Image Encryption Based on Double Random Phase Encoding

Zhe Liu, Mee Loong Yang, Wei Qi Yan
Department of Computer Science
Auckland University of Technology, Auckland New Zealand 1010

***Abstract*—**In this paper, we propose an improved image encryption algorithm based on double random phase encoding (DRPE). Our contribution is the design of a new algorithm which uses Discrete Cosine Transform (DCT) to replace Discrete Fourier Transform (DFT) so as to avoid operations on complex numbers. Thus, we use a logistic map to generate random matrices instead of random phase masks in the traditional DRPE so as to decrease the number of secret key. We tested the algorithm using five types of attacks, the results indicate that the improved algorithm overcomes weaknesses of traditional scrambling methods, it has shown strong resilience against statistical attacks. The advantage of this algorithm is that it is convenient to verify whether the encrypted images have been tampered.

Keywords—image encryption; double random phase encoding; chaotic scrambling; discrete cosine transform; logistic map

I. Introduction

Optical cryptographic techniques have been widely used in image security because this kind of techniques can deal with a large amount of data rapidly with image processing algorithms. In particular, image encryption has attracted public attention since the DRPE has been proposed [1]. DRPE uses the techniques such as 4f and Fourier Transform (FT) enabling the spatial and spectral information to be encrypted [1]; the image encryption is implemented by using random-phase encoding for both the input and the Fourier planes; in this way, the whole encryption process converts the input image into white noise. The decryption is conducted by using its inverse process. The decrypted image is correctly obtained only if the secret key and its spatial information are exactly matched. In general, the random phase masks could be treated as secret keys and the key space is very large; thus, it is extremely difficult to reconstruct the original image by using blind deconvolution only.

There are two problems with DFT-based DRPE. First of all, the secret keys refer to two random phases *M* and *N*, these two matrices have the size as same as its resolution of the original image; therefore, they are too large. The second problem is DRPE based on Discrete Fourier Transform (DFT) which requires a large storage. Because of these two problems, the computing costs of DRPE are very high. Therefore, we believe that our improved algorithm reduces the costs greatly.

In this paper, we propose a new algorithm using DCT instead of traditional DFT in DRPE. The encrypted image is a real matrix so that an amount of data for encryption has been reduced. Based on traditional scrambling algorithm, we propose a new algorithm. We use a few parameters to generate a chaotic map, this map could be treated as the random matrix for DRPE. The initial parameters are regarded as the secret key so that the size of this key has been greatly reduced. Because the chaotic map is very sensitive to these parameters, a minor change will cause great influence which makes it difficult to break the encryption without the secret key.

We will introduce the background of this paper in Section II. Our method is depicted in Section III. The results and analysis are presented in Section IV as well as the conclusion and future work are stated in Section V.

II. BACKGROUND

In this section, the methods of optical image encryption and chaotic system encryption will be detailed.

A. Optical image encryption

Since the double random phase encoding (DRPE) was proposed in 1995 [1], a large number of image encryption algorithms based on DRPE have been proposed, DRPE technique thus witnessed the development of optical cryptography. With deep investigation of this technique, the defects of DRPE have been realized. For example, the 4f system requires complex conjugate phase plate during the decrypted process [1] and the encrypted image is a complex matrix, etc. Based on these shortcomings, the corresponding improvement has been developed.

In 2000, an optical image encryption was proposed based on joint transform correlator (JTC) [2]. In this work, the original image and one of the phase plates, which is used as the encryption key, are put together on the JCT input plane; then, the Fourier Transform is adopted. After the transform, the joint Fourier power spectrum is obtained as the encrypted image. During the decryption process, the phase plate, which is used as the decryption key, is arranged at the corresponding position on the space plane; the encrypted image is arranged on the Fourier spectrum plane through frequency domain filtering and inverse Fourier transform. In this way, JTC encryption overcomes the disadvantages of traditional DRPE. As the encrypted image is based on a Fourier power spectrum, it is workable and unnecessary to let the complex conjugate phase plate be as the secret key; the improvement of secret key on the input plane only changes the position of decrypted image; therefore, the quality of decrypted cannot be affected.

In traditional DRPE, there are only two phase plates as secret keys. In order to obtain more keys and improve performance, Fractional Fourier Transform (FFT) is proposed as a more general DRPE scheme [3]. There are three planes: input plane, encrypted plane and output plane. The FFT has three parameters connecting any two out of three planes; thus, not only has the scheme used two phase plates as the secret keys, but also the six parameters can also be supplied as the secret key, the key space is greatly enlarged.

In 2000, a generalized image encryption algorithm based on fractional Fourier transform [4] was proposed, this method allows us to use a new generalized fractional Fourier transform instead of random phase mask. In this algorithm, the period of fractional Fourier transform is extended to any integer; thus, the period and transformation index are regarded as two secret keys. The generalized fractional Fourier transform is based on realignment of traditional fractional Fourier transform which is called multistage FRT or multichannel FRT.

In 2013, a multi-image encryption algorithm was proposed based on cascaded fractional Fourier transform [5]. In this method, the input images are successively encrypted using a series of encryption keys until a final encrypted image is obtained. The algorithm not only works for the encryption of multiple images, but also is very secure. Because there are so many secret keys, the algorithm can be applied to multi-user authentication.

In 2004, a new method, which encrypts the image in the Fresnel domain [6], has three planes: input plane, encryption plane, and output plane. Unlike encryption, the method does not require lenses; instead, it uses Fresnel diffraction to encrypt images. In the process of encryption, the original image is modulated first by using the phase plate in the input plane. Next, the Fresnel diffraction is employed; the image proceeds at the encryption plane and it is modulated for the second time. Finally, the Fresnel diffraction is applied one more time. In the process of encryption, not only the two phase plates are employed as the secret key, but also the two diffraction distances have been applied as the keys.

Discrete cosine transform (DCT) was widely used in image encryption and information hiding [7]. In 2010, a color image encryption algorithm was proposed based on Arnold transform and DCT [8]. DCT was chosen because the pixel value of the image is defined in the real domain and the matrix still remains in the real domain after the transformation. On the other hand, the partition operation was applied before Arnold transform so that the operation can be clearly seen. As a result, the security of the encrypted images was improved successfully.

B. *Chaotic-based encryption*

Chaos-based encryption algorithm is the most widely used algorithm till today. Chaotic system is a nonlinear dynamic system [9] which can produce pseudo-random sequence with good randomness and is very suitable for data encryption. The chaotic system was proposed for data encryption [10]. Since then, chaotic cryptography as a branch of cryptography has been investigated broadly.

Relying on randomness, which is generated by the chaotic system, digital images have been encrypted by using chaotic mapping algorithm such as CKBA encryption method [11], Kolmogorov flows-based encryption systems [12], image replacement and encryption [13] and chaotic logistic map-based encryption [14].

In combination with the corresponding mathematical methods, the initial values of two logistic sequences are generated by using an external key with the length of eighty bytes and eight types of operations to encrypt the pixels of the image. Each of the 16 pixels of the image is grouped into a small block, and each bit of the pixel is operated by using the logistic chaotic sequence. Therefore, the robustness of this algorithm is very high, and the capability against attacks of the algorithm is also strong.

In 2012, the standard map [15] was improved so that it could change the pixel positions. In the chaotic mapping algorithms, the chaotic sequence, which is generated by using secret key stream, is usually used to scramble the pixels. For this improved algorithm, it not only relates to secret key in the scrambling process, but also associates to pixel positions which have been scrambled. This scrambling method improves the security of the encryption and enhances its ability against various attacks.

In this paper, we propose a new image encryption algorithm based on chaotic mapping and DRPE. We combine theoretical analysis and experimental results together and use MATLAB to implement the algorithm. We also apply five typical methods to verify the encrypted images; finally, the anti-attack analysis will be given.

III. Our Method

In this section, we firstly introduce a widely used chaotic scrambling method based on logistic map. Then, we design an improved method by using DCT-based DRPE and traditional DFT. Afterwards, we will implement the new encryption method which combines chaotic scrambling and DCT together; we will describe the experimental steps for each method as well.

A. *Method 1: Chaotic scrambling based on logistic map*

The logistic map is a polynomial mapping, which has been widely used for image encryption. The traditional logistic map generates a chaotic sequence, and the number of elements in this sequence is equal to the number of pixels in the original image. We will explain how to use the logistic map for image encryption. Eq. (1) is used as the logistic map to generate the random sequence and furthermore to encrypt a digital image [14].

$$X_{n+1} = \mu X_n(1 - X_n) \tag{1}$$

where $X_n \in [0,1]$ and $\mu \in [0,4]$ is a constant. The previous work has shown that when $X_0 \in [0,1]$, the logistic map works in a chaotic state; in this case, the sequence which is generated by using logistic map is aperiodic and non-convergent, and if X_0 is beyond the range of $[0,1]$, the sequence converges to a particular value. In our experiment, we selected μ on the interval [3.569,4] and used the generated sequence to encrypt an image directly. We sort the double precision sequence which is generated by using the logistic map, we scramble the location of each pixel of the original image. We used MATLAB to implement the process as:

Step 1. Convert the original color image into greyscale one, the size of the greyscale image is W × H ;

Step 2. Given the logistic initial values X_0 and the parameter μ as two secret keys, after iterated the computation for W × H times, a random W × H matrix is obtained.

Step 3. Convert the image from a two-dimensional matrix into a one-dimensional sequence. We sort the result by following the way in Step 2;

Step 4. Covert the one-dimensional sequence in Step 3 back into two-dimensional image to obtain the encrypted image.

The decryption is the reverse process of its encryption. The encrypted image is transformed into one dimensional vector. Because we know the method in Step 2, if we use the right secret keys (X_0 and μ), we will get the one-dimensional sequence of original image. Finally, we transpose this one-dimensional sequence into two-dimensional matrix, the decrypted image is obtained.

B. Method 2: Chaotic map based on DRPE by using DCT

DRPE was implemented using an optical setup called 4f system which is illustrated in Fig.1.

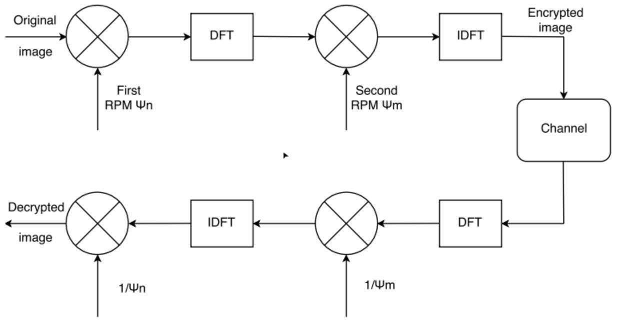


Fig.1. The work flow of DRPE by using DFT

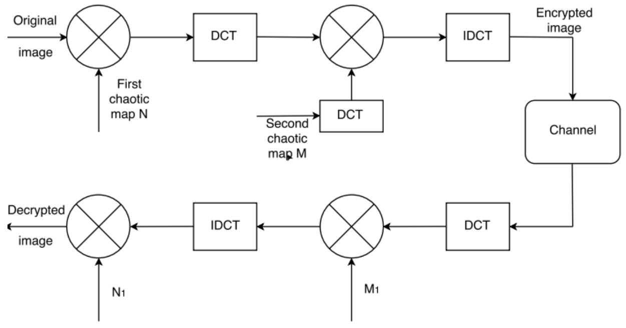


Fig.2. The work flow of DRPE by using DCT

Now, let's consider a primary intensity image $\mathrm{OI}(x,y)$, where x and y are the coordinates of a pixel in spatial domain, u and v represent the corresponding coordinates in Fourier domain. Let $\mathrm{EI}(x,y)$ denote the encrypted image, $N(x,y)$ and $M(x,y)$ stand for two uniformly distributions. To encode $\mathrm{OI}(x,y)$ into a white stationary sequence, two random phase masks are used: $\Psi_n(x,y) = exp[2i\pi N(x,y)]$ and $\Psi_m(x,y) = exp[2i\pi M(x,y)]$. We thus perform two operations. First, we multiply this image by using the first phase mask $\Psi_n(x,y)$; then, we conduct convolution of this image by using the impulse response $H(x,y)$, which is a phase transfer function and $H(x,y) = M(x,y)$. The impulse response $H(x,y)$ is defined by using Fourier transform.

$$\mathrm{DFT}\{H(x,y)\} = H(u,v) = \Psi_m(u,v) = exp[2i\pi M(u,v)] \quad (2)$$

where $N(x,y)$ and $M(x,y)$ are secret keys. The encryption function is

$$\mathrm{EI}(x,y) = \{\mathrm{OI}(x,y)\cdot \Psi_n(x,y)\} * \mathrm{IDFT}\{\Psi_m(u,v)\} \quad (3)$$

Since we have used convolution operation in Eq. (3), the convolution theorem is represented as Eq. (4)

$$f * g = \mathrm{IFT}[\mathrm{FT}(f)\cdot \mathrm{FT}(g)] \quad (4)$$

where f and g are two integrable functions, FT refers to Fourier transforms and IFT refers to its Inverse Fourier transforms.

Based on Fig.1 and the convolution theorem, we use Eq. (5) to encrypt a plaintext and the decryption is a reserve process of encryption.

$$\mathrm{EI}(x,y) = \mathrm{IDFT}\{\mathrm{DFT}[\mathrm{OI}(x,y)\cdot \Psi_n(x,y)]\cdot \Psi_m(u,v)\} \quad (5)$$

Based on traditional DFT and 4f system, we use DCT to replace DFT and proposed the new method. Meanwhile, DCT is a transformation related to the traditional Fourier transform, it is similar to DFT, but it only uses real arithmetic operations to process the image. Using DCT to facilitate the process of image encryption and decryption, it avoids complex operations. Therefore, we design the DCT method based on DRPE; in the traditional DRPE system, we use two random phase matrices $N(x,y)$ and $M(x,y)$ as secret keys which are uniformly distributed in $[0,1]$, the size of these two matrices is equal to the original image $\mathrm{OI}(x,y)$. We see that the amount of secret keys is too large, so it's inconvenient for transmission. Based on logistic mapping, we use Eq. (1) to generate chaotic maps and the traditional random phase matrices are replaced by using the generated chaotic maps so that the initial value x_0 and parameter μ of the chaotic maps can be utilized as secret keys, the size of secret keys is reduced effectively. Based on Fig.2, the encryption process can be presented as following steps:

Step 1. Select a set of independent random parameters (x_{01}, μ_1), where $X_{01} \in [0,1]$ and $\mu_1 \in (3.569, 4]$ are constants. We use (x_{01}, μ_1) to generate chaotic map N as the first random matrix;

Step 2. Select another set of independent random parameters (x_{02}, μ_2), where $X_{02} \in [0,1]$ and $\mu_2 \in (3.569, 4]$ are constants, we use (x_{02}, μ_2) to generate chaotic map M as the second random matrix;

Step 3. The original image **I** is multiplied by using the first chaotic map N to get $\mathbf{I}_1$=N·**I**.

Step 4. Apply the DCT transform to the cyphertext $\mathbf{I}_1$ we got in Step 3, then apply the DCT transform to the second chaotic map M, we get DCT(M).

Step 5. Multiply the cyphertext from Step 4 by using DCT(M) to get $\mathbf{I}_2$= DCT(M)·$\mathbf{I}_1$;

Step 6. Apply Inverse-DCT (IDCT) to $\mathbf{I}_2$ to get the encrypted image E(**I**) =IDCT($\mathbf{I}_2$) and transmit it to receivers along with the keys.

When a receiver received the keys and the encrypted image E(**I**), the image could be decrypted, the decryption is a reverse process of encryption, which is represented as following steps:

Step 1. DCT will be first applied to the encrypted image E(**I**), $\mathbf{I}'_2$=DCT(E(**I**));

Step 2. For the matrix DCT(M), calculate its inverse matrix and get matrix M_1 =$[\mathrm{DCT(M)}]^{-1}$, then multiply the cyphertext $\mathbf{I}'_2$ we got in Step 1 by M_1;

Step 3. Apply Inverse-DCT (IDCT) to the cyphertext $\mathbf{I}'_1$=IDCT($\mathbf{I}'_2 \cdot M_1$) we got from Step 2;

Step 4. For the matrix N, calculate its inverse matrix and get matrix N_1, then multiply by N_1 to get the decrypted image $\mathbf{I}' = \mathbf{I}'_1 \cdot \mathrm{N}^{-1}$

IV. Results and Discussions

In this section, we present the dataset and the results of our experiments. To evaluate the performance, we introduce the specific attacks and the relevant image metrics. We will also provide the results corresponding to algorithm evaluation for each encryption method.

In our experiments, the traditional method based on logistic chaotic map as well as the proposed method based on DRPE using DCT were tested by using four sample images as shown in Fig.3. During the experiment, we applied five types of attacks to the encrypted images: Gaussian noise, salt-and-pepper noise, average filter, image cropping and image rotation.

Given the original image, the decrypted image and the image size $\mathrm{W} \times \mathrm{H}$, we use five metrics to measure the encrypted images: Mean Square Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Normalization Cross Correlation (NCC), Number of Pixels Change Rate (NPCR), and Structure Similarity Index (SSIM).

(a) Airplane (b) Lake (c) Lena (d) Pepper

Fig.3. Four images with the size of 512×521in the dataset.

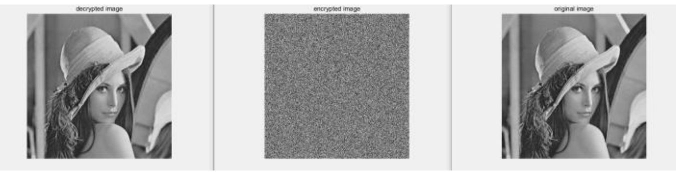


Fig.4. The original, encrypted and decrypted images in Method 1.

A. *Image scrambling based on logistic chaotic map*

Let the logistic parameter $\mu = 3.8$ and the initial value $X_0 = 0.5$, we used 4 original images in the dataset to conduct our experiments. We chose image Lena to illustrate the results, the encrypted and decrypted images are shown in Fig.3.

Based on the results, we see that the location of each pixel has been changed after logistic mapping. From the decrypted images, we see that the details of original image are perceptual. We find that all of the four results meet the expectations and the encryption method based on logistic map has satisfactory performance.

As we know, the initial value X_0 and parameter μ were used as secret keys in this method. We used original image Lena as the example to conduct the sensitivity test of secret key. Let the logistic parameter $\mu = 3.8$ and the initial value $X_0 = 0.5$, we analyze the sensitivity of secret keys. The results are as shown in Fig. 5.

In Fig.5, x-axis shows the difference between stochastic secret key and real secret key. The Normalized Cross Correlation (NCC) between the decrypted image and the original image. The NCC is distributed on the interval $[-1,1]$, larger the NCC, higher the similarity between two images. During the test, we fixed one secret key and slightly tuned the other. In Fig.5, when one of the secret key is correct, if the other has a small deviation, the decrypted results will be different from the decrypted result. Thus, we cannot get the original one from the incorrect result. This conclusion shows the sensitivity of secret keys for chaotic scrambling algorithm based on logistic map.

We applied five attacks to all the images in the dataset, the performance of specific metrics against each attack for each image was similar. We selected the results for image Lena as the example for our analysis in Table I. For the attack methods, average filter and image rotation show lower similarity between the decrypted image and its original image. Compared with other three attack methods, the results reflect that the chaotic scrambling method can resist Gaussian noise, salt-and-pepper noise and image cropping. The reason is that these three methods only change a part of pixels in the encrypted image. For the attack methods average filter and image rotation, these two methods modify all of the pixels in the encrypted pixels, the chaotic scrambling method cannot resist such intensive attacks.

Utilizing the scrambling method based on logistic map, we generated a chaotic sequence which contains the same number of pixels as the original image. Then, we used this sequence to scramble the image, the scrambling result is achieved. The method resists noise attack and image cropping attack preferably, but it cannot resist intensive attack (average filter and image rotation); meanwhile, the sensitivity of secret key for this method is high so that the security level has been improved. However, this method requires large amount of calculations, the processing time is longer, and the logistic map only changes the location of each pixel, the encrypted image does not change the pixel distribution compared with the original image. Therefore, this method cannot resist statistical attack.

B. *Method 2: DRPE based on DCT*

We used four original images in the dataset to verify the encryption algorithm, we chose the image Lena to generate the results in Fig.6. From these figures, we see the original images and the decrypted images are different obviously. Therefore, the proposed algorithm is successful.

In our proposed algorithm, DCT is applied to encrypt the images; thus, the pixel intensity has been changed. Compared the encrypted images with the original ones, the histogram will be different significantly. We used image Lena as the example to generate the result.

We used different initial values and parameters to run the test, In Fig.7, we used $x_{01} = 0.703, x_{02} = 0.264, \mu_1 = 3.938, \mu_2 = 3.611$. With regard to the greyscale image, the histogram will be increased sharply as shown in Fig 7(a). When the original image is encrypted, because the pixel intensity has been modified, the histogram will be changed correspondingly. In Fig.7 (b), we see that the pixels are on a normal distribution. In this case, it is difficult for an attacker to decrypt the image only by using the histogram of the encrypted image; thus, it will reduce the possibility to be decrypted through the histogram only.

As we know, (x_{01}, μ_1) and (x_{02}, μ_2) in logistic map are used as secret keys in proposed method, we let $x_{01} = x_{02} = 0.5, \mu_1 = \mu_2 = 3.8$, we analyze the sensitivity of secret keys, and the results are illustrated as Fig. 8. We also fixed 3 out of 4 secret keys, and changed the other secret keys to run the test, In Fig.8, we see that the decrypted result is more sensitive to secret keys x_{02} and μ_2 than secret keys x_{01} and μ_1, so the deviations of x_{01} and μ_1 have limited impact on decryption, but the deviation of x_{02} and μ_2 have great impact on decryption.

We have applied five attacks to all encrypted images, the results show that all images have been decrypted unsuccessfully. We selected the image Lena as the sample for evaluation, the results are shown in Table II. The results for the others are similar to the results of Lena. Compared with the results from the chaotic scrambling method, the DCT-based method cannot resist the tampers from image cropping, average filtering or image rotating, which means that the proposed method is much robust to attacks even if we change a little bit of pixels in encrypted image, the decryption is still failure. Based on this venerability, we easily verify whether an image has suffered attacks or not.

This encryption method is based on traditional double random phase encoding and 4f method. In order to facilitate the whole process, we replace the traditional DFT with DCT to avoid complex operations; we also substitute traditional random phase matrices with chaotic maps. Two sets of initial values and parameters were used as secret keys so that the amount of secret keys has been decreased. With regard to secret key sensitivity test, the sensitivity for this method is high, so the security level has been improved; With regard to anti-attack ability, because this method has changed the intensity of each pixel, the pixel distribution has been modified correspondingly. Based on the histogram of the encrypted image, we see that it follows normal distribution, the method can resist statistical attack; thus, the security level is high; on the other hand, we have applied five attacks to this method, and the decryption is failure.

V. Conclusion and Future Work

In this paper, we briefly introduced image encryption; then, we designed a method based on logistic map and proposed a new method based on DRPE by using DCT and chaotic maps. We provided the analysis for these two methods. The combined method overcomes the shortcoming. The experimental results along with the anti-attack ability and secret key sensitivity have been analyzed on details. Our future work will be on image encryption using multiple ways, especially in using the methods from artificial neural network and artificial intelligence.

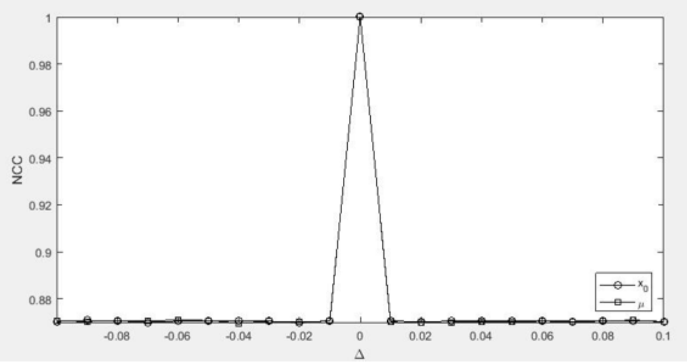


Fig.5. The sensitivity test of secret key for Method 1

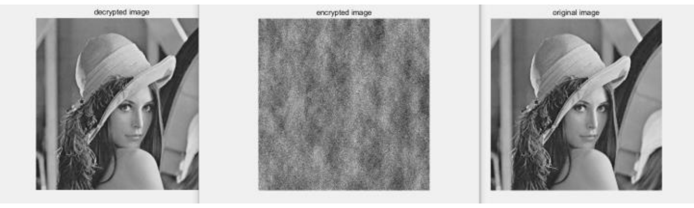
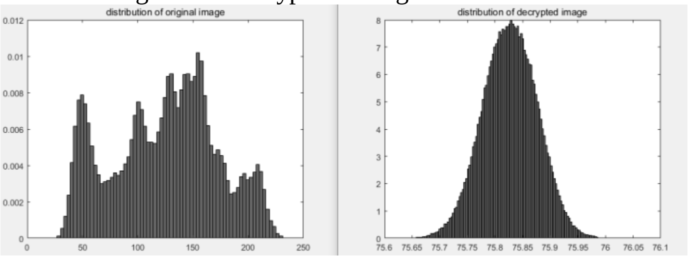


Fig.6. The encryption using the method 2.



(a) (b)

Fig.7. The histograms of the original image and its encrypted image, (a) the histogram of the original image, (b) the histogram of the encrypted image.

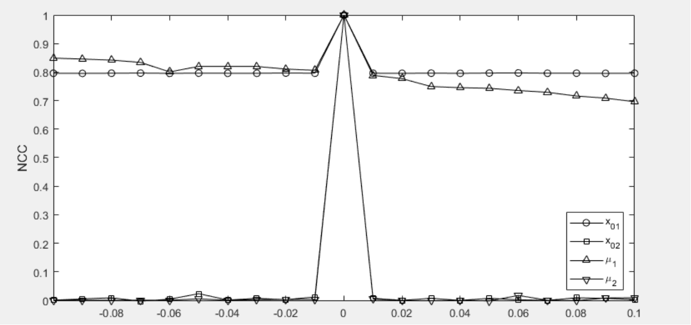
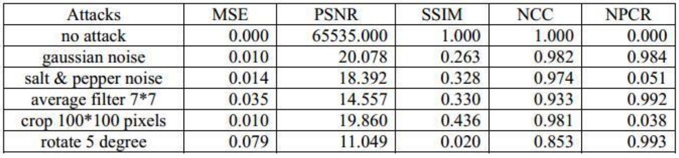


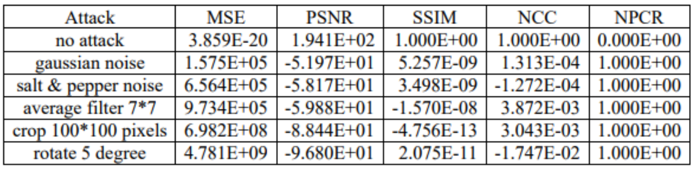
Fig.8. The sensitivity test of each key for Method 2

Table I. Image metrics for chaotic scrambling



Attacks	MSE	PSNR	SSIM	NCC	NPCR
no attack	0.000	65535.000	1.000	1.000	0.000
gaussian noise	0.010	20.078	0.263	0.982	0.984
salt & pepper noise	0.014	18.392	0.328	0.974	0.051
average filter 7*7	0.035	14.557	0.330	0.933	0.992
crop 100*100 pixels	0.010	19.860	0.436	0.981	0.038
rotate 5 degree	0.079	11.049	0.020	0.853	0.993

Table II. Specific metrics for DCT based encryption



Attack	MSE	PSNR	SSIM	NCC	NPCR
no attack	3.859E-20	1.941E+02	1.000E+00	1.000E+00	0.000E+00
gaussian noise	1.575E+05	-5.197E+01	5.257E-09	1.313E-04	1.000E+00
salt & pepper noise	6.564E+05	-5.817E+01	3.498E-09	-1.272E-04	1.000E+00
average filter 7*7	9.734E+05	-5.988E+01	-1.570E-08	3.872E-03	1.000E+00
crop 100*100 pixels	6.982E+08	-8.844E+01	-4.756E-13	3.043E-03	1.000E+00
rotate 5 degree	4.781E+09	-9.680E+01	2.075E-11	-1.747E-02	1.000E+00

REFERENCES

[1] Refregier, P., & Javidi, B. (1995). Optical image encryption based on input plane and Fourier plane random encoding. *Optics Letters*, *20*(7), 767-769.

[2] Nomura, T., & Javidi, B. (2000). Optical encryption using a joint transform correlator architecture. *Optical Engineering*, *39*(8), 2031-2035.

[3] Unnikrishnan, G., Joseph, J., & Singh, K. (2000). Optical encryption by double-random phase encoding in the fractional Fourier domain. *Optics letters*, *25*(12), 887-889.

[4] Zhu, B., Liu, S., & Ran, Q. (2000). Optical image encryption based on multifractional Fourier transforms. *Optics letters*, *25*(16), 1159-1161.

[5] Kong, D., Shen, X., Xu, Q., Xin, W., & Guo, H. (2013). Multiple-image encryption scheme based on cascaded fractional Fourier transform. *Applied optics*, *52*(12), 2619-2625.

[6] Situ, G., & Zhang, J. (2004). Double random-phase encoding in the Fresnel domain. *Optics Letters*, *29*(14), 1584-1586.

[7] Ahmed, N., Natarajan, T., & Rao, K. R. (1974). Discrete cosine transform. *IEEE Transactions on Computers*, *100*(1), 90-93.

[8] Liu, Z., Xu, L., Liu, T., Chen, H., Li, P., Lin, C., & Liu, S. (2011). Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains. *Optics Communications*, *284*(1), 123-128.

[9] Li, T. Y., & Yorke, J. A. (1975). Period three implies chaos. *The American Mathematical Monthly*, *82*(10), 985-992.

[10] Matthews, R. (1989). On the derivation of a “chaotic” encryption algorithm. *Cryptologia*, *13*(1), 29-42.

[11] Guo, J. I. (2000). A new chaotic key-based design for image encryption and decryption. In *IEEE International Symposium on Circuits and Systems, Geneva*. (Vol. 4, pp. 49-52).

[12] Scharinger, J. (1998). Fast encryption of image data using chaotic Kolmogorov flows. *Journal of Electronic imaging*, *7*(2), 318-325.

[13] Guan, Z. H., Huang, F., & Guan, W. (2005). Chaos-based image encryption algorithm. *Physics Letters*, *346*(1), 153-157.

[14] Pareek, N. K., Patidar, V., & Sud, K. K. (2006). Image encryption using chaotic logistic map. *Image and Vision Computing*, *24*(9), 926-934.

[15] Fu, C., Chen, J. J., Zou, H., Meng, W. H., Zhan, Y. F., & Yu, Y. W. (2012). A chaos-based digital image encryption scheme with an improved diffusion strategy. *Optics Express*, *20*(3), 2363-2378.

[16] Feng, C., & Ye, H. (2017). A Digital Image Encryption Algorithm Based on Improved ZigZag Transformation and Chaotic Sequence. Computer Science and Application, 7(6), 554-561

[17] Mohamed, M. A., Samrah, A. S., & Fath Allah, M. I. (2017). DWT versus WP Based Optical Color Image Encryption Robust to Composite Attacks. *Advances in OptoElectronics*, *2017*.

[18] Fan, H., & Li, M. (2017). Cryptanalysis and Improvement of Chaos-Based Image Encryption Scheme with Circular Inter-Intra-Pixels Bit-Level Permutation. *Mathematical Problems in Engineering*, *2017*.

[19] Thajeel, S. A., Kadhim, L. M., & Abdlateef, S. A. (2017). A New Color Image Watermarking Technique Using Multiple Decompositions. *Journal of Theoretical & Applied Information Technology*, *95*(10).

[20] Wang, Z., Simoncelli, E. P., & Bovik, A. C. (2003). Multiscale structural similarity for image quality assessment. In *Asilomar Conference on Signals, Systems and Computers* (Vol. 2, pp. 1398-1402).

[21] Fan, H., & Li, M. (2017). Cryptanalysis and Improvement of Chaos-Based Image Encryption Scheme with Circular Inter-Intra-Pixels Bit-Level Permutation. *Mathematical Problems in Engineering*, *2017*.

[22] Mohamed, M. A., Aboutaleb, M., Abdel-Fattah, M. G., & Samrah, A. S. (2015). Hybrid watermarking scheme for copyright protection using chaotic maps cryptography. *International Journal of Computer Applications*, *126*(4).

[23] Liu, Z., Li, S., Liu, W., Wang, Y., & Liu, S. (2013). Image encryption algorithm by using fractional Fourier transform and pixel scrambling operation based on double random phase encoding. *Optics and Lasers in Engineering*, *51*(1), 8-14.

[24] Liu, Z., Gong, M., Dou, Y., Liu, F., Lin, S., Ahmad, M. A., ... & Liu, S. (2012). Double image encryption by using Arnold transform and discrete fractional angular transform. *Optics and Lasers in Engineering*, *50*(2), 248-255.

[25] Wu, J., Zhang, L., & Zhou, N. (2010). Image encryption based on the multiple-order discrete fractional cosine transform. *Optics Communications*, *283*(9), 1720-1725.

[26] Liu, Z., Guo, Q., & Liu, S. (2006). The discrete fractional random cosine and sine transforms. *Optics communications*, *265*(1), 100-105.

[27] Liu, Y., Lin, J., Fan, J., & Zhou, N. (2012). Image encryption based on cat map and fractional fourier transform. *Journal of Computational Information Systems*, *8*(18), 7485-7492.

[28] Rao, K. R., & Yip, P. (2014). *Discrete cosine transform: algorithms, advantages, applications*. Academic press.

[29] Zhang, Y., & Xiao, D. (2013). Double optical image encryption using discrete Chirikov standard map and chaos-based fractional random transform. *Optics and Lasers in Engineering*, *51*(4), 472-480.

[30] Song, Z. Z. (2013) *Image Encryption Algorithm Based On Chaotic Mapping And Ddouble Random Phase Encoding Technology* (Master's thesis, Harbin Institute of Technology).