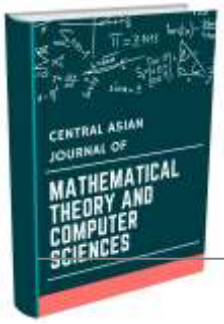


CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
https://cajmtcs.centralasianstudies.org

Volume: 04 Issue: 08 | Aug 2023 ISSN: 2660-5309

Hyper-Chaos and Public-Key Cryptography Based Optical Image Encryption Method

A. Rajesh
Assistant Professor, Department of CSE (DATA SCIENCE),
CMR Institute of Technology, India

Y. Ram Kumar
Assistant Professor, Department of CSE(DATA SCIENCE),
CMR Institute of Technology, India

Abstract

To secure the transmission and distribution of complex keys in optical transformation-based image encryption networks, an original optical image encryption looks at based on hyper-chaos and public key cryptography can be employed. The original image is then encrypted in the specular domain using hyper-chaotic phase filters and double random phase encoding. To perform asymmetric, imagine encryption, public key encryption systems are used to assign and manage the hyper-chaotic system's setting values, system parameters, including the frequency diffraction system parameters. During the decryption process, the receiver generates hyper-chaotic random phase masks by decrypting the private keys in the public key cryptosystem and optically decrypts the encrypted image. Finally, the generated key stream is used to generate the final encryption image by performing an end-to-end circular modulus diffusion operation on all rows and columns. In addition, the key sequence has been connected to the plain image, which could notify the user to the chosen plaintext and known plaintext attack.

ARTICLE INFO

Article history:
Received 13 Jun 2023
Revised form 15 July 2023
Accepted 31 Aug 2023

Key words: *private key, RSA Algorithm*

---***---

Introduction

The significance of multidimensional data transmission in modern society has increased because of the rapid growth of the Internet, information technology, and digital communications. In human existence, image is a crucial data carrier that can be utilized to communicate instances immediately. Major consequences have occurred in recent years primarily a consequence of releases of digital imagine data. As a result, image encryption protection has become more crucial. Conventional methods of encryption utilize a one-dimensional a character to store and encrypt data.

For the instance of images, the computation of algorithms for encryption is severely because to the huge amount of data, and the significant association between neighboring pixels requires a sufficiently lengthy key stream for a high security level. For a result, a new method of encryption for secure image transmission has to be provided. A chaotic structure is a deterministic system which demonstrates seemingly random irregular motions and exhibits uncertain, unrepeatable, and unexpected behavior. This chaotic system is sensitive to getting started conditions and demonstrates pseudo randomness, ergodicity, and aperiodicity. A chaotic framework when combined with an image encryption method may significantly improve security and anti-cracking abilities [1]. Chaotic systems include characteristics such as sensitivity to initial values, strong pseudo-randomness, and periodicity, which make them appropriate for image encryption. Since Matthews caused chaos theory to cryptography in 1989, its importance in the area of data security has increased. Conventional encryption methods, including Logistic mapping-based encryption methods, offer a basic foundation and a cheap selection cost, and were frequently used in early image encryption. When the standard RSA method encrypts the entire hyper-chaotic random phase mask, the issue of key distribution in encryption systems is solved and the processing execution advantage is overcome. To produce hyper-chaotic random phase masks, the initial chaotic sequences generated by the two hyper-chaotic systems are applied. Second, the primary image is disorganized and encrypted utilizing Fresnel domain double random phase encoding.

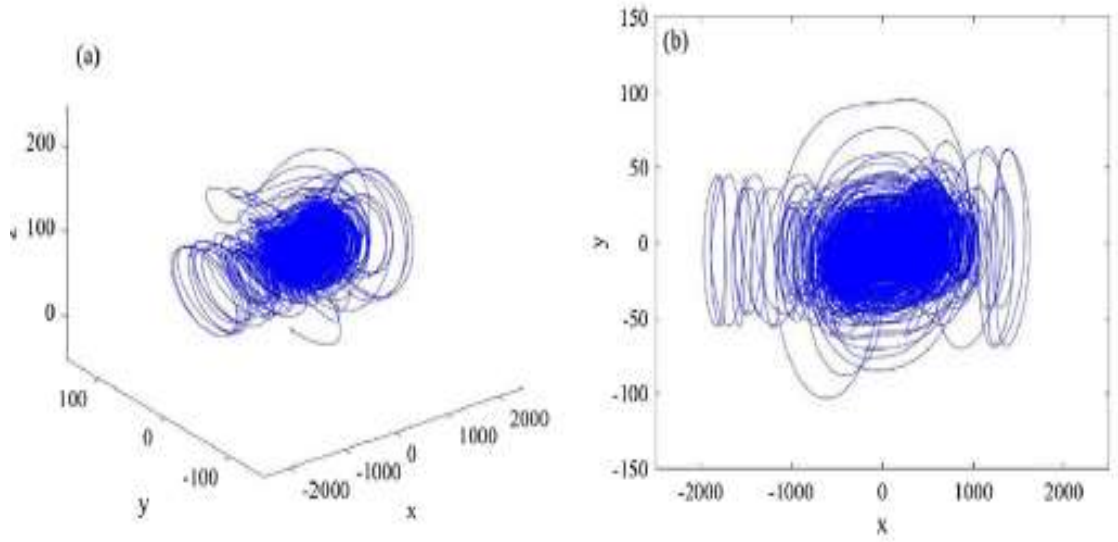


Figure 1: The Chen system's hyper-chaotic attractor

I. Related Work

Traditional encryption methods, including the data cryptography framework and algorithms, were recently proposed in the available research. Previous studies identified an issue in the picture cryptography application procedure because digital images include multiple key qualities, such as a high degree of correlation and redundancy between neighboring pixels. It can be useful in image scrambling and diffusion encrypting. Albahrani et al. [2] proposed a block method-based image encryption method that uses a chaotic cross map as a map. Yu et al. [3] created an original image encryption approach based on a short-time fractional Fourier transform (FrFT) and a hyper chaotic system which increases defense against usual attacks. To enhance anti-interference performance, a diffusion operation and feedback mechanism were established. In addition, the employing of a hyper chaotic system increases key space and increases sensitivity to all key. Identified a color image encryption approach based on a hyper chaotic system that can compress and encrypt an image based on reconstructed visual demands. Huang et al. [4] indicated a nonlinear optical image encryption system capable of encrypting images in both the spatial and frequency domains, with phase truncation and bitwise exclusive-OR (XOR) operation expanding the multi-image encryption to it. A simple and efficient picture encryption technique based on several piece-wise linear chaotic map systems was devised in. To get a satisfactory encryption result, rotational permutation operations and block diffusion techniques were used. Examined the use of matrix semi-tensor product theory in a novel chaotic picture encryption method that involves a Boolean network, scrambling, and diffusion. In this study, the chaotic cryptosystem is combined with the RSA approach, which is based on public key cryptography [5], to create an asymmetric encryption system that uses the RSA algorithm to encrypt system parameters. This method tackles the problem of key distribution in encryption systems while also solving the processing performance disadvantage that occurs when the standard RSA algorithm encodes a full hyper-chaotic random phase mask.

.

II. Methodology

1. RSA Algorithm

The RSA approach is the ideal selection for asymmetric encryption merely because it is commonly utilized, but also because it provides more privacy through the generation of large prime integers for the public key, private key 'd', and modulus 'n'. Due to its resilience to various attacks, the Rivest Shamir Adleman (RSA) algorithm is based on cryptography using public keys and has been recognized as one of the greatest successes in IT security [6]. The RSA Algorithms were the most widely utilized public key cryptography, and one of the issues connected to maintaining customer confidence is the requirement for better safety. RSA, on the other hand, is slow, needs key deposit, and is often inappropriate for use in a variety of applications. In terms of speed and security, researchers should investigate developing new ways that incorporate multiple factors with the objective to enhance the performance of secure network communication. According to the RSA Algorithm, the public key 'e' may be used to factor n. Many RSA Algorithm modification research projects have been conducted with the alteration of modulus 'n' but without the modification of public key 'e'.

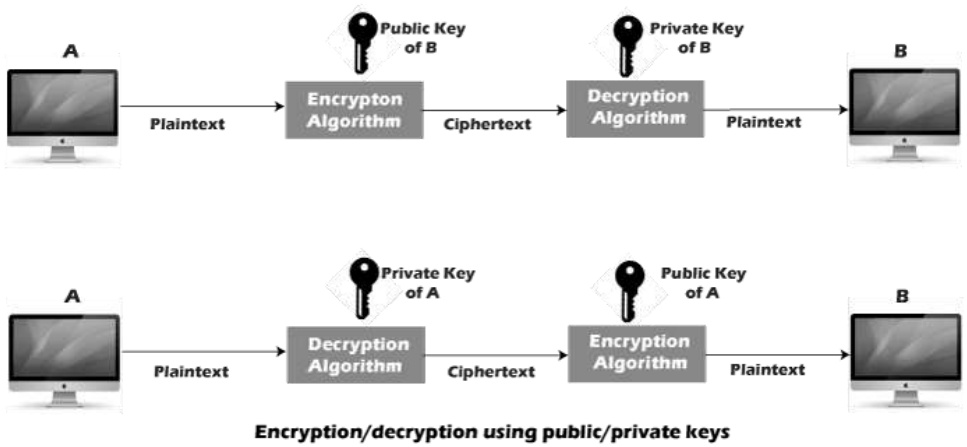


Figure 2: The RSA Algorithm's Original Flow

Steps:

1. Select the two prime numbers, p and q, by random with secret.
2. Compute$n = p * q$, $\varphi(n) = (p-1)(q-1), where\ \varphi(n)\ is\ the\ Euler\ function\ of\ n$
3. Randomly select $e\ in\ range\ 1 < e < \varphi(n). satisfying\ ged(e, \varphi(n)) = 1, where\ e\ and\ \varphi(n)\ are\ prime\ numbers$
4. Calculate the decryption key d, where e*d=1 mod ($\varphi(n)$).
5. Open integers n and e, and keep d in secret
6. Encrypt plaintext m to be cipher text c by c=$m^e\ mod\ n$
7. Decrypt cipher text c to be plaintext m by m = $c^d\ mod\ n$

2. Hyper-chaos and RSA-based optical image encryption scheme

As observed in Fig. 3, the present research offers an original asymmetric optical image encryption system based on the Fresnel transform, Hyper-chaotic random phase masks (HRPMs), and the RSA algorithm[7]. The usual Fresnel transform-based double random phase encoding tackle may be represented by a lens less 4 f system. In the standard DRPE method, two separate random phase plates are employed to turn the input image into a white noise-like image. When set up, the random phase plates select a similarly dispersed white noise matrix. As a result, there is no explicit building method needed for the standard DRPE for obtaining a random matrix. As a result, this paper improves the random matrix construction and transmission method, performs double random phase encoding in the Fresnel domain with random phase masks produced by various hyper-chaotic sequences, and then encrypts the system parameters through the RSA algorithm to achieve asymmetric optical image encryption [8]. The four-wing hyper-chaotic system and the Chen 4D hyper-chaotic system, accordingly, establish the random phase masks C1, C2, and C3. Taking the four-wing hyper-chaotic system as an example, we first set the system's beginning values, x1, y1, z1, and w1, and then continuously build hyper-chaos. Then, we build the Fibonacci iteration sequence using the nested Fibonacci sequence subscript, and finally, we rearrange the hyper-chaos sequence based on the random phase size.

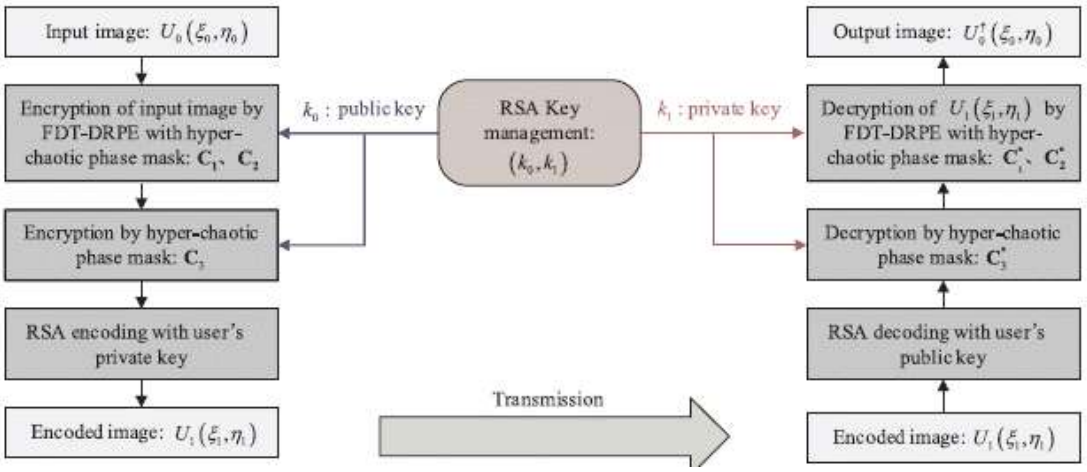


Figure 3: Block structure of asymmetric system encryption and decryption methods

The optical decryption process of the algorithm is shown in Figure 4. After performing private key decryption to find the key sequence (Key-I, Key-II, and Key-III), Fresnel diffraction parameters, and z of the encryption system, the computer develops a suitable optical decryption system that produces the hyper-chaotic sequence. The decrypted hyper chaotic phase plates C1, C2, and C3 have been received by the spatial light modulators SLM1, SLM2, and SLM3, where represents the conjugate operation[9].

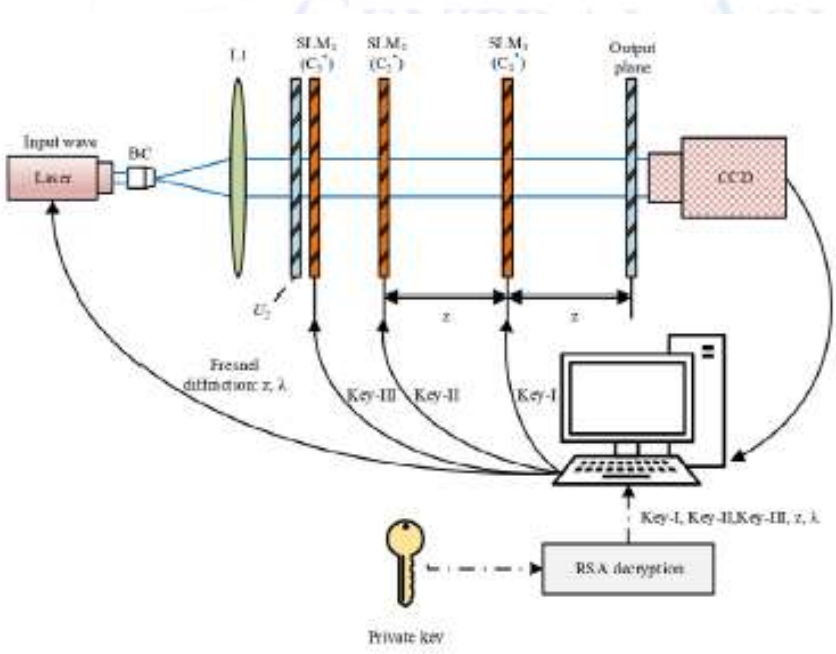


Figure 4: The optical decryption the mechanism is represented.

3. Scrambling Method

Scrambling is an usual method for arranging pixels. It can be used to encrypt a sequence utilizing a certain rule. In the present research, the scrambling approach compares the position of the elements in the original sequence to the position of the elements in the pseudorandom sequence s.=$\{s_1, s_2, s_3 \dots \dots s_M\}$ of equal length, and then to obtain the new sequence s=$\{s_1, s_2, s_3 \dots \dots s_M\}$ by rearranging the sequence s=$\{s_1, s_2, s_3 \dots \dots s_M\}$ with a specific rules. Using this method, the encrypted sequence is generated by scrambling the original sequence to a new sequence [10]. The encrypted sequence is obtained when the

original sequence is scrambled to a new sequence according to the specified rule. The structure of the scrambling process appears in Figure 5.

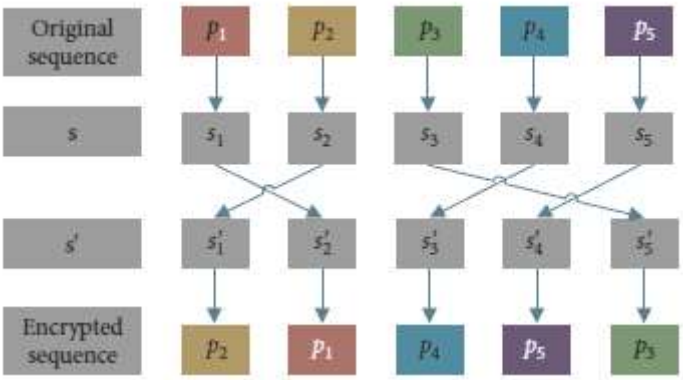
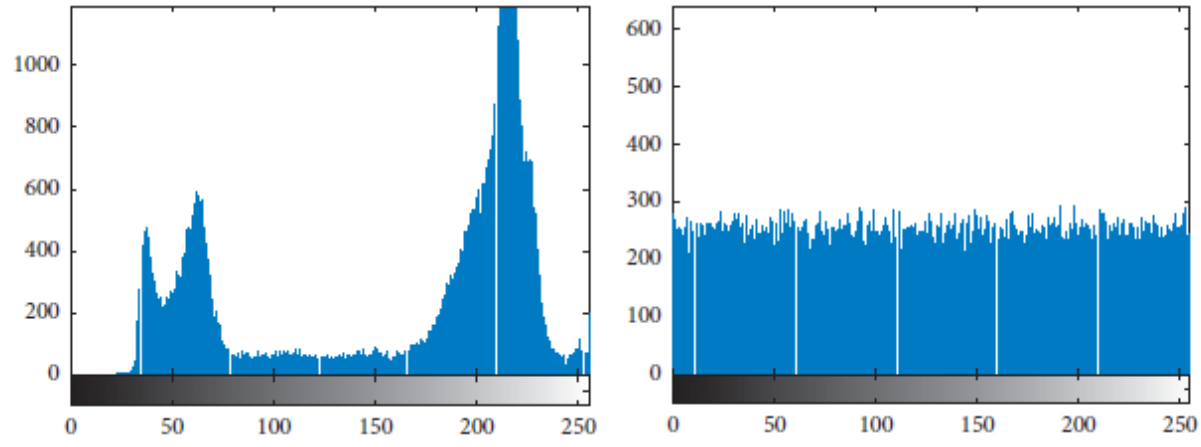


Figure 5: The scrambling process structure

III. Results

We performed statistical analysis attacks on encrypted images. A histogram may be utilized to identify the pixel value distribution of an image, and a good encryption method can produce a uniform and flat pixel value distribution. The encrypted image, once combined with the plaintext information, has an opportunity for revealing the plaintext information. The gray graphs of the Pepper plaintext image the cipher text image encrypted using the recommended approach are shown in Figure 6. The pixel distribution of the encrypted text picture is often uniform, which differs significantly from the gray histogram distribution of the original image[11].

The encryption results reported by are compared in Fig. 6(a) and (b)



(a) **(b)**

Figure 6: Plain and cipher image histogram analysis (a) Image of pepper; (b) Image of cipher

A total of 10,000 pixel combinations have been selected to be analyzed in the horizontal, vertical, and diagonal directions of the Pepper map and its encrypted image. The correlation coefficients are determined using the following equation.

$$r_{x,y} = \frac{E((x-E(x)).(y-E(y)))}{\sqrt{D(x).D(y)}} \quad (1)$$

IV. Conclusion

A method of encrypting optical images based on the hyper chaotic system and public key cryptography theory. To begin, hyperchaotic sequences are generated using the four-wing hyperchaotic system and the Chen 4D system, which involves the establishment of hyperchaotic random phase masks via preprocessing. The original image is then encoded using the Fresnel diffraction encryption method, which produces hyper-chaotic phase masks. The cipher text image is obtained after the hyper-chaotic random phase mask has blurred it. Finally, to guarantee key transmission security, the RSA approach is employed to encrypt the key sequences and Fresnel diffraction parameters.

The encryption system utilized in this study conducts asymmetric encryption of the hyper-chaotic system's starting values and system parameters, as well as the parameters of the optical Fresnel diffraction system, in accordance with the fundamental protocol of a public key encryption system. This approach not only compensates for the RSA algorithm's processing speed errors, but it additionally decreases the complexity of key transmission and improves the security of Fresnel domain double random phase encoding.

References

1. Y. Niu, Z. Zhou, and X. Zhang, “An image encryption approach based on chaotic maps and genetic operations,” Multimedia Tools and Applications, vol. 79, no. 35-36, pp. 25613–25633, 2020.
2. R. Parvaz and M. Zarebnia, “A combination chaotic system and application in color image encryption,” Optics & Laser Technology, vol. 101, pp. 30–41, 2018.
3. C. Lakshmi, K. -enmozhi, J. B. B. Rayappan, and R. Amirtharajan, “Hopfield attractor-trusted neural network: an attack-resistant image encryption,” Neural Computing and Applications, vol. 32, no. 15, pp. 11477–11489, 2020.
4. K. A. K. Patro, B. Acharya, and V. Nath, “Secure, lossless, and noise-resistive image encryption using chaos, Hyper-chaos, and DNA Sequence Operation,” *IETE Technical Review*, vol. 37, no. 3, pp. 223–245, 2019.
5. Z. Chai, S. Liang, G. Hu et al., “Periodic characteristics of the Josephus ring and its application in image scrambling,” *EURASIP Journal on Wireless Communications and Networking*, vol. 162, pp. 1–11, 2018.
6. X. Zhang, L. Wang, Z. Zhou, and Y. Niu, “A chaos-based image encryption technique utilizing hilbert curves and h-fractals,” *IEEE Access*, vol. 7, pp. 74734–74746, 2019.
7. Z. Hua, Y. Zhou, C.-M. Pun, and C. L. P. Chen, “2D Sine logistic modulation map for image encryption,” *Information Sciences*, vol. 297, pp. 80–94, 2015.
8. N. Benyamin, M. Sattar, and S. S. Mohammad, “A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process,” *Multimedia Tools&Applications*, vol. 71, no. 3, pp. 1469–1497, 2014.
9. Swathi, P. (2021). Industry Applications of Augmented Reality and Virtual Reality. *Journal of Artificial Intelligence, Machine Learning and Neural Network (JAIMLNN) ISSN: 2799-1172*, *1*(02), 14-18.
10. Ramana, S., Bhaskar, N., Murthy, M. R., & Sharma, M. R. (2023). Machine Learning for a Payment Security Evaluation System for Mobile Networks. In *Intelligent Communication Technologies and Virtual Mobile Networks* (pp. 347-356). Singapore: Springer Nature Singapore.

11. Swathi, P. (2022). Implications For Research In Artificial Intelligence. *Journal of Electronics, Computer Networking and Applied Mathematics (JECNAM) ISSN: 2799-1156*, *2*(02), 25-28.
12. Swathi, P. (2022). A Study On The Restrictions Of Deep Learning. *Journal Of Artificial Intelligence, Machine Learning and Neural Networks*, *ISSN-2799-1172*, *2*(2), 57-61.
13. Bhaskar, N., Ramana, S., & Kumar, G. M. (2023, January). Internet of Things for Green Smart City Application Based on Biotechnology Techniques. In *2023 International Conference on Artificial Intelligence and Knowledge Discovery in Concurrent Engineering (ICECONF)* (pp. 1-7). IEEE.
14. Ramana, S., Bhaskar, N., & Murthy, M. R. (2020). Three Level Gateway protocol for secure M-Commerce Transactions. *Solid State Technology*, *63*(6), 11155-11174.
15. Pothuganti, K. (2021). Long Short-Term Memory (LSTM) algorithm based prediction of stock market exchange. *International Journal of Research Publication and Reviews*, *2*(1), 90-93.
16. Swathi, P. (2013). Scope of Financial Management and Functions of Finance. *International Journal of Advanced in Management, Technology and Engineering Sciences. ISSN NO-2249-7455*, *3*, 109-116.