Algorithm Research of Known-plaintext Attack on Double Random Phase Mask Based on WSNs

Wei Wei[1,5], Marcin Woźniak[2], Robertas Damaševičius[3], Xiumei Fan[4], Ye Li[5]

[1] School of Computer Science and Engineering, Xi'an University of Technology, China
[2] Institute of Mathematics, Silesian University of Technology, Poland
[3] Software Engineering Department, Kaunas University of Technology, Lithuania
[4] School of automation and information engineering, Xi'an University of Technology, China
[5] Qilu University of Technology (Shandong Academy of Sciences); Shandong provincial Key Laboratory of Computer Network
weiwei@xaut.edu.cn, marcin.wozniak@polsl.pl, robertas.damasevicius@ktu.lt, xmfan@xaut.edu.cn, liye@sdas.org

Abstract

With the development and popularization of computer and Internet, information communication plays an irreplaceable role in the modern society. Security problems of the information exchange processing is put on the agenda. While the image as one of the most effective information carrier, has been widely used in various fields, such as residents living, national security, etc. How to ensure the safety of image transmission in the processing of nature was widespread attention, has become an important research direction in the field of information security the security of image. At present, has proposed a series of image encryption algorithm, the image encryption algorithm based on Fourier transform is a hot research topic, attracted a lot of attention. We studies and implements the image encryption algorithm based on double random phase encoding (DRPE) in this paper, implement the known plaintext attack method based on the understanding of the algorithm. In the encryption process, the first step is generating two random phase matrix, and modulating the image as a cipher image using the random phase function as the key. But because of the linear properties of the algorithm itself, the algorithm is not robust to the attacks, the simulation results also show this point.

Keywords Image encryption, Fourier transform, Double random phase encoding

1 Introduction

At present, the research of optical image encryption are developed rapidly. Lots of researchers focus on discussing the topics of information security, electronic imaging meeting, communications and multimedia security, etc. [1]. In addition, multimedia security are also concerned by the academic field. Currently, information security has caught world-wide attention. The research of multi-image encryption technology on information Security will be a subject of international frontier [2]. The inherent parallelism of light encourages increasing researches on optical information processing [3-4].

In all the possible applications, optical encryption is a promising direction. Refrégiér and Javidi's pioneering research on double random phase ecoding has paved the road for further new ideas of the optical security and encryption systems in large numbers [5]. DRP system derive a variety of new ways which have already been applied. However, only recently began a precise analysis of the DRPE security, and some weaknesses of the system began to appear. Carnicer and others proposed a way of chosen ciphertext attack [6]. The attacker recover the encryption key by tricking a legitimate user to decode some specially crafted images.

In early 1980s [6], optical technology has been applied to the field of information security [7-8]. This technology originally attached computer hologram on goods. However, since the computer hologram is visible, with the development of digital image processing technology, it is easy to retrieve the computer hologram by image processing and lose information security [9-10]. Therefore, people have to find some new security technologies with higher performance. Optical information processing technology, particularly the rise of virtual optical technology has brought new hope for information security. Optical information processing method, compared with traditional cryptography method, has the advantage of large information processing volume, fast parallel processing speed, high degree of freedom, strong robustness and so on. Thus the image encryption research based on virtual optical technology has high academic and practical value [11].

*Corresponding Author: Wei Wei; E-mail: weiwei@xaut.edu.cn
DOI: 10.3966/160792642019012001004

Optical information processing technology for image encryption has opened a new road. Since the 1990s, technology research in this field is very active. Internationally renowned academic organization SPIE, IEEE and the Optical Society of America have held several meetings and other related conference with these topics, and have repeatedly issued some conference proceedings and journals album [7-9] on optical information processing technology in order to open up a broad platform of exchange and learning for academics and promote further development of many key technologies in the field yet to be resolved, in-depth research and development of the theory. Currently the most widely used technology in business is an optical variable Device (OVD): holographic anti-counterfeiting technology using laser lamination [11]. In optical conversion system for digital image encryption and decryption, academic achievement made by professor Bahram Javidi research group at the University of Connecticut is quite representative. In 1995, they firstly proposed double random phase encoding optical encryption method based on 4-f optical signal processors [1]. This encryption method won two US patents in 1999, after which they continued to publish research achievements of image encryption and decryption by optical information processing [12-15].

In general, the development of image encryption and decryption technology mainly includes the following aspects: digital image encryption technology based on chaotic thoughts. Chaotic systems is a natural password system evolved from chaotic dynamics\ cite{16}. Image encryption algorithm adopts a new transformation method. The past encryption algorithms most of time used simple pixel scrambling method which was simpler but less safe. Then the Arnold transformation or magic transformation for image scrambling played a leading role in this field of studying the image encryption algorithm through new theories and development tools. In recent years, domestic and international academia continue to explore and research on the image encryption method based on optical transformation. The related cryptographic models have also been proposed [17-21].

In 2004, domestic scholars Luo Yong and Cheng Lizhi put forward an encryption algorithm based on wavelet transform with parameters; in 2005, image encryption algorithm based on wave [length multiplexing, location multiplexing and others has been validated; in 2005, Situ Guohai and Zhang Jingjuan proposed multi-image encryption through wavelength division and they proposed multi-image encryption through location multiplexing; to avoid interaction between images, Liu and Liu [16] proposed dual image encryption algorithm based on fractional Fourier transform (FRFT) in 2007; in 2009, Dafne Amaya, Myrian Tebaldi and others proposed multi-image encryption algorithm based on WDM of joint transform correlator framework; and in 2011, Sui Xiaoyu, Li SiKun, Liu Xiaoqing and others proposed to adopt a key multi-cycle to achieve multi-image encryption in the Fourier domain [22-27].

Cryptology includes ryptography and cryptanalysis. Our paper will focus on discussing how to use known plaintext attack to break a double random phase encoding system. Obviously, a chosen-plaintext, chosen-ciphertext, and other attacks can also accomplish the successful attack [28-33].

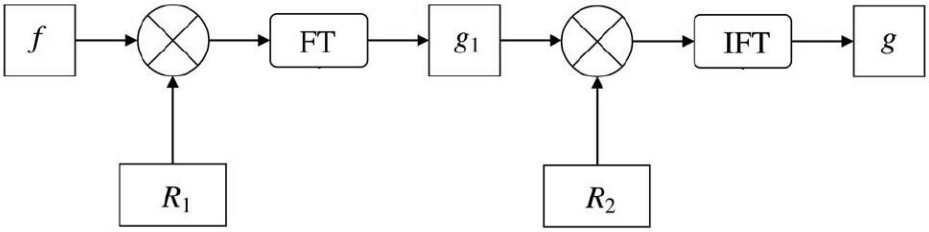
In this paper, our proposed method try our best to overcome the above mentioned shortcomings in other researchers' previous jobs. Our presented algorithm make the contribution to this domain. Our presented image encryption algorithm based on double random phase encoding technique is mainly discussed. The main work of the algorithm is to randomly generate two random phase matrixes, use the random phase function as the key to conduct Fourier transform and inverse Fourier transform on gray image being encrypted and modulate the image to similar cipher image with white noise. Decryption process is the reverse of encryption process. The use of phase retrieval algorithm can restore the former image. After understanding the fundamental knowledge of encryption algorithm, this paper studies known plaintext attack algorithms of this algorithm and put it into practice. Main tasks are as follows: Based on the basic concepts and theories of the Fourier transform and utilize these features in our scenario; Based on the Fourier transform analyze algorithm how to apply it into image encryption and decryption process; Based on primary double random phase encoding technique, encrypt a gray-scale image into ciphertext images within Fourier domain; Encrypt and decrypt the actual input image, analyze parameters transformation influence on encryption result; Design and implement a friendly demonstration system which operators can select an image input for encryption and decryption; Further research and implement the known-plaintext attack algorithm [38-52].

2 Image Encryption Based on Double Random Phase Encoding

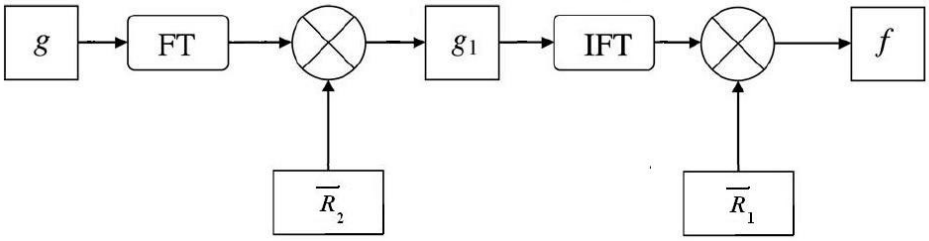
Based on the introduction mentioned, we make these specific contributions to this method. Using double random phase encoding algorithm (referred DRPE) to encrypt the plaintext into ciphertext. The flow chart of encryption and decryption is shown in Figure 1.

In Figure 1(a), $f(x,y)$ represents plain text image, and R_1 and R_2 represents random phase functions, also called encryption keys. FT represents Fourier transformation while IFT represents the inverse Fourier transform. g_1 represents an intermediate matrix generated, g represents the cipher text images $g(x,y)$, and symbols $\otimes$ represents the multiplication operation.

It can be seen, the core of DRPE are respectively applied random phase function (key) in the object plane and the spectrum of surface. DRPE algorithm firstly uses a key to matrix multiply the plaintext image $f(x,y)$, use Fourier transform it, use the second key to multiply and then use inverse Fourier transform to obtain the ciphertext images $g(x,y)$ [34-37].



(a) Flow chart of DRPE algorithm encryption



(b) Flow chart of DRPE algorithm Decryption

Figure 1. Double Random Phase Encoding Encryption & Decryption Flow Chart

2.1 Double random Phase Encoding Algorithm

Use double random phase encoding algorithm (referred DRPE) to encrypt the plaintext $g(x,y)$ into $f(x,y)$ ciphertext In Figure (a) & (b). In Figure 1(b), FT represents plain text images $f(x,y)$. $\overline{R_1}$ and $\overline{R_2}$ and is the conjugate matrix of R1 and R2. FT represents Fourier transformation while IFT represents the inverse Fourier transform. is an intermediate matrix generated, and g represents the ciphertext image $g(x,y)$. Symbol ⊗ represents the multiplication operation. Symbols ⊗ represents the multiplication operation. The flow chart of encryption and decryption is shown in Figure 1(b) [28-31].

2.2 Encryption Process

The flow chart of image encryption based on double random phase encoding technology is shown as Figure 2. Figure 2 image encryption based on double random phase encoding technology. Figure 2 represents plain text image, and and represents random phase functions, also called encryption keys. FT represents Fourier transformation while IFT represents the inverse Fourier transform. represents an intermediate matrix generated, g represents the cipher text images, and symbols represents the multiplication operation [53-58].

Assuming the image is to be encrypted, encryption process of the image is as follows: First, matrix multiplies with the plain text image, then use Fourier transform it, then use matrix multiplies with the resulting matrix, and finally use inverse Fourier transform to obtain the cipher text. and are the keys. The calculation formulas are as follows:

$$R_1(x,y) = \exp[jn(x,y)] \quad \textbf{(1)}$$

$$R_2(\alpha,\beta) = \exp[jb(\alpha,\beta)] \quad \textbf{(2)}$$

$n(x,y)$ and $b(\alpha,\beta)$ are the same-sized phase matrixes randomly generated compared with plain texts, and j is an imaginary number symbol. Then the encryption algorithm formula can be expressed as follows:

$$g(x,y) = IFT\{FT[f(x,y)R_1(x,y)] \cdot R_2(\alpha,\beta)\} \quad \textbf{(3)}$$

$f(x,y)$ represents plain text images while $R_1(x,y)$ and are random phase functions, namely the encryption keys. FT represents Fourier transformation while IFT represents the inverse Fourier transform. $g(x,y)$ represents cipher text images and symbols•represents multiplication [59-62].

2.3 Decryption

Image decryption based on double random phase encoding technique is presented in Figure 3. In this figure, f is plaintext image $f(x,y)$, $\overline{R_1}$ and $\overline{R_2}$ are conjugated matrices of random phase functions R_1 and R_2. *FT* refers to Fourier transform and *IFT* inverse Fourier transform. g_1 is a matrix generated during the

process, g refers to the encrypted image $g(x,y)$ and $\otimes$ multiplication. Decoding process is the inverse course of encoding. The formula is as follows [63]:

$$f(x,y) = IFT\{FT[g(x,y)]\overline{R_2}(\alpha,\beta)\} \cdot \overline{R_1}(x,y) \quad \textbf{(4)}$$

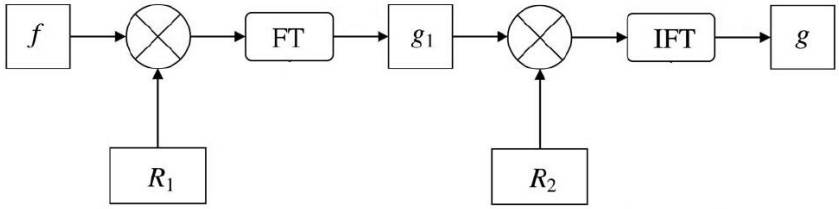


Figure 2. Image Encryption based on double random phase encoding technique

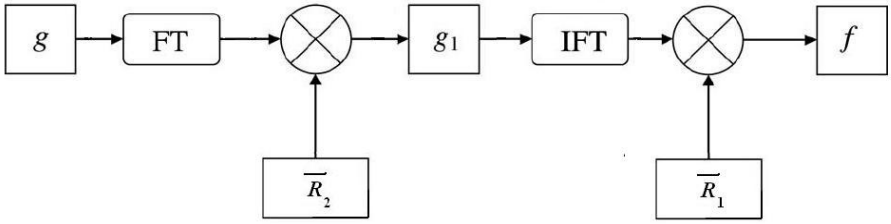


Figure 3. Image decryption based on double random phase encoding technique

Among which, $f(x,y)$ is plaintext image, $\overline{R_1}(x,y)$ and $\overline{R_2}(\alpha,\beta)$ are conjugated matrices of random phase functions R_1 and R_2. *FT* refers to Fourier transform and *IFT* inverse Fourier transform. $g(x,y)$ refers to the encrypted image and multiplication.

2.4 Criteria for Assessing Encryption and Decryption Algorithm

In general, mean square error(MSE) is used to assess encryption and decryption algorithm. It is defined as follows [64]:

$$MSE = \frac{1}{M \times N}\sum_{x=1}^{M}\sum_{y=1}^{N}\left|I_o(x,y) - I_i(x,y)\right|^2 \quad \textbf{(5)}$$

Among which I_o and I_i refer to the magnitude of exported image and imported image, respectively. M and N are the width and height of images. The value of MSE is smaller, the decrypted image and the original image are more similar, and the encryption algorithm effection is better. Sometimes, the assessment may also be made by using image correlation Corr, which can be presented by correlation coefficient and defined as follows [65]:

$$Corr = \frac{Cov(I_o, I_i)}{\sqrt{D(I_o)\sqrt{D(I_i)}}} \quad \textbf{(6)}$$

Among which $Cov(I_o, I_i)$ is the covariance of the imported image and the exported image.

$$Cov(I_o, I_i) = E\left[I_o - E(I_o)\right]E\left[I_i - E(I_i)\right] \quad \textbf{(7)}$$

$D(I)$ is the variance of $I(x,y)$:

$$D(I) = E\left[g - E(g)\right]^2 \quad \textbf{(8)}$$

Among which $E(\cdot)$ refers to mathematical expectation. The closer the value of correlation Corr is to 1, the decrypted image and the original image are the more similar, and encryption algorithm is the better [32-34, 66-67].

3 Known Plaintext Attack Algorithm

Cryptology includes such two aspects as cryptography and cryptanalysis. In cryptanalysis, based on knowledge of the attacker, attacks on block ciphers can be divided into the following types: ciphertext-only attack, known plaintext attack, chosen-plaintext attack and chosen-ciphertext attack, etc. This paper will focus on discussing how to use known plaintext attack to break a double random phase encoding system. From an abstract point of view, more usable resources are provided for a chosen-plaintext attack, so when a known plaintext attack can break through successfully, it is evident that a chosen-plaintext attack or chosen-ciphertext attack or other attacks will also finish the same process. The above mentioned and following equations are based on our own derivation formula process. All of simulation experiments are performed by Matlab platform [68-72].

When cryptanalysis is conducted for a cryptosystem, attackers are usually considered as to have known the operation of cryptographic algorithm, namely, complying with Kerekboffs hypothesis. In the following part, double random encoding system will be

analyzed by using known plaintext attack, assuming that the attacker has known several ciphertext (encrypted image) and corresponding plaintext(original image) itself. Taking one of the plaintext-ciphertext pair, the attacker attack through the following two steps:

1. First step: Obtaining the key of random phase function on the input plane by phase retrieve algorithm In known plaintext attack, the attacker has known a plaintext-ciphertext pair $\{f(x,y),g(x,y)\}$. Fourier transform of $g(x,y)$ is reversed so that $\varphi(\alpha,\beta)=FT[g(x,y)]$. Based on the encoding equation of encoding systems (see equation 4.3), it is deduced that:

$$\varphi(\alpha,\beta)=FT\{f(x,y)\exp[jn(x,y)]\}\exp[jb(\alpha,\beta)] \quad \textbf{(9)}$$

Among which, when $G(x,y)=f(x,y)\exp[jn(x,y)]$ **(10)**

$$G(\alpha,\beta)=FT\{G(x,y)\} \quad \textbf{(11)}$$

we have

$$\varphi(\alpha,\beta)=G(\alpha,\beta)\exp[jb(\alpha,\beta)] \quad \textbf{(12)}$$

When modular arithmetic is conducted for both sides of the equation in 12, we have

$$\left|\varphi(\alpha,\beta)\right|=\left|G(\alpha,\beta)\right| \quad \textbf{(13)}$$

In addition, because

$$\left|G(x,y)\right|=\left|f(x,y)\exp[jn(x,y)]\right|=f(x,y) \quad \textbf{(14)}$$

From equation 13 and 14, we can see that the attacker has already known the plaintext(original image) $f(x,y)$ and corresponding ciphertext(encrypted image) $g(x,y)$. So the problem has been transferred from seeking the key on input plane $\exp[jn(x,y)]$ to the intensity information on the known substance plane $\left|G(x,y)\right|$ (namely $f(x,y)$) and the Fourier plane $\left|G(\alpha,\beta)\right|$ (namely $\left|\varphi(\alpha,\beta)\right|$), and how to recover phase on the substance plane $\exp[jn(x,y)]$, among which $G(\alpha,\beta)=FT\{G(x,y)\}$. This is a typical phase recovery problem, which can be solved through iterative method by using multiple known phase recovery algorithm.

2. **Second step:** Deducing the key on spectrum plane from the key on input plane

In known plaintext attack, when the attacker has obtained the random phase function key on the input plane of 4-f system $\exp[jn(x,y)]$ through regular phase recovery algorithm, and the plaintext $f(x,y)$ and ciphertext $g(x,y)$ are already known, based on equation 4.12, random phase function key on the spectrum plane can be expressed as follows:

$$\exp[-jb(\alpha,\beta)]=FT\{f(x,y)\exp[jn(x,y)]\}/\varphi(\alpha,\beta) \quad \textbf{(15)}$$

Thus, two encryption keys of the double random phase encoding system, $\exp[jn(x,y)]$ and $\exp[jb(\alpha,\beta)]$, are fixed. Then, put them in equation 4.4 and the encoding system is broken.

3.1 Optical Implementation of This Encoding System

It is worth noting that with the help of some optoelectronic devices, this encoding and decoding scheme can not only be digitalized but also be implemented optically. Its illustrative diagram is shown in Figure 4.

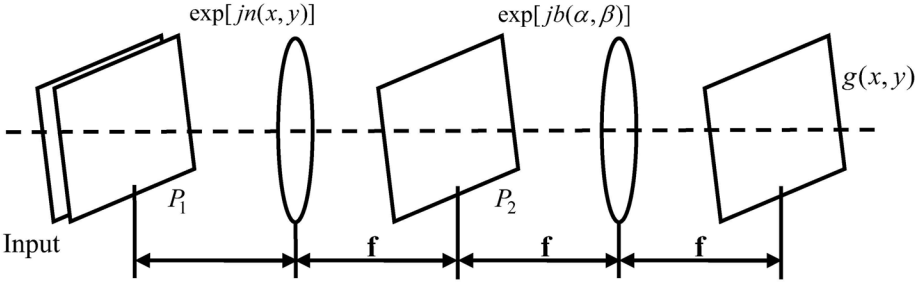


Figure 4. Illustrative diagram for double random phase encryption

In this figure, $f(x,y)$ refers to the image to be encrypted and $g(x,y)$ the encrypted image. x and y are space domain coordinates, and α and β frequency domain coordinates on the Fourier transform plane. $n(x,y),b(\alpha,\beta)$ are random arrays which obey two-dimensional normal distribution and their values are within the interval $[0,2\pi]$. Besides, both their convolution sum and mean value are zero. Therefore, they are two independent groups of random white noise. Hence, $\exp[jn(x,y)]$ and $\exp[jb(\alpha,\beta)]$ can be used as random mask plates with phase within $[0,2\pi]$. Double random phase encryption can be then described as follows: After being modulated by phase plate $\exp[jn(x,y)]$, the original image $f(x,y)$ undergoes Fourier transform. Further, the resultant frequency domain is modulated by phase plate $\exp[jb(\alpha,\beta)]$.

And then, after reverse Fourier transform, an encrypted image similar to white noise is obtained on the output plane.

If only the first phase plate is used for encryption, finally the resultant item obtained will be unsteady white noise whose statistic characteristics changes over time; while if only the second phase plate is used for encryption, the encrypted image will be decoded easily. Therefore, during encryption, two random phase plates play their roles of key together. None of them can be omitted. Based on the principle of optical reversibility, decryption is the inverse process of encryption. The illustrative diagram for decryption is shown in Figure 5.

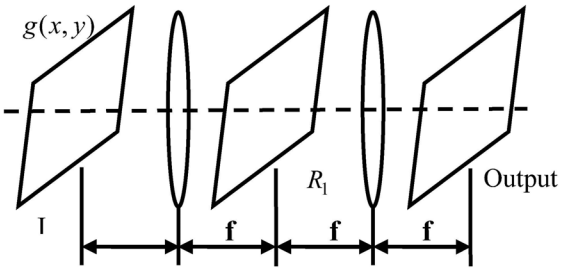


Figure 5. Illustrative diagram for double random phase decryption

Decryption key is the complex conjugate of encryption key. If $f(x,y)$ is a real function, we just need to save the random phase on Fourier plane to calculate its complex conjugate; if $f(x,y)$ is a virtual function, the complex conjugate of two random phase plates has to be obtained for decryption.

3.2 Experimental Results and Analysis

In order to verify the image encryption algorithm proposed based on phase recovery, here we make a relevant imitation experiment. Considering the principle of universality, we choose an image with 256×256 grayscale as the image to be encrypted. It is presented in Figure 6.

Figure 6. Original image

The encrypted image obtained by this algorithm is presented in Figure 7.

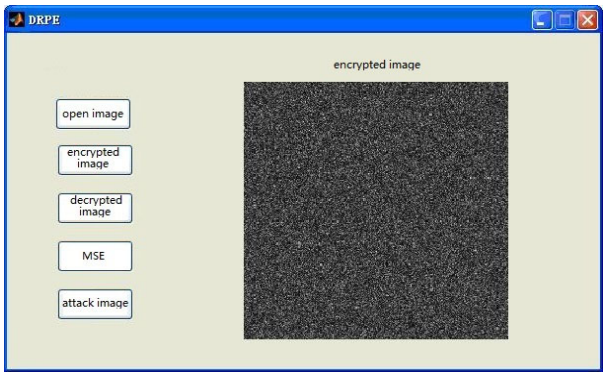


Figure 7. Encrypted image

From Figure 7, we can see that the encrypted image obtained by this algorithm doesn't show any trace of the original image at all. So, the encryption effect of this algorithm is good.

The decrypted image obtained by this algorithm is presented in Figure 8.

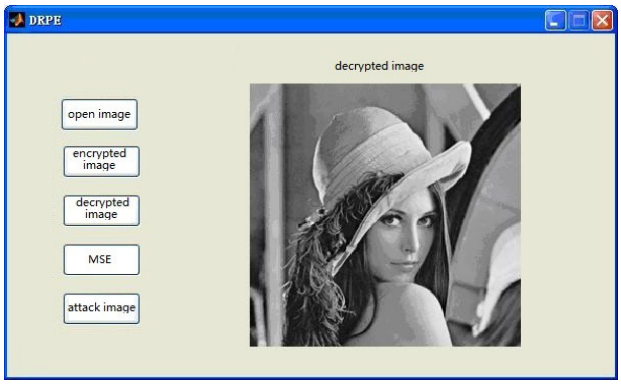


Figure 8. Decrypted image

From the decrypted image, we can see that the plaintext image has been decrypted correctly.

In order to verify the robustness of this algorithm based on double random phase encryption, we make a known plaintext attack and the result is shown in Figure 9.

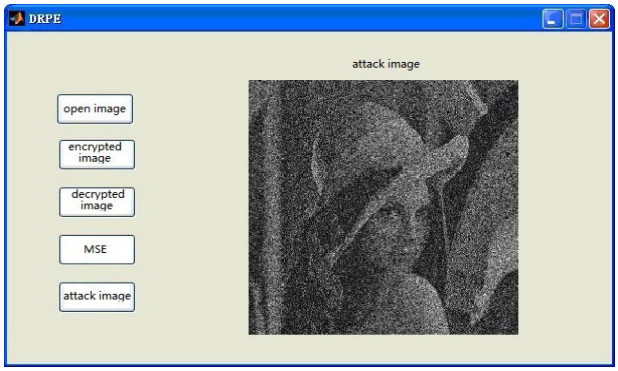


Figure 9. Attacked image

During the attack, the MSE values corresponding to different iterations are shown in Figure 10.

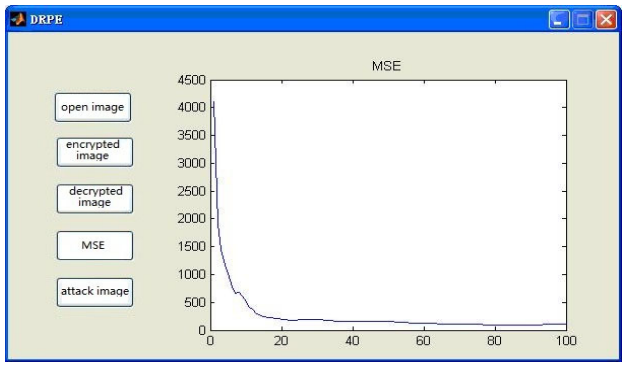


Figure 10. MSE values corresponding to different iterations

From Figure 9 and Figure 10, we can see that the robustness of image encryption algorithm based on double random phase encoding technique is poor. Illegal users may obtain relevant information about the image by attack algorithm.

4 Conclusion

In this paper, image encryption algorithm basedon double random phase encoding technique is implemented. In our algorithm, the original image, after being modulated by a phase plate, undergoes Fourier transform. Further, the resultant frequency domain is modulated by the second phase plate. And then, after reverse Fourier transform, an encrypted image similar to white noise is obtained on the output plane. It is confirmed in considerable imitation experiments that a plaintext image can be decrypted from a ciphertext image by using this algorithm. Illegal users may obtain relevant information about the image by attack algorithm. Our method make the improved contributions in the current job. We consider that future research should focus on the deciencies and shortcomings to further improve performance.

5 Competing Interests

The authors declare that they have no competing interests.

Acknowledgements

We would like to thank the anonymous reviewers for their valuable comments.

This job is supported by the National key R&D Program of China under Grant NO.2018YFB0203901.

This job is also supported by the Key Research and Development Program of Shaanxi Province (No. 2018ZDXM-GY-036) and Scientific Research Program Funded by Shaanxi Provincial Education Department (Program No. 2013JK1139) and Supported by China Postdoctoral ScienceFoundation (No. 2013M542370) and the Specialized Research Fund for the Doctoral Program of Higher Education of China (GrantNo. 20136118120010) and by the Open Program of Xiamen Key Laboratory of Computer Vision and Pattern Recognition, Huaqiao University(600005-Z17X0001).

References

[1] J. Shuyuan, Y. Xiaochun, F. Bin-Xing, Challenge of DDoS Attacks Detection. *ITLetters*, Vol. 6, No. 5, pp. 25-35, September 2008.

[2] Z. Changwang, Y. Jian-ping, C. Zhip-ing, etc. AQM Algorithms of Anti-DDoS Attacks. *Journal of Software*, Vol. 22, No. 9, pp. 2182-2192, 2011.

[3] W. Jianxin, R. Liang, X. Xuefeng. Simulation and Performance Assessments on Several Active Queue Management Algorithms. *Computer Engineering*, Vol. 33, No. 3, pp. 128-130, February, 2007.

[4] Song, Houbing, and Maité Brandt-Pearce. "A 2-D discrete-time model of physical impairments in wavelength-division multiplexing systems." *Journal of Lightwave Technology*, Vol. 30, No. 5, pp. 713-726, 2012.

[5] Q. Yong. Information potential fields navigation in wireless Ad-Hoc sensor networks. *Sensors*, Vol. 11, No. 5, pp. 4794-4807, 2011.

[6] F. LuPing, L. Shihua, C. Pan etc, *NS2 Network Simulation Basis and Application Beijing: National Defense Industry Press*, pp. 156-166, May, 2008.

[7] Song, Houbing, and Maité Brandt-Pearce. "A discrete-time polynomial model of single channel long-haul fiber-optic communication systems." Communications (ICC), *2011 IEEE International Conference on*. IEEE, 2011.

[8] L. Ming, Z. Heying, DOU Wen-hua. Performance Analysis and Control Model of Random Exponetial Marking Algorithms. *2005 Computer Engineering and Science*, Vol. 27, No. 9, pp. 66-68.

[9] S. Athuraliya, S.-H. Low, V.-H. Li, etal. REM Active QueueManagement. *IEEENetwork*, Vol. 15, No. 3, pp. 48-53, 2001.

[10] Y. XL, S. PY, Zhou B. Holes detection in anisotropic sensornets: Topological methods. *International Journal of Distributed Sensor Networks*, Vol. 23, No. 8(10), pp. 13505, October, 2012.

[11] K. Zhiheng, C. Rongxiang, D. Dejuan, *NS2 Simulation Experiment Multimedia and Wireless Network Communication Beijing: Electronic Industry Press*, pp. 315-331, March, 2009.

[12] H.-X Tan, W.-K. G. Seah. *Framework for Statistical Filtering Against DDoS Attacks in MANETsProceedings of the Second International Conference on Embedded Software and Systems (ICESS'05)*, 2005[C].Xi'an: T L XU, 2005: c1.

[13] Y.-C. Wu, H.-R. Tseng, W. Yang, etal. DdoS detection and traceback with decision tree and grey relational analysis. *Ad Hoc and Ubiquitous Computing*, Vol. 7, No. 2, pp. 121-136, 2011.

[14] T. Peng, C. Leckie, K. Ramamohanarao.Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS

Problems. *ACM Computing Surveys*, Vol. 39, No. 1, Article 3, pp. 1-42, April, 2007.

[15] Q. Xu, L. Wang, H. XH, P. Shen, W. Shi, L. Shan. GI/Geom/1 queue based on communication model for mesh networks. *International Journal of Communication Systems*, Vol. 1, No. 27(11), pp. 3013-29, November, 2014.

[16] X. Fan, M. Woźniak, H. Song, W. Li, Y. Li, P.-H. Shen. Control of Network Control System for Singular Plant. *Information Technology And Control*, Vol. 1, No. 47(1), pp. 140-50, January, 2018.

[17] X.-L. Yang, B. Zhou, J. Feng, P.-Y. Shen. Combined energy minimization for image reconstruction from few views. *Mathematical Problems in Engineering*, 2012 October, 31; 2012, Article ID 154630, pp. 15. Doi:10.1155/2012/154630.

[18] Y. Jiang, H. Song, R. Wang, M. Gu, J. Sun, and L. Sha, *Data-Centered Runtime Verification of Wireless Medical Cyber Physical System*, 2016.

[19] X. Fan, H. Song, X. Fan, & J. Yang, (1939). Imperfect information dynamic stackelberg game based resource allocation using hidden markov for cloud computing. *IEEE Transactions on Services Computing*, Vol. 11, No. 1, pp.78-89, February, 2016, Doi: 10.1109/TSC.2016.2528246.

[20] S. Zheng-guo, X. Liang-bo, W. Guang-jun, "Idle-slots elimination based binary splitting (ISE-BS) anti-collision algorithm for RFID," *IEEE Communications Letters*, Vol. 20, No. 12, pp. 2394-2397, 2016.

[21] L. Zhenhua, Y. Zhang, and L. Yunhao, Towards A Full-Stack DevOps Environment (PaaS) for Cloud-Hosted Applications. *Journal of Tsinghua Science and Technology (JTST)*, Vol. 22, No. 1, pp. 1-9, February, 2017.

[22] Y. Qiang, J. Zhang, A Bijection between Lattice-Valued Filters and Lattice Valued Congruences in Residuated Lattices. *Mathematical Problems in Engineering*, Vol. 36, No. 8, pp. 4218-4229, 2013.

[23] Y. Jiang, Y. Yang, H. Liu, H. Kong, M. Gu, J. Sun, and L. Sha, 2016, April. FromState ow Simulation to Veried Implementation: A Verication Approach and A RealTime Train Controller Design. *In 2016 IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS)* (pp. 1-11). IEEE.

[24] H.-M, Srivastava Y. Zhang, et al. A local fractional integral inequality on fractal space analogous to Anderson's inequality//Abstract and Applied Analysis. *Hin dawi Publishing Corporation*, Vol. 46, No. 8, pp. 5218-5229, 2014.

[25] J. Guo, H. Zhang, Y. Sun, and R. Bie, "Square-root unscented Kalman lteringbased localization and tracking in the internet of things," *Personal and Ubiquitous Comput*, Vol. 18, No. 4, pp. 987-996, April, 2014.

[26] Jiangshe Zhang, et al. Big Data Analytics Enabled by Feature Extraction Based on Partial Independence. Neurocomputing. 2017 Dec 29, Vol. 288, pp. 3-10, DOI: 10.1016/j.neucom. 2017.07.072.

[27] V. Singh, I. Gupta, and H.-O. Gupta, "ANN-based estimator for distillation using Levenberg-Marquardt approach," *Engineering Applications of Articial Intelligence*, Vol. 20, No. 2, pp. 249-259, March, 2007.

[28] H. Zhang and T.-A. Gulliver, "Capacity of time-hopping PPM and PAM UWB multiple access communications over indoor fading channels," EURASIP J. Wireless Commun. and Networking, Article ID 273018, 2008.

[29] V. Singh, I. Gupta, and H.-O. Gupta, "ANN-based estimator for distillation using Levenberg-Marquardt approach," *Engineering Applications of Articial Intelligence*, Vol. 20, No. 2, pp. 249-259, March, 2007.

[30] C. Paar, J. Pelzl, Chapter 6: Understanding cryptography. In A Textbook for Students and Practitioners Introduction to Public-Key Cryptography. Springer Berlin/Heidelberg, pp. 149-170, 2009.

[31] M.-N. Kasirian, R.-M. Yusu, An integration of a hybrid modi ed TOPSIS with a PGP model for the supplier selection with inter dependent criteria, *International Journal of Production Research*, pp. 1-18, 2012.

[32] D.-C. Parkes, M.-O, Rabin, S.-M. Shieber, C.-A. Thorpe, practical secrecy-preserving, veriably correct and trust-worthy auctions, *Proceedings of the 8th international conference on Electronic commerce: The new ecommerce: innovations for conquering current barriers, obstacles and limitations to conducting successful business on the internet*, pp. 70-81, 2006.

[33] J. Brickell, V. Shmatikov, Privacy Preserving Graph Algorithms in the SemiHonest Model, Advances in Cryptology ASIACRYPT 2005, LNCS, Springer Berlin/ Heidelberg, pp. 3788: 236-252, 2005.

[34] T. Pedersen. Non-Interactive and Information-Theoretic Secure Veriable Secret Sharing. In Advances in Cryptology (CRYPTO), volume 576 of LNCS, pages 129-140. Springer Berlin /Heidelberg, 1992.

[35] Richard Crandall and Carl Pomerance. Prime Numbers: A Computational Perspective (1st edition ed.). Springer. ISBN 0-387-94777-9. Chapter 5: Exponential Factoring Algorithms, pp. 191C226, 2001.

[36] D. Hui, Q. Yong, W. Wei, Houbing Song. A two-time-scale load balancing framework for minimizing electricity bills of Internet Data Centers[J]. Personal and Ubiquitous Computing, Vol. 20, No. 5, pp. 681-693, 2016.

[37] Song, Houbing, and Mait Brandt-Pearce. "A 2-D discrete-time model of physical impairments in wavelength-division multiplexing systems." *Journal of Lightwave Technology*, Vol. 30, No. 5, pp. 713-726, 2012.

[38] L. Yang, Q. Yong, H. Jinsong, C. Wang, and L. Yunhao, Shelving Interference and Joint Identification in Large-scale RFID Systems, *IEEE Transactions on Parallel and Distributed Systems*, Vol. 26, No. 11, pp. 3149-3159, November, 2015.

[39] X. Min, Q. Yong, W. Kui, Z. Jizhong, L. Mo, Using Potential to Guide Mobile Nodes in Wireless Sensor Networks, *Ad Hoc & Sensor Wireless Networks*, Vol. 12, No. 3-4, pp. 229-251, 2011.

[40] Z. Pengfei, Q. Yong, Z. Yangfan, C. Pengfei, Z. Jianfeng, and Michael Rung-Tsong Lyu, An Automatic Framework for Detecting and Characterizing the Performance Degradation of Software Systems, *IEEE Transactions on Reliability*, Vol. 63,

No. 4, pp. 927-943, December, 2014.

[41] W. Peijian, Q. Yong, L. Xue, Power-Aware Optimization for Heterogeneous Multi-tier Clusters, *Journal of Parallel and Distributed Computing*, Vol. 74, No. 1, pp. 2005-2015, January, 2014.

[42] Q. Ya-nan, Y. Qi, D. Hou, Tensor Field Model for higher-order information retrieval. *Journal of Systems and Software*, Vol. 84, No. 12, pp. 2303-2313, December, 2011.

[43] R. Jianbao, Q. Yong, D. Yuehua, Y. Xuan, and Y. Shi, nOSV: A lightweight nested-virtualization VMM for hosting high performance computing on cloud. *Journal of Systems and Software*, Vol. 124, No. 2, pp. 137-152, 2017.

[44] R. Jianbao, Q. Yong, D. Yuehua, W. Xiaoguang, and Y. Shi. AppSec: A Safe Execution Environment for Security Sensitive Applications. *In Proceeding of the 11th ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments (VEE)*, Vol. 50, No. 7, pp. 187-199, 2015.

[45] C. Pengfei, Y. Qi, L. Xinyi, H. Di, and Michael Rung-Tsong Lyu,, ARF-Predictor: Effective Prediction of Aging-Related Failure Using Entropy, *IEEE Transactions on Dependable and Secure Computing*, DOI: 10.1109/TDSC. 2016.2604381.

[46] X. Shengdong and W. Yuxiang, "Construction of Tree Network with Limited Delivery Latency in Homogeneous Wireless Sensor Networks," *Wireless Personal Communications*, Vol. 78, No. 1, pp. 231-246, 2014.

[47] W. Xiaoguang, Q. Yong, W. Zhi, et al. Design and Implementation of SecPod: A Framework for Virtualization-based Security Systems. *IEEE Transactions on Dependable and Secure Computing*, DOI: 10.1109/TDSC.2017.2675991.

[48] X. Shengdong and W. Yuxiang, "Construction of Tree Network with Limited Delivery Latency in Homogeneous Wireless Sensor Networks," *Wireless Personal Communications*, Vol. 78, No. 1, pp. 231-246, 2014.

[49] H. Song, W. Li, P. Shen, A. Vasilakos, Gradient-driven parking navigation using a continuous information potential field based on wireless sensor network. Information Sciences, Vol. 408, No. C, pp. 100-114, DOI: information: 10.1016/ j.ins.2017.04.042, October, 2017.

[50] S. Zheng-guo, X. Liang-bo, L. Gang, X.-L. Alex, "Fast splitting based tag identification algorithm for anti-collision in UHF RFID system," *IEEE Transactions on Communications*, 2018, Doi: 10.1109/TCOMM.2018.2884001.

[51] S. Jian, S. Zheng-guo, Victor C.-M. Leung, C. Yong-rui, "Energy efficient tag identification algorithms for RFID: survey, motivation and new design," *IEEE Wireless Communications*, 2018.

[52] L. Zhang, GUO De-ke, Shen Pei-yi, "Applications of information navigation method in wireless sensor networks," *Journal on Communications*, Vol. 33 No. Z2, pp. 146-152, 2012.

[53] Y. Zhao, W. Wei, B.-S. Hou, L. Wei, The hardware design of intelligent circuitbreaker, *Energy Education Science and Technology Part A: Energy Science and Research.1*, pp. 695-702, 2014.

[54] Y. Zhao, Y. Chen, G. Zhang, W. Wei, Research on the VXI fault diagnosis for computer network based on immune genetic algorithm in process of data transfer, *Computer Modelling and New Technologies*, 5B, pp. 71-75, 2013.

[55] Y. Zhao, Y. H. Zhong, W. Wei, Simulation and analysis of access channel in CDMA communication system, *Journal of simulation*, Vol. 4, No. 1, pp. 57-59, 2016.

[56] Y. Jiang, H. Zhang, Z. Li, Y. Deng, X. Song, M. Gu, and J. Sun, 2015. Design and optimization of multiclocked embedded systems using formal techniques. *IEEE Transactions on Industrial Electronics*, Vol. 62, No. 2, pp. 1270-1278.

[57] S. Jian, H. Dan-feng, T. Jun-lin, C. Hai-peng, "An efficient anti-collision algorithm based on improved collision detection scheme," *IEICE Transactions on Communications*, Vol. E99-B, No. 2, pp. 465-469, 2016.

[58] Song, Houbing, and Maité Brandt-Pearce. "Range of influence and impact of physical impairments in long-haul DWDM systems." *Lightwave Technology*, Journal of Vol. 31, No. 6, pp. 846-854, 2013.

[59] J. Yu, Z. Hehua, Z. Huafeng, L. Han, S. Xiaoyu, G. Ming, S. Jiaguang: Design of Mixed Synchronous/Asynchronous Systems with Multiple Clocks. *IEEE Trans*. Parallel Distrib. Syst. Vol. 26, No. 8, pp. 2220-2232, 2015.

[60] J. Wu, S. Guo, J. Li, D. Zeng, Big data meet green challenges: Greening big data. *IEEE Systems Journal*, Vol. 10, No. 3, pp. 873-887, September, 2016.

[61] Song, Houbing, and Maite Brandt-Pearce. "Model-centric nonlinear equalizer for coherent long-haul fiber-optic communication systems." *Global Communications Conference (GLOBECOM)*, 2013 IEEE. IEEE, 2013.

[62] L. Zhenhua, W. Weiwei, W. Christo, C. Jian, Q. Chen, J. Taeho, Z. Lan, L. Kebin, L. Xiangyang, and L. Yunhao. FBS-Radar: Uncovering Fake Base Stations at Scale in the Wild. *The 24th Network and Distributed System Security Symposium (NDSS)*, February, 26-March, 1, 2017, San Deigo, CA, US.

[63] S. Zheng-guo, H. Dan-feng, W. Guang-jun, "An effective frame breaking policy for dynamic framed slotted Aloha in RFID," *IEEE Communications Letters*, Vol. 20, No. 4, pp. 692-695, 2016.

[64] J. Wu, H. Hu, M. Uysal, High-rate distributed space-time-frequency coding for wireless cooperative networks. *IEEE Transactions on Wireless Communications*, Vol. 10, No. 2, pp. 614-25, February, 2011.

[65] S. Jian, S. Zheng-guo, W. Guang-jun, C.-M, Victor. Leung, "A time efficient tag identification algorithm using dual prefix probe scheme (DPPS)," *IEEE Signal Processing Letters*, Vol. 23, No. 3, pp. 386-389, 2016.

[66] S. Jian, S. Zheng-guo, X. Liang-bo, W. Guang-jun, "Idle-slots elimination based binary splitting (ISE-BS) anti-collision algorithm for RFID," *IEEE Communications Letters*, Vol. 20, No. 12, pp. 2394-2397, 2016.

[67] J. Su, H. Song, H. Wang, & X. Fan, (2018). Cdma-based anti-collision algorithm for epc global c1 gen2 systems. *Telecommunication Systems*, Vol. 67, No. 3, pp. 1-9.

[68] Z. Sun, H. Song, H. Wang, X. Fan, Energy Balance-Based

Steerable Arguments Coverage Method in WSNs. *IEEE Access*. Vol. 20, No. 99, March, 2017, DOI: 10.1109/ ACCESS.2017.2682845.

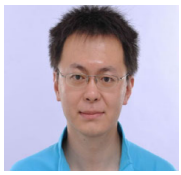
[69] H. Song, H. Wang, X. Fan, Research and Simulation of Queue Management Algorithms in Ad Hoc Network under DDoS Attack. *IEEE Access*, Vol. 5, pp. 27810-27817, 2017, March, Vol. 13, No. 99, DOI: 10.1109/ACCESS.2017. 2681684.

[70] X. Fan, H. Song, & H. Wang, (2017). Video tamper detection based on multi-scale mutual information. *Multimedia Tools & Applications*, pp. 1-18, DOI: 10.1007/ s11042-017-5083-1, 2017.

[71] J. Wu, S. Guo, J. Li, D. Zeng, Big data meet green challenges: Big data toward green applications. *IEEE Systems Journal*, Vol. 10, No. 3, pp. 888-900, September, 2016.

[72] J. Wu, I. Bisio, C. Gniady, E. Hossain, M. Valla, H. Li, Context-aware networking and communications: Part 1 [guest editorial]. *IEEE Communications Magazine*, Vol. 52, No. 6, pp. 14-5, June, 2014.

Biographies



Wei Wei is a senior member of IEEE, an associated professor of School of Computer Science and Engineering, Xi'an University of Technology, Xi'an 710048, China. He received his Ph.D. and M.S. degrees from Xian Jiaotong University in 2011 and 2005, respectively. He ran many funded research projects as principal investigator and technical members. His research interest is in the area of wireless networks, wireless sensor networks Application, Image Processing, Mobile Computing, Distributed Computing, and Pervasive Computing, Internet of Things, Sensor Data Clouds, etc. He has published around one hundred research papers in international conferences and journals. He is an editorial board member of FGCS, AHSWN, IEICE, KSII, etc. He is a TPC member of many conferences and regular reviewer of IEEE TPDS, TIP, TMC, TWC, and many other Elsevier journals.

Marcin Woźniak received diplomas in applied mathematics and computational intelligence, Master Degree in 2007 from the Silesian University of Technology and PhD in 2012 from the Czestochowa University of Technology. He is an Assoc. Professor at Institute of Mathematics of the Silesian University of Technology in Gliwice, Poland. In his scientific career, he was visiting University of WÅ´ srzburg, Germany in 2007 (for part of the studies), University of Lund, Sweden in 2016 (as a guest from the ministerial program for young research professors) and University of Catania, Italy in 2015 and 2017 (as invited professor for research projects and grants). His main scientific interests are neural networks with their applications together with various aspects of applied computational intelligence. He is a scientific supervisor in editions of "the Diamond Grant" and "The Best of the Best" programs for highly gifted students from the Polish Ministry of Science and Higher Education. Marcin Woźniak was/is organizer and session chair on various international conferences and symposiums, like IEEE SSCI, IEEE FedCSIS, APCASE, ICIST, ICAISC, WorldCIST.

Robertas Damaševičius graduated at the Faculty of Informatics, Kaunas University of Technology (KTU) in Kaunas, Lithuania in 1999, where he received a B.Sc. degree in Informatics. He finished his M.Sc. studies in 2001 (cum laude), and he defended his Ph.D. thesis at the same University in 2005. Currently, he is a Professor at Software Engineering Department, KTU and lectures robot programming and software maintenance courses. His research interests include brain-computer interface, bioinformatics, data mining and machine learning. He is the author or co-author of over 100 papers as well as a monograph published by Springer.

Xiumei Fan is a professor in Schoolof Automation and Information Engineering, Xi'an University of Technology. She received B.S. degree in electron information engineering from Tianjin University in 1989 and Ph.D. degree in communication and information system from Northern Jiaotong University in 2001. Her current research interests focus on Wireless Broadband Network, VANET, DTN, and Mobile Internet.

Ye Li is an Associate Research Fellow, doctor of engineering, tutor of master's degree. He is currently Deputy Director of Shandong provincial computer center and director of Shandong Provincial Key Laboratory of computer network. It is also the vice chairman of Shandong Provincial Department, deputy secretary of the Shandong computer society, the Executive Committee of the Ji'nan branch of the Chinese computer society, the Editorial Committee of the Shandong science, the Committee of the Academy of Sciences of the Shandong Academy of Sciences, and the young academic leader of the Academy of Sciences of Shandong province.