ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 10, Issue 6, June 2023

Image Encryption Based on Chaotic Map

[1] Ranju Kumari Yadav, [2] Satya Venkata Rudhira Daita, [3] Kh.Motilal Singh

[1] [2] [3] Department of CSE, K L Deemed To Be University (KLU), Vaddeswaram, Guntur, Andhra Pradesh, India
Corresponding Author Email: [1] 2000032143cse@gmail.com, [2] 2000031160cse@gmail.com, [3] khmotilal@kluniversity.in

***Abstract*— Data security has emerged as a primary priority as data interchange across open networks and the Internet is expanding quickly. One method that could be utilized to solve this issue is data encryption. Data can be presented in text, image, audio, multimedia, etc. formats. In this present-modern world, photographs are used most frequently in multimedia applications. AES, RSA, DES, as well as other vintage picture encryption methods exhibit lower levels of security in addition to having minimal counterattack functionality.**

It was decided to adopt chaos-based cryptography as a solution to this issue. Because of their sensitivity to the initial conditions and control settings, chaotic systems can be employed for photo encryption. In the area of chaos-based imagery encryption, there have been lot of studies done. An endeavor has been made in this article to review the elements and techniques used for image encryption.

Keywords: Encryption, Image, chaotic maps, security.

I. INTRODUCTION

The privacy of data during transmission is crucial in the modern era since we may infer a lot of information from an image. As in this modern era a lot of images are shared with various sources without any security. Several asymmetric and symmetric cryptographic algorithms have been created for the safe and secure transfer of images. Text, picture, audio, video, and other types of data can be transmitted. Various tactics are utilized to safeguard sensitive picture data from unwanted access for each category of data. To provide security on open networks like the internet, where digital systems are continually evolving, data encryption is therefore used. Cryptography is the study of techniques for safe communication when an adversary is present. It deals with difficulties like key distribution, encrypted data, and authentication, to name a few. Image enhancement is a technique that safeguards photos by changing the original photo into a confusing one. Image encryption has applications in military surveillance, multimedia applications, medical knowledge, healthcare, digital communications, and many more. Image encryption using chaotic maps is a technique that uses the random and unpredictable behaviour of chaotic maps to scramble and secure the contents of an image. A chaotic map is a mathematical function that generates seemingly random and unpredictable sequences of numbers.

The use of chaotic maps for image encryption is based on the fact that small changes in the initial conditions of the chaotic map can lead to large changes in the output sequence. This makes it difficult for an attacker to reproduce the same sequence of pseudo-random numbers and decrypt the image without the correct secret key

1.1. Image Encryption Methodologies

Image encryption is the process of converting an image into a coded form so that it can only be read or accessed by authorized persons. Chaotic maps can be used in image encryption to create a high level of complexity and randomness, making it difficult to decrypt the image without the proper decryption key.

Here are three common image encryption methodologies that use chaotic maps:

- *Logistic Map:* The Logistic Map is a type of chaotic map that can be used for image encryption. In this method, the original image is converted into a one-dimensional array of pixels, which is then used to generate a chaotic sequence using the Logistic Map. The chaotic sequence is then used to give rise to a secret key, which is used to encrypt the image.
- *Arnold Transform and Chaotic Map:* In this method, the original image is first transformed using the Arnold Transform, which rearranges the pixels of the image in a specific pattern. Then, a chaotic map is used to generate a secret key, which is used to encrypt the transformed image. This method provides a high level of security because the image is transformed before it is encrypted, making it difficult to decrypt the image without the proper decryption key.
- *DNA Sequence-Based Chaotic Map:* This method uses a DNA sequence-based chaotic map to generate a secret key, which is then used to encrypt the image. The DNA sequence is converted into a binary sequence, which is then used to generate a chaotic sequence using the chaotic map. The chaotic sequence is then used to make the secret key, which is used to encrypt the image.

These are just a few examples of image encryption methodologies that use chaotic maps. There are many other methods and variations that use different chaotic maps and encryption techniques.

1.2. Synopsis of the chaos theory for cryptography

The Chaos Theory is a mathematical concept that deals with systems that are highly sensitive to initial conditions and

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 10, Issue 6, June 2023

display unpredictable behavior over time. This property of chaotic systems has been used in cryptography to develop encryption algorithms that are difficult to crack.

In chaos-based cryptography, the key used to encrypt and decrypt the message is generated by a chaotic system. The system produces a sequence of random numbers that are used as the encryption key. Since the chaotic system is highly sensitive to initial conditions, even a small change in the input parameters of the system can result in a completely different output. This makes it difficult for an attacker to predict the key used for encryption without knowledge of the initial conditions.

Chaos-based cryptography has several advantages over traditional cryptographic methods. For example, it is resistant to brute force attacks as guessing the key requires knowledge of the initial conditions of the chaotic system. Additionally, the randomness of the chaotic system used to generate the key makes it difficult to perform statistical analysis or frequency analysis attacks.

However, there are also some challenges associated with chaos-based cryptography. One of the main challenges is the need for accurate and precise initial conditions. Any errors in the initial conditions can result in completely different outputs and make the encryption and decryption process difficult or impossible.

Overall, the Chaos Theory has proved to be a promising area for cryptography research and has the potential to lead to the development of new and more secure encryption methods.

1.3. Literature Survey

Many researchers have attempted in the past to use the ECC field's capabilities for security applications. In this area, we've highlighted few of the pertinent labour. During his research, Ray C. [4] described the construction of a generator that creates user-defined custom ECC hardware automatically.

ECC engineering is depicted by Alessandro Cilardo et al as a challenging interdisciplinary subject of study that includes disciplines like computer-aided learning and electromechanical engineering [5]. 32-bit RAM computer with output. An overview of ECC for wireless security is given by Kristin Lauter [3]. It emphasises the performance advantages of employing ECC rather than conventional RSA cryptography in wireless situations. For ECC on GF, C. J. McIvor et al. [6] present a new tool design (p). A high performance EC cryptography approach for common curves on GF(p) is described in Gang Chen's work [7]. [8] defines the public key cryptography standard specification.

Williams Stallings et al. [9] provide a succinct overview of ECC ideas. In a study given by Kevin M. and published by SangookMoon, redundant transcoding from the Radix 4 Booths algorithm is used to create a novel scalar point multiplication technique that is more effective than double and add [II]. His ECC was subjected to a brute force attack by UC Berkeley's Tiny OS, which looked through the operating system for wireless sensor networks [10].

This attack takes advantage of the brief lifespan of the pseudo-random number generators used by cryptosystems to produce private keys. Jaewon Lee's article [12] outlines his three algorithms for carrying out scalar multiplication in EC defined in finite fields with better features, like OEA (Optimal Extension Field). According to Liu Yongliang [13], Aydose et al . However, inside attackers are not the only ones who can exploit Protocol S through man-in-the-middle assaults. They suggested a brand-new ECC-based wireless authentication system. [14] includes comprehensive mathematical treatments and covers the entire spectrum of EC domains. It is suggested to use his ECC-based cryptosystem in text-based applications due to the popularity of his work on ECC and its widespread use. Future versions of the proposed work could include XML-based apps.

II. CHAOTIC IMAGE ENCRYPTION LAYOUT

Chaotic image encryption is a technique that uses chaotic systems to scramble the pixels of an image to make it unreadable without the decryption key. The basic layout of chaotic image encryption involves the following steps:

1. Key generation: A secret key is generated using a chaotic system such as a Lorenz system or a logistic map. The key should be sufficiently long and random to ensure the security of the encryption.

2. Image preparation: The image to be encrypted is transformed into a matrix of pixels. Each pixel can be represented as a set of values that define its color or intensity, such as RGB values.

3. Pixel scrambling: The pixels of the image are scrambled using a chaotic permutation algorithm. The permutation algorithm rearranges the pixels of the image according to a chaotic sequence generated from the secret key. This process ensures that the original image cannot be recovered without the decryption key.

4. Pixel substitution: The scrambled pixels are then replaced with new pixel values using a chaotic substitution algorithm. The substitution algorithm maps the original pixel values to new values based on a chaotic sequence generated from the secret key. This process adds an additional layer of security to the encryption by replacing the original pixel values with random values.

5. Output: The final encrypted image is generated by combining the scrambled and substituted pixels. The resulting image appears random and unintelligible, making it impossible to decipher without the decryption key.

To decrypt the image, the same key must be used to reverse the pixel substitution and permutation algorithms in the reverse order. The decrypted image will be an exact copy of the original image.

ISSN (Online) 2394-2320

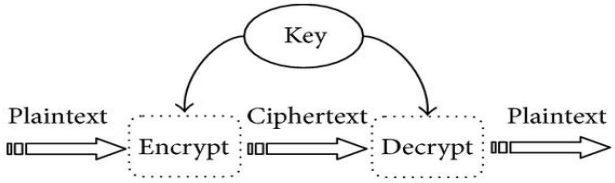
International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 10, Issue 6, June 2023

III. SIMULATION

Simulation of image encryption using chaotic map involves creating a computer program that utilizes a chaotic map to scramble the pixels of an image in a way that makes it difficult to decipher without the decryption key.The simulation can be performed using various chaotic maps, such as the Lorenz system, the logistic map, or the Henon map.

3.1. Encryption Process



The encryption process in chaotic maps typically involves the following steps:

1. Choose a chaotic map: There are many different chaotic maps that can be used for encryption, such as the logistic map or the Henon map. The choice of map will depend on the specific requirements of the encryption scheme.
2. Choose initial conditions: The chaotic map requires an initial condition to start generating its sequence. This can be any number within the range of the map.
3. Generate a pseudorandom sequence: Apply the chaotic map to the initial condition to generate a sequence of pseudorandom numbers. This sequence can be used as a one-time pad to encrypt a message.
4. Encrypt the message: To encrypt a message, convert it to binary and then use the pseudorandom sequence as a one-time pad to perform XOR (exclusive OR) with the binary message. This results in a ciphertext that can be transmitted to the recipient.
5. Decrypt the message: To decrypt the ciphertext, the recipient must have access to the same chaotic map and initial condition used to generate the pseudorandom sequence. They can apply the map to the initial condition to regenerate the pseudorandom sequence and then use it to perform XOR with the ciphertext to recover the original message.

The general steps involved in simulating image encryption using a chaotic map are as follows:

1. Load the image to be encrypted : The first step is to load the image to be encrypted into the simulation program. The image to be encrypted into the simulation program. The image can be in any standard format, such as JPEG,BMP, or PNG.
2. Convert the image to a matrix of pixels: The image is then converted into a matrix of pixels, with each pixel represented by its RGB values or grayscale intensity value.
3. Generate a secret key using a chaotic map: The next step is to generate a secret key using a chaotic map. The chaotic map generates a sequence of random numbers that are used to scramble the pixels of the image.
4. Scramble the pixels using the secret key: The pixel values of the image are scrambled using the secret key generated in the previous step. The scrambling is usually performed using a permutation algorithm that rearranges the pixels according to the chaotic sequence generated by the map.
5. Substitute the scrambled pixels using the secret key: The scrambled pixels are then substituted with new pixel values using a chaotic substitution algorithm. The substitution algorithm maps the original pixel values to new values based on a chaotic sequence generated from the secret key.
6. Save the encrypted image: The final step is to save the encrypted image in a format that can be later decrypted. The encrypted image appears random and unintelligible, making it difficult to decipher without the decryption key.

To decrypt the image, the same secret key must be used to reverse the substitution and permutation algorithms in the reverse order. The decrypted image will be an exact copy of the original image.

IV. SECURITY ANALYSIS

Image encryption using chaotic maps is a technique that uses chaotic systems to generate a sequence of random numbers that are used to scramble the pixels of an image. This method is intended to make the image data unreadable to anyone who does not have the encryption key.

4.1. Table

Chaos Map	Pros	Cons
Logistic Map	Simple and efficient, well-studied	Weak to chosen plaintext attacks, periodic behavior
Henon Map	Highly chaotic , good randomness	Limited range, computationally expensive
Tent Map	Simple and efficient, good randomness	Limited range, not fully chaotic
Loren System	Highly chaotic, good randomness	High computational overhead.
Arnold Cat Map	Good for permutation, efficient implementation	Not fully chaotic, weak to brute force attacks.
Chua Circuit	Highly chaotic, good randomness	High computational overhead, complex implementation

A security analysis of an image encryption system using chaotic maps typically involves evaluating the following aspects:

1. Key space: The size of the key space determines the number of possible keys that can be used to encrypt and decrypt the image. The larger the key space, the more secure the encryption system is. A larger key space makes it more difficult for an attacker to guess the encryption key.
2. Randomness of the key: The key used for image encryption should be random and not repeatable. This ensures that it is difficult for an attacker to guess the key and recreate the original image.
3. Resistance to known attacks: The encryption system should be resistant to known attacks, such as statistical analysis, frequency analysis, and brute-force attacks. A good encryption system should make it difficult for an attacker to gain any meaningful information about the original image or the encryption key.
4. Sensitivity to initial conditions: Chaotic maps are highly sensitive to initial conditions, which means that even a small change in the initial conditions can result in a completely different output. This property is useful in image encryption, as it makes it difficult for an attacker to reproduce the encryption key. However, the encryption system should also be designed to handle small variations in the initial conditions, which can occur during transmission or storage.
5. Efficiency: The encryption system should be computationally efficient and should not add significant overhead to the image data. This ensures that the encryption process does not degrade the quality or resolution of the image.

Overall, a secure image encryption system using chaotic maps should have a large key space, use a random and non-repeating encryption key, be resistant to known attacks, and be designed to handle variations in the initial conditions. An effective security analysis should evaluate each of these factors and provide a comprehensive assessment of the encryption system's ability to protect image data from unauthorized access.

V. CONCLUSION

In conclusion, image encryption using chaotic maps is a powerful technique that can provide a high level of security and privacy for sensitive images. Chaotic maps like the Logistic map or the Mao chaotic map generate pseudo-random sequences of numbers that can be used to encrypt images in a way that makes it difficult for unauthorized users to decrypt them.

The main advantage of using chaotic maps for image encryption is the ability to generate a seemingly random and unpredictable sequence of numbers that can serve as a cryptographic key. Additionally, the encryption process is fast and efficient, making it suitable for use in real-time image transmission and storage applications.

However, there are some challenges associated with using chaotic maps for image encryption. One major challenge is the need to carefully choose the parameters and initial conditions of the chaotic map to ensure that the resulting encrypted image is secure and cannot be easily decrypted by unauthorized users.

Image encryption using chaotic maps is a popular method for securing image data from unauthorized access. Chaotic maps have proven popular to be effective tools for generating complex and unpredictable encryption keys, which can be used to scramble the image data and make it difficult to decipher.

REFERENCES

[1] A. Kumar and M. Kumar, "A comprehensive review on chaotic map-based image encryption techniques," Journal of Ambient Intelligence and Humanized Computing, vol. 10, no. 7, pp. 2641-2656, 2019.

[2] S. K. Mohapatra and S. K. Sahoo, "A survey on chaos-based image encryption techniques," Multimedia Tools and Applications, vol. 78, no. 17, pp. 24721-24756, 2019.

[3] X. Wang and J. Yang, "A survey of image encryption algorithms based on chaotic maps," Journal of Information Hiding and Multimedia Signal Processing, vol. 6, no. 3, pp. 612-624, 2015.

[4] R. K. Singh, A. K. Singh, and S. Singh, "A survey of chaotic map-based image encryption techniques," Journal of Computational and Theoretical Nanoscience, vol. 14, no. 3, pp. 1528-1541, 2017.

[5] Y. Zhang, X. Li, and F. Wang, "A survey of chaotic map-based image encryption techniques," in Proceedings of the 2014 IEEE International Conference on Image Processing (ICIP), pp. 2774-2778, 2014.

[6] C. Li, X. Liu, and S. Yu, "A survey of chaos-based image encryption," in Proceedings of the 2016 IEEE International Conference on Information and Automation (ICIA), pp. 2229-2233, 2016.

[7] M. U. Altaf, A. R. Al-Ali, and M. H. Ahmed, "A comprehensive survey on image encryption using chaotic maps," Journal of Electronic Imaging, vol. 27, no. 5, 2018.

[8] S. D. Khairnar and P. R. Deshmukh, "A survey on chaos-based image encryption techniques using pixel shuffling and substitution," Multimedia Tools and Applications, vol. 78, no. 12, pp. 16747-16777, 2019.

[9] M.Aydos, T.Yanik and C.K.Kog, "High-speed implementation of an ECC based wireless authentication protocol on an ARM microprocessor," lEEProcCommun.,Vol. 148, No.5, pp. 273-279, October 2001.

[10] N.Koblitz, Elliptic Curve Cryptosystems, Mathematics ofComputation, volA8, 1987, pp.203 -209. The Benefits of Elliptic Cryptography for Wireless Security,by Kristin Lauter, IEEE Wireless Communications, pp. 62- 67, Feb. 2006.

[11] Alessandro, Luigi Coppolino, Nicola Mazzocca, and Luigi Romano,"Elliptic Curve Cryptography Engineering", Proceedings of the IEEE, Vol. 94, no. 2, pp. 395 - 406, Feb. 2006.

[12] Ray C. C. Cheng, Nicolas Jean, Wayne Luke, and Peter Y. K Cheung, “Customizable Elliptic Curve Cryptosystems" , IEEE Trans. On VLSI Systems, vol. 13, no. 9, pp. 1048-1059, Sep. 2005.

[13] C. 1. McIvor, M. McLoone, and 1. V. McCanny, "Hardware elliptic curve cryptographic processor over GF(p)," IEEE Trans. Papers, vol. 53, no. 9, pp. 1946-1957, Sep. 2006.

[14] Kevin M. Finnigin, Barry E. Mullins, Richard A. Raines, Henry, "Cryptanalysis of an elliptic International Journal of Security and Networks, Vol. 2, No. 3/4, "Curve Cryptosystem for Wireless Sensor Networks,"

[15] Gang Chen, and Hongyi Chen, " A High-Performance Elliptic Curve Cryptographic Processor.