The ISC Int'l Journal of Information Security

ISeCure

July 2012, Volume 4, Number 2 (pp. 115–124)

http://www.isecure-journal.org

Improving Security of Double Random Phase Encoding with Chaos Theory Using Fractal Images☆

Motahareh Taheri [1,*] and Saeed Mozaffari [1]

[1] *Electronic and Computer Department, Semnan University, Semnan, Iran*

ARTICLE INFO.

Article history:
Received: 13 December 2011
Revised: 13 January 2013
Accepted: 5 March 2013
Published Online: 27 August 2013

Keywords:
Double Random Phase Encoding(*DRPE*), Fractal Image Generation, Julia Set, Mandolrot Set, Chaos Theory, Two-Dimensional Coupled Logistic Map, Combination of Data Hiding and Cryptography.

ABSTRACT

This study presents a new method based on the combination of cryptography and information hiding methods. Firstly, the image is encoded by the Double Random Phase Encoding (*DRPE*) technique. The real and imaginary parts of the encoded image are subsequently embedded into an enlarged normalized host image. *DRPE* demands two random phase mask keys to decode the decrypted image at the destination. The two random phase masks are regenerated by the chaos theory using a fractal image. To enhance its security, instead of sending the second phase mask directly, the initial conditions and the parameter of the chaotic map and the fractal image are transferred to the authorized user through a secure channel. Experimental results reveal that the proposed method not only enjoys high security but also resists the commonplace attacks.

1 Introduction

Optical image encryption and digital image watermarking have been used extensively for data protection and copyright purposes [1]. Among various methods, Double Random Phase Encoding (*DRPE*) technique has a high level of security [2–5] which is used for image encryption [6–11] and image watermarking [12–15]. Protecting information from unauthorized users is the cardinal objective of information hiding methods. To increase the information security, watermarking and image hiding techniques are usually employed in conjunction with encryption methods. Encryption methods are based on some secret keys. without,which it is almost impossible for an unauthorized person to reconstruct the original information.

Double random phase encoding (*DRPE*) was proposed by Refregier and Javidi in 1995 to encrypt an input image [6]. The input image is disarranged by two random phase masks, located at input and Fourier planes in a 4f optical system (Figure 1). Since encryption and decryption keys are conjugate to each other, *DRPE* can be regarded as a symmetrical key system. To reconstruct the input image, decryption keys (random phase masks) are required to be sent through a secure channel. Sending large phase masks is a major shortcoming of *DRPE* method. Real and imaginary parts of the encoded image are embedded into a large enough normalized host image after being modulated with sine and cosine function. The modulation process reduces visual degradation and enhances its transparency.

In this study, a new method for phase masks generation is proposed based on the chaos theory and using the fractal image. Instead of transmitting large phase masks, only parameters and initial condition of chaos and fractal image are sent through a private channel. In the following, details of *DRPE* algorithm

☆ This article is an extended/revised version of an ISCISC'11 paper.

* Corresponding author.

Email addresses: taheri@semnan.ac.ir (M. Taheri), mozaffari@semnan.ac.ir (S. Mozaffari)

ISSN: 2008-2045

are presented.

By random phase encoding in both the input (PM1) and the Fourier planes (PM2), a plain image is converted to a complex-amplitude encoded image, whose real and imaginary parts can be considered as independent stationary white noise [6]. In the 4f optical system, the distance between the two phase masks (PM1 and PM2), the two lenses (L1 and L2), and input and output images (f and g) are set to be f (focus length of the lens). A plaintext image, f(x,y), is multiplied by the first phase mask PM1, and the Fourier-transformed image is multiplied by the second phase mask PM2, which corresponds to a cipher key. The image is then inverse-Fourier transformed, and a cipher-text imag $g(x,y)$ is obtained as follows:

$$g(x,y) = FT^{-1}\{FT\{f(x,y).\theta(x,y)\}.\varphi(u.v)\} \quad (1)$$

To reconstruct the input image, the following process should be performed.

$$f(x,y) = FT^{-1}\{FT\big(g(x,y)\big).\exp[-i2\pi\varphi_0(u,v)] \\ .\exp[-i2\pi\theta_0(x,y)]\} \quad (2)$$

In (2), $\theta_0(x,y)$ and $\varphi_0(u,v)$ denote the two phase-functions inserted in the input plane and Fourier plane respectively, and their values are randomly distributed over the interval [0,1].

The decryption procedure is similar to that of the encryption but in the reversed order. The two phase masks employed in the *DRPE* system are utilized to diffuse and confuse information and make it more robust to resist attacks and distortions. However, *DRPE* is not adequately sensitive to phase masks and slight variation in them leads to an output image resembling the original one.

2 Related Work

This section addresses the state-of-the-art techniques in *DRPE*. Since this research focuses on the combination of information hiding and cryptography, related studies are also categorized into two distinct groups. In the first group, previous efforts for mask generation are briefly explained (cryptography). The proposed methods for encrypted image insertion or random phase embedding into a host image are presented in the second subsection (information hiding).

2.1 Methods for Phase Masks Generating

As mentioned before, *DRPE* algorithm requires two random phase masks. In the original form, these masks (keys) are transmitted to the authorized user through a secure channel for decryption. Besides high volume data transmission, this method considerably

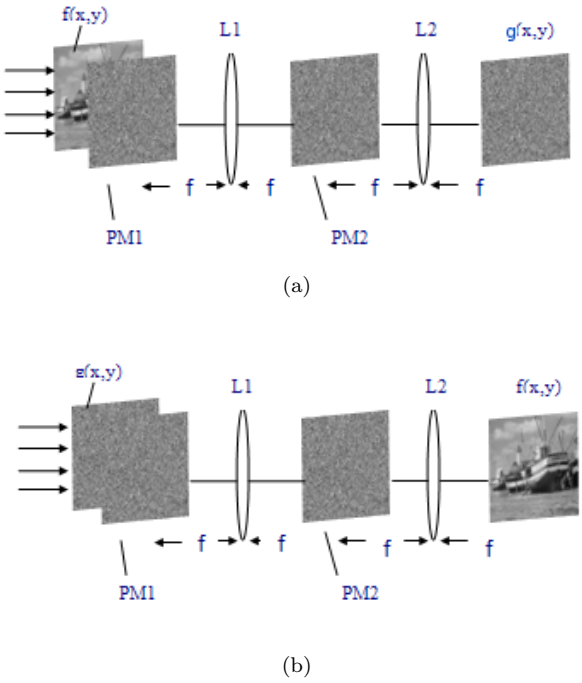


Figure 1. Double random phase encoding process: (a) encoding step and (b) decoding step.

reduces *DRPE* security. To approach this problem, several methods have been recommended.

A cascaded iterative Fourier transform (CIFT) algorithm is presented for optical security applications [8]. Compared with previous methods, this algorithm employs an improved searching strategy: modifying the phase distributions of both masks synchronously as well as enlarging the searching space. Two phase masks are generated from the plaintext image through a cascaded iterative Fourier transform method. This method obviates the need of encoded image transmission and the two encoding keys are inserted into the host image. In the receiver, the two keys are extracted from the host image and the input image is reconstructed.

In [9], phase mask2 (PM2) is generated by an affine transformation through a pseudo-random pattern generated from a source image. The mask hinges on the affine transformation parameters and the iteration number that controls their randomness. Affine transformation is implemented by using the operation of reflection, translation, rotation, shearing and scaling. This procedure offers the advantage over the conventional *DRPE* technique that does not need to send the encrypting mask itself to the authorizer user [9]. Instead of sending large keys, the source image and 18 parameters which indicate the affine transforms are sent through a secure channel.

Four chaotic maps (logistic, tent, Kaplan-Yorke, and Ikeda) have been employed to generate the ran-

dom phase masks [10]. The logistic and the tent maps are one-dimensional while the Kaplan-York and the Ikeda maps are two-dimensional chaotic maps. In a similar method, random phase masks are generated using iterative chaos functions such as logistic map, tent map and the Kaplan-Yorke map [11].

2.2 Methods for Hiding Encoded Image

In the following, proposed methods for hiding encoded image into an arbitrary host image are discussed. In the standard method, encrypted image contains real and imaginary parts which are embedded into two distinct host images [12]. The host image containing the encrypted image is called combined image. The host image is subtracted from the combined image. Then, the obtained image is encrypted by *DRPE* algorithm. Although reconstructed image of this method has good quality, its security is not high enough due to sending host and combined images.

In the second decoding method proposed in [12], just the combined image is required to reconstruct the encoded image. The reconstructed image consists of noisy version of the secret image. Noise characteristics rely on the host images property. The higher gray level values impose higher noise on the reconstructed image. Consequently, the signal-to-noise ratio (SNR) of the reconstructed image and combined image are decreased and increased, respectively.

In another attempt, Zhou and Chen proposed a new method [13] to address the mentioned problem of the standard method. To hide the encoded image, only one host image with the same size of the input image is utilized. First, the size of host image is doubled by copying each pixel into its four neighbouring pixels in the output image Afterwards, the imaginary and real parts of encoded image are added and subtracted from the enlarge host image. In this manner the encrypted image is almost invisible in the combined image. The encrypted image can be readily reconstructed by subtracting adjacent pixels of the combined image. In this method, the host image is not needed for reconstruction. Moreover, the quality of the reconstructed image is independent from the host image. However, owing to the direct insertion of the encrypted image pixels into the host image, quality of the combined image is diminished.

To solve this problem, Zhang *et al.* proposed a new method in which two phase masks are generated from secret image using cascaded iterative Fourier transform (CIFT) approach [14]. Sine and cosine of one phase mask is added to the enlarged host image rather than adding real and imaginary parts of encoded image to the enlarged host image with neighbor pixel value subtraction (NPVS) algorithm. Such transformation lowers visual distortions in the combined image. However, the second phase mask should be sent to the authorized user through a private channel. The original hidden image is first encrypted into two phase masks [14]. The cosine and sine functions of one of the phase masks are subsequently embedded into an enlarged host image in the DCT domain [14]. By extracting the watermark of the enlarged superposed image and decryption, the hidden image can be retrieved.

To obviate the need for the second phase mask transmission, a hybrid method based on the *DRPE* and RSA algorithm is proposed in [15]. First, two phase masks are generated from the source image and plaintext image via CIFT algorithm. As a substitute for the encoded image, the source image and two phase masks are inserted into the enlarged host image. To reconstruct the secret image, the reverse process is performed.

3 Propose Method

As mentioned earlier, since combination of information hiding and cryptography approaches are proposed in this study, each of them are explained separately in the following two subsections.

3.1 Phase Masks Generation

The *DRPE* algorithm needs two random phase masks located at input plane (PM1) and Fourier plane (PM2). In this study, phase mask2 (PM2) is generated by the chaos theory using the fractal image. Thus, there is no need to send the phase mask directly to the authorizer user. Instead, the set of passwords and parameters that leads to the construction of the phase mask is transmitted. Furthermore, the proposed method obviates the need for sending the source image. Compared to previous methods, the parameters needed for the generation phase are much less. Figure 2 shows the overview of the phase mask generation process. By means of arbitrary parameters, the fractal set produces a unique fractal image used as the input image for chaos block to generate PM2.

The proposed phase mask generation method enjoys several advantages compared to the conventional *DRPE* system. Instead of sending the phase masks to the authorizer user, the set of parameters such as the coordinates, zoom level, iterations, etc for fractal image construction and initial condition of the chaos theory are transmitted. Therefore, security of the *DRPE* is considerably increased. The second advantage is the keys with very small memory footprint.

A few numbers represent a unique key, and a few parameters would have to be stored. The third advantage is key robustness. If the attacker estimates parts of the key, a resemble fractal image is generated, yet the original image cannot be attained. In the following, a more detailed description of the fractal image and chaos function is presented.

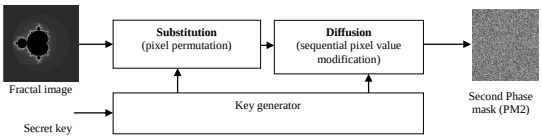


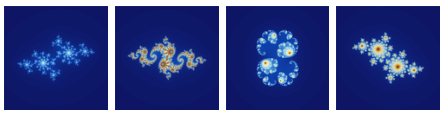
Figure 2. Second phase mask generation method.

3.1.1 Fractal Image

This research aims to use a fractal image as an input to chaos module to generate second phase mask in the encryption/decryption *DRPE* process. Fractal images contain meager information, but posses high-level of visual complexity [16]. A Fractal image can be generated using Julia set or Mandelbrot set. They are well known sets on the complex plane that create infinitely detailed images. The Mandelbrot Set is not real fractals by definition; however, it is semi-self similar and still shows infinite detail. Thus it is usually called fractal as well.

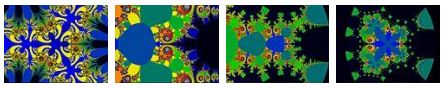
For Julia set of each pixel, iterated complex function such as $z_{n+1} = az_n^2 + c$ is applied in which z and c are complex numbers [17]. z is initially the coordinates of the pixel and will be updated in each iteration. Depending on the pixel's coordinates, after some iteration z will either go to infinity, or remain in a circle with a radius 2 around the origin of the complex plane forever. The points that remain in the circle are the ones that belong to the Julia set. The color value of the pixel is the iteration number before the distance of z to the origin becomes larger than radius 2. Different values of c yield different Julia sets which may be connected or disconnected. Figure 3 demonstrates some Julia images generated by $z_{n+1} = z_n^2 + c$ iteration method with different c values. Using different iteration forms leads to complicated fractal images as displayed in Figure 4.

The Mandelbrot set is defined by the same iteration process used in Julia sets, but applied differently. Instead of using the complex plane to represent the different choices of z, Mandelbrot represents different values of c. To generate an image, for each c start with $z = 0$ and generate sequence of z_n by $z_{n+1} = az_n^2 + c$ iteration system. If the sequence does not run away to infinity, then the point c belongs to Mandelbrot set. As with Julia sets, pixel's color is set to black if the sequence produced by the c at its center does not run away to infinity. Otherwise, the pixel's color is determined by how quickly the sequence gets farther than 2 from the origin. The Mandelbrot set provides more details in the zooming image. Figure 5 demonstrates an image sequence zooming with different geometrical structures [18]. In this study, Julia and Mandelbrot fractal images are generated by Fractal Explorer software available at [19].



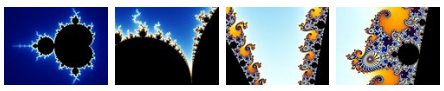
(a) (b) (c) (d)

Figure 3. Julia set fractal images using $z_{n+1} = az_n^2 + c$ with different c values: (a) $c = -0.70176 - 0.3842i$, (b) $c = -0.8 + 0.156i$, (c) $c = 0.285 + 0.01i$, and (d) $c = -0.4 + 0.6i$.



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

Figure 4. Julia set fractal images using different iteration functions: (a) $z_n + 1 = \exp(z_n^3) - 0.59$, (b) $z_n + 1 = z\exp(z_n) + 0.04$, (c) $z_n + 1 = z_n^3 \exp(z_n) + 0.33$, and (d) $z_n + 1 = z_n^4 \exp(z_n) + 0.41$.



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

Figure 5. Mandelbrot set image sequence zooming.

3.1.2 Chaos Function

Chaos functions have been primarily applied to develop the mathematical models of the non-linear systems. Several interesting properties have been reported for chaos function [17]. Being sensitive to the initial conditions renders it proper for authentication applications. One-dimensional chaotic system has the advantage of high efficiency and simplicity. However, two-dimensional chaotic maps are inherently excellent candidates for image encryption in that they need two seed values which increase the confusion in the encryption technique. More confusion in the encryption makes the system more secure. Hence, the two-dimensional coupled Logistic map has been used in this study to generate phase mask needed for the *DRPE*. The two-dimensional coupled Logistic map is described as follows [20–22]:

$$x_{n+1} = \mu_1 x_n / [1 - x_n] + \gamma_1 y_n^2 \quad (3)$$

$$y_{n+1} = \mu_2 y_n / [1 - y_n] + \gamma_2 (x_n^2 + x_n y_n) \quad (4)$$

$$n = 1, 2, 3, \ldots, N \times N, 0.15 < \gamma_1 < 0.21$$
$$0.13 < \gamma_2 < 0.15, 2.75 < \mu_1 < 3.14$$
$$2.75 < \mu_2 < 3.45$$

Where $N \times N$ denotes the size of the plaintext image.

The initial values of $x(0)$, $y(0)$ and the parameters μ_1, μ_2 are used as the key in this research. Chaos function necessitates two stages: diffusion and substitution (Figure 2). In the diffusion stage, the pixel values are modified sequentially so that a subtle variation in one pixel scatters to almost all pixels in the whole image. In substitution stage, interleaving algorithm is employed and image pixels are permuted secretly, without any change in their values.

Details of random image generation by chaos function are described as follows:

Step(1): First choose an arbitrary source image (fractal image in this paper).

Step(2): Perform the permutation process in which pixel's position are changed according to periodic interleaving [23]:

- The input image matrix with the size of $N \times N$ is converted into a vector with size of $1 \times N^2$.
- The interleave parameter is chosen. It is a scalar integer value in the range of [0 to $2^{32} - 1$] that determines the specific permutation.
- The first element in the image vector is preserved; whereas, other elements are permuted according to the specified interleave parameter.
- The reverse process of interleaving is performed to obtain the original input image with the size of $N \times N$.

Step(3): Perform the diffusion process.

- Obtain s from the current state of the chaotic map:

$$s_{n+1} = \text{mod}(\text{floor}(x_{n+1} + y_{n+1}) \times 2^{16}, 256) \quad (5)$$
$$n = 1, 2, 3, \ldots, N^2$$

- Calculate the cipher-pixel value using the values of the currently operated pixel and the previously operated pixels [3]:

$$P(k) = s(k) \oplus \{mod(o(k) + s(k)), 256\} \oplus P(k-1) \quad (6)$$

Where $o(k)$, $P(k)$ are the currently operated pixel and random image pixel, respectively, and $P(k-1)$ is the previous random image pixel. Set the initial value $P(0)$ as a constant [21, 22].

Since the chaos function is highly sensitive to its initial condition and parameters, slight discrepancy results in a different output image. The encrypted output image of chaos function is employed as PM2. Table 1 displays the initial condition and parameters for fractal image and chaos functions used in this research. The parameters of chaos system were mentioned in Eqs. (3) and (4), Julia and Mandelbrot sets have several parameters including coordinate of the central point of the complex plane (DX, DY), zoom and iteration numbers, real and imaginary parts of complex number z (RE,IM), and a and c coefficients in $z_{n+1} = az_n^2 + c$.

A plaintext image can be encoded and decoded subsequent to PM2 generation with the fractal image and the chaos theory. An arbitrary random phase mask is used as PM1. The encoding and decoding processes are presented in Figures 6 and 7 respectively.

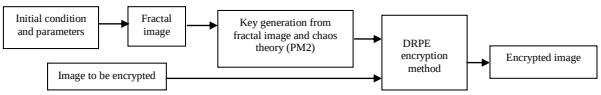


Figure 6. The encryption process.

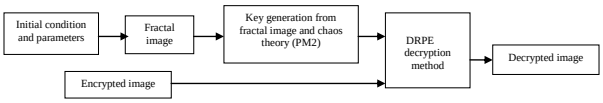


Figure 7. The encryption process.

3.2 Information Hiding

In the proposed method, the encrypted image is inserted into a normalized host image and as a substitute for the embedding random phase masks, only their keys are transmitted through a private channel. Since real and imaginary parts of the encoded image are modulated by sine and cosine functions, the detrimental effect of the direct information superposition are considerably reduced.

In this study, to maintain quality of the combined image and boost its robustness to attacks, instead of using original form of the host image, its normalized version is utilized. Figure 9 displays the influence of normalized host image on the quality of the combined image evaluated by *PSNR* criterion. Figure 8 shows the overall process of the encoded image insertion and extraction.

3.2.1 Information Hiding Algorithm

Subsequent to generating two random phase masks, the encoded image is obtained by (1). The encoded image has real and imaginary parts. The proposed method for encrypted image hiding is similar to [14], in which random phases are hidden. However, in this

Table 1. Initial condition and parameters employed in this paper.

Methods	Parameters							
Chaos theory	$x_0 = 0.94$	$y_0 = 0.84$	$\mu_2 = 3.2$	$\mu_1 = 3$	$\gamma_2 = 0.14$	$\gamma_1 = 0.17$	Interleaving parameter= 100	
Julia set	DX= -1.6	DY = 1.6	Zoom =1	Iteration=68	RE=0.45		IM =0.25	
Mandelbrot set	DX= -4	DY = 4	Zoom =1	Iteration=151	RE=0.5	IM =0.5	c=1	a=0.5

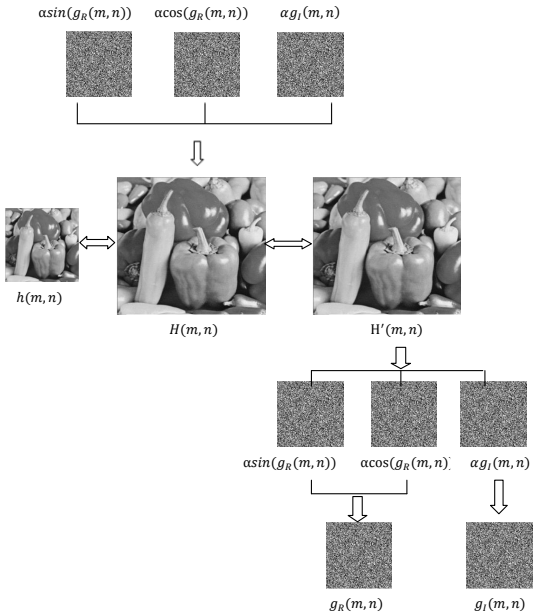


Figure 8. Illustration of the information hiding and extraction processes.

study the normalized host image is utilized. An arbitrary host image, $(h(m,n))$ with the same size as the plain image is selected. The normalized host image can be obtained as follows:

$$hn(m,n) = \frac{h(m,n) - h_{min}}{h_{max} - hmin} \tag{7}$$

Where h_{min} and h_{max} are minimum and maximum amplitudes of the host image, respectively.

Afterwards, the size of the normalized host image is doubled by replicating one of its pixels into its four neighboring pixels as follows [20]:

$$\begin{cases} H(2m-1,2n-1) = hn(m,n) \\ H(2m-1,2n) = hn(m,n) \\ H(2m,2n-1) = hn(m,n) \\ H(2m,2n) = hn(m,n) \end{cases} \quad \begin{matrix} \\ m = 1,2,3,\ldots,M \\ n = 1,2,3,\ldots,N \\ \\ \end{matrix} \tag{8}$$

Next, real and imaginary parts of encoded image are embedded into the enlarged normalized host image $(H(x,y))$.To increase transparency, real or imaginary parts of the encoded image are modulated by sine and cosine functions and are then embedded into the normalized enlarged host image [14, 20].

$$\begin{cases} H'(2m-1,2n-1) = \alpha H(2m-1,2n-1) \\ \qquad\qquad + \cos(g_R(m,n)) \\ H'(2m-1,2n) = \alpha H(2m-1,2n) \\ \qquad\qquad + \sin(g_R(m,n)) \\ H'(2m,2n-1) = \alpha H(2m,2n-1) + g_I(m,n)) \\ H'(2m,2n) = \alpha H(2m,2n) \end{cases}$$

Above, $H'(.,.)$ represents the combined image and α is a constant. The value of α is subject to the weight selection criterion and the correlation detection procedure. The large value of α will distort the cover image over the entire image plane, resulting in the degradation of the watermarked image for visual inspection. A small value of α represents the low-bit coding, which is vulnerable to deliberate attacks for which the mark information can easily be removed from the watermarked image [15].

(a) (b)

Figure 9. Effect of normalization process on the combined image's quality: (a) combined image using original host image ($PSNR = 30.7868$) and (b) combined image using normalized host image ($PSNR = 78.7456$).

3.2.2 Extraction of the Hidden Information

The embedded information is extracted by the reverse process. First, real and imaginary parts of the encoded image are extracted from the combined image as follows [15, 20]:

$$\cos(g_R(m,n)) = H'(2m-1,2n-1) - H'(2m,2n) \tag{9}$$

$$\sin(g_R(m,n)) = H'(2m-1,2n) - H'(2m,2n) \tag{10}$$

$$g_1(m,n) = H'(2m,2n-1) - H'(2m,2n) \tag{11}$$

From Eqs. (9) and (10), complex number A can be obtained.

$$\begin{aligned} A(m.n) &= [H'(2m-1,2n-1) - H'(2m,2n)] \\ &\quad + i[H'(2m-1,2n) - H'(2m,2n)] \\ &= \cos(g_R(m,n)) + i\sin(g_R(m,n)) \\ &= exp(g_R(m,n)) \end{aligned} \tag{12}$$

From (12), the real part of encoded image is yielded.

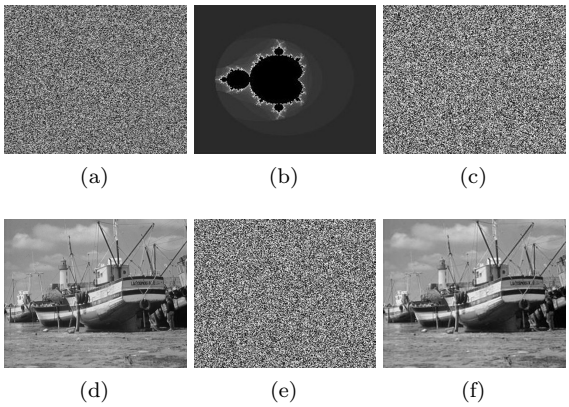
$$g_R(m,n) = angle(A(m,n)) \tag{13}$$

With (11), the imaginary part of the encoded image is obtained.

Through real and imaginary parts, the encoded image is obtained. Consequently, with two phase masks and encoded image *DRPE* can reconstruct the secret image.

4 Experimental Result

The proposed method is demonstrated with numerical simulations in MATLAB R2008b environment. The plaintext image and phase keys in the following simulations have pixels and quantified to 8 bits. The first random phase (PM1) is generated randomly Figure 10a. The fractal image which is used as input image of chaos algorithm is shown in Figure 10b. Figure 10c demonstrates PM2 which is generated by chaos algorithm. The second row in Figure 10 displays the encryption and decryption results.



(a) (b) (c)

(d) (e) (f)

Figure 10. The results of the proposed method: (a) fractal image, (b) first phase mask(PM1), (c) second phase mask(PM2), (d) plaintext image, (e) encrypted image ($PSNR = 58.4447$), and (f) ciphertext image($PSNR = 78.4509$).

The phase masks in the *DRPE* method should be as random as possible. However, randomness is more critical for PM2. Randomness can be explored by histogram analysis and correlation coefficients measurement between adjacent pixels. Figures 11b and 11e show the histogram of the PM2s generated by Julia and Mandelbrot fractal images which are nearly uniform. Correlation coefficients using 3000 pairs of two horizontal adjacent pixels randomly selected from PM2s are calculated:

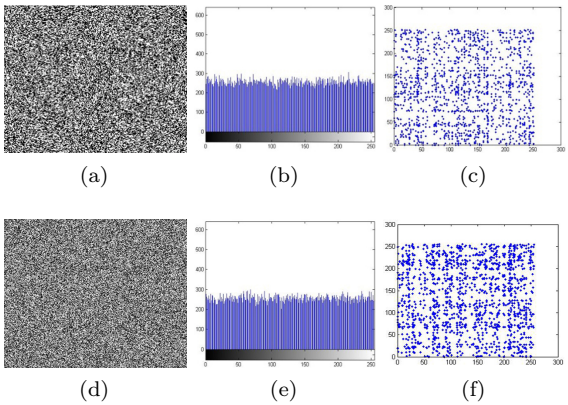
$$r_{xy} = \frac{|\mathrm{Cov}(x,y)|}{\sqrt{D(x)}\sqrt{D(y)}},$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, E(y) = \frac{1}{N}\sum_{i=1}^{N} y_i \tag{14}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2, D(y) = \frac{1}{N}\sum_{i=1}^{N}(y_i - E(y))^2 \tag{15}$$

$$\mathrm{Cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{16}$$

According to Figure 11c and 11f, correlation coefficient of phase mask generated by Mandelbrot is less than Julia fractal image. Due to higher randomness, Mandelbrot phase mask is used as the second phase mask in the *DRPE* algorithm.



(a) (b) (c)

(d) (e) (f)

Figure 11. Effect of normalization process on the combined image's quality: (a) PM2 generated from Julia set, (b) histogram of (a), (c) correlation analysis of (a) $r = 0.2219$, (d) PM2 generated from Mandelbrot set, (e) histogram of (d), and (f) correlation analysis of (d) $r = 0.0439$.

Although the original fractal image and the one generated by incorrect parameters Table 2 seem similar, the plain image cannot be reconstructed. This indicates that the proposed method is very sensitive to the keys. Figure 12 depicts the difference between these fractal images. According to Figures 12c and 12f, Mandelbrot set is more sensitive than Julia set. Since Mandelbrot fractal image is more sensitive to its initial parameters and generates more random phase mask, it is employed in this study.

Despite the fact that 25% of pixels in phase masks are changed and the conventional *DRPE* method is adopted, the encrypted image is still recognizable. The combination of cryptography methods like chaos and fractal with *DRPE* considerably raises its security. Using incorrect keys or initial parameters results in different phase masks and consequently different decrypted image as presented in Figure 13.

To compare the quality of original and decoded images, Mean Square Error (*MSE*) and Peak Signal to

Table 2. Parameters of incorrect fractal images.

Julia set	DX= -1.6	DY = 1.6	Zoom =1	Iteration=68	RE=0.45	IM =0.255		
Mandelbrot set	DX= -4	DY = 4	Zoom =1	Iteration=151	RE=0.5	IM =0.5	c=1	a=0.505

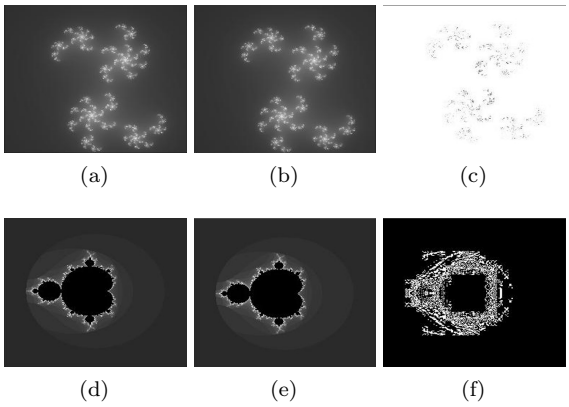


Figure 12. Comparing sensitivity of Julia and Mandelbrot sets to initial parameters: (a, b) two fractal images generated by Julia set with different parameters, (c) difference of (a) and (b) (shown in negative format), (d, e) two fractal images generated by Mandelbrot set with different parameters, and (f) difference of (c) and (d).

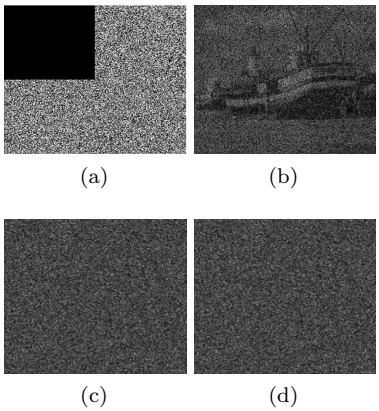


Figure 13. Comparing key sensitivity in conventional *DRPE* method and the proposed method: (a) occluded phase mask in conventional *DRPE* method, (b) decrypted image using phase mask (a), (c) decrypted image in the proposed method with incorrect $y_0 = 0.0084$, and (d) decrypted image in the proposed method with incorrect fractal parameter $C = 0.505$.

Noise Ratio (*PSNR*) are applied. *MSE* and *PSNR* are defined as follows:

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} [Image_{reconstructed}(i,j) - Image_{original}(i,j)]^2 \quad (17)$$

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \quad (18)$$

where $M \times N$ is size of the image. Obviously, lower *MSE* and higher *PSNR* values are desirable.

5 Security Analysis

Encryption methods should be robust to noise and attacks. In this section, performance of the proposed method is evaluated applying different kinds of noises and superimposing commonplace attacks. In the following, robustness of the proposed and the conventional *DRPE* method for phase mask generation is compared. After the encryption process and utilizing each of the aforementioned methods, the encrypted image is embedded into a host image. Different attacks may be imposed on the combined image. Cropping attack, also called occlusion, is one of the most common types that makes some parts of the image totally black. Low-pass filtering is another typical attack to eliminate image's details. In the following, a Gaussian low-pass filter is used. Transmitting the image through a comminucation channel, it may be affected by some noise. This section examines the impact of Gaussian white noise on watermark detection. Figures 14-16 compare the proposed method and the standard *DRPE* method under these attacks. Based on Figure 14, cropping robustness of the proposed method is the same with the conventional *DRPE* method. Nonetheless, the proposed method outperforms the conventional *DRPE* method in the case of low-pass and Guassinan noise attacks (Figures 15 and 16).

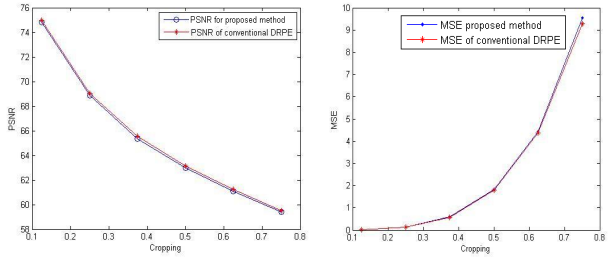


Figure 14. Robustness to cropping attack.

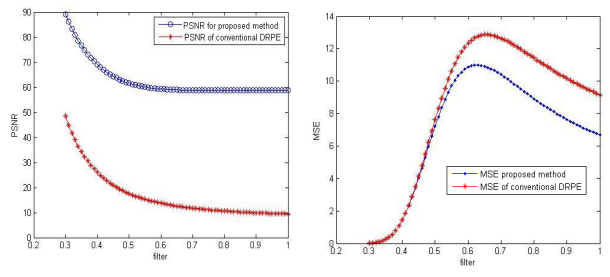


Figure 15. Robustness to Gaussian low-pass filtering attack.

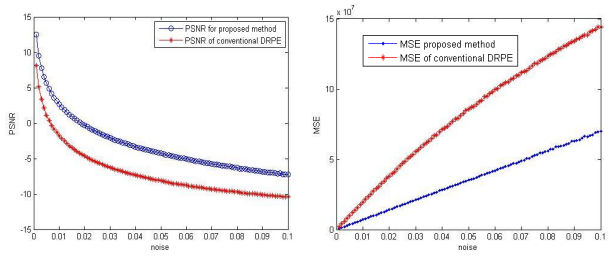


Figure 16. Robustness to Gaussian white noise attack.

6 Conclusion

In the conventional *DRPE* method, two random phase masks are required to reconstruct the original image. These large keys should be transmitted through a secure channel. Another drawback of the conventional *DRPE* method is its low sensitivity to the keys (phase masks). In this study, phase masks are obtained by chaos using fractal image as its input image. To generate this phase masks, the initial condition and parameters of chaos and parameters of fractal image should be transmitted through a secure channel. Number of keys is much less than the conventional *DRPE* method and other state-of-the-art techniques. Minor changes in one of these parameters are enough to produce a drastic change in phase mask and consequently inhibit the plain image retrieval. The encoded image can be hidden in an enlarged normalized host image after being modulated by sine and cosine functions. This method eliminates the detrimental effect of the direct information superposition on the decrypted image. The experimental results reveal that the regenerated image not only has high quality, but it resists the common attacks.

References

[1] B. Javidi, "Optical and digital techniques for information security," *Advanced Science and Technologies for Security Applications, Springer, New York*, Volume 1, 2005.

[2] Y. Sheng, X. Yan-hui, and L. Ming-tang, Y.Shuia and S. Xin-juani, "An improved method to enhance the security of double random-phase encoding in the Fresnel domain," *Optics & Laser Technology*, Volume 44, pp. 51–56, 2012.

[3] W. He, X. Peng, and X. Meng, "A hybrid strategy for cryptanalysis of optical encryption based on double-random phase–amplitude encoding," *Optics & Laser Technology*, Volume 44, pp. 1203–1206, 2012.

[4] J. Sang, H. Xiang, N. Sang, and L. Fu, "Increasing the data hiding capacity and improving the security of a double-random phase encoding technique based information hiding scheme," *Optics Communications*, Volume 282, pp. 2713–2721, 2009.

[5] J. Sang, H. Xiang, L. Fu, and N. Sang, "Security analysis and improvement on a double-random phase encoding technique based information hiding method," *Optics Communications*, Volume 282, pp. 2307–2317, 2009.

[6] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Optics Letters*, Volume 20, pp. 767–769, 1995.

[7] G. Unnikrishnan, J. Joseph and K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," *Optics Letters*, Volume 25, pp. 887–889, 2000.

[8] G. Situ and J. Zhang, "A cascaded iterative fourier transform algorithm for optical security application," *Optik-International Journal for Light and Electron Optics*, Volume 114, pp. 473–477, 2003.

[9] F. Mosso, M. Tebaldi, R. Torroba, and N. Bolognini, "Double random phase encoding method using a key code generated by affine transformation," *Optik-International Journal for Light and Electron Optics*, Volume 122, pp. 529–534, 2011.

[10] N. Singh and A. Sinhai, "digital image watermarking using gyrator transform and chaotic maps," *Optik-International Journal for Light and Electron Optics*, Volume 121, pp. 1427–1437, 2010.

[11] N. Singh and A. Sinhai, "optical image encryption using fractional fourier transform and chaos," *Optics and Lasers in Engineering*, Volume 46, pp. 117–123, 2008.

[12] Z. Xin, L. Dong, Y. Sheng, L. Da-hai, and H. Jian-Ping, "A method for hiding information utilizing double random phase encoding technique," *Optic and Laser Technology*, Volume 39, pp. 1360–1363, 2007.

[13] X. Zhou and J. G. Chen, "Information hiding based on double-random phase encoding technology," *Journal of Modern Optics*, Volume 53, Number 12, pp. 1777–1783, 2006.

[14] H. Zhang, L. Z. Cai, X. F. Meng, X. F. Xu, X. L. Yang, and X. X. Shen, "Image watermarking based on iterative phase retrieval algorithm and sine-cosine modulation in the discrete- cosine – transform domain," *Optics Communications*, Volume 278, pp. 257–263, 2007.

[15] Y. Sheng, Z. Xin, M. S. Alam, L. Xi, and L. Xiao-feng, "Information hiding based on double random-phase encoding and public-key cryptography," *Optics Express*, Volume 17, Number 5, pp. 3270–3284, 2009.

[16] W. Xing-yuan, L. Fan-ping and W. Shu-guo, "Fractal image compression based on spatial correlation and hybrid genetic algorithm," *Journal of Visual Communication and Image Representation*, Volume 20, pp. 505–510, 2009.

[17] M. Braverman, "Hyperbolic Julia Sets are Poly-Time Computable," *Electronic Notes in Theoretical Computer Science*, Volume 120, pp. 17–30, 2005.

[18] R. Valerij, "symmetry of the modified mandelbrot set," *pi in the sky (9)*, pp. 20–21, 2005.

[19] http://www.eclectasy.com/Fractal-Explorer/

[20] Y Wang, K-W. Wong X. Liao, and G. Chen, "A chaos-based image encryption algorithm with variable control parameters," *Chaos, Soliton and Fractals*, Volume 41, Number 4, pp. 1773–1783, 2009.

[21] M. Taheri and S. Mozaffari, "A hybrid approach for double random phase encoding technique reinforcement," *20th Iranian Conference on Electrical Engineering*, 2012.

[22] M. Taheri and S. Mozaffari, "Increasing security of double random phase encoding technique using chaos theory and hash function," *9th international isc conference on information security and cryptology*, September 2012.

[23] J-B. Lee, H-H. Ko, and H-S. Koo, "Digital Image Encryption Method Using Interleaving and Random Shuffling," *Proceedings of the 6th WSEAS international conference on Multimedia systems & signal processing*, pp. 76–81, April 2006.

Motahareh Taheri received her B.S. and M.S. degrees in Electronic Engineering from Semnan University in 2010 and 2012, respectively. Her research interests are image processing and encryption.

Saeed Mozaffari received his B.S., M.S., and Ph.D. degrees in Electronic Engineering from Amirkabir University of Technology, Tehran, Iran. Since 2006, he has been a faculty member in Electrical and Computer Department of Semnan University. His research interests include digital image processing, computer vision, and pattern recognition.