A Comprehensive Security and Performance Analysis of Chaotic-Based Hybrid Image Encryption Algorithms

P. Sivakumar(✉), A. Kalyani, V. Thanuja, G. Nohitha, and S. L. Sai

Sasi Institute of Technology and Engineering, Tadepalligudem, India
sivakumarperumal@sasi.ac.in

Abstract. The susceptibility of digital image communication is a crucial issue in the domain of digital transfer. The image encryption literature has presented numerous cryptosystems to enhance communication security. Image encryption is a widely recognized mechanism employed to uphold the confidentiality of images across a dependable and unrestricted public medium. Recent advancements in image encryption algorithms have utilized various methodologies, including symmetric, asymmetric, chaotic, and spatiotemporal chaos. This scholarly article presents an overview of the diverse categories of image encryption algorithms and their applications. It effectively synthesizes the contributions made by the examined methodologies and compares them across a range of technical perspectives. Further, it outlines both the researcher's and developer's perspectives on the current challenges in these as well as the existing gaps in these domains. This summary provides a concise overview of image encryption requirements, image characteristics, and common parameters used to analyze the effectiveness of encryption algorithms. The article delves into the limitations of current image encryption algorithms and outlines Prospective avenues for research and developmental trends in chaotic systems-based image encryption.

Keywords: Image encryption · Cryptography · Symmetric · Asymmetric · Chaos-based techniques

1 Introduction

In cases where machine learning algorithms are used, privacy issues can arise when collecting image datasets, especially for surveillance applications. Image encryption is a methodology utilized to safeguard the secrecy of sensitive pictures, including medical, military, and personal images. A scheme for image encryption that is learnable can encrypt pictures that furnishes them incomprehensible to humans. However, the network can be trained using these encrypted images, thus enabling privacy protection. Image encryption is a methodology utilized to safeguard sensitive images, including medical, military, and personal images.

P. Pareek et al. (Eds.): IC4S 2024, LNICST 599, pp. 191–206, 2025.
https://doi.org/10.1007/978-3-031-77081-4_16

Several traditional algorithms for image encryption formerly been used for secure image communication. Traditional algorithms like AES, DES, Blowfish, and RSA are widely used in data encryption. However, some of these algorithms may be vulnerable to side-channel attacks, which exploit unintended information leakages. Blowfish, a traditional encryption algorithm, can be computationally inefficient and may require multiple coding rounds, potentially wasting device resources. The computational workload on decoders can be increased by the demands of blowfish encryption, which involves complex numerical operations such as duplication, exchange, and turning to generate keys. This algorithm might not provide the same degree of protection as more sophisticated encryption techniques. The Blowfish algorithm may not be suitable for applications that demand high levels of security against advanced attacks [1, 2]. Other than the data size AES is found to hide all details regarding the original image, which is seen as a limitation in certain applications where additional image information needs to be preserved. One of the disadvantages regarding data security and privacy is that it can restore the same image file after encryption and decryption [3]. Later AES with a combination of Chaotic systems is introduced which makes use of an Arnold chaos sequence for key generation and adds a layer of randomness and adding intricacy to the encryption procedure, increasing its defence against attacks [4].

DES does not provide built-in support for data integrity or authentication, which are important aspects of secure communication. The rapidity of comprehensive key searches against DES after the initiation of 1990 caused apprehension among DES clients. However, clients were disinclined to replace DES due to the substantial time and financial resources required to modify cryptographic algorithms that are widely adopted and integrated into extensive security systems. The practical strategy was to modify how DES is used rather than altogether abandon it. This prompted the creation of modified versions of DES known as Triple DES (also known as 3DES occasionally) [5].

A new triple-image encryption scheme [6] was introduced, utilizing chaos, S-box, and image compressing. It combines three plain images with a stochastic matrix system to construct a new image and then performs pixel scrambling and diffusion operations to obtain a cipher image. The stochastic matrix adds dynamicity to cipher images, ensuring they remain distinct even with identical ordinary images and secret keys. The proposed model has been proven to effectively resilient to general types of attacks through experimental results and simulation analysis. Decrypted images can exhibit significant distortions when the compression rate is less than 0.5. Small variations in images can lead to varying observation matrices, necessitating the transmission of extreme values for decryption. The identification of a decrypted image becomes challenging when a portion of the encrypted image information is vanished during transmission.

The new scheme employs DNA strand level scrambling [7] and a chaotic system. Random data is manipulated to produce arbitrary numbers for key image generation and DNA encoding. The swapping of single image strands and performing an XOR operation has to be performed in between the swapped image and the DNA-encoded key image is used to analyze diffusion effects. The DNA-encoded pixels are decoded into decimal form using area of arbitrary numbers. DNA-based encryption is primarily a theoretical concept and is not commonly used in practice due to the significant challenges and limitations.

Chaos-based encryption algorithms [8] are attracting notice due to their responsiveness to initial conditions, randomness, and certainty. Experts have developed effective image encryption algorithmic rules based on chaos, with conservative chaotic systems providing higher protection and reliability compared to dissipative chaotic systems. The difference types of Convolutional Neural Networks are majorly used in computer vision and image processing tasks like image reconstruction and classification.

This survey aims to deduce performance analysis and security of different image encryption schemes in comparison with chaotic systems.

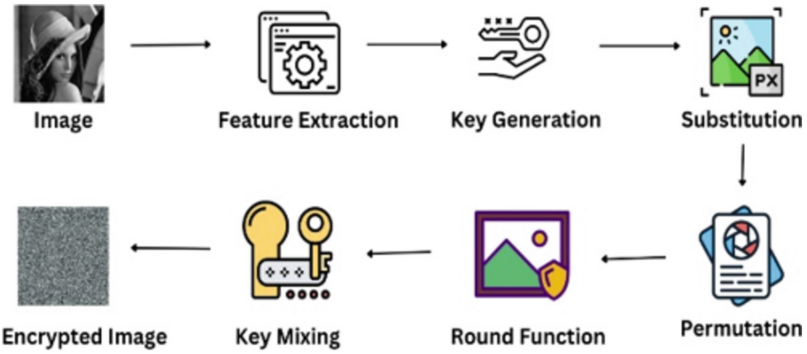

Fig. 1. General architecture of Image Encryption approach.

Figure 1 describes the steps involved in encrypting an image, several steps are typically involved, beginning with the extraction of features from the image data. These features could encompass various characteristics such as pixel values or colour histograms. Following feature extraction, a cryptographic key is generated to serve as the foundation for encryption. This key should be sufficiently random and lengthy to ensure robust security. Subsequently, a substitution process takes place, wherein the extracted features are replaced with other values based on the encryption key. Additionally, permutation rearranges the order of features in the image data, further complicating the encryption. Introducing a round-off function obscures the original values, adding another layer of intricacy to the process of encryption. Key mixing integrates the encryption key with the encrypted image data, ensuring that decryption is only feasible with the accurate key. Finally, encryption is performed using the modified image data and encryption key, effectively scrambling the image in a manner that can only be reversed through decryption. These steps collectively contribute to safeguarding the image data from unauthorized access or tampering.

Section 2 is about the Background study Sect. 3 speaks about related work, Sect. 4 is brief about the analysis and discussion of Sect. 3, Sect. 5 addresses the challenges involved in encrypting an image and ultimately Sect. 6 provides the conclusion of the paper.

2 Background Study

Image encryption is an efficacious technique to communicate classified information, and it continues to captivate the attention of researchers as the usage of images in digital communication has witnessed a phenomenal surge. The ensuing are some salient points to consider regarding image encryption: The objective of encrypting images is to heighten their security and preserve their confidentiality. Encryption is implemented to boost data security and enhance image security. As a result, the encrypted image exhibits an imperviousness to any conceivable form of cryptanalysis. Image encryption is an efficacious technique to communicate confidential information. Image encryption continues to entice researchers as the usage of images in digital communication has witnessed a phenomenal surge.

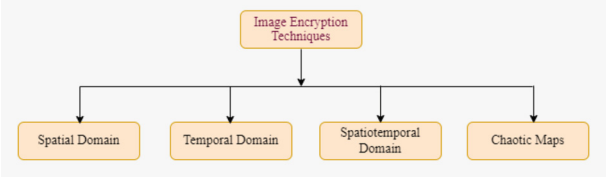

Fig. 2. Classification of Image Encryption Techniques

Figure 2 gives a brief explanation of various image encryption techniques. Multiple techniques have been devised to encrypt images, including classical and contemporary techniques, spatial, temporal, and spatiotemporal domains, and chaotic maps. Spatial image encryption techniques involve directly manipulating the pixel values of images in the spatial domain to encrypt them. Temporal image encryption techniques are methods used to encrypt images in the time domain, which involves manipulating the sequence of images over time.

3 Related Work

This section discusses the methodology involved in different image encryption algorithms and the advantages and disadvantages of them.

Vandana Rathore *et al.* [9] proposed an image encryption technique with the help of chaotic Henon maps, edge maps, and binate bit plane decomposition to generate a cipher image. The developed scheme is designed in three major phases: Key-Generation, Encryption, and Decryption. Experimental analysis and simulation are conducted to assess the security and robustness of encrypted images, demonstrating their sensitivity to various attacks. However, there are some disadvantages like the sensitivity dependence to seed values of chaotic maps can be a disadvantage as it may affect the privacy of the encryption method. The use of edge detection filters and binary bit plane decomposition for confusion may introduce noise or artifacts in the enciphered image, potentially affecting the standards of the decrypted image.

Zhongyun Hua *et al*. developed a chaotic system to improve image encryption algorithms by addressing the limitations of existing maps and algorithmic structures, focusing on a wide, continuous range. The authors created a 2D-LTMM map to overcome chaotic map limitations using the LTMM-CIEA algorithm to simultaneously encrypt three-color images. The paper does not provide any comparative analysis or evaluation of the LTMM-CIEA algorithm against other image encryption algorithms [10–13].

A new form of encryption that utilizes keys extracted from DNA and plaintext images was introduced by Jan Sher Khan et al., resulting in a chaotic visual selection. However, the paper does not explicitly mention a specific challenge that the authors were trying to solve. The proposed scheme uses random DNA sequences and plaintext images for chaotic visual selective encryption. It uses three single-dimension chaotic maps to increase key space, introduce diffusion in plain images, and break connections among adjacent pixels through row and column jumbling. However, it requires more time than traditional methods [14].

Ahmad Pourjabhar Kari et al. tackled the challenge of creating a invulnerable image encryption scheme using hybrid chaotic maps. The scheme employed confusion and diffusion phases for pixel scrambling, with confusion using Arnold's cat map and diffusion using the Sine map, and Tent map, Logistic map in combination. The diffusion phase efficiency is enhanced through exclusive OR, exchange, and transform operations, providing a dual layer of security however, it has drawbacks such as high computation costs and implementation difficulties [15–18].

Muhammad Akram *et al*. developed a highly effective image encryption technique based on chaos. They used the imitating jigsaw method to address the challenge of achieving both security and speed in image encryption. The technique includes three stages: preprocessing, encryption, and postprocessing. During preprocessing, the actual image is partitioned into blocks and subjected to random rotation and shifting with the help of control sequences furnished by the hyperchaotic Lorenz system. The preprocessing stage is vulnerable to differential attacks, while the encryption stage divides and encrypts the pre-processed image using control sequences and key blocks. In the post-processing phase, the encrypted image is split into smaller blocks and subjected to random rotation and shifting again using control sequences associated with the encrypted image and keys. This enhances the diffusion properties [19].

The challenge solved by Sara T. Kamal et al. [20] was the need for a high level of protection for medical images transmitted through the network to prevent unauthorized usage and potentially severe problems. The paper introduces a new encryption algorithm for securing grey and color medical images transmitted via a network, utilizing image dividing, zigzag pattern scrambling, rotation, random permutation, and diffusion. The introduced approach is evaluated for security using various analysis techniques and time complexity. The proposed algorithm outperforms existing encryption methods in achieving high-performance security levels for successfully encrypting medical images.

A novel algorithm for triple-image encryption and concealing algorithm for big data, integrating 2D chaotic system, compressive sensing, and 3D discrete cosine transform offered by Wang *et al*. The algorithm enhances encryption efficiency by encrypting and embedding multiple grayscale images into a single-color carrier image. The algorithm uses 2D wavelet transform to represent three grayscale images, scrambles them using

index sort and 3D zigzag scrambling, and compresses them into an image carrier in color using 3D DCT. While it offers visual security, robustness, decryption quality, and operating efficiency, it may not be suitable for scenarios requiring multiple images [21–27].

Yannick Abanda et al. [28] developed an image encryption technique, joining Hartley and Duffing chaotic oscillators to create an optimized map. The map is evaluated for chaos using a novel nonlinear time series analysis method. The encrypted image is constructed by combining the optimized map with a mathematical function designed by the authors. The proposed cryptosystem, tested on pictures like Barbara, Lena, Man, and Mandrill, demonstrated satisfactory performance, but no further analysis or evaluation of its weaknesses or vulnerabilities is provided.

A lightweight image encryption algorithm that reduces time and memory, using Arnold and logistic maps to decrease the correlation coefficient between adjoining pixels, a crucial parameter for an ideal system [29]. The quality and integrity of the encrypted image may be affected by this. However, it might not provide the same degree of security as complex encryption techniques like RSA, AES, and DES.

Ruifeng Han et al. [30] developed an algorithm to maintain digital image security in IoT applications. The algorithm aims to achieve a high unique average changing intensity (UACI $>$ 30.96%) and have only a single pixel variation from the actual image, a challenge in most of the image encryption algorithms. The algorithm mitigates encrypted images' vulnerability to plaintext and known-plaintext attacks, improving existing algorithms' functionality while preserving their benefits.

Jiangjian Xu et al. [31] introduced a new color image encryption algorithmic technique that reduces complexity and operation count by integrating bit-plane and chaotic systems. The algorithm extracts an RGB image's three channels, represents gray values as Eight-bit binary digits, swaps the gray values of the greater and lower four bits, and randomizes the position of each four-bit binary digit using a logistic chaotic sequence. The transformed image is scrambled and shuffled using the Chen chaos sequence. The enciphered image is transformed into a decimal number and combined to generate an encrypted color image.

The RC5 encryption algorithm faced limitations in terms of data collection and the use of only one function (XOR) during the encryption process. The paper tackled challenges by developing the RC5 algorithm and introducing a new security level using two keys with four states instead of the traditional two states. This development increases the security of the algorithm against hacking methods [32].

Zhiqiang Cheng et al. [33] introduced a Double-Encrypted face image encryption model, focusing on the security of face information in the context of the openness of the Internet. The cryptosystem uses a two-round encryption process, with the first encrypting they identify the face image and the second encrypting the entire image. This method, which combines scrambling and diffusion techniques, increases the difficulty of unauthorized access for attackers.

Yanqi Zhou et al. [34] provided an image encryption approach that uses an optimization algorithm inspired by the artificial bee colony algorithm and chaotic bit-plane decomposition. The SHA-256 hash algorithm calculates the hash value of a plaintext

picture, which serves as the beginning value for the fractional Lorenz hyperchaotic system. The image is then scrambled and split into four equal-sized sub-images, and the SHA-256 hash technique determines the initial value for the Sine-Tent-Logistic chaotic system. The resulting chaotic sequence replaces the image's pixel values. The artificial bee colony algorithm's fitness function is determined by ciphertext image information entropy, and its experimental simulation and security analysis demonstrate its excellent encryption effectiveness and resistance to general attacks.

The paper [35] presented a novel self-adaptive encryption scheme for quantum images, mitigating the quantum threat to traditional cryptographic methods. It employs a unique PRNG comprising a chaotic-based hash function and a Tent-Chebyshev chaotic map multiplication for enhanced randomness and key space. The PRNG extracts its seed from input images, bolstering resistance to chosen and known-plaintext attacks. Encryption involves two rounds of operations utilizing CNOT, Toffoli, and Swap quantum gates, each driven by a PRNG-generated pseudorandom sequence. The scheme boasts lower time complexity compared to counterparts and demonstrates robustness and efficiency in experiments. It innovates with its PRNG design, self-adaptive nature, and the integration of scrambling and XOR diffusion in encryption. Security analysis confirms its superior security and lower complexity relative to recent schemes, while statistical analysis evaluates its resistance to attacks. Key metrics include histogram, correlation coefficients, information entropy, UACI, and NPCR, reinforcing its efficacy against adversarial threats.

A unique image encryption approach created by Jameel Arif et al. [36] relies on chaos, permutation, and substitution. The proposed method uses a single Substitution Box to overcome challenges in current image encryption techniques. It has been rigorously tested and compared with advanced encryption algorithms, proving highly resistant to common statistical attacks and plaintext attacks, demonstrating remarkable sensitivity to these attacks.

Xinyu Gao *et al.* addressed the challenge of efficiently encrypting and transmitting multiple images. The proposed encryption algorithm combines different grayscale images into a single-color image through various channels and scrambles and diffuses the image for enhanced security. The encryption operations are assisted by the fractional hyperchaotic system, which provides pixel confusion and diffusion [37].

A new image encryption algorithm suggested by Alrubaie et al. combines dynamic DNA sequence encryption with a chaotic 2D Logistic Map for reliable decryption and encryption. The paper does not explicitly mention a specific challenge that the authors were trying to solve, but it can be inferred that they were trying to enhance the confidentiality and reliability of encrypted images using this new approach [38].

From this context, it can be understood that the single image encryption algorithm cannot withstand the attacks in this era but in combination with chaotic systems make them resilient.

4 Analysis and Discussions

Research papers have evaluated that using criteria like encryption and decryption time, entropy, loss in intensity, PSNR, NPCR, and UACI, research publications have assessed the security and efficacy of several picture encryption techniques. Table 1 presents the comparison of these metrics among different algorithms.

Table 1. Analysis of Common Metrics using Lena Image.

Authors	Methodology	NPCR (%)	UACI (%)
Rathore *et al.* [9]	Bit-Plane Decomposition	99.5179	33.3461
Khan *et al.* [14]	Visually Selective Image Encryption	90.1978	30.0263
Hua *et al.* [10]	2D Logistic, Sine-Coupling map	99.5519	32.8111
Pourjabbar *et al.* [19]	Chen Logistic Hybrid chaotic map	99.7298	33.4810
Akraam *et al.* [23]	Multiple Chaotic maps	99.6460	33.4271
Wang *et al.* [27]	Triple Image Encryption	99.6292	-
Abanda *et al.* [28]	Permutation Large slope entropy	99.5771	35.082
Ferdush *et al.* [29]	Arnold and logistic chaotic maps	99.53	26.51
Xu *et al.* [30]	Bit-Plane Chen Chaotic System	99.6136	33.4783
Jamil *et al.* [31]	Bit-plane Chen Chaotic System	99.6192	-

4.1 NPCR

NPCR is the absolute number of pixel changes between any two images, typically the actual image and the encrypted image. It is used to analyze the strength of image encryption algorithms. The formula for computing NPCR is:

$$NPCR = \frac{1}{NXM} \sum_{i=1}^{N} \sum_{j=1}^{M} \delta(p1(i,j), p2(i,j)) \quad (1)$$

Here N, and M in (1) are the dimensions of the images. p1(i, j) and p2 (i, j) are the pixel values at position (i, j) in the original and encrypted images respectively and δ is the Kronecker delta function, which is equal to 0, when the two pixel values are same and 1, otherwise (Fig. 3).

The formula represented by (1) is for calculating NPCR. The purpose of NPCR is to express the strength of image encryption algorithms. This method estimates the resilience of an image encryption algorithm to differential attacks, which involve altering a single pixel in the actual image and observing its impact on the image encrypted. A high NPCR value indicates that a minor alteration in the original image significantly alters the encrypted image, making it challenging for attackers to decrypt. NPCR is typically calculated as a percentage of the total amount of pixels in the image. The strength of the image encryption algorithm is directly proportional to the higher the NPCR value.

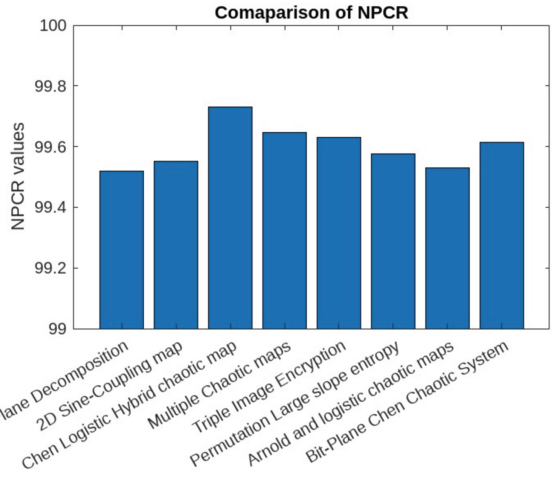

Fig. 3. Comparison of NPCR values

4.2 UACI

UACI is a method that computes the strength of image encryption algorithms. When the change in one image is subtle, then it computes the average difference in color intensities of two images. The formula for computing UACI is:

$$UACI = \frac{1}{NXM} \sum_{i=1}^{N} \sum_{j=1}^{M} |P_1(i,j) - P_2(i,j)| \tag{2}$$

Here N and M describes the dimensions of the images in terms of row and column respectively, $P_1(i,j)$ and $P_2(i,j)$ denote the pixel values of the corresponding locations in the two images being compared, the double summation indicates that the calculation is performed over each pixel in both images

The UACI metric, which is used to gauge how well image encryption techniques work, is measured by Eq. (2). When the change in one image is subtle, UACI determines the average difference in color intensity of two photographs (Fig. 4).

By changing a small piece of the initial image and then observing the impact on the encrypted image, UACI evaluates how resilient an image encryption technique is against selective attacks. A low UACI number implies that even a very small change to the source image will make the encrypted image to change dramatically, making it complex for attackers to crack the encryption. The strength of the image encryption technique increases with the UACI value.

The method-level comparison of various Image Encryption algorithms is depicted in Table 3.

The understanding from Table 2 is that using chaotic systems it is ensured that the encrypted image is resilient to attacks like differential attacks, key Sensitivity analysis, and Noise attacks. Here it is observed that chaos is not showing resilience to brute-force attack.

Table 3 represents the non-chaotic methods of resilience towards attacks like brute force, differential and key sensitivity analysis, and Noise attack. It is observed that most

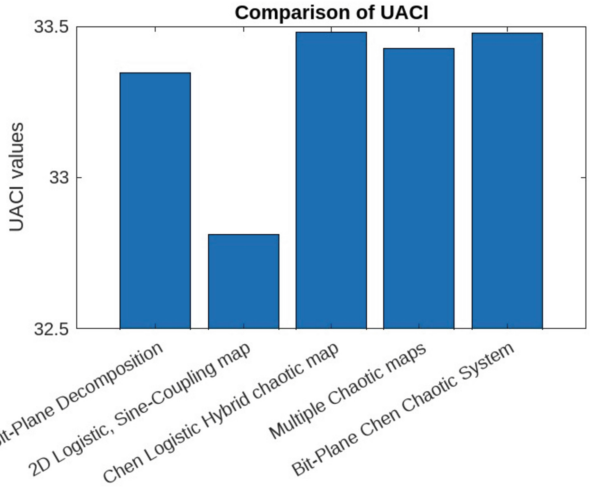

Fig. 4. Comparison of UACI values.

Table 2. Chaotic Methods Resilience to Attacks.

Authors	Algorithm	BFA	DA	KSA	NA	SA	DLA
Akraam *et al.* [23]	Chaotic	×	✓	✓	✓	✓	✓
Hua *et al.* [10]	Chaotic	✓	✓	✓	✓	✓	✓
Wei *et al.* [18]	Chaotic	✓	✓	✓	✓	✓	✓
Iqbal *et al.* [7]	Chaotic	✓	✓	✓	✓	✓	✓

BFA – Brute Force Attack, DA – Differential Attack, KSA – Key Sensitivity Analysis, NA – Noise Attack, SA – Statistical Attack, DLA – Data Loss Attack.

Table 3. Non-Chaotic Methods Resilience to Attacks.

Authors	Algorithm	BFA	DA	KSA	NA	SA	DLA
Guru *et al.* [8]	Triple DES	✓	✓	✓	✓	✓	✓
Jamil *et al.* [31]	RC5	✓	✓	×	✓	✓	✓
Mohanad *et al.* [2]	Lightweight Image Encryption and Blowfish Decryption	×	✓	×	✓	✓	✓
Han *et al.* [30]	Hash-based	✓	✓	✓	×	✓	✓
Manoj *et al.* [3]	Advanced Encryption Standard	✓	✓	✓	✓	✓	✓

of the non-chaotic methods are resilient to Differential attack but most of them do not show much resilience towards key sensitivity analysis.

Table 4. Hybrid Image Encryption Methods Resilience to Attacks.

Authors	Algorithm	BFA	DA	KSA	NA	SA	DLA
Khan *et al.* [14]	Visually Selective Image Encryption	×	✓	✓	✓	✓	✓
Man *et al.* [11]	Double Image Encryption and Chaotic	✓	✓	✓	✓	✓	✓
Pourjabbar *et al.* [19]	Triple Image Encryption	×	✓	✓	×	×	✓
Alrubai *et al.*[29]	Encoding and Logistic Maps	×	✓	×	×	✓	✓
Wang *et al.* [27]	Triple Image Encryption and Chaos	×	×	×	✓	✓	✓
Abanda *et al.* [28]	Permutation Large Slope Entropy	×	×	✓	×	✓	✓
Ferdush *et al.* [29]	Arnold and Logistic Chaotic Maps	×	×	✓	×	✓	✓
Zhu *et al.* [15]	Double chaotic S-Boxes	×	✓	✓	×	×	✓
Zhu *et al.* [16]	Quadratic Polynomial Chaotic Maps	✓	×	✓	×	✓	✓
Arif *et al.* [36]	VMICE Image Encryption	×	✓	×	×	✓	×

From Table 4, it is identified that the Double encryption algorithm in combination with Chaotic systems provides great resilience to all the attacks mentioned in the above table. Table 5 represents the performance analysis of various image encryption systems. Here the performance analysis of different image encryption algorithms is evaluated using encryption time, decryption time, and time complexity. The units of ET and DT are seconds (Figs. 5 and 6).

Table 5. Performance Analysis of Different Image Encryption Algorithms.

Authors	Algorithm	E T	D T	T C
Lu *et al.* [23]	LSS Chaotic Map and Single S-Box	1.48	NM	NM
Pourjabbar *et al.* [19]	1-D chaotic Maps	0.2	0.2	O (n^2)
Cheng *et al.* [20]	Hyper Chaotic Systems	0.1	0.1	O (M*N)
Stalin *et al.* [21]	4D Logistic Map	1.0	1.0	O (n^2)
Yu *et al.* [22]	Hyper chaotic systems	0.5	0.6	O (N^2 log N)
Huang *et al.* [10]	Chaotic systems	2.5	2.5	O (n^3)
Xingyuan wang *et al.* [27]	Chaotic Systems and 3D DCT	0.73	2.7	NM

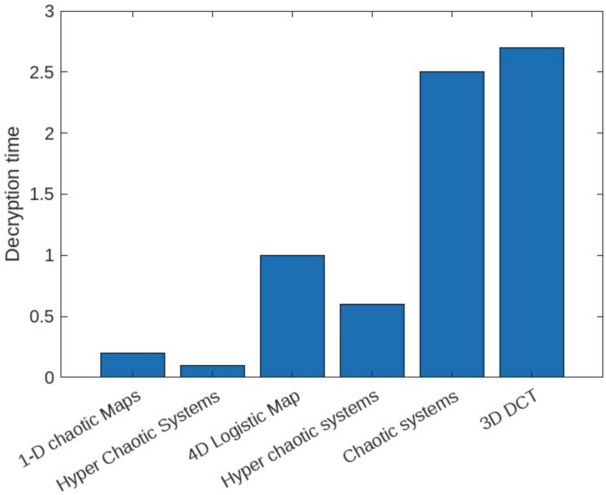

Fig. 5. Comparison of Encryption Times.

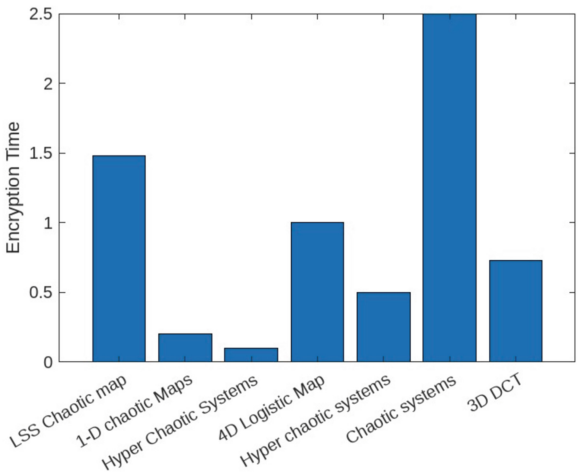

Fig. 6. Comparison of existing methods Decryption Times.

5 Challenges and Gaps

The efficacy and safety of image encryption are contingent upon addressing several challenges. Some of the challenges in image encryption include:

5.1 Resilience to Cryptanalysis or Attack

Image encryption algorithmic techniques should be sturdy against various types of attacks, such as statistical, brute force, and differential attacks.

5.2 Processing of an Encrypted Image

Encrypted images may require processing for compression, retrieval, selective encryption, and thumbnail-preserving encryption. Image encryption algorithms should ensure that these processing tasks can be performed efficiently and uncompromising the security of the encrypted image.

5.3 Key Management Complexities

Image encryption algorithms require the use of secret keys to encrypt and decrypt images. Managing these keys can be complex, especially in large-scale applications.

5.4 Computational Overhead

Image encryption algorithms can be computationally intensive, necessitating substantial processing power and memory resources.

5.5 Robustness Against Attacks

Image encryption algorithms should be developed to maintain the security of encrypted images against various attacks, like noise addition, cropping, and rotation.

5.6 Key Space and Key Sensitivity

Image encryption algorithms should have a huge key space to forbid easy guessing or brute-force attacks. The key should be sensitive to small changes to prevent significant changes to the encrypted image, even if they are minor.

The development and implementation of image encryption algorithms are crucial in addressing these challenges. Researchers continue to work on developing new and improved image encryption algorithms that address these challenges and provide robust and secure image encryption solutions.

6 Conclusion

The exploration of chaotic systems for image encryption was analyzed and discussed in detail. This survey paper highlights their potential and merits as a promising approach in the field of image security. Chaotic systems offer a unique blend of unpredictability, complexity, and sensitivity to initial conditions, which can greatly enhance the robustness of image encryption techniques. As demonstrated through various methods and algorithms discussed in this survey, chaotic systems have shown their effectiveness in safeguarding sensitive visual information from unauthorized access and tampering. One of the primary benefits of chaotic systems is their capacity to provide a high degree of security while maintaining computational efficiency. This makes them appropriate for real-time applications and resource-constrained environments, where rapid encryption and decryption of images are essential. Chaotic systems can be seamlessly integrated with existing encryption methods to create hybrid approaches that combine the strengths of both chaotic as well as conventional cryptographic techniques.

References

1. Kaur, A., Singh, G.: A random selective block encryption technique for secure image cryptography using blowfish algorithm, pp. 1290–1293 (2018). https://doi.org/10.1109/ICICCT.2018.8473273
2. Saddam, M., Ibrahim, A., Mohammed, A.: A lightweight image encryption and blowfish decryption for the secure Internet of Things (2020). https://doi.org/10.1109/ISMSIT50672.2020.9254366
3. Mokhnache, A., Lahcene, Z., Radjah, F.: Comparative analysis between a pixel-wise image encryption scheme and AES in a web application context. Clust. Comput. (2023). https://doi.org/10.1007/s10586-023-04126-3
4. Arab, A., Rostami, M.J., Ghavami, B.: An image encryption method based on chaos system and AES algorithm. J. Supercomput. **75**, 6663–6682 (2019). https://doi.org/10.1007/s11227-019-02878-7
5. Guru, J., Srivatsava, M., Sheeja, R.: Implementation of triple DES ALGORITHM in data hiding and image encryption techniques. Int. J. Adv. Sci. Technol. **29**, 10549–10559 (2020)
6. Lidong, L., Jiang, D., Wang, X., Zhang, L., Rong, X.: A dynamic triple-image encryption scheme based on chaos, S-Box and image compressing. IEEE Access **8**, 210382–210399 (2020). https://doi.org/10.1109/ACCESS.2020.3039891
7. Iqbal, N., et al.: DNA strands level scrambling based color image encryption scheme. IEEE Access **2020**, 1–15 (2020). https://doi.org/10.1109/ACCESS.2020.3025241
8. Man, Z., Li, J., Di, X., Sheng, Y., Liu, Z.: Double image encryption algorithm based on neural network and chaos. Chaos Solitons Fractals **152**, 111318 (2021). https://doi.org/10.1016/j.chaos.2021.111318
9. Rathore, V., Pal, A.K.: An image encryption scheme in bit plane content using Henon map based generated edge map. Multimed. Tools Appl. **80**, 22275–22300 (2021). https://doi.org/10.1007/s11042-021-10719-0
10. Hua, Z., Yi, S., Zhou, Y.: Medical image encryption using high-speed scrambling and pixel adaptive diffusion. Signal Process. **144** (2017). https://doi.org/10.1016/j.sigpro.2017.10.004
11. Khan, J.S., et al.: DNA and plaintext dependent chaotic visual selective image encryption. IEEE Access, 1 (2020). https://doi.org/10.1109/ACCESS.2020.3020917
12. Zhu, S., Zhu, C., Cui, H., Wang, W.: A class of quadratic polynomial chaotic maps and its application in cryptography. IEEE Access, 1 (2019). https://doi.org/10.1109/ACCESS.2019.2902873
13. Artuğer, F., Özkaynak, F.: A novel method for performance improvement of chaos-based substitution boxes. Symmetry **12**, 571 (2020). https://doi.org/10.3390/sym12040571
14. Ghebleh, M., Kanso, A.: A novel secret image sharing scheme using large primes. Multimed. Tools Appl. **77**, 11903–11923 (2018). https://doi.org/10.1007/s11042-017-4841-4
15. Movafegh Ghadirli, H., Nodehi, A., Enayatifar, R.: An overview of encryption algorithms in color images. Signal Process. **164**, 163–185 (2019). https://doi.org/10.1016/j.sigpro.2019.06.010
16. Li, C., Feng, B., Li, S., Kurths, J., Chen, G.: Dynamic analysis of digital chaotic maps via state-mapping networks. IEEE Trans. Circuits Syst. I Regul. Pap., 1–14 (2019). https://doi.org/10.1109/TCSI.2018.2888688
17. Li, S., Ding, W., Yin, B., Zhang, T., Ma, Y.: A novel delay linear coupling logistics map model for color image encryption. Entropy **20**, 463 (2018). https://doi.org/10.3390/e20060463
18. Kumar Patro, K.A., Acharya, B.: An efficient colour image encryption scheme based on 1-D chaotic maps. J. Inf. Secur. Appl. **46**, 23–41 (2019). https://doi.org/10.1016/j.jisa.2019.02.006
19. Song, W., Zheng, Y., Fu, C., Shan, P.: A novel batch image encryption algorithm using parallel computing. Inf. Sci. **518**, 211–224 (2020). ISSN 0020-0255. https://doi.org/10.1016/j.ins.2020.01.009

20. Pourjabbar Kari, A., Habibizad Navin, A., Bidgoli, A.M., Mirnia, M.: A new image encryption scheme based on hybrid chaotic maps. Multimed. Tools Appl. **80**(2), 2753–2772 (2020). https://doi.org/10.1007/s11042-020-09648-1
21. Cheng, G., Chen, H.: A novel color image encryption algorithm based on hyperchaotic system and permutation-diffusion architecture. Int. J. Bifurc. Chaos **29**, 1950115 (2019). https://doi.org/10.1142/S0218127419501153
22. Zhang, L.Y., Liu, Y., Wang, C., Zhou, J., Zhang, Y., Chen, G.: Improved known-plaintext attack to permutation-only multimedia ciphers. Inf. Sci. **430–431**, 228–239 (2018). ISSN 0020-0255. https://doi.org/10.1016/j.ins.2017.11.021
23. Akraam, M., Rashid, T., Zafar, S.: A chaos-based image encryption scheme is proposed using multiple chaotic maps. Math. Probl. Eng. **2023**, 1–13 (2023). https://doi.org/10.1155/2023/2003724
24. Mohamed, ElKamchouchi, Moussa: A novel color image encryption algorithm based on hyperchaotic maps and mitochondrial DNA sequences. Entropy **22**, 158 (2020). https://doi.org/10.3390/e22020158
25. Fang, D., Sun, S.: A new secure image encryption algorithm based on a 5D hyperchaotic map. PLoS ONE **15**, e0242110 (2020). https://doi.org/10.1371/journal.pone.0242110
26. Aqeel-ur-Rehman, Liao, X., Hahsmi, M.A., Haider, R.: An efficient mixed inter-intra pixels substitution at 2bits-level for image encryption technique using DNA and chaos. Optik Int. J. Light Electron Opt. **153**, 117–134 (2018). https://doi.org/10.1016/j.ijleo.2017.09.099
27. Wu, X., Wang, K., Wang, X., Kan, H., Kurths, J.: Color image DNA encryption using NCA map-based CML and one-time keys. Signal Process. **148**, 272–287 (2018). https://doi.org/10.1016/j.sigpro.2018.02.028
28. Abanda, Y., Tiedeu, A., Kom, G.: Image encryption with fusion of two maps. Secur. Commun. Netw. **2021**, 1–16 (2021). https://doi.org/10.1155/2021/6624890
29. Ferdush, J., Begum, M., Uddin, M.S.: Chaotic lightweight cryptosystem for image encryption. Adv. Multimed. **2021**, 1–16 (2021). https://doi.org/10.1155/2021/5527295
30. Han, R.: A hash-based fast image encryption algorithm. Wirel. Commun. Mob. Comput. **2022**, 1–8 (2022). https://doi.org/10.1155/2022/3173995
31. Xu, J., Zhao, B., Wu, Z.: Research on color image encryption algorithm based on bit-plane and Chen chaotic system. Entropy **24**, 186 (2022). https://doi.org/10.3390/e24020186
32. Salim Jamil, A., Rahma, A.M.S.: Image encryption based on multi-level keys on RC5 algorithm. Int. J. Interact. Mob. Technol. **16**, 101–115 (2022). https://doi.org/10.3991/ijim.v16i17.34335
33. Cheng, Z., Wang, W., Dai, Y., Li, L.: A high-security privacy image encryption algorithm based on chaos and double encryption strategy. J. Appl. Math. **2022**, 1–14 (2022). https://doi.org/10.1155/2022/9040702
34. Zhou, Y., Wang, E., Song, X., Shi, M.: Image encryption algorithm based on artificial bee colony algorithm and chaotic system. Secur. Commun. Netw. **2022**, 1–20 (2022). https://doi.org/10.1155/2022/1444676
35. Ismail Abdelfatah, R.: Quantum image encryption using a self-adaptive hash function-controlled chaotic map (SAHF-CCM). IEEE Access **10**, 107152–107169 (2022). https://doi.org/10.1109/ACCESS.2022.3212899
36. Arif, J., et al.: A novel chaotic permutation-substitution image encryption scheme based on logistic map and random substitution. IEEE Access **10**, 12966–12982 (2022). https://doi.org/10.1109/ACCESS.2022.3146792

37. Gao, X., Yu, J., Yan, H., Mou, J.: A new image encryption scheme based on fractional-order hyperchaotic system and multiple image fusion (2021). https://doi.org/10.21203/rs.3.rs-494660/v1
38. Alrubaie, A.H., Khodher, M.A.A., Abdulameer, A.T.: Image encryption based on 2DNA encoding and chaotic 2D logistic map. J. Eng. Appl. Sci. **70**, 60 (2023). https://doi.org/10.1186/s44147-023-00228-2