International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 6 June 2023, pp: 390-397 www.ijaem.net ISSN: 2395-5252

Secure Image Encryption Scheme based on chaotic maps

Sahithyan S, Naveen Balaji J, Santhosh Kumar S, Dr. G A Sathish Kumar

Department of Electronics and Communication Engineering, Sri Venkateswara College of Engineering, Chennai, India

Department of Electronics and Communication Engineering, Sri Venkateswara College of Engineering, Chennai, India

Department of Electronics and Communication Engineering, Sri Venkateswara College of Engineering, Chennai, India

Department of Electronics and Communication Engineering, SriVenkateswara College of Engineering Chennai, India

----

Date of Submission: 05-06-2023 Date of Acceptance: 16-06-2023

ABSTRACT—Secure image transmission is one of the most challenging problems in the age of communication technology. Millions of people use and transfer images for either personal or commercial purposes over the internet. One way of achieving secure image transmission over the network is encryption techniques that convert the original image into a non-understandable or scrambled form, called a cipher image, so that even if the attacker gets access to the cipher they would not be able to retrieve the original image. Among many algorithms, due to the superiority of chaos technology, when the image is encrypted with chaos technology, the cipher text presents a randomness, which makes the possibility of deciphering greatly reduced.

Keywords— Image encryption, chaos technology, cipher image

I. INTRODUCTION

Data transmission in any parts of the world is made easier because of wireless transmission. Among them, digital image and digital video have become the important content of data transmission. These digital images must be in secured form to be transmitted over the networks. In recent years, information transmission and sharing based on digital images often face the problems of data theft, tampering, deletion, and attack, which have caused great losses to the owners or publishers of digital images. To overcome this difficulty, digital data that has to be transmitted needs to be encrypted. Digital images can be processed as a two- dimensional data set, cryptographic systems that directly use text-encryption techniques often face problems of inefficiency in encryption and decryption, low practicability, and low security. Researching a cryptographic system or encryption method suitable for digital image encryption is the only way to protect the security of digital images in the network environment.

Conventional algorithms or techniques mainly include digital image encryption based on digital image encryption based on image compression coding, pixel transformation, digital image encryption based on random sequence and digital image encryption based on image key. The proposed algorithm uses chaos technology for image encryption. The chaos technology is difficult to crack and randomness, which makes the digital image encryption technology based on chaos technology become a more reliable digital image encryption technology. The image content occupies vital characteristics like high redundancy, space, capacity and correlation among the bit pixels as parameters for image encryption.

II. EXISTING SYSTEM

A. Digital Water marking Technology

The technology adopts the signature processing of digital images and adds custom watermark information to the original digital images to protect the copyright of digital images. It is one of the important technical means for image security protection in the Internet. However, the disadvantage of digital watermarking technology is that the visibility of digital images cannot be avoided. Usually, only the copyright of the image is not infringed, and when the content of the digital image needs to be protected, there is nothing that can be done.

B. Image encryption based on DNA coding

Image encryption algorithms based on DNA coding involve four basic processes. It involves scrambling the pixel position of the image by using a chaotic sequence and then the scrambled image matrix to the DNA sequence. Secondarily disturbing the DNA sequence matrix by using a chaotic sequence combined with addition, subtraction, XOR, or complement operation, or a combination of these operations and obtaining the encrypted image by DNA decoding and recombination.

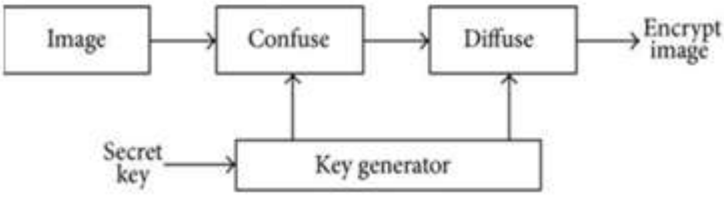


Image encryption process by DNA coding

C. The digital image protection method

Image encryption technology and its basic principle is to encrypt the digital information contained in the digital image, and get the completely different encrypted images of the appearance and the original digital image, so that the content of the digital image cannot be viewed directly. When the digital image is needed for viewing or using, the corresponding decryption algorithm is used to calculate and decrypt the encrypted image to restore the original content of the digital image, which is an important means for digital image content protection in a distributed environment with high security requirements.

III. PROPOSED SYSTEM

The secure image transmission in the proposed algorithm involves chaotic map generation for image encryption and decryption. Encryption convert the original image into a non-understandable or scrambled form, called a cipher image, so that even if the attacker gets access to the cipher they would not be able to retrieve the original image. It utilizes two encryption techniques chaotic sequences and linear feedback shift registers, to generate encryption keys that are used to encrypt the image data.

A. Symmetric-keyencryption

Symmetric-key encryption is a type of encryption that uses the same key for both encryption and decryption. This means that the key must be kept secret, and anyone who has access to the key can decrypt the message. Symmetric-key encryption is faster than asymmetric-key encryption, but the security of the message relies the key remaining secret.

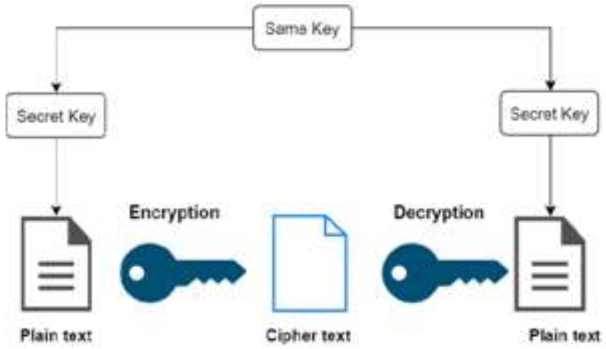
B. Cryptography:

The concept of cryptography and its history, including ancient methods such as substitution ciphers and modern methods such as AES and RSA.

Cryptography involves techniques for secure communication in the presence of third parties, and has been used throughout history for secrecy and confidentiality.

Substitution ciphers involve replacing plain text letters with other letters or symbols, while modern methods use complex algorithms and mathematical principles for encryption and decryption.

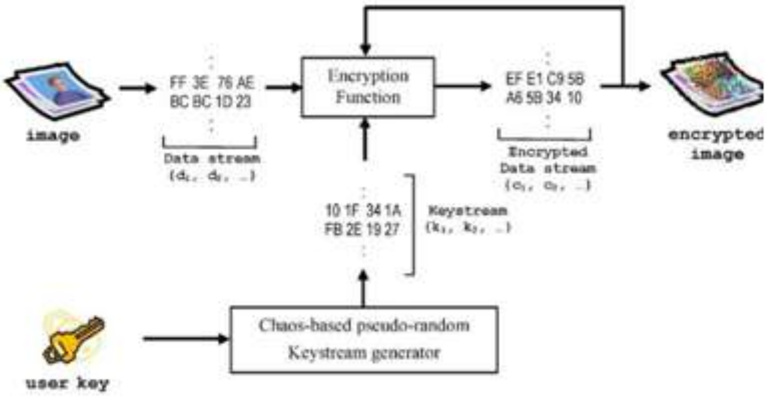
Substitution ciphers involve replacing plaintext letters with other letters or symbols, while modern methods use complex algorithms and mathematical principles for encryption and decryption.



C ..Probability Theory:

This involves concepts such as probability distributions, which describe the likelihood of different outcomes. The probability distributions such as the uniform distribution are used to generate random numbers that are used in the encryption process.

The use of random numbers adds an element of randomness to the encryption process, making it more difficult for unauthorized parties to access the original image data. The use of probability distributions ensures that the encryption process is secure and that the encrypted data is difficult to predict



D. Chaotic systems

Chaotic systems are complex, dynamic systems that exhibit highly unpredictable behavior. They are used in cryptography for generating random keys and sequences. The unpredictable nature of chaotic systems makes them useful for cryptography, as it is difficult for an attacker to predict the key or sequence generated by the system. Examples of chaotic systems used in cryptography include the Lorenz system, the logistic map.

Chaos theory is a non-deterministic theoretical system based on nonlinear systems and randomness. The definition of chaotic system is as follows:

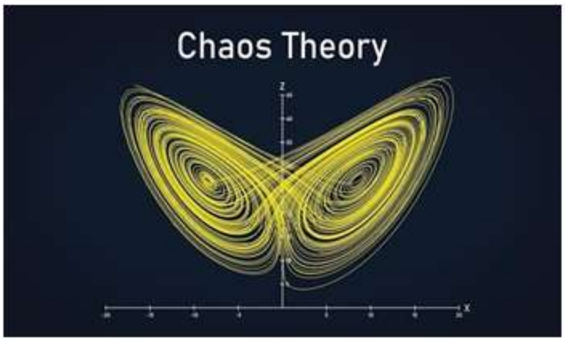
1) The period off(x) does not have an upper bound;
2) Let S be an uncountable subset of I, then the following conditions are true:

$$\forall x, y \in S, x \neq y, \lim_{n->\infty} \sup | f^n(x) | - f^n(y) | > 0$$

$$\forall x, y \in S, \lim_{n->\infty} \inf | f^n(x) - f^n(y) | = 0$$

$$\forall x \in S, \lim \sup_{n>\infty-} | f^n(x) - f^n(y) | > 0$$

$$(\text{y is any periodic point of f(x)})$$



Chaos theory

E. Random chaotic sequence generation

The random number generation method in the computer cannot achieve complete randomness, the sequence obtained by chaotic mapping is a pseudo random sequence. The distribution function of the logistic pseudo random sequence is shown in the following formula:

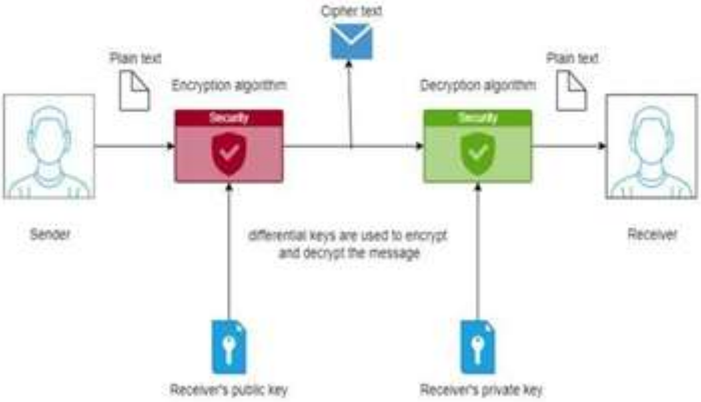
$$\rho(x) = \begin{cases} \left(\pi\sqrt{1-x^2}\right)^{-1} & x \in (0,1) \\ 0 & x \notin (0,1) \end{cases}$$

The corresponding random number sequence is automatically generated according to the initial value setting and is used for stream encryption processing of the digital image.

F. Image encryption

In cryptography, encryption is defined as the process of converting useful information into an unrecognizable form to protect it from unauthorized access. Image encryption is used to protect images from unauthorized access and modification. Encryption algorithms are applied to the image to produce an encrypted image that cannot be easily deciphered without the encryption key. The encrypted image can be transmitted securely stored on a device without the risk of being accessed by unauthorized users.

The image content occupies vital characteristics like high redundancy, space, capacity and correlation among the bit pixels,that demands some kind of encryption technique where the purpose is to securely transmit the image over the network and decrypting on the other end.



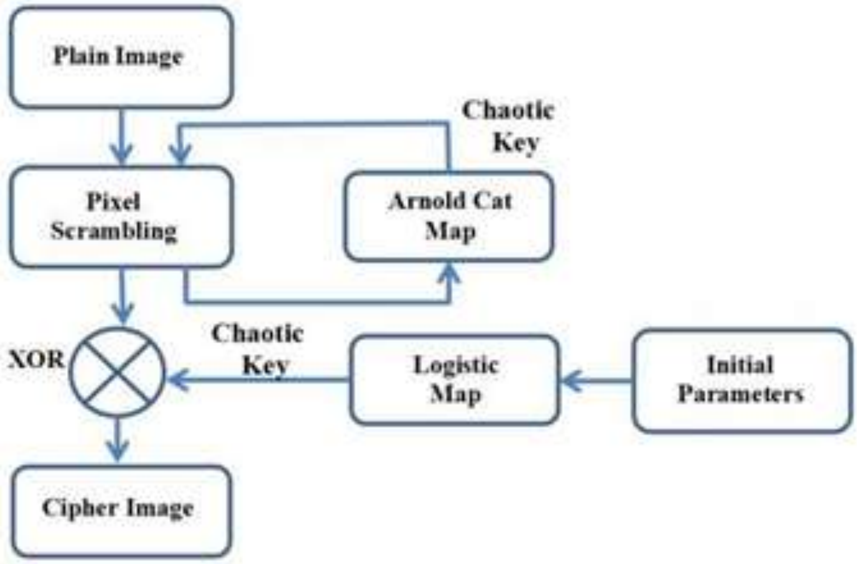
F.MATLAB software

The proposed algorithm utilizes MATLAB software for its chaotic sequence generation and image encryption. MATLAB is a programming platform designed specifically for engineers and scientists to analyse and design systems and products that transform our world. The MATLAB language is a matrix- based language allowing the most natural expression of computational mathematics. It allows matrix manipulations, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs written in other languages.

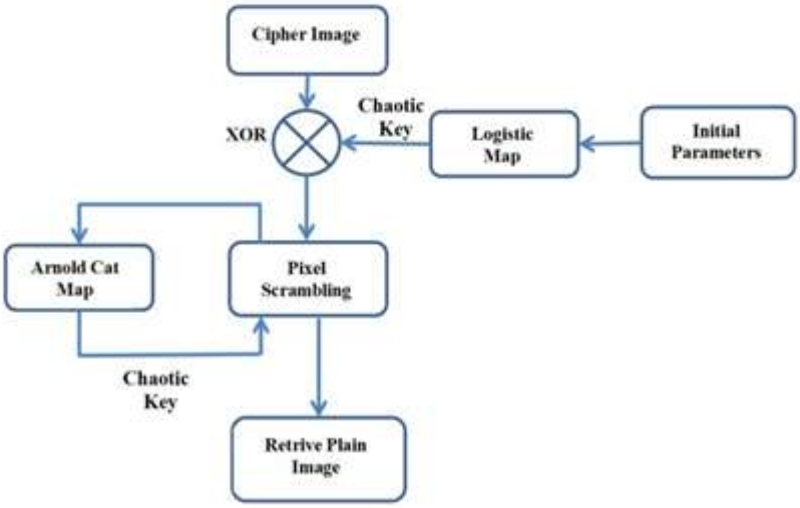
H.Proposed algorithm

The image encryption algorithm for secure transmission involves the following processes:

1) The algorithm is based on a combination of the Arnold cat map and the logistic map to achieve better security and efficiency for image encryption.
2) In the first stage, the plain image is scrambled using the Arnold cat map, which is a permutation-based chaos map that provides high levels of randomness.
3) The second stage involves diffusion, where the scrambled image is further encrypted using the logistic map. The logistic map is a one-dimensional chaotic map that provides a high degree of unpredictability.
4) The logistic map is used to generate a chaotic key sequence, which is then XORed with the scrambled image to obtain the encrypted image.
5) To decrypt the image, the inverse operations are performed in reverse order. The logistic map is used to generate the same chaotic key sequence that was used for encryption, and the encrypted image is XORed with this key to obtain the scrambled image.
6) The scrambled image is then unscrambled using the inverse Arnold cat map to obtain the original plain image.
7) The security of the algorithm is based on the properties of chaos, which provide a high degree of randomness and unpredictability, making it difficult for attackers to obtain the original image.
8) The algorithm is also computationally efficient, making it suitable for real-time image encryption applications



Encryption



Decryption

Flowchart of proposed algorithm

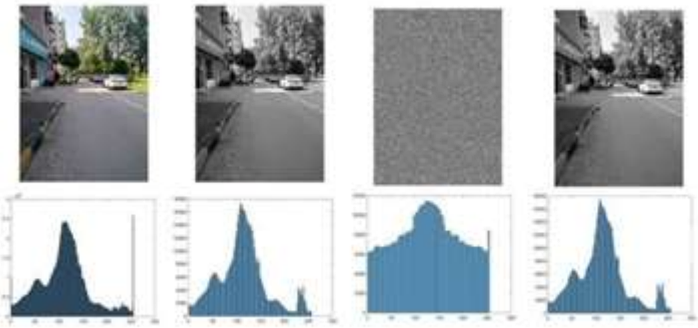


Image intensities

H.Applications of proposed system

a. Secure communication: The algorithm can be used to encrypt and decrypt messages, files, or images sent over the internet or other communication channels, ensuring that the data remains private and secure.

b. Data storage: The algorithm can be used to encrypt and decrypt data stored on local or remote devices, protecting sensitive information from unauthorized access or theft.

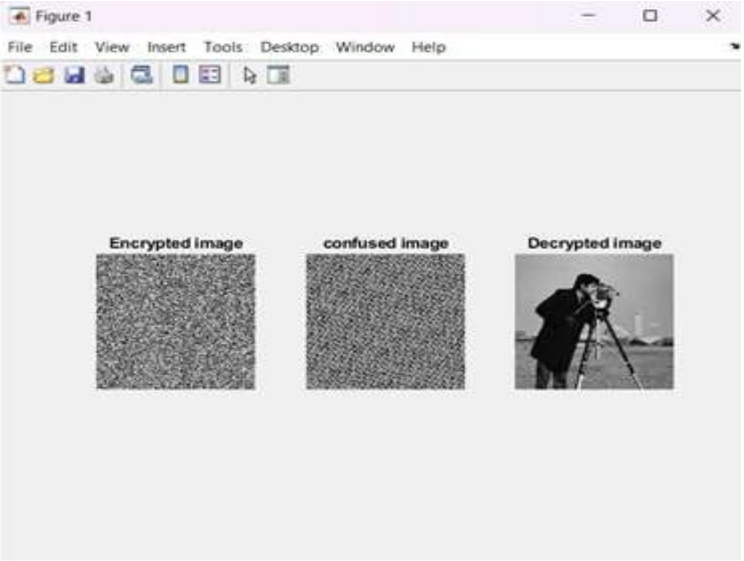
c. Medical imaging: The algorithm can be used to encrypt and decrypt medical images, such as X-rays or CT scans, which contain sensitive patient and prevent unauthorized access to medical records.

d. Military and government applications: The algorithm can be used in encrypting sensitive military or government data, such as classified documents or surveillance images.

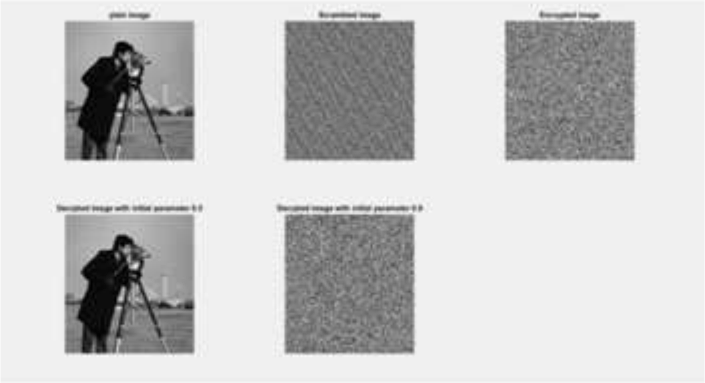
IV. RESULTS AND DISCUSSION

The following image represents that the original image is converts into gray scale image which undergoes chaotic sequence generation and finally gives encrypted image as an output.

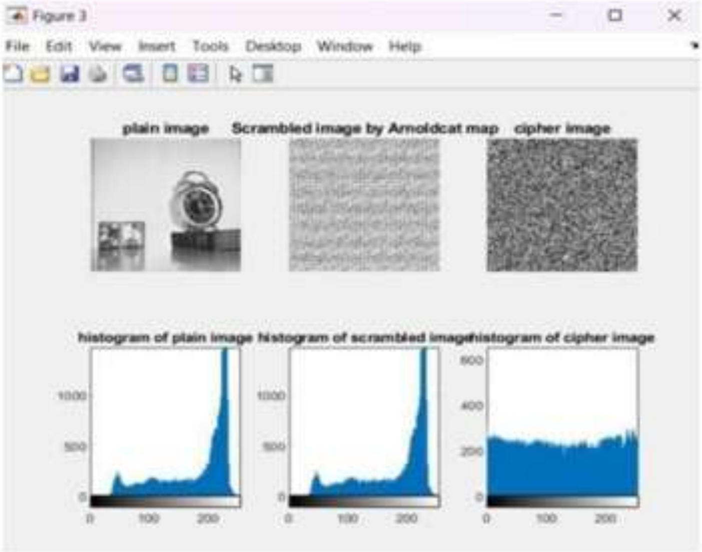
Ciphered Image



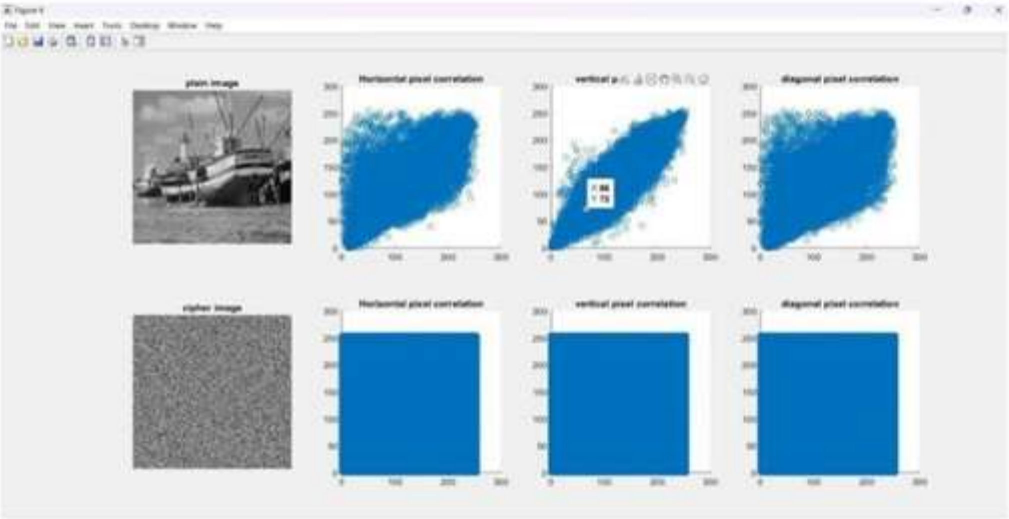
Encrypted, Confused & Decrypted image


plain image
Scrambled image
Encrypted image
Decrypted image with initial parameter 0.2
Decrypted image with initial parameter 0.9

Key Sensitivity Analysis



Histogram Analysis


plain image
Horizontal pixel correlation
vertical pixel correlation
diagonal pixel correlation
cipher image
Horizontal pixel correlation
vertical pixel correlation
diagonal pixel correlation

Correlation Analysis

V. CONCLUSION

The proposed algorithm uses a combination of chaotic and pseudo random sequences to generate the encryption and decryption keys. This makes it more secure than traditional encryption methods that rely solely on pseudo random sequences. This algorithm is relatively fast and complexity is less. The algorithm can be modified easily by changing the chaos seed, LFSR seed, and chaos constant. This allows users to customize the level of security and complexity to fit their specific needs.

REFERENCES

[1]. Chuman, T.; Sirichotedumrong, W.; Kiya, H. Encryption- then-compression systems using gray scale-based image encryption for JPEG images. IEEE Trans. Inf. Forensics Secur. 2018, 14, 1515– 1525. [CrossRef]

[2]. Elhoseny, M.; Shankar, K.; Lakshmanaprabu, S.; Maseleno, A.; Arunkumar, N. Hybrid optimization with cryptography encryption for medical image security in Internet of Things. Neural Comput. Appl. 2020, 32, 10979–10993. [CrossRef]

[3]. Sitaula, C.; Shahi, T.B.; Aryal, S.; Marzbanrad, F. Fusion of multi-scale bag of deep visual words features of chest X-ray images to detect COVID-19 infection. Sci. Rep. 2021, 11, 23914. [CrossRef] [PubMed]

[4]. Dang, P.P.; Chau, P.M. Image encryption for secure internet multimedia applications. IEEE Trans. Consum. Electron. 2000, 46, 395–403. [CrossRef]

[5]. Zhao, R.; Zhang, Y.; Xiao, X.; Ye, X.; Lan, R. TPE2: Three-pixel exact thumbnail-preserving image encryption. Signal Process. 2021, 183, 108019. [CrossRef]

[6]. K.F. Wang, S. Zhuang, X.R. Zhao, JPEG image encryption algorithm based on three-dimensional multi- chaotic system [J]. Applied Mechanics & Materials 734, 554 –557 (2015) 27. C.

[7]. Wang, L., Cao, Y., Jahanshahi, H., Wang, Z. and Mou, J., 2023. Color image encryption algorithm based on Double layer Josephus scramble and laser chaotic system. Optik, 275, p.170590.

[8]. Alexan, W., Elkandoz, M., Mashaly, M., Azab, E. and Aboshousha, A., 2023. Color Image Encryption Through Chaos and KAA Map. IEEE Access, 11, pp.11541-11554.

[9]. Zhu, Y., Wang, C., Sun, J. and Yu, F., 2023. A chaotic image encryption method based on the artificial fish swarms algorithm and the DNA coding. Mathematics, 11(3), p.767.

[10]. Xiuli, G. Zhihua, Y. Ke, et al., An image encryption scheme based on three-dimensional Brownian motion and chaotic system [J]. Chinese Physics B 26(2), 99