Chaos Based Image Encryption Techniques: A Review

Bhavana Sharma[1], Jaspreet Singh[2]

[1]*Assistant Professor, Dept. of CSE, The North Cap University, Gurugram, Haryana, India*
[2]*Student, Dept. of CSE, The North Cap University, Gurugram, Haryana, India*

Abstract - *Digital images are a common part of multimedia communication, and in the current scenario they are frequently used to transmit data. Therefore, their security is a major concern for them. Chaos maps are good for encrypting images because they are chaotic, ergodic, and highly sensitive to initial conditions. Many of the past proposed image encryption methods relied on low-dimensional chaotic maps, which are the least secure and have limited resistance to brute force and statistical attacks. In attempt to overcome this difficulty, researchers have created a variety of high-dimensional chaotic maps. This review article gives a scientific evaluation of a variety of studies conducted over the recent years that have employed chaotic in various forms to process digital images in the encryption.*

***Key Words*: Image Encryption, Chaotic Systems, Logistics Map, Performance Metrics, Arnold Map, Cryptography**

1. INTRODUCTION

The security of images has become a big problem because we are exchanging more information through the internet [1]. To protect confidential photographs from unauthorized users, many encryption techniques have been developed in recent years [2].

Cryptography is a science and method of keeping data safe from prying eyes by storing and transferring it in an unreadable format for attackers [3]. In reality, cryptographic methods are supposed to be tough to crack. As a result, encryption is critical to the security of digital content [4]. Due to the quantity and redundancy of image data, current encryption algorithms are not suitable for encrypting image data, and hence cannot guarantee the data's security and confidentiality [5]. Over the last few decades, various approaches for encrypting image data have also been presented, with chaotic-based encryption being the most powerful and widely used due to its erratic and uncertain character [6].

1.1 OVERVIEW OF CHAOTIC MAP THEORY

For chaotic-based picture encryption, one-dimensional and multi-dimensional chaotic maps are utilised. The use of multi-Dimension chaotic maps improves the security of picture encryption by virtue of its complicated structure and the inclusion of numerous parameters, but also increases the difficulty of implementing the method [7].

Matthews employed chaotic to encrypt data for the first time in the late 1980s, while Habutsu et al. published the first chaotic block cypher algorithm in 1991. In 1998, Baptista published a chaotic encryption scheme. In addition, Friedrich stated that to achieve a high level of security, the picture encryption method should be repeated in two steps: diffusion and permutation [8]. The permutation stage is required to minimise the high correlation between adjacent pixels. Permutation methods are divided into two categories: pixel and bit level. The diffusion phase is responsible for modifying pixel values in order to develop an oscillatory behavior and avoid the attack [9].

Almost all proposals for chaotic-based picture encryption are inspired by two factors: I the potential for reduces the computational effort when compared to standard encryption; and (ii) purported security issues when classical cyphers are applied on images [10].

1.2 IMAGE ENCRYPTION USING A CHAOTIC SYSTEM

Non-chaos techniques and chaos-based or are two types of picture encryption. In chaos-based approaches, initial conditions are extremely important. If we modify something in the starting situation, the entire outcome will change [11], [12], [13], [14], [15], [16].

Healthcare, military, online communication, photo messaging applications for smart phones, multimedia systems, images used in healthcare, Tele-medicine, and government papers are just few of the applications of the encryption concept based on chaos [14].

Diffusion and Confusion are the two phases of a chaos-based encryption method. The chaos-based picture encryption technique is depicted in block diagram in Figure 1. The phase of confusion occurs when the position of pixels is scrambled without changing their value. The purpose of a diffusion phase is to alter the estimation of each pixel in the image [11], [17]. Figure 2 illustrates the connection between chaotic map theory and cryptography.

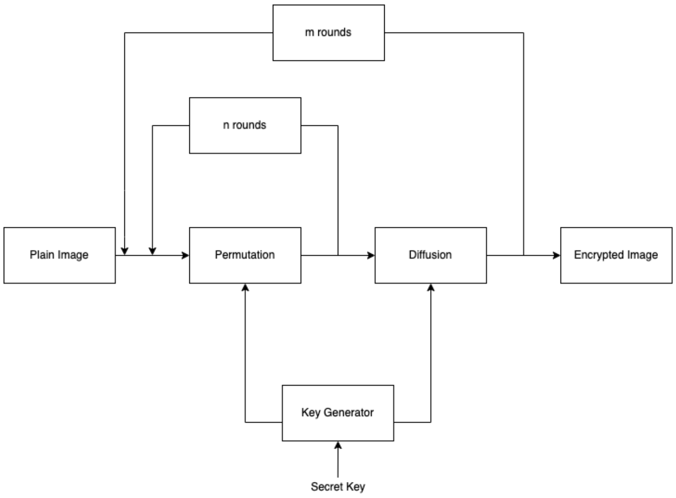

Fig -1: Chaotic Encryption Algorithms Approach

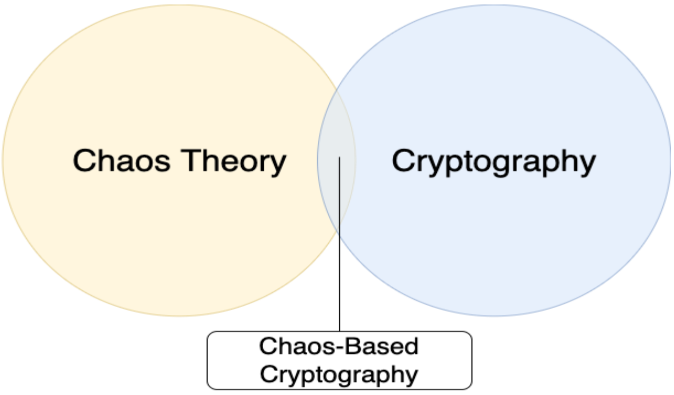

Fig 2: Chaos Based Cryptography

2. KEY SECURITY EVALUATIONS

2.1 KEY SECURITY ASSESSMENT

In both the encoding and decoding processes, a good encryption method should concentrate on the encryption key. The total number of unique keys that can be used to encrypt data is known as the key space estimate. The text pictures are sent out in the open, while the security key is sent out in secret. The security key must have a size that is difficult to estimate by brute force attackers and be sensitive to such an attack in order to be valid

2.2 EVALUATION OF DIFFERENTIAL ATTACK

The differentiated attack is a frequent and extremely successful security strategy. Two metrics that may be used to measure the resilience of image computation encoding to differential assault are the unified average change intensity (UACI) and the formally number of pixels change rate (NPCR).

Where,

$$NPCR = \frac{\sum_{i\,j} E(k,l) \times 100\%}{q \times p} \quad (1)$$

$$UACI = \frac{1}{q \times p}\left[\frac{\sum_{i\,j} |d_1(k,l) - d_2(k,l)|}{255}\right] \times 100\% \quad (2)$$

$$E(k,l) = \begin{cases} 1, \text{ when } d_1(k,l) \neq d_2(k,l) \\ 0, \text{ when } d_1(k,l) = d_2(k,l) \end{cases}$$

$d1(k,l)$ *and* $d2(k,l)$ Described as encrypted image before and after one pixel of original image is changed.

2.3 EVALUATION OF CORRELATION COEFFICIENT

An encrypted image with a constrained connection between pixel values should be produced by a precise encrypted image. Using correlation analysis to uncover correlations between the cipher's pixel values would be the most efficient technique to determine the suggested picture 's security. In a number of orientations, the pixels of an original image are always tightly connected to their neighbours. In this vein, a good picture encryption algorithm should be able to remove significant correlations between nearby pixels.

$$C_{xy} = E\left[\frac{(x-\mu_x)(y-\mu_y)}{\sigma_x \sigma_y}\right] \quad (3)$$

where E(.) is the expectation value and μ & σ are the standard deviation and mean value respectively.

2.4 HISTOGRAM EVALUATION

The histogram is a technique for determining how encrypted picture data is distributed. The histogram should be uniform, keeping in mind the fundamental purpose of surviving alone and statistical attacks, which is the goal. A histogram analysis can be used to examine the uneven distribution of pixel values in an encrypted picture. It's reasonable to believe that the pixels in an encrypted image are scattered equally, making brute force assaults to extract the plain image challenging.

3. LITERATURE REVIEW

3.1 CHAOTIC ENCRYPTION TECHNIQUE, 2014 [18]

They provide a novel way to creating the brand-new chaotic map on this examine, as well as a higher photo encryption scheme based on it. A significantly more maximal Lyapunov exponent means that this lately built chaotic map has many higher chaotic capabilities for encryption. In addition, the Arnold's Cat Map & unconventional chaotic map based totally image encryption technique has been devised and demonstrated to be solid. The security analysis & simulation out- comes that this approach not only meets the want of envision encryption, however, also offers advanced effectiveness and security, making it suitable for a wide range of programs.

3.2 CHAOTIC ENCRYPTION TECHNIQUE, 2015 [19]

An efficient picture encryption system primarily based on lookup table-based totally confusion and diffusion is proposed on this paper. In contrast to conventional chaos-primarily based block , the proposed method requires a long way much less chaotic map iteration and no measuring operation. As a result, their technique is extra efficient and has a faster encryption speed. Furthermore, their approach has ideal noise resistance and robustness towards statistics loss. All of these benefits make the proposed system ideal for actual-time stable image transmission in real-international networks.

3.3 CHAOTIC ENCRYPTION TECHNIQUE, 2016 [20]

They suggested an image encryption technique that is based on a chaotic inertial neural network & piecewise linear chaotic map(PWLCM). The data is encrypted using the chaotic signals generated by the inertial neural network. A chaotic system (a continuous system) and a chaotic map(a discrete system) are both included in the algorithm. They scrambled the image's pixel values at random before encrypting it with the outputs of an inertial chaotic neural network.

3.4 CHAOTIC ENCRYPTION TECHNIQUE, 2017 [21]

The authors of this study present a new image block encryption technique based on a number of frequently used chaotic maps. The image blocking strategy in this algorithm
and specific chaotic maps are used to implement both substitution and shuffling algorithms.

Table -1: Comparison of Different Chaotic Map Systems based on Encryption Algorithms Results in Papers

Paper	Cipher-Text Image Entropy	Image Name	NPCR	UACI	Key Space	Correlation of Encryption Image		
						H	V	D
[18]	7.9977	Lena	99.54	33.36	10^{48}	0.0063	0.0062	0.0069
[19]	7.9991	Lena	99.63	33.52	2^{193}	-0.0180	0.0035	-0.0020
[20]	7.9991	Peppers	-	-	10^{84}	-0.0007	0.0006	0.0002
[21]	7.9978	Lena	99.58	33.36	2^{231}	0.0012	0.0013	0.0020
[22]	7.9993	Lena	99.61	33.48	2^{428}	0.0013	0.0008	0.0066
[23]	7.9994	Lena	99.60	33.44	-	-0.0043	-0.0007	0.0030
[24]	7.9994	Airplane	99.62	33.90	-	0.0006	-0.0011	0.0029
[25]	7.9975	Lena	99.62	33.41	$2^{40}+2^{384}+2^{8}$	2.9903e-04	−3.4722e-05	−2.7381e-05
[26]	7.9994	Lena	99.60	33.47	2^{504}	0.0013	-0.0012	-0.0015
[27]	7.9959	Lena	99.62	33.46	2^{398}	0.0019	0.0035	0.0008
[28]	7.9915	Lena	99.60	33.45	-	0.0006	-0.0017	-0.0008
[29]	7.9994	Lena	99.62	33.49	-	0.0008	0.0006	0.0033
[30]	7.9970	Lena	99.63	30.34	2^{425}	0.0023	-0.0016	-0.0013

3.5 CHAOTIC ENCRYPTION TECHNIQUE, 2018 [22]

This study presents a new and safe image encryption strategy based on the hyper-chaotic Lorenz system and hash function. They used the traditional encryption architecture of diffusion & permutation in their scheme. The information from the original image and the first key are used to construct the initial conditions of the hyper-chaotic Lorenz system, which is used in permutation and key stream creation methods.

3.6 CHAOTIC ENCRYPTION TECHNIQUE, 2019 [23]

This study presents an image encryption technique based on the Chaotic Coupled Sine Map (CCSM), a one-dimensional chaotic map. A dynamic approach is introduced to the block- based image scrambling after the of the new chaotic map and the block size is dynamically configurable.

3.7 CHAOTIC ENCRYPTION TECHNIQUE, 2020 [24]

In this study, they presented a novel system that is less computationally intensive and more secure. A three-dimensional Lorenz chaotic map and a fractal-key shuffling mechanism form the basis of the system. The confusion -

Table -2: Review of Chaotic Maps

Paper	Title	Author	Algorithms	Features	Parameters	Research Gap
[18]	A new image alternate encryption algorithm based on chaotic map	Wang & Guo	Shuffle & Diffusion, 0,1 Sequence	Highly Secure, High Key sensitivity, High key space	Logistic Map, XOR	Differential attack can be used to defeat this strategy. An example of a well-known plaintext attack.[31]
[19]	An efficient image encryption scheme using lookup table based on confusion & diffusion	Chen, Zhang	Confusion & diffusion, Latin square, LUT based permutation.	Larger key space, higher key sensitivity	Lookup table used	Combination attacks using both chosen-plaintext and chosen-cipher attacks were utilized to break this method because of its inherent fault that the same key was used in both permutation stages as well as diffusion.[32]
[20]	Synchronization of an Inertial Neural Network With Time-Varying Delays and Its Application to Secure Communication	Shanmugam Lakshmanan et al.	S-Box, P-Box, PRNG, Shuffling. RK-4	Robust and resistant against different security attacks	PWLCM, chaotic inertial neural network.	The encryption technique is completely reliant on the secret key and has little to no reliance on awaiting plain pictures. It is possible to decrypt an encrypted image using a chosen-plaintext attack, which eliminates the necessity for a secret key.[33]
[21]	Image Block Encryption algorithm based on chaotic map	L.Liu, S.Hao. et al.	Shuffling & Substitution Algorithm	Larger Key Space, Key sensitive	Arnold Map, Baker Map	With a few chosen plain images, the Secret Key may be easily obtained. Every security metric in use is unable to verify its true security performance.[34]
[22]	A novel plaintext -related image encryption scheme using hyper-chaotic system	Zhen Li et al.	Permutation Algorithm, Hash Functions	Effective at resisting the known/selected plaintext attack, resist entropy attacks	Lorenz Map	It has two flaws, one of which may be exploited by creating a special picture and then permuting the permuted image.[35]
[23]	Digital image scrambling based on a new-dimensional coupled sine map	Behzad Irani et al.	Block-based image scrambling	Better performance, High security, Reliable & safe	Logistic Map, Sine Map	Secret keys were extracted, and the original plain image was retrieved.[36]

[24]	A novel hybrid Secure Image Encryption Based on Julia Set of Fractals & 3D Lorentz Map	Fawad Masood et al.	Confusion, Diffusion, Shuffling	Higher Security, High Sensitivity, Low peak to SNR	3D Lorenz Map, XOR	Encryption keys may be obtained using only three plain text images that have been chosen.[37]
[25]	Chaotic image encryption algorithm based on hybrid multi-objective particle swarm optimization and DNA sequence	Xingyuan Wang, Yanpei Li	Fisher-Yates shuffling, Multi-objective particle swarm optimization algorithm, SHA-384	High Key Space, High Key Sensitivity.	Logistic Map, DNA	-
[26]	Image Encryption based on Roulette Cascaded Chaotic System & Alienated Image Library	X.Wang, P.Liu	Roulette Wheel Selection, SHA-512, Scrambling Diffusion.	High Key Space, High Key Sensitivity	Logistic, Logistic-Sine, Logistic-Tent, Sine-Tent.	Very Complex.
[27]	A novel color image encryption scheme based on a new dynamic compound chaotic map & S-Box	Tahir S. Ali et al.	PRNG, S-Box, SHA-256, RSA.	High Key Space, High Key Sensitivity.	PWLCM, Tent Map.	It is based on multi-chaotic maps, which may necessitate a huge amount of memory as well as increased computing expenses.
[28]	Bit-Level Color image encryption using Logistic-Sine-Tent-Chebyshev(LSTC) Map	S.M.Basha et al.	Diffusion, Cyclic Shift.	Resistant to statistics attacks, High Key Space.	LSTC Map.	Slower Computing Speed than the Traditional Encryption Algorithms.
[29]	A Novel Chaotic Permutation-Substitution Image Encryption Scheme Based on Logistic Map and Random Substitution	Khan et al.	S-Box, AES, SHA-256	Robust against statistical attacks.	XOR, Logistic Map	Only grayscale photographs, not colour images, may be utilised with their proposed system.
[30]	RGB Image Encryption through Cellular Automata, S-Box and the Lorenz System	Wassim Alexan et al.	Cellular Automata, S-Box, PRNG	Any statistical, differential, or brute-force attacks are resistant to the suggested approach.	Lorenz, XOR	Dissipative and poor ergodicity characterize the Lorenz system utilized in the third stage, compared to conservative chaotic dynamical systems.

property has been applied to the shuffled picture, further confusing the pixels. A three-dimensional Lorenz chaotic map was used for the diffusion process, which distorted each pixel in the picture.

3.8 CHAOTIC ENCRYPTION TECHNIQUE, 2021 [25]

This study investigates a multi-objective particle swarm optimization (MOPSO), DNA encoding sequence, and one-dimensional Logistic map-based image encryption technique. The key in this research is made up of a sub-key sequence chosen via particle swarm optimization (PSO), an image hash value, and a shuffle mark bit. Using a logistic map and DNA encoding, generate random DNA mask pictures and then combine it with the DNA encoding sequence that has been block-shuffled to create an encryption system. The iterative PSO technique is based on the information entropy and correlation coefficient, and the location value of a particle reflects a position of the picture. Finally, gets the best and returns the current value of the best particle.

3.9 CHAOTIC ENCRYPTION TECHNIQUE, 2022 [26]

This research uses the roulette jump selection chaotic system and alienated image library transformation to develop an image encryption technique. The fitness of each system is determined by the algorithm using the original image. Run different chaotic systems through a fitness test to see which ones are the most fit and then use the roulette method to control their parameters in order to reduce their dynamic degradation. This study presents a transformation that operates on plain images and many pictures in the agreed image library, significantly increasing encryption security. Synchronous scrambling diffusion is used in scrambling diffusion. An image is simultaneously scrambled and diffused by a pair of row and column mapping arrays, and its pseudo-random sequence is sorted in a row and column order.

3.10 CHAOTIC ENCRYPTION TECHNIQUE, 2022 [27]

This paper presents a new technique for encrypting and colour images using the S-box and chaotic system. For this, a hybrid technique is used. The software creates encrypted versions of images based on a master key. After encrypting with the receiver's public key, the master key is delivered to him using the asymmetric technique RSA. The symmetric technique is used in encrypting and data. During the encryption phase, the created S-box by PWLCM substitutes picture pixel values, resulting in a visual confusion and diffusion. For generating random chaotic sequence values, the tent logistic system is used as a PRNG. The sequence was mixed with substituted picture pixels values and their previous values using a mixing technique. To create a noise-like effect in the encrypted image, a self-mixing technique is used on the image components.

3.11 Chaotic Encryption Technique, 2022 [28]

Based on the Logistic-Sine-Tent-Chebyshev (LSTC) map, the research presents a bit-level chaos based image encryption scheme. The image is first disassembled into its component of red, blue, and green. Each component of a picture is converted to an 8-bit binary plane. The LSTC map, XOR operation, and cyclic shifts are used to scramble two binary elements by mutual diffusion of two sequences. A chaos map is used to perform binary element confusion, which is subsequently translated into binary bit planes. The binary element is swapped and turned into another binary bit plane using the chaos map. Combining binary bit planes creates individual text image components. Finally, the encrypted image component and the text picture are joined to create the text picture.

3.12 CHAOTIC ENCRYPTION TECHNIQUE, 2022 [29]

This work offers a new chaos-based image encryption solution based on permutation and substitution a single Substitution Box to tackle challenges in current picture encryption approaches (S-Box). The recommended technique employs chaotic permutation, substitution, and the XOR operator. AES S-Box is used to obtain the lowest amount of correlation between the image pixels. In their suggested method, encryption is done in two phases. The first stage generates encryption keys from the picture using the SHA-2 256 hashing. After then, the hash is divided into multiple portions, each of which is mapped between 0 and 1, making it excellent for logistic mapping. The image pixels are permuted in columns and rows in the second stage using numbers produced using a chaotic logistic map. The logistic map's beginning population is made up of the hash values created in the first step. The XOR operation is done to the permuted picture pixels and the logistic map's integers after permutation. Following that, the picture is subjected to a replacement method. This research looks at logistic maps and employs AES and reverse S-Boxes to replace pixel values. The encryption quality worsens when a large number of less secure S-Boxes are for picture encryption.

3.12 CHAOTIC ENCRYPTION TECHNIQUE, 2022 [30]

This paper proposes an image encryption strategy to help in the solving of such a problem. The planned strategy's execution is divided into three parts. The first stage uses Rule 30 cellular automata to generate the initial encryption key. A tried-and-true S-box with a transformation, modular inverses, and permutation is used in the second step. Finally, the third stage employs a Lorenz system solution to produce the second encryption key. This three-stage method's combined impact assures that Shannon's confusion and diffusion aspects of a system are used, enhancing the security and resilience of the encrypted pictures. Combining the S-box with the PRNG from both the cellular automata and the Lorenz system as keys results in well-encrypted pictures with the needed non-linearity and complexity.

4. CONCLUSION

The chaotic image encryption method is one of the best ways to encrypt an image. In this work, different chaotic picture encryption algorithms are looked at, discussed, and assessed.

The primary purpose of this work is to give an integrated look at how the chaotic map has been used in encrypting over the last ten years, along with other techniques that we have talked about in our research based on the years and techniques that support the chaotic map. We shared our research so that other researchers could build on it by choosing the right chaotic map strategies. Because of this, we gave each academic researcher a summary of the many studies that used chaotic maps.

When we send information over a medium that isn't secure, information security becomes more and more important. A safe way to send data can be done in a number of ways. One is to encrypt the data, which is set up to be sent in a mixed way and decoded when the data is needed. The article talks about different chaotic maps that are used to encrypt pictures, as well as their pros and cons.

REFERENCES

[1] F. Kabir and J. Kaur, *Color Image Encryption for Secure Transfer over Internet: A survey*, pp. 860–863, 2017.

[2] R. Rajoriya, K. Patidar, and S. Chouhan, "A survey and analysis on color image encryption algorithms," *ACCENTS Transactions on Information Security (TIS)*, no. 3, pp. 1–5, 2018.

[3] E. Solak, "Cryptanalysis of Chaotic Ciphers," *Studies in Computational Intelligence*, vol. 354, pp. 227–256, 2011. [Online]. Available: https://doi.org/10.1007/978-3-642-20542-2_7

[4] G. Sathishkumar, K. Bhoopathy Bagan, and N. Sriraam, "Image Encryption Based On Diffusion And Multiple Chaotic Maps." *International Journal of Network Security & Its Applications*, vol. 3(2), pp. 181–194, 2011. [Online]. Available: https://doi.org/10.5121/ijnsa. 2011.3214

[5] A. Jolfaei and A. Mirghadri, "An image encryption approach using chaos and stream cipher," *Journal of Theoretical and Applied Information Technology*, vol. 19, no. 2, pp. 117–125, 2010.

[6] Hamood, M. S. S. & Rahim, O. Mohammad, and Farook, "Chaos Image Encryption Methods: A Survey Study," *Bulletin of Electrical Engineering and Informatics*, vol. 6, 2017.

[7] D. Arroyo, J. Diaz, and F. B. Rodriguez, "Cryptanalysis of a one round chaos-based Substitution Permutation Network," *Signal Processing*, vol. 93, no. 5, pp. 1358–1364, 2013. [Online]. Available: https://doi.org/10.1016/j.sigpro.2012.11.019

[8] Fathi-Vajargah, M. Behrouz, V. Kanafchian, and Alexandrov, "Image encryption based on permutation and substitution using Clifford Chaotic System and logistic map," *Journal of Computers*, vol. 13, no. 3, pp. 309– 326, 2018.

[9] P. Ping, J. Fan, Y. Mao, F. Xu, and J. Gao, "A Chaos Based Image En- cryption Scheme Using Digit-Level Permutation and Block Diffusion," *IEEE Access*, vol. 6, pp. 67 581–67 593, 2018.

[10] M. Preishuber, T. Hütter, S. Katzenbeisser, and A. Uhl, "Depreciating Motivation and Empirical Security Analysis of Chaos-based Image and Video Encryption," *IEEE Transactions on Information Forensics and Security*, pp. 2137–2150, 2018.

[11] N. F. Elabady, H. M. Abdalkader, M. I. Moussa, and S. F. Sabbeh, "Image encryption based on new one-dimensional chaotic map," in *2014 International Conference on Engineering and Technology (ICET)*, 2014, pp. 1–6. [Online]. Available: 10.1109/ICEngTechnol.2014.7016811

[12] L. Liu and S. Miao, "A new simple one-dimensional chaotic map and its application for image encryption," *Multimedia Tools and Applications*, vol. 77, 08 2018. [Online]. Available: 10.1007/s11042-017-5594-9

[13] Chun-Yan Song, Yu-Long Qiao, and Xing-Zhou Zhang, "An image encryption scheme based on new spatiotemporal chaos," *Optik - International Journal for Light and Electron Optics*, vol. 124, no. 18, pp. 3329–3334, 2013. [Online]. Available: https://doi.org/10.1016/j. ijleo.2012.11.002

[14] J. Shah and J. S. Dhobi, "REVIEW OF IMAGE ENCRYPTION AND DECRYPTION TECHNIQUES FOR 2D IMAGES," *International Journal of Engineering Technologies and Management Research*, vol. 5, no. 1,

pp. 81–84, 2018. [Online]. Available: 10.29121/ijetmr.v5.i1.2018. 49.

[15] A. H. Abdullah, R. Enayatifar, and M. Lee, "A hybrid genetic algorithm and chaotic function model for image encryption," *AEU - International Journal of Electronics and Communications*, vol. 66, no. 10, pp. 806–816, 2012. [Online]. Available: https://doi.org/10.1016/j.aeue.2012.01.015

[16] J. Fridrich, "Image encryption based on chaotic maps," in *1997 IEEE International Conference on Systems, Man, and Cybernetics. Computational Cybernetics and Simulation*, vol. 2, 1997. [Online].Available: 10.1109/ICSMC.1997.638097

[17] C. Wei-bin and Z. Xin, "Image encryption algorithm based on Henon chaotic system," in *2009 International Conference on Image Analysis and Signal Processing*, 2009, pp. 94–97. [Online]. Available: 10.1109/IASP.2009.5054653

[18] X. Zhang and Y. Cao, "A Novel Chaotic Map and an Improved Chaos- Based Image Encryption Scheme," *The Scientific World Journal*, vol. 2014, 2014. [Online]. Available: https://doi.org/10.1155/2014/713541

[19] J. Chen, Z. Zhu, and C. Fu, "An efficient image encryption scheme using lookup table-based confusion and diffusion," *Nonlinear Dyn*, vol. 81, pp. 1151–1166, 2015. [Online]. Available: 10.1007/s11071-015-2057-6

[20] S. Lakshmanan, M. Prakash, C. P. Lim, R. Rakkiyappan,

P. Balasubramaniam, and S. Nahavandi, "Synchronization of an Inertial Neural Network With Time-Varying Delays and Its Application to Secure Communication," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 29, no. 1, pp. 195–207, 2018. [Online].Available: 10.1109/TNNLS.2016.2619345

[21] L. Liu, S. Hao, J. Lin, Z. Wang, X. Hu, and S. Miao, "Image block encryption algorithm based on chaotic maps," *IET Signal Processing*, vol. 12, no. 1, pp. 22–30, 2018. [Online]. Available: https://doi.org/10.1049/iet-spr.2016.0584

[22] Z. Li, C. Peng, and L. Li, "A novel plaintext-related image encryption scheme using hyper-chaotic system," *Nonlinear Dynamics*, vol. 94, pp. 1319-1333, 2018. [Online]. Available: hhttps://doi.org/10.1007/s11071-018-4426-4

[23] B. Y. Irani, P. Ayubi, F. A. Jabalkandi, M. Y. Valandar, and M. J. Barani, "Digital image scrambling based on a new one-dimensional coupled Sine map," *Nonlinear Dyn*, vol. 97, pp. 2693–2721, 2019. [Online]. Available: https://doi.org/10.1007/s11071-019-05157-5

[24] F. Masood, J. Ahmad, S. A. Shah, S. S. Jamal, and I. Hussain, "A Novel Hybrid Secure Image Encryption Based on Julia Set of Fractals and 3D Lorenz Chaotic Map," *Entropy*, vol. 22, no. 3, 2020. [Online].Available: 10.3390/e22030274

[25] X. Wang and Y. Li, "Chaotic image encryption algorithm based on hybrid multi-objective particle swarm optimization and DNA sequence," *Optics and Lasers in Engineering*, vol. 137, p. 106393, 2021. [Online].Available: https://doi.org/10.1016/j.optlaseng.2020.106393

[26] X. Wang and P. Liu, "Image encryption based on roulette cascaded chaotic system and alienated image library," *Vis Comput*, vol. 38, pp. 763–779, 2022.

[27] T. S. Ali and R. Ali, "A novel color image encryption scheme based on a new dynamic compound chaotic map and S-box," *Multimed Tools Appl*, vol. 81, pp. 20 585–20 609, 2022. [Online]. Available: https://doi.org/10.1007/s11042-022-12268-6

[28] S. M. Basha, P. Mathivanan, and A. B. Ganesh, "Bit level color image encryption using Logistic-Sine-Tent-Chebyshev (LSTC) map," *Optik*, vol. 259, p. 168956, 2022. [Online]. Available: https://doi.org/10.1016/j.ijleo.2022.168956

[29] J. Arif, M. A. Khan, B. Ghaleb, J. Ahmad, A. Munir, U. Rashid, and A. Y. Al-Dubai, "A Novel Chaotic Permutation-Substitution Image Encryption Scheme Based on Logistic Map and Random Substitution," *IEEE Access*, vol. 10, pp. 12 966–12 982, 2022. [Online]. Available: 10.1109/ACCESS.2022.3146792

[30] W. Alexan, M. Elbeltagy, and A. Aboshousha, "RGB Image Encryption through Cellular Automata, S-Box and the Lorenz System," *Symmetry 2022*, vol. 14, pp. 443–443, 2022. [Online]. Available: https://doi.org/10.3390/sym14030443

[31] W. S. Yap, R. C. Phan, and W. C. Yau, "Cryptanalysis of a new image alternate encryption algorithm based on chaotic map," *Nonlinear Dyn*, vol. 80, pp. 1483–1491, 2015.

[32] M. Li, D. Lu, and Y. Xiang, "Cryptanalysis and improvement in a chaotic image cipher using two-round permutation and diffusion," *Nonlinear Dyn*, vol. 96, pp. 31–47, 2019.

[33] M. Ahmad, M. Z. Alam, S. Ansari, D. Lambić, H. D. AlSharari, S. M. Thampi, El-Sayed M. El-Alfy, S. Mitra, and L. Trajkovic, "Cryptanalysis of an Image

Encryption Algorithm Based on PWLCM and Inertial Delayed Neural Network," *J. Intell. Fuzzy Syst.*, vol. 34, no. 3, pp. 1323–1332, jan 2018. [Online]. Available: 10.3233/JIFS-169428

[34] Y. Ma, C. Li, and B. Ou, "Cryptanalysis of an image block encryption algorithm based on chaotic maps," *Journal of Information Security and Applications*, vol. 54, p. 102566, 2020. [Online]. Available: https://doi.org/10.1016/j.jisa.2020.102566

[35] L. Liu, Z. Zhang, and R. Chen, "Cryptanalysis and Improvement in a Plaintext-Related Image Encryption Scheme Based on Hyper Chaos," *IEEE Access*, vol. 7, pp. 126 450–126 463, 2019. [Online]. Available: 10.1109/ACCESS.2019.2938181

[36] Y. Liu, Z. Qin, and X. Liao, "Cryptanalysis and enhancement of an image encryption scheme based on a 1-D coupled Sine map," *Nonlinear Dyn*, vol. 100, pp. 2917–2931, 2020.

[37] N. Munir, M. Khan, S. S. Jamal, M. M. Hazzazi, and I. Hussain, "Cryptanalysis of hybrid secure image encryption based on Julia set fractals and three-dimensional Lorenz chaotic map," *Mathematics and Computers in Simulation*, vol. 190, pp. 826–836, 2021. [Online]. Available: https://doi.org/10.1016/j.matcom.2021.06.008