Al-Salam Journal for Engineering and Technology
Journal Homepage: http://journal.alsalam.edu.iq/index.php/ajest
e-ISSN: 2790-4822 p-ISSN: 2958-0862

Chaotic Systems in Cryptography: An Overview of Feature-Based Methods

Saba J. Hamadi[1]*, Emad A. Mohammed[1]

[1]Computer engineering technology, North technical university, Mosul, 41002, Iraq.

*Corresponding Author: Saba J. Hamadi

DOI: https://doi.org/10.55145/ajest.2025.04.01.016
Received September 2024; Accepted November 2024; Available online November 2024

ABSTRACT: The increasing growth of Information and Communication Technology has influenced rapid changes in the method of data transmission and storage, especially through the Internet. These rapid exchanges and storage of large volumes of data have also brought in newer and unexpected challenges concerning security. Consequently, the protection of sensitive information against unauthorized access has emerged as a major concern for sectors such as finance, healthcare, government, and personal data management. With time, cryptographic techniques have emerged as the cardinal solutions that can keep data safe from breaches or cyber-attacks. Cryptography offers various techniques in encoding data to prevent unauthorized access to data and protect confidentiality, integrity, and authenticity. Chaotic encryption systems are one of the innovative approaches to cryptography to which much attention has been turned by the research community over time. Chaotic encryption systems are based on the principles of chaos theory and exhibit important features that include high sensitivity to initial conditions, unpredictable behavior, and complex dynamics. These properties are particularly helpful in encryption, as they allow for complex transforms of information, were, without the proper keys, it would be highly impossible for unauthorized entities to decipher encrypted content. Chaotic encryption has especially shown promising applications in image encryption, where traditional cryptography methods often cannot work properly due to the large data size and structure of the visual information. The principle of image encryption using chaotic maps then consists in using mathematical functions with inherent features of randomness and sensitivity, which introduce extreme complexity into the encryption images, resulting in a visually unrecognizable and resistant characteristic to cryptanalysis. Some chaotic systems such as the Logistic Map, Lorenz System, and Henon Map have been used to securely encrypt an image by scrambling its pixels and changing their intensities according to initial chaotic conditions. This paper reviews the efficacy and potential of chaotic encryption systems in enhancing the security of data, and more importantly, image data, through reviewing some basic principles of chaos theory, benefits, and limitations of different chaotic maps, and discussing some recent chaotic encryption methods.

Keywords: Chaotic system, Image encryption, cryptography, chaos-based image encryption

1. INTRODUCTION

While cryptographic methods have been in place and applied to safeguard data confidentiality against its possible abuse, as all forms of data types-text, audio, video, picture-must be exchanged and stored via the Internet, where it is very easy to intercept the information being exchanged [1].

Image encryption is the best method for keeping secrecy while storing or sending photos over a network. Applications of image encryption can be seen in areas such as multimedia systems, military communications, internet communications, and medical research. Images differ from text in several ways: they have large data capacity, correlation between neighboring pixels, and the degree of sensitivity. Many techniques of encryption have been developed to deal with the issues about picture encryption. Although they have long been in use, a number of traditional encryption techniques like RSA, DES, triple DES, and AES are not practical for image encryption.

Traditional encryption algorithms like RSA, DES, and AES suffer from a number of drawbacks concerning image encryption: large data size, insufficiency in terms of visual scrambling or blurring, redundancy in data, possible fixed-

*Corresponding author: saba.jasem@ntu.edu.iq

block-size-related security threats and vulnerabilities, distortion, and loss of quality, and not suitable for high-security image applications.

There is much redundancy in digital images, and this makes the process of text more efficient. These algorithms also tend to perform slowly because they are required to encrypt a very large number of blocks. The feature now becomes one of the main drawbacks with regards to real-time applications such as live video streams or secure image-based communications.

Another problem is inadequate visual obfuscation: digital images have a lot of repetitive visual patterns or color similarities. The problem is that traditional encryption algorithms process data in regular blocks, making the visibility of at least partial patterns in an encrypted image possible. Data redundancy can expose aspects of the image's original structure, while in many cases, it results in a "leakage" of the original visual information in the encrypted version.

The security risks of fixed block sizes include reliance on fixed blocks, being vulnerable to various analytical attacks, which can cause distortion, or loss of quality; quality is difficult to preserve after decryption. High-security image applications, like medical or surveillance applications, do require very high levels of obfuscation; however, the traditional algorithms do not provide that much randomization of pixels, making images more susceptible.

Another challenge is complicated decryption, because digital images do require fast and efficient decryption, which refers to different real-time applications. Traditional methods require a great deal of processing power during the decryption phase, reducing the speed of data access or delaying the application in question.

In general, all the traditional methods mentioned above in image encryption have some serious disadvantages, including slowness, lack of sufficient visual obfuscation, reliance on fixed block processing, and failure to meet the quality and speed requirements set by real-time applications or high-definition image processing. Alternative approaches are chaotic-based encryption methods with greater randomness and dispersion, providing a better fit for secure, fast, visually lossless image encryption.

The weakness of these techniques in image encryption is more evident when the size of the image is larger [2]. Recently, chaotic systems-based cryptography has become very popular and is applied in different image encryption techniques. Chaotic systems show the behavior of pseudo randomness and possess a number of important features: unpredictable orbital growth, increased sensitivity to beginning circumstances and factors, ease of hardware and software implementation to boost the rate of encryption, etc. All this and other characteristics of chaotic systems-based cryptography are related to the most important properties of cryptography, such as confusion and diffusion [3].

2. LITERATURE OF REVIEW

In the past decade, a lot of image encryption techniques have been explored. Some of these researches are presented in the following section.

In the work of Xing-Yuan Wang et al. [4] , Chaotic system and bit cycle shift of the pixel is utilized to perform the picture encryption. They also have applied random integer value of same dimension as plain picture on cycle bit-level shift. The chaotic map was then used to obtain the key for encrypting the scrambled picture. Using different parameters, Lingfeng Liu and Suoxia Miao [5] introduced an image encryption technique based on logistic maps. Their method may strengthen resistance against the phase space reconstruction assault by randomly varying the settings. In the paper of Chanil Pak and Lilian Huang [6] , Developing a new chaotic system with two of three 1-D chaotic maps, which include the logistic map, the sine map, and the Chebyshev map, for image encryption has a Lyapunov exponent in addition to high information entropy. Based on the linear-non-linear-linear conversion structure, chaotic image encryption has achieved an improvement compared to the methods based on a linear-permutation-non-linear-diffusion structure. The authors, S. Abdulnabi and M. Sabbih [7], provide a new approach in this article to get beyond the drawbacks of earlier image encryption methods: In their method, they have used Duffing chaotic map in order to mix all the image pixels, while Cross-Chaotic map has been utilized to shuffle after the generated picture has been divided into a collection of blocks. In order to conduct pixel diffusion, they use Lagrange interpolation to construct a number of polynomial equations and ultimately get a key image employing snails of square numbers. Sura F. proposed a novel method for encrypting grayscale images [8]. Four equal-sized blocks were created out of the picture, and each block had a 90-degree clockwise rotation. The confusion was produced using a permutation sequence, while the diffusion was produced by a masking sequence that altered the pixel values in the picture. Four distinct chaotic maps-one for each block-the Cross, Ikeda, Chebyshev, and quadratic maps-have been examined in this study. Ultimately, the four encrypted blocks have been concatenated to create the cipher image. Ibtisam A. and Sarab M. proposed using a technique for constructing a cipher for colored images that connects 1D logistic and sine chaotic maps [9]. Finite accuracy error was identified by Lucas G. Nardoa and Erivelton G. [10] Thus, randomness was introduced by the Chua system, hence advocating a new approach towards image encryption in this regard. Keystream generated by the Chua system and a factor obtained from a plain picture was used. Further, to encrypt the image, the XOR operation was applied on to the keystreams. Akram Belazi and Muhammad Talha [11] merged chaotic systems, hash functions, and DNA technology to create a medical picture encryption system. In the image-encryption technique of Moatsum Alawida and Azman Samsudin[12] , In order to couple into two new chaotic systems, the Tent–Logistic–Tent and the Tent–Sine–Tent, three one-dimensional chaotic maps—the Tent, Logistic, and Sine—will be used as seed maps. The

permutation and diffusion procedures then use the two novel chaotic systems. Cong Xu and Jingru Sun suggested a bitplane matrix rotation-based picture encryption method using two hyper chaotic systems. [13] . Yujia Liu and Zhaoguo Jiang[14] accomplished optical image encryption by combining the Chen 4D hyper chaotic system with RSA with four wings. In the last step of the procedure, the RSA is used to asymmetrically encode the key and generate the corresponding public and private keys.

In this line, the authors of [15] The implementation of chaotic maps in a medical image encryption system, along with dynamic substitution boxes, is proposed as a strategy to enhance patient privacy and safeguard medical data. 10[16] presented the 2D-LTMM, a 2D Logistic-Tent modular map. Later, they present a color picture encryption technique based on 2D-LTMM, which can simultaneously encrypt three color planes of images by crossing plane permutation and non-sequential diffusion. Ali Shakiba proposed in [17] An image-encryption algorithm utilizing Chebyshev polynomials in conjunction with a chaotic pseudo-random number generator (PRNG) to emulate the functionality of a one-time pad. This algorithm features an expanded key space. Additionally, it possesses sufficient security measures to withstand chosen-plaintext attacks. Yabin Zhang and Li Zhang [18] The integration of various methods has been attempted, specifically focusing on asymmetric image encryption utilizing a hyper chaotic system, DNA-level operations, Cat map techniques, and phase-truncated fractional Fourier transform. Their method exhibits robust resistance to the two-step iterative amplitude-phase retrieval methodology.

To enhance the security of the encryption system, Yang Chen and Pan Ping [19] A new chaotic measurement matrix was developed utilizing Chebyshev mapping and logistic mapping. Then they utilized the nonrepeated scrambling and bilateral diffusion techniques to encrypt the measurement matrix. A deep learning model is combined with chaos-based image encryption, Qing Zhang and Yong Yan [20] were able to safely retrieve photos while successfully concealing the original image's content information via the use of a feature vector and ciphertext fusion approach. Huda R. Shakir et al.[21] proposes a new image encryption technique using a 4D-chaotic system and DNA computing. The algorithm consists of two phases, permuting pixel positions and performing DNA encryption operations. The method provides effective encryption performance along with elevated security levels. Hosny et al. [22] suggested encrypting the color image by combining the Fibonacci matrix with the fractional Chen hyper chaotic system. They also suggested dividing the color image into sub blocks for diffusion encryption and encrypting the image using the random number produced by the fractional Chen hyper chaotic system. Although the algorithm can withstand attacks well, it is unable to address the issue of significant correlation between the three color picture channels. Using a combination of chaotic maps-the modified Arnold cat map (ACM), the Newton leapnik dynamic system (NLDS), and the logistic Gaussian chaotic system (LOGAS)—Wadii Boulila et al. [23] have offered a hybrid technique to color image encryption. Using SHA512, two-dimensional Arnold map scrambling, NLDS encryption, and dynamic S-boxes generated by LOGAS, the Plaintext color image layers were initially watermarked. This procedure makes the system reliant on Plaintext. It is shown that the procedure is secure via many simulations and tests. M. Al-Hassani [24] proposed new approach for a secure data cryptosystem using Chaos Theory. The proposed method generates a significant quantity of unexpected probabilities, calculated as the factorial of the number of rows multiplied by the number of columns, by constructing a two-dimensional key matrix that matches the dimensions of the original image and processing the fractional components of the matrix through a designated function. For the specified control settings, the 1-Dimensional logistic chaotic map is used to create these random numbers. The permutations of double layers of rows and columns to the values of the numbers are created for a predetermined no. of steps. After that, an active solution for data encryption to every file type-inatra, audio, video, etc. Will be under an XOR operation between the key matrix and the original image.

A new color image encryption scheme has been proposed by Xiaoyuan Wang et al. [25], This system is constructed using a tri-valued colester and is based on a hyper chaotic framework. The process of encryption involves the application of permutation-diffusion and synchronization within the hyper chaotic system. The initial key is generated through the utilization of Hilbert curves, ciphertext feedback, permutation operations, and the hash value of plaintext images. Experimental investigations have demonstrated superior encryption performance and resilience against multiple forms of attacks.

Shuliang Sun [26] presented a new cryptosystem working with a 6D hyper chaotic system and random signal insertion. Starting values are obtained in the system by adding up all the plaintext pixels. Further, functions like diffusion, cycle shift, and scrambling are applied to obtain an encrypted picture. Simulation data has proved that the proposed technique, due to large key space, high sensitivity, and resistance against many kinds of attacks, is far more secure than most conventional image encryption systems.Wei Feng et al.[27] A 3D Lorenz chaotic system of fractional order and a 2D sinusoidally bound polynomial hyper-chaotic map have been proposed. The techniques described above were subsequently utilized to develop the MIEA-FCSM multi-image encryption algorithm. The inclusion of a fourth parameter in the fractional-order 3D Lorenz chaotic system enhances both security and key space. The 2D-SCPM structure is more suitable for real-world implementation due to its simplicity. Dynamic diffusion, scrambling, and chaotic random replacement effectively encrypt the fusion of a 2D pixel matrix. Heping Wen et al.[28] presented a new study focuses on picture encryption techniques while discussing the security of storing and transmitting multimedia information. It criticizes the inadequate security metrics and susceptibility to chosen-ciphertext attacks of the Bit-level Confusion and Image Encryption Algorithm (BCIEA). Through theoretical research and practical data, the authors

offer a unique attack approach that takes use of these weaknesses. With little computational and data complexity, the suggested technique is able to effectively retrieve original photos from encrypted equivalents. The results imply that cryptographic processes should be more complicated and that encryption systems should steer clear of comparable keys. G. Cao et al.[29] introduce the 2D-SCM chaotic system, gives a comparison with 2D-LSCM, and presents hyper chaotic behavior with wider space of motion. The randomness test is conducted by applying the NIST manual; the generated sequences are random with high confidence. They proposed a two-step procedure for constructing orthogonal Latin squares that efficiently facilitated the scrambling process. They introduced one more pixel transformation based on modulo 65537 and also included a 2-PM to enhance its bijective features as well as to provide integrity to the ciphertext generated. Finally, the encryption algorithm expanded the running key space from 256 to 65536, thus providing more security. The algorithm also tests its robustness in terms of resistance to differential attacks and execution speed. Finally, it concludes that the algorithm arrives at a perfect balance between security and efficiency above other methods.

3. FUNDAMENTAL PRINCIPLES OF RECENT CRYPTOGRAPHY

Cryptography and cryptanalysis are two aspects of modern cryptography. In order to prevent information from being stolen and exploited by unauthorized parties during transmission, cryptography changes data in accordance with the principles of information integrity, secrecy, and consistency. Passwords are analyzed and deciphered using cryptanalysis. Both branches are autonomous and support one another.

The terms "plaintext" and "ciphertext" refer to unencrypted and encrypted data, respectively; the conversion of plaintext to ciphertext is referred to as encryption, while the reverse conversion of ciphertext to plaintext is referred to as decryption. The encryption and decryption process is entirely managed by the key. The encryption key is used during the encryption process, while the decryption key is used during the decryption phase. Fig. 1 depicts the encryption and decryption structure. A password can be categorized as symmetric or asymmetric based on the shared use of the same key for both encryption and decryption algorithms. The picture encryption technique is categorized within the symmetric cryptosystem, attributed to its data volume and the requirement for rapid encryption and decryption speeds [30].

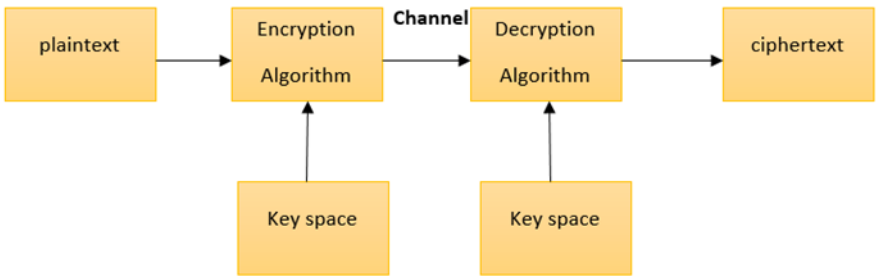

FIGURE 1. - The framework for encryption and decryption

4. CHAOS-BASED IMAGE ENCRYPTION OVERVIEW

Image data typically necessitate greater storage capacity relative to text data and exhibit significant redundancy, characterized by strong correlations among adjacent pixels. Consequently, conventional encryption algorithms do not adequately fulfill the criteria for image encryption. The application of chaos theory in image encryption represents a relatively recent development. Chaotic systems exhibit significant sensitivity to initial conditions, where minor errors can result in vastly different trajectories of motion. The trajectory, while potentially bounded under specified initial conditions, cannot be predicted over extended periods without knowledge of those initial conditions. Chaotic systems exhibit properties such as high ergodicity, determinism, and pseudo-randomness, which are advantageous for image encryption. These characteristics are shown Fig .2.

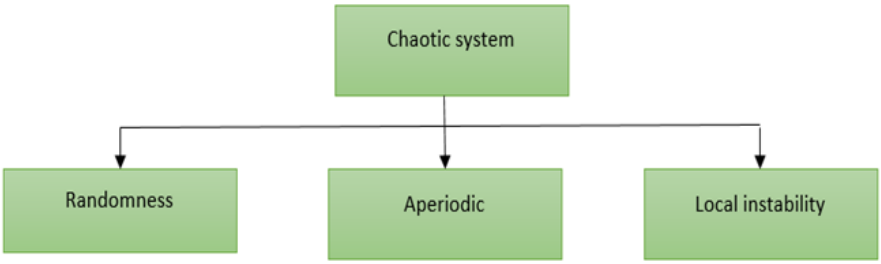

FIGURE 2. - Diagram illustrating the features of a chaotic system

Chaos-based image encryption technology can be divided into different types according to different classification methodologies. For instance, it can be classified on the basis of processing techniques of the original image. Besides, it can also be divided into two sorts: chaotic image encryption with block cipher and chaotic image encryption with stream cipher. Its encryption can be divided into two main divisions, symmetric key chaos picture encryption, and asymmetric key chaos image encryption, according to the key's properties. Chaotic systems are mathematically dimensional, ranging from one-dimensional systems with one variable to multidimensional systems with multiple variables, enhancing complexity and security. They can be linear, nonlinear, discrete, or continuous, with some using differential equations and others working in discrete time steps. They are used in encryption stages for random key generation, distortion in pixel distribution, and disturbance of pixel values. Independent chaotic systems depend on chaotic maps like logistic maps or Henon maps, while hybrid systems use traditional encryption algorithms like AES and DES for added security. Chaotic systems also have sensitivity to initial conditions, allowing for different outcomes and control of system parameters. These factors are crucial in determining the classification of chaotic systems for security and efficiency in various encryption needs [31].

Chaotic encryption schemes face challenges like complex key management, implementation difficulties, numerical accuracy, exposure to attacks, and limited key space. To overcome these, researchers can implement strong key management systems, enhance chaotic algorithms, use high-precision compute libraries, and regularly recalibrate the chaotic map. In real-time applications like live video streaming and high-speed communication networks, lightweight chaotic maps optimized for velocity and hardware-accelerated solutions can be used. Chaotic encryption lacks universally recognized standards, complicating its integration into systems. To address these limitations, researchers should advocate for standardized protocols and algorithms, and develop internal rules for bespoke implementations. Solutions include comprehensive key management, algorithm refinement, improved accuracy, hybrid encryption, increased key space, hardware acceleration, standardization, and adaptive parameter modifications.

5. AN ALGORITHM FOR PICTURE ENCRYPTION'S SECURITY ANALYSIS INDEX

Given the specificity of images, it is essential to evaluate the following elements while developing a chaotic image encryption method. [32] The assessments include key space analysis, key sensitivity analysis/plaintext sensitivity analysis, information entropy analysis, number of pixels change rate (NPCR) analysis, unified average changing intensity (UACI) analysis, histogram analysis, and correlation coefficient analysis. An efficient picture encryption algorithm must meet the above specified criteria; nevertheless, given the rapid progression of cryptographic analysis methods, these criteria just reflect the existing security assessment standards. As technology advances, more rigorous safety regulations will be implemented. Figure 3 depicts the encrypted ciphertext image, with the Lena plaintext image as an example.

FIGURE 3. - The results of encryption and decryption: (a) Original image; (b) Encrypted image; (c) Reconstructed image

Simultaneously, an overview of the five prevalent security analysis indicators is presented in the table .1.

Table 1. - Overview of prevalent security analysis methodologies indicators

Security Indicators	Special Feature
Correlation analysis of diagram of adjacent pixel	The correlation coefficients between neighboring pixels in the appropriate direction of ciphertext pictures should approximate zero
Entropy analysis	An increased information entropy in cipher text images is preferable, with an ideal value of 8.
Key space analysis	The key space in cryptography is essential for ensuring the security of the encryption system. It is necessary for the key space to reach 2^{200}.
Differential attack	Two indicators are identified: NPRC and UACI. The optimal value for NPRC is 0.9961, while the optimal value for UACI is 0.3347.
Time complexity analysis	Reduced algorithm runtimes are preferable

6. COMPARATIVE SCHEME ANALYSIS

Security analysis examines protective systems, evaluating risks, weaknesses, and susceptibility to attacks. It employs mathematical models, penetration testing, and risk assessments to evaluate the efficacy of security solutions. The objective is to augment security and ascertain preventative strategies. Table.2 shows a comparison between some of previous works in terms of security analyses.

Table 2. - will describe how the previous systems are compared

Ref	Key space	Histogram Analysis	Correlation coefficient			UACI	NPCR	PSNR	Entropy
			H	D	V				
[5]	2^{128}	Fairly uniform	0.0021	0.0033	0.0046	33.71	99.63	-	7.9995
[7]	-	Fairly uniform	-0.0091	-0.0137	0.02424	33.147	99.696	7.9992	9.7896
[8]	2^{419}	Fairly uniform	-0.000314	-0.000228	0.000697	35.4075	99.543	-	-
[9]	2^{112}	Fairly uniform	0.0004	-0.0005	0.0002	33.4975	99.616	8.6752	7.9993
[10]	2^{175}	Fairly uniform	0.00405	0.00113	0.00302	33.41	99.57	-	7.9968
[11]	2^{716}	Fairly uniform	0.0013	0.0057	-0.0049	33.4121	99.653	-	7.9974
[12]	2^{312}	Fairly uniform	−0.0017	−0.0019	−0.0084	33.50	99.62	-	7.9975
[13]	2^{544}	Fairly uniform	0.0015	−0.0006	−0.0137	33.54	99.62	7.9709	7.9975
[14]	2^{1773}	Fairly uniform	−0.0247	−0.0031	−0.0129	33.3246	99.506	-	7.9942
[17]	-	Fairly uniform	0.0111	0.0005	0.0138	50.0256	99.612	-	7.9992
[18]	-	Fairly uniform	0.0018	-0.0014	0.0003	33.46	99.59	-	7.9975
[19]	2^{300}	Fairly uniform	−0.0032	−0.0071	0.0123	33.5234	99.624	32.726	7.9972
[21]	2^{627}	Fairly uniform	0.00305	-0.00191	0.00305	33.3656	99.606	3.89162	7.9998
[22]	2^{100}	Fairly uniform	− 0.0096	− 0.0162	0.0027	33.4694	99.614	29.6366	7.9973
[23]	-	Fairly uniform	0.0005	-0.0047	0.1313	36.11	99.60	9.60	7.9980
[25]	$>2^{100}$	Fairly uniform	0.0007	0.0011	−0.0031	33.46	99.6	-	7.9895

The table provides a comparative examination of several chaotic encryption methods based on key criteria assessing encryption efficacy, unpredictability, sensitivity, and attack resistance. The key space is a crucial element in assessing the robustness of an encryption algorithm, with systems such as [8] and [13] demonstrating a significant advantage due to key spaces surpassing (22000), rendering them very resistant to brute-force assaults. Systems such as [5] and [22], which possess comparatively smaller key spaces of around (2100) may exhibit increased susceptibility to developments in cryptanalysis. The prominent method regarding key space is [14], guaranteeing resilience against exhaustive search assaults.

All systems provide "relatively uniform" histogram distributions, indicating efficient encryption. Uniform histograms conceal the inherent structure of the original picture, complicating pattern recognition for attackers. Correlation coefficients assess the unpredictability of pixel distributions in encrypted pictures, with the majority of systems indicating coefficients around zero or marginally negative values, which is optimal. The most effective methods, such as [5], provide very low correlation coefficients, indicating better encryption randomness.

The measurement of Unified Average Changing Intensity (UACI) and Number of Pixels Change Rate (NPCR) offers insights into the equilibrium between encryption and distortion. Reduced PSNR values indicate more encryption distortion, which is advantageous for safe encryption. Nevertheless, systems lacking published PSNR values prioritize encryption strength only, neglecting the quality of the reconstructed encrypted picture.

Entropy study reveals ideal randomness, since most systems exhibit remarkable performance in this parameter, regularly yielding values around 7.999. Systems such as [5] (7.9995) and [21] (7.9998) attain near-optimal randomization, guaranteeing minimum statistical information loss.

In conclusion, whereas the majority of chaotic encryption systems excel in the assessed metrics, disparities in key space, correlation coefficients, and UACI values underscore differing degrees of resilience and efficacy. Future improvements should concentrate on expanding key space, improving entropy, and balancing encryption robustness with computing performance for practical applications.

7. CONCLUSION

It has evaluated several chaos-based image encryption techniques from 2016 to 2024.The security of digital images is crucial, especially when sent over an unsecured network.

A thorough examination of various encryption schemes is necessary to guarantee security efficacy and improve the effectiveness of the encryption methods. This article summarizes current research on picture encryption methods using chaotic systems. The amalgamation of chaotic systems, DNA encoding, S-boxes, machine learning algorithms, and intricate mathematical models offers a feasible resolution to the issue of picture security, possessing considerable importance for both scholarly inquiry and practical implementation. In conclusion, the methodologies used in this work for real-time picture encryption are all beneficial. Each scheme has a distinct methodology that makes it suitable for various applications. Given the continual emergence of new encryption technologies, classical encryption, characterized by its speed and safety, will consistently maintain a high level of security. Recent picture encryption approaches improve security by providing a framework that makes the encryption algorithms more intricate and sophisticated than a chaotic approach. All innovations include advantages and disadvantages, which is why new technologies have been created.

Future research should not only conduct comprehensive investigations into image information security but also explore emerging security challenges associated with advancements in network and information technologies.

FUNDING

None

ACKNOWLEDGEMENT

The authors extend their appreciation to the Computer Technology Engineering Department of the Technical Engineering College of Mosul, North Technical University, for their significant collaboration in executing this work. The authors express gratitude to the anonymous reviewers for their insightful feedback.

CONFLICTS OF INTEREST

The authors declare no conflict of interest

REFERENCE

[1] P. R. Sankpal and P. A. Vijaya, "Image encryption using chaotic maps : A survey," Proc. - 2014 5th Int. Conf. Signal Image Process. ICSIP 2014, pp. 102–107, 2014, doi: 10.1109/ICSIP.2014.80.

[2] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurc. Chaos*, vol. 16, no. 8, pp. 2129–2151, 2006, doi: 10.1142/S0218127406015970.

[3] C. Li, G. Luo, K. Qin, and C. Li, "Chaotic image encryption schemes: A review," in *Proc. Int. Conf. EAME*, vol. 86, no. EAME, pp. 261–263, 2017, doi: 10.2991/eame-17.2017.61.

[4] X. Y. Wang, S. X. Gu, and Y. Q. Zhang, "Novel image encryption algorithm based on cycle shift and chaotic system," *Opt. Lasers Eng.*, vol. 68, pp. 126–134, 2015, doi: 10.1016/j.optlaseng.2014.12.025.

[5] L. Liu and S. Miao, "A new image encryption algorithm based on logistic chaotic map with varying parameter," *Springerplus*, vol. 5, no. 1, pp. 1–12, 2016, doi: 10.1186/s40064-016-1959-1.

[6] C. Pak and L. Huang, "A new color image encryption using combination of the 1D chaotic map," *Signal Processing*, vol. 138, pp. 129–137, 2017, doi: 10.1016/j.sigpro.2017.03.011.

[7] S. A. Thajeel and M. S. H. Al-Tamimi, "An improve image encryption algorithm based on multi-level of chaotic maps and Lagrange interpolation," *Iraqi J. Sci.*, vol. 59, no. 1A, pp. 179–188, 2018, doi: 10.24996/IJS.2018.59.1A.19.

[8] S. F. Yousif, "Grayscale image confusion and diffusion based on multiple chaotic maps," *Proc. 1st Int. Sci. Conf. Eng. Sci. - 3rd Sci. Conf. Eng. Sci. ISCES 2018*, pp. 114–119, 2018, doi: 10.1109/ISCES.2018.8340538.

[9] I. A. Taqi and S. M. Hameed, "A new color image encryption based on multi-chaotic maps," *Iraqi J. Sci.*, vol. 59, no. 4, pp. 2117–2127, 2018, doi: 10.24996/IJS.2018.59.4B.17.

[10] L. G. Nardo, E. G. Nepomuceno, J. Arias-Garcia, and D. N. Butusov, "Image encryption using finite-precision error," *Chaos, Solitons and Fractals*, vol. 123, pp. 69–78, 2019, doi: 10.1016/j.chaos.2019.03.026.

[11] A. Belazi, M. Talha, S. Kharbech, and W. Xiang, "Novel medical image encryption scheme based on chaos and DNA encoding," *IEEE Access*, vol. 7, pp. 36667–36681, 2019, doi: 10.1109/ACCESS.2019.2906292.

[12] M. Alawida, A. Samsudin, J. S. Teh, and R. S. Alkhawaldeh, "A new hybrid digital chaotic system with applications in image encryption," *Signal Processing*, vol. 160, pp. 45–58, 2019, doi: 10.1016/j.sigpro.2019.02.016.

[13] C. Xu, J. Sun, and C. Wang, "A novel image encryption algorithm based on bit-plane matrix rotation and hyper-chaotic systems," *Multimed. Tools Appl.*, vol. 79, no. 9–10, pp. 5573–5593, 2020, doi: 10.1007/s11042-019-08273-x.

[14] Y. Liu, Z. Jiang, X. Xu, F. Zhang, and J. Xu, "Optical image encryption algorithm based on hyper-chaos and public-key cryptography," *Opt. Laser Technol.*, vol. 127, p. 106171, 2020, doi: 10.1016/j.optlastec.2020.106171.

[15] S. Ibrahim *et al.*, "Framework for efficient medical image encryption using dynamic S-boxes and chaotic maps," *IEEE Access*, vol. 8, pp. 160433–160449, 2020, doi: 10.1109/ACCESS.2020.3020746.

[16] Z. Hua, Z. Zhu, S. Yi, Z. Zhang, and H. Huang, "Cross-plane colour image encryption using a two-dimensional logistic tent modular map," *Inf. Sci.*, vol. 546, pp. 1063–1083, 2021, doi: 10.1016/j.ins.2020.09.032.

[17] A. Shakiba, "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.*, vol. 33, no. 5, pp. 562–571, 2021, doi: 10.1016/j.jksuci.2019.03.003.

[18] Y. Zhang, L. Zhang, Z. Zhong, L. Yu, M. Shan, and Y. Zhao, "Hyper chaotic image encryption using phase-truncated fractional Fourier transform and DNA-level operation," *Opt. Lasers Eng.*, vol. 143, p. 106626, 2021, doi: 10.1016/j.optlaseng.2021.106626.

[19] C. Yang, P. Pan, and Q. Ding, "Image encryption scheme based on mixed chaotic Bernoulli measurement matrix block compressive sensing," *Entropy*, vol. 24, no. 2, 2022, doi: 10.3390/e24020273.

[20] Q. Zhang, Y. Yan, Y. Lin, and Y. Li, "Image security retrieval based on chaotic algorithm and deep learning," *IEEE Access*, vol. 10, pp. 67210–67218, 2022, doi: 10.1109/ACCESS.2022.3185421.

[21] H. R. Shakir, S. A. A. Mehdi, and A. A. Hattab, "Chaotic-DNA system for efficient image encryption," *Bull. Electr. Eng. Informatics*, vol. 11, no. 5, pp. 2645–2656, 2022, doi: 10.11591/eei.v11i5.3886.

[22] K. M. Hosny, S. T. Kamal, and M. M. Darwish, "Novel encryption for color images using fractional-order hyper chaotic system," *J. Ambient Intell. Humaniz. Comput.*, vol. 13, no. 2, pp. 973–988, 2022, doi: 10.1007/s12652-021-03675-y.

[23] F. Masood *et al.*, "A novel image encryption scheme based on Arnold cat map, Newton-Leipnik system and logistic Gaussian map," *Multimed. Tools Appl.*, vol. 81, no. 21, pp. 30931–30959, 2022, doi: 10.1007/s11042-022-12844-w.

[24] M. D. Al-Hassani, "A novel technique for secure data cryptosystem based on chaotic key image generation," *Baghdad Sci. J.*, vol. 19, no. 4, pp. 905–913, 2022, doi: 10.21123/bsj.2022.19.4.0905.

[25] X. Wang, X. Zhang, M. Gao, Y. Tian, and C. Wang, "A color image encryption algorithm based on hash table, Hilbert curve and hyper-chaotic synchronization," 2023.
[26] S. Sun, "A new image encryption scheme based on 6D hyper chaotic system and random signal insertion," *IEEE Access*, vol. 11, pp. 66009–66016, 2023, doi: 10.1109/ACCESS.2023.3290915.
[27] W. Feng *et al.*, "Exploiting newly designed fractional-order 3D Lorenz chaotic system and 2D discrete polynomial hyper-chaotic map for high-performance multi-image encryption," pp. 1–30, 2023.
[28] H. Wen, Y. Lin, and Z. Feng, "Cryptanalyzing a bit-level image encryption algorithm based on chaotic maps," *Eng. Sci. Technol. Int. J.*, vol. 51, p. 101634, 2024, doi: 10.1016/j.jestch.2024.101634.
[29] G. Cao, Y. Tao, X. Liu, and T. Zhang, "Image encryption based on a coined chaotic system and high-intensity encryption primitives," *IEEE Access*, vol. 12, pp. 92043–92061, 2024, doi: 10.1109/ACCESS.2024.3423691.
[30] J.-P. Aumasson, *Serious Cryptography: A Practical Introduction to Modern Encryption*. 2017. [Online]. Available: http://www.mypetskunk.com/uploads/1/0/6/1/106105481/seriouscrytography_ebook.pdf
[31] A. Fernández-Díaz, "Overview and perspectives of chaos theory and its applications in economics," *Mathematics*, vol. 12, no. 1, 2024, doi: 10.3390/math12010092.
[32] G. Veena and M. Ramakrishna, "A survey on image encryption using chaos-based techniques," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 1, pp. 379–384, 2021, doi: 10.14569/IJACSA.2021.0120145.