Image Encryption Algorithm Based on Chaos cryptography: Survey

1st Deshdeepak Shrivastava
Research Scholar
Jagannath University Jaipur

2nd Dr. Renu Bagoria
Professor
Jagannath University Jaipur

3rd Dr. Aditya Vidyarthi
Professor
ITM, Gwalior

***Abstract*—Given the constantly growing trend of data being shared via public networks like the Internet, data security has become a pressing issue. One possible solution to this problem is to encrypt the data. The information can be in any form, including text, graphics, sound, video, etc. It is true that the majority of modern multimedia apps rely heavily on the use of images. Traditional approaches to picture encryption like AES, DES, RSA, and others offer weak security and can easily be broken. Chaotic cryptography was used to successfully resolve this problem. Images can be encrypted using chaotic systems because of their extreme sensitivity to both beginning conditions and control parameters. A lot of work and progress have been made in the field of chaos-based picture encryption throughout the years. The goal of this work is to try a review of the many different facets and methods of design that go into image encryption.**

***Index Terms*—Image, chaotic system, logistic map, encryption**

I. Introduction

Because the transmission of data via electronic means is expanding at a rapid rate, it is becoming increasingly important to guard the data's confidentiality and prevent unauthorized access to it. The users' reputations and personal information are compromised as a result of security flaws. Text, images, audio, and video files, among other types, may be among the data that is traded. When it comes to preventing unauthorized access to confidential image data, different protection methods are employed for the various types of data that exist today. Encryption of data is therefore done for the purpose of confirming security over the internet. The study of methods that allow for secure communication despite the presence of an adversary is known as cryptography. Encryption, authentication, and the distribution of keys are just a few of the issues that are addressed by this solution. The process of encrypting images involves transforming the original picture into one that is much more difficult to decipher than the original. This provides an additional layer of protection for the images. Images are typically distinct from textual data in a number of ways. The basic concept behind image encryption is to treat a two-dimensional image as if it were a one-dimensional data stream, and then to encrypt this stream using a text-based cryptosystem. This strategy is referred to as the navel approach [1]. This strategy is suitable for text files, audio files, image files, and video files with a low bit rate that can be transmitted over a dedicated and quick channel. Unfortunately, it's possible that these encryption algorithms won't work properly with certain image file formats, such as JPEG, PNG, BMP, and others. i.e. Images can be encrypted using traditional cryptosystems, but doing so is not recommended because the size of an image is almost invariably much larger than the size of the corresponding textual data. In addition, the decrypted text should be identical to the original text, whereas for image data, it is not necessary for this requirement to be met. When an image is decrypted, it may have some slight distortion, but this is typically not a problem because of the way the human brain processes visual information.

II. Classification of chaotic system

Over the course of the previous ten years, chaotic systems have been proposed as a component of research and extensively investigated in order to develop cryptosystems for the storage of multimedia data. For example, analogue chaotic communication [2] is one of the two distinct directions that chaotic cryptography has taken, and there has been almost no interaction between the two. The most significant distinction between these two approaches is that a cypher requires a predetermined secret key in the first case, but the system itself serves as the key in the second. Cryptosystems are able to function based on the deployment of chaotic systems. cryptosystems can be divided as discrete and continous system shown in Figure 1. The following discussion will be limited to the first class of chaotic cryptosystems, which are cyphers that are based on chaotic maps. This will be done in the following section (discrete systems). The relative comparisons of various image encryption algorithms based on chaotic maps that have been discussed in the literature are outlined in table 1.

III. Literature survey

In this part of the article, we will talk about the many different methods that are currently available for encrypting and decrypting images. A New Chaotic Algorithm for Image Encryption by [9] discussed a new chaotic algorithm for image encryption. In this algorithm, the author uses Henon chaotic maps for secure image encryption in order to ensure safe data transfer. The grayscale values that are present in the image are laid out in a completely haphazard fashion. The initial value and key image are both used in this Henon chaotic map, which serves as the map's secret key. In the paper [10] authored, ”Cryptanalysis of a substitution–diffusion based image cypher using chaotic standard and logistic map," the authors used a standard map, which is a tool that is utilised in image encryption schemes. In the article [12] the topic of colour image encryption is discussed in relation to multi-chaotic systems. [13] in this research, the authors have combinedly utilised some of the unlimited folded maps, specifically 3D-Baker maps, Henon maps, and logistic maps, for the purpose of encrypting images. However, the future scope of this paper was the fact that the histogram that was plotted after the strong encryption was not distributed uniformly. In the paper [14] the authors scrambled the row and column for each pixel in the input image by utilising two 1-D discrete Chebyshev chaotic sequences.

In [15] Pixel Mapping Table (PMT) and logistic mapping are the two methods that have been utilised for the encoding process in this research work. In the beginning, PMT was utilised in order to create confusion and heighten the level of uncertainty within the initial image. After that, replacement of rows and columns was carried out. The last step of the process involved applying the logical operation XOR to a random vector that had been generated using a logistic map.

IV. METHODOLOGY

In this section, our focus will be on the processes that are employed when encrypting and decrypting images.

A. Encryption

The process of encrypting data, such as multimedia or confidential documents, in such a way that only authorized parties are able to access it is what is known as an encryption technique. Encryption can be used to secure data such as multimedia or documents. The decryption key for these files will be provided to the authorized parties by the sender, and they will be the only ones who will be able to access them. In order to encode the input image, we will be utilizing symmetric and private key encryption. Keys That Are Symmetric: Both the encryption and decryption keys are the same when using this method. In order to ensure the safety of the data transmission, both the sender and the receiver need to use the same keys. Private Keys: Messages can be encrypted using a key that is only known to the sender and the recipient of the message using a type of encryption known as private key encryption.

B. properties of chaotic system

The fact that chaos is distinguished by a large number of primary properties makes it an appealing candidate for use in the development of robust cryptosystems. It is characterized by a sensitive dependence on the initial conditions, nonlinearity, determinism, ergodicity, nonperiodicity, and the inability to be predicted [11]. Table 2 provides a concise summary of the properties of chaos.

C. Bifurcation Diagram

The use of a bifurcation diagram, which is one of the most important tools for researching the behaviour of dynamic systems, is recommended. It is an important graphical tool that can identify the system cycles, which can range from periodic to chaotic orbits depending on the control parameters of the system. It does so by plotting the control parameter of the continuous system or the discrete map against the steady state solution. The bifurcation diagram is very important because it illustrates the sudden appearance of a qualitative behaviour when a certain parameter is changed. This plot demonstrates why the bifurcation diagram is so important. This change in behaviour is known as bifurcation, and it takes place at points known as bifurcation points [12]. Because it is so easy to plot and identify the chaotic and non-chaotic regimes using this diagram, the bifurcation diagram is one of the most popular research methods for analysing dynamic systems. This is due to the fact that using this diagram requires very little effort on the part of the researcher. It also helps in identifying the period-doubling path that leads to chaos, which is another advantage. However, due to the fact that it is dependent on the sensitivity of the human eye, its exploitation is a laborious process [8].

D. Lyapunov Exponent

The Lyapunov exponent is a measure that can be used to determine how sensitive and predictable a dynamic system is to changes in the conditions under which it was initially set [15]. The average logarithmic rate of separation or convergence of two nearby points of two time series Xt and Yt that are separated by an initial distance of $\delta R0 = ||X0 - Y0||$ is how it is computed numerically. The two time series in question are Xt and Yt. Using the following equation, one can determine the value of the Lyapunov exponent:

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} ln \frac{\Delta Ri}{\Delta R0} \quad (1)$$

Here λ is a Lyapunov exponents associated with a dynamic system that has n dimensions. The presence of a positive Lyapunov exponent in a system indicates that the system is chaotic. On the other hand, the Lyapunov exponent has seen a lot of use in the context of integer-order dynamical systems, particularly those for which the equation of the system is already known. This method cannot be utilised in the examination of experimental data or a fractional-order dynamical system because the equation for either of these systems is unknown. In these kinds of situations, the Lyapunov exponent cannot be calculated without first performing a phase space reconstruction [14]. Additionally, the number of dimensions of the dynamical system has a direct correlation with the level of difficulty involved in computing the Lyapunov exponent [11]. A survey, which results are presented in Table 1, comes to the conclusion that chaos-based image encryption is the most sought-after method for securing an image. This is due to the inherent properties that chaos possesses. The authors have also demonstrated and established the effectiveness of a chaos-based cryptosystem by using performance measures such as key space analysis, key sensitivity analysis, peak signal-to-noise ratio (PSNR), and unified average change in key length. analysis of statistical attacks, and changes in net pixel count

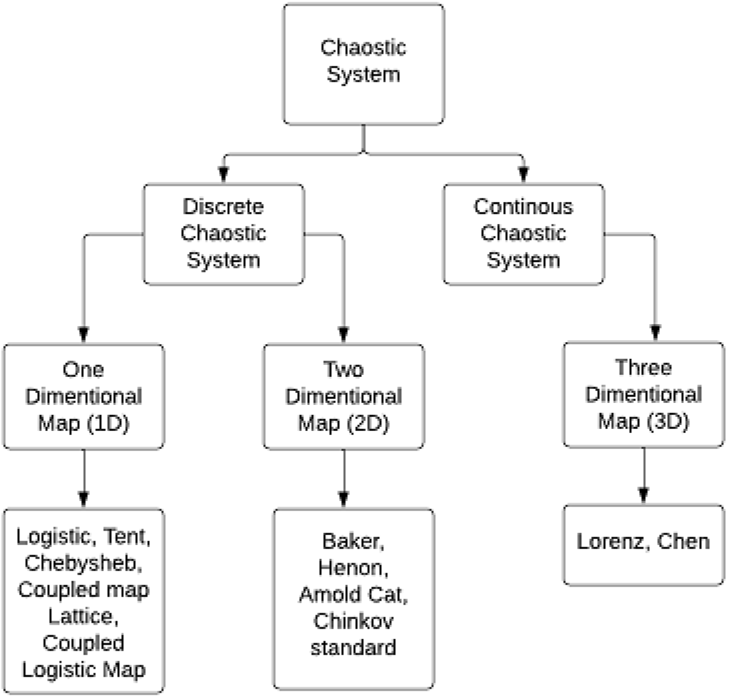
Chaostic System
Discrete Chaostic System
Continous Chaostic System
One Dimentional Map (1D)
Two Dimentional Map (2D)
Three Dimentional Map (3D)
Logistic, Tent, Chebysheb, Coupled map Lattice, Coupled Logistic Map
Baker, Henon, Amold Cat, Chinkov standard
Lorenz, Chen

Fig. 1. Types of Chaostic system

TABLE I
PROPERTIES OF CHAOTIC SYSTEM

S. No	Properties	Remarks
1	Initial condition sensitive	A relatively minor adjustment to the parameters of the starting point can result in a significant shift in the output.
2	Nonlinearity	The input and the result are not directly related to one another in any way.
3	Deterministic	Mathematical equations can be used to model and quantitatively govern the process, and the process can also be approached quantitatively, at least to some extent.
4	Unpredictable	The effect of many interactions, when added together in a particular order, results in an outcome that cannot be predicted.
5	NonPeriodic	The model generates values based on chance.

and intensity (UACI) NPCR, the information entropy, and the grey value difference (GVD).

As a result, the nonlinear will be the primary focus of this review paper. a component of the chaos-based image encryption, as well as a review of the new chaotic systems have been proposed in a number of works, including the techniques for detecting chaos that are used in the study of these systems. In addition, the work done by Muthu and his colleagues [22] was inspiring. in light of the fact that it is essential to examine all of the chaos detection techniques. The central idea behind [22] was to Investigate the dynamic tendencies exhibited by the modified logistic map, which it was asserted had an infinite capacity for key storage [9]. On the other hand, the bifurcation diagram was used to analyse this map. and the Lyapunov exponent is only applicable for a restricted control range value for the parameter of [0, 10]. The bifurcation is depicted in Figure 1. diagram as well as the Lyapunov exponent found in this range.

V. CONCLUSION

The encryption technology that is based on chaotic systems has been a topic of discussion for more than a decade due to the high hopes that it will have a wide range of applications in a variety of industries. Because of this, the development of a brand-new encryption algorithm is required in order to satisfy the challenges and prerequisites of an effective cryptosystem. There have been many different cryptosystems suggested as potential solutions to the security issues, but the majority of them are not robust enough to withstand the threats. cryptographers have come up with a variety of different attacks. The current state of the art regarding recent developments in chaotic image encryption technology as well as several important observations are presented in this article. The cryptosystems are broken down into their respective

TABLE II
SUMMARY OF LITERATURE REVIEW

S. No	Authors	Finding
1	Kumar et al. [2]	review of image encryption techniques based on chaos system Advantage and disadvantage of chaotic maps used in image encryption
2	Sharma et al.[5]	Survey on image encryption in various domain like spatial and frequency.
3	Jain et al.[4]	Comparison anlysis on the various parameter of image encryption techniques like the complexity of the system, map, key value
4	Suneja et al.[6]	confusion and diffusion method Review and compare chaotic maps
5	Movafegh et al.[7]	Image encryption based techniques review from (2005-2018
6	moatsum et al [3]	confusion-diffusion operations with secret key

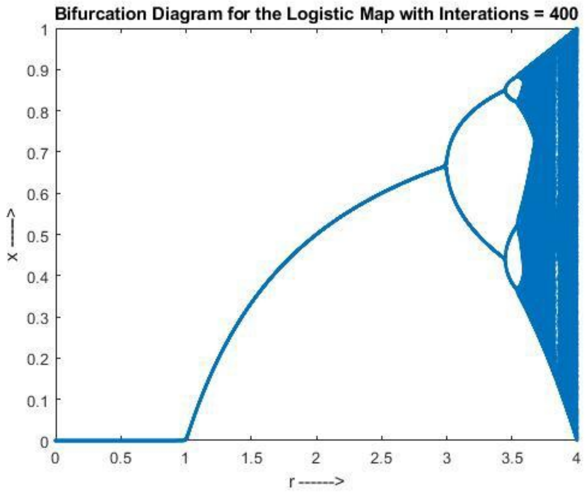

Fig. 2. Bifurcation diagram

classes so that the various qualities of the algorithms can be compared. into three categories, including chaotic maps, hyper chaotic systems, and spatiotemporal systems, respectively. The fundamental operating principle of typical algorithms from across all categories has been covered in this article to shed light on the categories' respective strengths and weaknesses. The level of security provided by a cryptosystem is directly proportional to the complexity of the chaotic system used in its design. This particular choice of It is more important to have an appropriate chaotic system than it is to have a specific design procedure for the encryption algorithm. The cypher can be easily cracked regardless of how well and securely the cryptosystem is designed; all that matters is whether or not the chaotic system was selected correctly. Because the traditional cryptographic approach provides the highest level of security but moves at a glacial pace for multimedia applications, it is possible to combine it with faster chaotic algorithms in order to make it work in real time. In addition to the security concern, other important considerations include performance and implementation costs. These considerations, along with the security concern, greatly restrict the application range in real time. Future research will need to address the challenge of developing a chaotic encryption algorithm for compressed images that, in conjunction with an authentication scheme, aims to achieve a high level of security while maintaining a high level of efficiency.

REFERENCES

1.ungju Moon, Jong-Jin Baik, Jaemyeong Mango Seo, Chaos synchronization in generalized Lorenz systems and an application to image encryption, Communications in Nonlinear Science and Numerical Simulation, Volume 96, 2021, 105708, ISSN 1007-5704, https://doi.org/10.1016/j.cnsns.2021.105708.

2. Gurpreet Kaur, Rekha Agarwal, Vinod Patidar, Color image encryption system using combination of robust chaos and chaotic order fractional Hartley transformation, Journal of King Saud University - Computer and Information Sciences, Volume 34, Issue 8, Part B, 2022, Pages 5883-5897, ISSN 1319-1578, https://doi.org/10.1016/j.jksuci.2021.03.007.

3. Moatsum Alawida, Je Sen Teh, Abid Mehmood, Abdulhadi Shoufan, Wafa' Hamdan Alshoura, A chaos-based block cipher based on an enhanced logistic map and simultaneous confusion-diffusion operations, Journal of King Saud University - Computer and Information Sciences, Volume 34, Issue 10, Part A, 2022, Pages 8136-8151, ISSN 1319-1578, https://doi.org/10.1016/j.jksuci.2022.07.025.

4. Hosny KM. Multimedia security using chaotic maps: principles and methodologies. New York: Springer; 2020.

5. Sharma M, Kowar MK. Image encryption techniques using chaotic schemes: a review. Int J Eng Sci Technol. 2010;2(6):2359–63.

6. Jain Y, Bansal R, Sharma G, et al. Image encryption schemes : A complete survey. Int J Signal Process Image Process Pattern Recognit. 2016;9(7):157–92.

7. Suneja K, Dua S, Dua M. A review of chaos based image encryption.In: Proc. 3rd Int. Conf. Comput. Methodol. Commun. ICCMC 2019; 2019. pp. 693–8.

8. Muthu JS, Murali P. Comment on “An image encryption algorithm based on modified logistic chaotic map.” Opt Int J Light Electron Opt. 2019;207:163843.

9. Zhang Y, He Y, Li P, Wang X. A new color image encryption scheme based on 2DNLCML system and genetic operations. Opt Lasers Eng. 2020;128:106040.

10. Suri S, Vijay R. A Pareto-optimal evolutionary approach of image encryption using coupled map lattice and DNA. Neural Comput Appl. 2019. https:// doi. org/ 10. 1007/ s00521-019- 04668-x.

11. Rajagopal K, Akgul A, Moroz IM, et al. A simple chaotic system with topologically different attractors. IEEE Access. 2019;7:89936–47.

12. Çavuşoğlu Ü, Panahi S, Akgül A, et al. A new chaotic system with hidden attractor and its engineering applications: analog circuit realization and image encryption. Analog Integr Circuits Signal Process. 2019;98(1):85–99.

13. Gottwald GA, Melbourne I. The 0–1 test for chaos: a review. Lect Notes Phys. 2016;915:221–47.

14. Delgado-Bonal A, Marshak A. Approximate entropy and sample entropy: A comprehensive tutorial. MDPI. 2019. https:// doi. org/ 10. 3390/ e2106 0541.

15. Mansouri A, Wang X. A novel one-dimensional sine powered chaotic map and its application in a new image encryption scheme. Inf Sci (N Y). 2020. https:// doi. org/ 10. 1016/j. ins. 2020. 02. 008.

16. Yang F, Mou J, Ma C, Cao Y. Dynamic analysis of an improper fractional-order laser chaotic system and its image encryption application. Opt Lasers Eng. 2020;129:106031.

17. Muthu JS, Paul AJ, Murali P. An efficient analyses of the behavior of one dimensional chaotic maps using 0–1 test and three state test. IEEE Recent Adv Intell Comput Syst. 2020;2020:125–30. https:// doi. org/ 10. 1109/ RAICS 51191. 2020. 93324 70.

18. Peng ZW, Yu WX, Wang JN, et al. Dynamic analysis of sevendimensional fractional-order chaotic system and its application in encrypted communication. J Ambient Intell Humaniz Comput. 2020. https:// doi. org/ 10. 1007/ s12652-020- 01896-1.