ISSN : 2455-9679
SJIF Impact Factor : 6.008

IJRTSM
INTERNATIONAL JOURNAL OF RECENT TECHNOLOGY SCIENCE & MANAGEMENT

"REVIEW ON DIGITAL IMAGE ENCRYPTION BASED ON CHAOTIC CRYPTOGRAPHY "

Ravi Yadav [1], Amit Shrivastava [2]

[1] *M.Tech. Scholar, Department of Electronics and Communication Engineering, VNS Faculty of Engineering Bhopal, Madhya Pradesh, India*

[2] *Associate Professor, Department of Electronics and Communication Engineering, VNS Faculty of Engineering Bhopal, Madhya Pradesh, India*

ABSTRACT

Since it was first used to secure images, chaos has been one of the best sources for cryptography. This paper takes a close look at how chaos-based image-encryption algorithms were made. It looks at symmetric and asymmetric algorithms block ciphers and stream ciphers, as well as how they were put together with other technologies. Chaos's unique qualities, such as its sensitivity to starting conditions, topological transitivity, and "pseudo-randomness," make it easy to compare it to other areas of study and improve methods for encrypting images. This paper also talks about how chaotic image encryption can be used in the real world and what problems it faces right now. This is meant to encourage researchers to keep making improvements and adding to what's already there. It could also be used to predict how chaos-based image encryption will change in the future.

Key Words: *Chaos, image encryption, chaotic system, image encryption based on chaos, chaotic map, and encryption.*

I. INTRODUCTION

Chaos is a pseudo-random and unpredictable motion exhibited in a deterministic dynamical system due to its sensitivity to initial values and parameters. Chaos theory grew out of the study of the three-body problem by [1]. After many studies, [2] came up with, which was the first example of a chaotic answer coming from a deterministic equation in a dissipative system. "Period Three Implies Chaos" was the first book to use the word "chaos" to describe this event. In an article, [3] proposed the Logistic map. This map was then studied in depth by [4], who suggested that this map could be used by anyone. Since then, there has been a lot of growth in the study of chaos. A chaotic system is a complicated and highly dynamic system that is sensitive to initial conditions, doesn't follow a straight line, doesn't repeat itself, etc. In the area of nonlinear dynamics, the study of chaotic systems has become an important topic because they are hard to predict and control. Chaos systems can be used in many different ways and in many different areas. In finance, chaotic

ISSN : 2455-9679
SJIF Impact Factor : 6.008

systems are used to model how financial markets work and to come up with methods for trading. In biology, chaotic systems are used to study how biological systems work and how populations change over time. In neural networks, chaotic systems are used to describe how neurons work and to come up with new algorithms for machine learning and AI. Also, chaotic systems are often used in cryptography to make safe communication systems because of how similar their structure is [5]. [6] Said that the "chaotic encryption" method should be used. Since then, scientists have looked at how systems change from a well-ordered state to a chaotic one, as well as how chaotic systems work. In the years that followed, there was a lot of study on chaos-based cryptography, which is now also being used in the real world.

Image Encryption-In a time when the Internet is growing quickly, it is easy for personal information to get out when a lot of pictures are processed and shared over the network. Because of this, pictures need to be encrypted and protected in some way. The data in a picture has special qualities, like a large capacity, high redundancy, and a high correlation between pixels. Because of this, image encryption has special structural requirements. Image encryption is a way to protect privacy and security by changing image data into a coded form. Encryption algorithms are often used to make a picture hard to understand for people who are not supposed to see it. Image encryption is required to make sure those private images, like personal, trade, and government secrets, are kept safe. In digital image processing, image encryption works by making it hard for unauthorized people to get to pictures, making it less likely that they will be stolen or changed. Digital watermarks and property information can also be kept safe with image encryption. Also, it's important to know that while picture encryption reduces security risks, it doesn't stop all security breaches or changes. So, for complete image encryption to work, it's important that the algorithms used to encrypt images are safe and reliable. In order to reach this goal, more and more encryption algorithms based on different technologies have been proposed for image encryption, such as chaos-based encryption [7,8], S-Box-based encryption [9,10], optical encryption [11], compression encryption [12], frequency-domain-based encryption, and DNA-based encryption. The major purpose of this paper is to explain the chaos-based image encryption scheme.

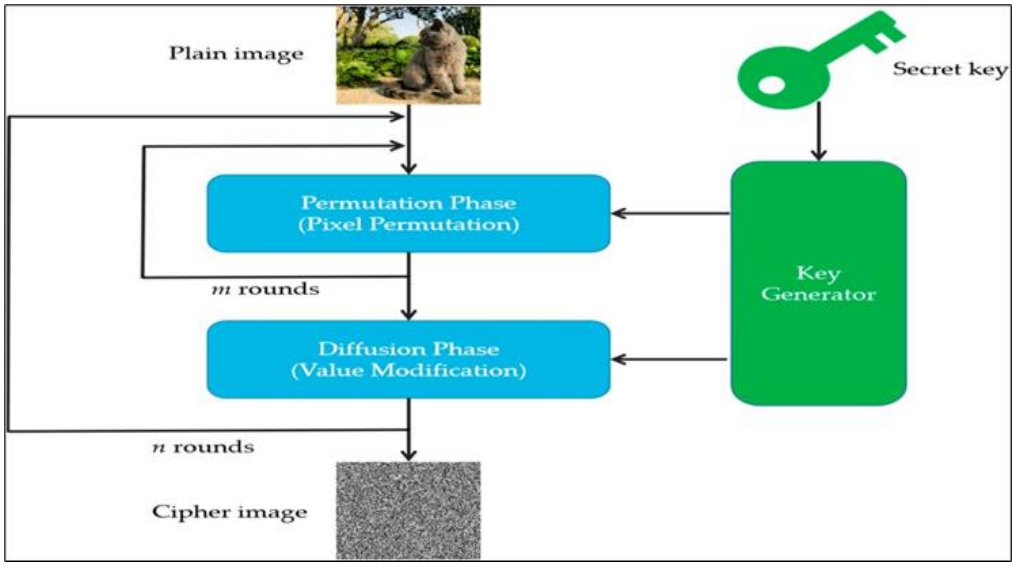

Figure 1. The architecture of permutation–diffusion chaotic image encryption

ISSN : 2455-9679
SJIF Impact Factor : 6.008

Chaos-Based Image Encryption-Image data generally take up more space than text data, and pixels that are close to each other have a lot in common with each other. So, traditional ways of encryption can't meet the needs of image encryption. But using chaos theory to secure images is a new way to do things. Chaos systems are very sensitive to how they start, and even small changes to how they start can make them move in very different ways. Even though the chaotic trajectory can be controlled once the starting conditions are known, it is impossible to predict the trajectory over a long period of time without knowing the initial conditions. Also, chaotic systems have other important qualities for picture encryption, such as high ergodicity, determination, and pseudo-randomness.

A-Chaos-Based Image Encryption Based on Symmetric Encryption

In symmetric encryption, the private key or hidden key is used for both encryption and decryption. Both the encrypt or and the decrypt or use the same key. To send the key, you need a secure route. When used to secure images, symmetric encryption can be split into spatial-domain chaotic image encryption and frequency-domain chaotic image encryption based on the transform domain used for encryption.

B-Chaotic Image Encryption Based on the Spatial Domain

In picture encryption, the image itself is called the "spatial domain." Since digital pictures are made up of many pixels, spatial-domain-based image encryption means working directly with the pixels. This can involve moving pixels or blocks around in a picture, changing the value or position of pixels in the original image, or doing other similar things. At the moment, most chaotic image encryption methods use spatial-domain encryption, while others use frequency-domain encryption.

II. LITERATURE REVIEW

Chaos-based picture encryption can be put into different types based on how it is put into groups. One way to classify it is by how the original picture is processed, which can be split into chaotic image encryption based on a block cipher and chaotic image encryption based on a stream cipher. It can also be put into two groups based on the way the key works: symmetric key chaotic image encryption and asymmetric key chaotic image encryption. Based on these two groups, we'll talk about chaos-based image encryption in this part. Song, W.et.al.2023 [13]. It's important to note that the following parts talk about the schemes in the order in which they were first published. Also, it is supposed that readers know a little bit about how chaotic systems work.

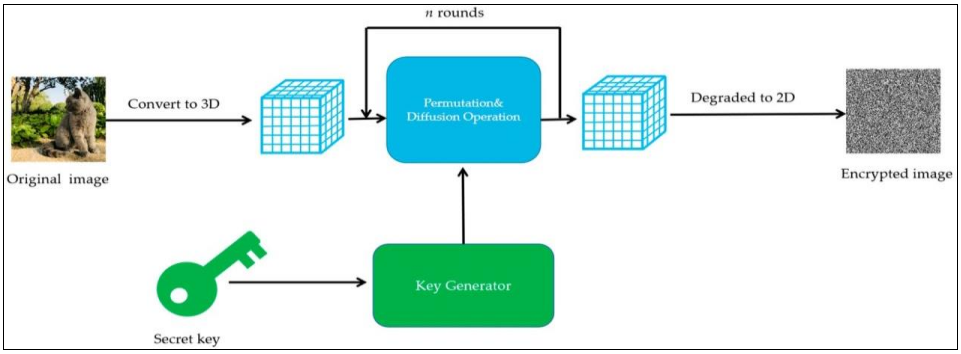

Figure 2 the process of the image-encryption algorithm

ISSN : 2455-9679
SJIF Impact Factor : 6.008

The main structure of a chaotic image encryption algorithm based on the spatial domain is a permutation–diffusion architecture, which is made up of two stages of iteration. During the permutation step, the pixel's position is changed, but its value stays the same. During the diffusion phase, the values of each pixel are changed one by one, so that even a small change in one pixel affects almost all of the other pixels in the picture. This is how the process works:

Based on how the original picture is processed, symmetric spatial-domain image encryption algorithms can be split into two types: block cypher and stream cypher. In block-cipher-based image encryption algorithms, the picture is encrypted or changed in groups of bits called blocks that are all the same length. In stream-cipher-based algorithms for encrypting images, the digital picture is turned into a stream of bits so that it can be processed.

Wu, X., Wang, et al. [14] introduced a chaotic image-encryption algorithm that replaces all of the original image's blocks and then shuffles its pixels with a chaotic sequence made by a Logistic map based on the permutation principle. In their study, they also talk about its VLSI architecture.

In contrast to previous chaos-based image encryption algorithms Wang, X. et.al.2021 [15], which needed the image to be encrypted as a square, Wu, Z. et.al.2019 [16] proposed a different chaotic image encryption method based on a Baker map. The improved symmetric method can be used to encrypt images of different sizes. This method also adds some extra security features to the cypher image, such as password binding, ECB, and CBC modes.

Jiao, K. et al. [17] suggested a chaos-based image encryption method that uses a 2D Standard map for confusion, a Logistic map for diffusion, and a Tent map to generate keys for sub-key generation and distribution. Then, in Xu, Q.2020 [18], a certain diffusion effect in the replacement stage caused by simple sequential add-and-shift operations was added to the scheme to save a lot of time on the whole encryption process.

Liu, Y, et al. 2020 [19] suggested a 3D method for encrypting images that is built on Chen's chaotic system. After iteration and preprocessing, Chen's system got three discrete variable sequences. These sequences were XORed with different parts of the original picture to get the encrypted image.

Ye, G., et al. 2021 [20] looked at the flaws in the suggested image encryption and made it better in three ways: The encryption or decryption phase needs M rounds of operations. The keystream depends on both the starting conditions and the grey value of the plain image. The keystream is made by chained mode, which links any two adjacent pixels. After M rounds of repetition, this makes it harder to see how pixels are linked together.

Ye, G.2022 [21] built on Luo, Y. et al.2019 [22] to create a Logistic-map-based image encryption in which the plaintext block is permuted using a key-dependent shift method and then encrypted using a permutation–diffusion-based technique.

Laiphrakpam et al. (2018) [23] came up with a way to encrypt images using Logistic maps. In the method, they used two Logistic maps. The first one is used to come up with amounts from 1 to 24 for the second Logistic map's first condition. Also, the pixels of a picture are encrypted using an external 80-bit secret key and eight different types of operations. The result of the Logistic map determines which of these is used for a given pixel.

Liu, H.; Kadir, et al. 2016 [24] showed a way to encrypt images using basic operations, nonlinear transformation functions, and a chaotic Tent map. This algorithm's cryptographic work is based on blocks of bits instead of blocks of

ISSN : 2455-9679
SJIF Impact Factor : 6.008

pixels. It uses session keys with 256 bits to turn a plain picture with 256 bits into a cypher image with the same number of bits.

Shakiba, A et.al. 2021 [25] introduced the nearest-neighbor coupled-map lattices (NCMLs), in which a pseudo-random sequence is generated with an NCML and an S-Box of AES. In addition, a 128-bit external key is used to reset the pixel values of the image blocks with the pseudo-random sequence. Meanwhile, the lattice values of the NCML are utilized to relocate image blocks.

Wang et al. (2018) [26] came up with a way for encrypting chaotic images using the Linear Diophantine Equation (LDE) and PWLCM. The LDE is an equation with integral values for one or more variables, for which the solutions must be integers.

Wang, J. et al. (2018) [27] came up with a new 1D chaotic system based on a Logistic map. This system was then used in picture encryption to reduce the digital degradation of chaotic systems with key space. The difference between two pseudo-orbits was used to make the pseudo-random sequence, which was used to encrypt a picture.

C-The Challenges of Chaos-Based Image Encryption

Studying the current challenges of chaos-based image encryption is important for improving its various aspects and addressing potential vulnerabilities. By identifying these challenges, researchers can gain new insights and inspiration for developing new and more effective encryption techniques that can provide a high degree of security, efficiency, and usability. These challenges can be seen as opportunities for further research and development in the field of image encryption.[27]

Chaos-based image encryption refers to the process of using chaotic systems or chaotic maps to encrypt digital images for secure transmission or storage. While it offers certain advantages, such as high sensitivity to initial conditions and encryption keys, it also presents several challenges. Here are some of the key challenges associated with chaos-based image encryption:

Security Analysis: One of the major challenges is conducting a rigorous security analysis of the encryption scheme. Chaos-based encryption algorithms often rely on the assumption that the chaotic maps used possess ideal properties, such as randomness and unpredictability. However, analyzing the security of chaotic systems is a complex task, and vulnerabilities may exist that could be exploited by attackers

Key Space and Key Management: Chaos-based encryption schemes typically require a large and robust key space to ensure security. Generating and managing such keys can be challenging. The keys need to be truly random, securely distributed, and kept confidential. Moreover, key synchronization between the sender and receiver is crucial for successful encryption and decryption, which can be difficult to achieve in practical scenarios.

Computational Efficiency: Encryption and decryption processes need to be computationally efficient for real-time applications. While chaos-based algorithms can offer high security, they often suffer from slow encryption and decryption speeds. This can limit their usability, especially in resource-constrained environments or applications that require fast processing.

Robustness to Attacks: Chaos-based encryption schemes must be robust against various attacks, such as chosen-

ISSN : 2455-9679
SJIF Impact Factor : 6.008

plaintext attacks, known-plaintext attacks, ciphertext-only attacks, or brute-force attacks. Additionally, they should be resistant to statistical analysis, differential attacks, and other cryptanalytic techniques. Ensuring the robustness of chaos-based encryption algorithms is a significant challenge.

Sensitivity to Image Transformations: Images are often subjected to various transformations, such as compression, resizing, or filtering, during transmission or processing. Chaos-based encryption schemes may be sensitive to these transformations, leading to a degradation of the encrypted image quality or potential decryption failures. Achieving robustness against such transformations is a considerable challenge in chaos-based image encryption.

Standardization and Interoperability: To ensure widespread adoption and compatibility across different platforms and systems, standardization of chaos-based encryption algorithms is essential. Developing common standards and protocols that facilitate interoperability is a challenge due to the diverse range of chaotic systems and encryption techniques proposed in the literature.

Practical Implementation Challenges: Implementing chaos-based encryption algorithms in real-world scenarios can be challenging. Factors such as hardware constraints, power consumption, and integration with existing systems need to be considered. Additionally, achieving a balance between security, efficiency, and usability is a non-trivial task.

III. CONCLUSION

Chaos-based image encryption is still one of the best ways to protect pictures. This paper gives a full review and discussion of chaos-based image encryption, including symmetric and asymmetric encryption, to help you understand how it has changed over time. There is also a summary of the schedule and an evaluation of how well image-encryption algorithms work. The paper also talks about how chaotic systems can be used with other technologies to secure images. These technologies include neural networks, genetic algorithms, DNA technology, cellular automata, blockchain, elliptic curve, and others. The unique features of chaos-based encryption, such as its sensitivity to initial conditions, topological transitivity, and pseudo-randomness, make it possible for researchers from different fields to work together and improve picture encryption methods. Chaos-based image encryption is also very important in real-world uses. In this study, there are examples of how this could be used in the medical field, the Internet of Things, the microcontroller field, and the satellite field. But chaos-based picture encryption still has some problems and problems to solve. This study mostly talks about two problems: how to protect against cryptanalysis or attacks, and how to process encrypted images. Still, these problems are not just problems; they are also opportunities that can lead to more study and development to fix what isn't working and give hope for the future of chaotic image encryption. Overall, chaos-based image encryption is a promising way to encrypt images, but it needs more study and development to make it safer, faster, and easier to use. In a world that is becoming more digital, we can keep personal information safe and private by tackling problems and looking for new ways to do things.

REFERENCES

[1] Avrutin, V.; Gardini, L.; Sushko, I.; Tramontana, F. Continuous and Discontinuous Piecewise-Smooth One-Dimensional Maps: Invariant Sets and Bifurcation Structures; World Scientific: Singapore, 2019.
[2] Leonel Rocha, J.; Taha, A.-K. Allee's effect bifurcation in generalized logistic maps. Int. J. Bifurc. Chaos 2019, 29, 1950039.

ISSN : 2455-9679
SJIF Impact Factor : 6.008

[3] Li, C.; Luo, G.; Qin, K.; Li, C. An image encryption scheme based on chaotic tent map. Nonlinear Dyn. 2017, 87, 127–133.
[4] Nepomuceno, E.G.; Nardo, L.G.; Arias-Garcia, J.; Butusov, D.N.; Tutueva, A. Image encryption based on the pseudo-orbits from 1D chaotic map. Chaos Interdiscip. J. Nonlinear Sci. 2019, 29, 061101.
[5] Liu, L.; Miao, S. A new image encryption algorithm based on logistic chaotic map with varying parameter. SpringerPlus 2016, 5, 289.
[6] Pak, C.; Huang, L. A new color image encryption using combination of the 1D chaotic map. Signal Process. 2017, 138, 129–137.
[7] Nardo, L.G.; Nepomuceno, E.G.; Arias-Garcia, J.; Butusov, D.N. Image encryption using finite-precision error. Chaos Solitons Fractals 2019, 123, 69–78.
[8] Santos, T.A.; Magalhães, E.P.; Basílio, N.P.; Nepomuceno, E.G.; Karimov, T.I.; Butusov, D.N. Improving Chaotic Image Encryption Using Maps with Small Lyapunov Exponents. In Proceedings of the 2020 Moscow Workshop on Electronic and Networking Technologies (MWENT), Moscow, Russia, 11–13 March 2020; pp. 1–4.
[9] Hua, Z.; Zhu, Z.; Yi, S.; Zhang, Z.; Huang, H. Cross-plane colour image encryption using a two-dimensional logistic tent modular map. Inf. Sci. 2021, 546, 1063–1083
[10] Li, X.; Xie, Z.; Wu, J.; Li, T. Image encryption based on dynamic filtering and bit cuboid operations. Complexity 2019, 2019, 7485621.
[11] Xu, C.; Sun, J.; Wang, C. A novel image encryption algorithm based on bit-plane matrix rotation and hyper chaotic systems. Multimed. Tools Appl. 2020, 79, 5573–5593.
[12] Xu, J.; Zhao, B.; Wu, Z. Research on color image encryption algorithm based on bit-plane and Chen Chaotic System. Entropy 2022, 24, 186.
[13] Song, W.; Fu, C.; Zheng, Y.; Tie, M.; Liu, J.; Chen, J. A parallel image encryption algorithm using intra bitplane scrambling. Math. Comput. Simul. 2023, 204, 71–88.
[14] Wu, X.; Wang, D.; Kurths, J.; Kan, H. A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system. Inf. Sci. 2016, 349, 137–153.
[15] Wang, X.; Liu, C.; Jiang, D. A novel triple-image encryption and hiding algorithm based on chaos, compressive sensing and 3D DCT. Inf. Sci. 2021, 574, 505–527.
[16] Wu, Z.; Zhang, X.; Zhong, X. Generalized chaos synchronization circuit simulation and asymmetric image encryption. IEEE Access 2019, 7, 37989–38008
[17] Jiao, K.; Ye, G.; Dong, Y.; Huang, X.; He, J. Image encryption scheme based on a generalized Arnold map and RSA algorithm. Secur. Commun. Netw. 2020, 2020, 9721675.
[18] Xu, Q.; Sun, K.; Zhu, C. A visually secure asymmetric image encryption scheme based on RSA algorithm and hyperchaotic map. Phys. Scr. 2020, 95, 035223.
[19] Liu, Y.; Jiang, Z.; Xu, X.; Zhang, F.; Xu, J. Optical image encryption algorithm based on hyper-chaos and public-key cryptography. Opt. Laser Technol. 2020, 127, 106171.
[20] Ye, G.; Jiao, K.; Huang, X. Quantum logistic image encryption algorithm based on SHA-3 and RSA. Nonlinear Dyn. 2021, 104, 2807–2827.
[21] Ye, G.-D.; Wu, H.-S.; Huang, X.-L.; Tan, S.-Y. Asymmetric image encryption algorithm based on a new 3D-ILM chaotic map. Chin. Phys. B 2022, 32, 030504.
[22] Luo, Y.; Ouyang, X.; Liu, J.; Cao, L. An image encryption method based on elliptic curve elgamal encryption and chaotic systems. IEEE Access 2019, 7, 38507–38522

ISSN : 2455-9679
SJIF Impact Factor : 6.008

[23] Laiphrakpam, D.S.; Khumanthem, M.S. A robust image encryption scheme based on chaotic system and elliptic curve over finite field. Multimed. Tools Appl. 2018, 77, 8629–8652.
[24] Liu, H.; Kadir, A.; Li, Y. Asymmetric color pathological image encryption scheme based on complex hyper chaotic system. Optik 2016, 127, 5812–5819.
[25] Shakiba, A. A randomized CPA-secure asymmetric-key chaotic color image encryption scheme based on the Chebyshev mappings and one-time pad. J. King Saud Univ.-Comput. Inf. Sci. 2021, 33, 562–571
[26] Wang, J.; Wang, Q.-H.; Hu, Y. Asymmetric color image cryptosystem using detour cylindrical-diffraction and phase reservation & truncation. IEEE Access 2018, 6, 53976–53983.
[27] Zhang, Y.; Zhang, L.; Zhong, Z.; Yu, L.; Shan, M.; Zhao, Y. Hyperchaotic image encryption using phase-truncated fractional Fourier transform and DNA-level operation. Opt. Lasers Eng. 2021, 143, 106626.