zhang, and X. Peng, "Vulnerability to ciphertext-only attack of optical encryption scheme based on double random phase encoding," Opt. Express **23**, 18955-18968 (2015).
28. T. Li and Y. Shi, "Attack on optical double random phase encryption based on the principle of ptychographical imaging," Chin. Phys. Lett. **33**, 014206 (2016).
29. H. Li, "Image encryption based on gyrator transform and two-step phase-shifting interferometry," Opt. Lasers Eng. **47**, 45-50 (2009).
30. J. Rodrigo, A. Tatiana, and L. María, "gyrator transform: properties and applications," Opt. Express **15**, 2190-2203 (2007).
31. M. Juan, O. Vilardy, S. Maria, and E. Pérez-Cabré, "Secure image encryption and authentication using the photon counting technique in the Gyrator domain," in *Proc. 20th Symposium on Signal Processing, Images and Computer Vision* (STSIVA)(Colombia, Sept. 2015), pp. 1-6.
32. S. Rajput, D. Kumar, and N. Nishchal, "Photon counting imaging and phase mask multiplexing for multiple images authentication and digital hologram security," Appl. Opt. **54**, 1657-1666 (2015).
33. H. Feistel, "Cryptography and computer privacy," Sci. Am. **228**, 15-23 (1973).
34. S. Gupta and S. Yadav, "Performance analysis of cryptographic hash functions," Int. J. Sci. Res. **4**, 2319-7064 (2015).
35. C. Blondeau and K. Nyberg, "New links between differential and linear cryptanalysis," Lect. Notes Comput. Sci. **7881**, 388-404 (2013).
36. V. Goyal, A. O'Neill, and V. Rao, *Correlated-input secure hash functions* (Springer, 2011).
37. W. Stallings, *Cryptography and Network Security Principles and Practice* (Prentice Hall, 2011).
38. J. Castro, J. Sierra, A. Seznec, A. Izquierdo, and A. Ribagorda, "The strict avalanche criterion randomness test," Math. Comput. Simul. **68**, 1-7 (2005).
39. A. ALabaichi, R. Mahmod, and F. Ahmad, "Analysis of some security criteria for S-boxes in blowfish algorithm," Int. J. Digit. Content Technol. Appl. **7**, 8-20 (2013).