POLARIS GLOBAL JOURNAL OF SCHOLARLY RESEARCH AND TRENDS

Chaos-Based Image Encryption Techniques: A Comprehensive Survey

DOI: https://doi.org/10.58429/pgjsrt.v4n4a220

Reving Masoud Abdulhakeem[1,*] and Nechirvan Asaad Zebari[2]

1 Department of Computer Science, College of Science, van yüzüncü yıl university, Turkey.
2 Department of Information Technology, Lebanese French University.

*Corresponding author E-mail: reving.abdulhakeem@gmail.com.

ARTICLEINFO **ABSTRACT** **E-ISSN: 2961-3809**

Because of the rapid expansion of digital and multimedia applications in today's world, more multimedia data are being created and transmitted through networks in the areas of art, recreation, advertising, education, training, and commerce. These types of data may include sensitive information that should not be obtained by the general public. The protection of the confidentiality, integrity, security, and privacy of photos, in addition to the authenticity of images, has therefore become a key concern for the transmission and storage of images. In recent years, a variety of encryption strategies have been developed and used to prevent secret photographs from being seen by people who are not allowed to view them. The purpose of this study is to create an image cryptosystem, and it includes a discussion of the many features of current picture encryption approaches that are based on chaos. First, a fundamental introduction to cryptography and picture encryption is provided in this article. Next, a study of several chaotic-based image encryption approaches and related works for each methodology discussed follows. Finally, the paper concludes with some conclusions. In conclusion, the primary objective of this research is to analyze the workings of a number of chaotic-based picture encryption algorithms that are now in use so as to be of assistance in the development of new chaotic-based image encryption methods in the not-too-distant future.

KEYWORDS
Cryptography, Image encryption, Chaotic maps, Multimedia Security, Confidential Data Protection

How to cite:
Abdulhakeem, R. M., & Zebari, N. A. (2025). Chaos-Based Image Encryption Techniques: A Comprehensive Survey. *Polaris Global Journal of Scholarly Research and Trends*, 4(1), 1-11. https://doi.org/10.22219/pgjst.v4n4a220

1. Introduction

In prior years, the primary concern was the safety and authenticity of the data. However, with the rapid growth of networks, data leakage occurs in the process of sending and storing data across computer networks, and these networks are susceptible to a wide variety of attacks. As a result, the security and authenticity of the data have become less of a priority in recent years. Before the data can be transported or kept, it has to be encrypted so that it is protected from any number of threats and maintains its integrity [1]. As a direct result of this, concerns about data encryption and network security are seen as important topics. At the moment, people believe that pictures are the most essential source of information. Image encryption has a wide range of potential applications, including but not limited to wireless communication, multimedia systems, medical imaging, telemedicine, and even military communication [2]. As a result of advances in communication technology, new forms of transmission media, including still photos and moving video, are becoming more commonplace in the process of information dissemination. When they are sent over a variety of public routes, digital photographs that have not been subjected to any kind of special processing and that include sensitive information are susceptible to being intercepted and used by hackers. Encryption is a useful tool that is often used for the purpose of maintaining the confidentiality of information. Traditional text encryption standards, however, such as the data encryption standard (DES), the advanced encryption standard (AES), and the Rivest–Shamir–Adleman (RSA) algorithm, are unable to efficiently encrypt images due to their enormous data volumes, high levels of temporal redundancy, and high levels of spatial redundancy [3].

Every single member of society now recognizes the significance of data protection. Large corporations have been dragged into the dispute as a result of server data leakages that disclose all of the information that was previously saved on a user's device. Even while the data is analyzed and secured in a variety of ways to ward off assaults and safeguard digital content from being compromised, it is frequently the case that these procedures are not sufficient to keep the information and assets secure. This fact presents a significant obstacle, not only for the protection of personal information but also for online safety [4]. Encryption of data is useful in situations like these. The transformation of readable data into outcomes that cannot be read is one of the primary functions of encryption. These days, the most popular apps used all over the world are built on the concept of sharing and storing photographs in the cloud. Encryption of images has emerged as one of the most indispensable instruments in the modern digital environment. A digital picture may be identified by its inherent properties, which include bulk data, strong pixel correlation, and duplication, among other characteristics. As a result, picture encryption is a very significant technique that must be used to protect sensitive information [5].

The plain picture is converted into a cipher image via the process of image encryption. When it comes to preventing unauthorized access to different types of information, various strategies and features that are specific to those types of information are used. Consequently, data encryption is carried out in order to guarantee safety throughout the unblocked systems phase, which is characterized by a change in the value of the pixel. A numerical number is used to represent each individual pixel. The size of a pixel is equal to the picture size divided by the size of the matrix. The number of pixels that run the length and breadth of an image is referred to as the matrix size, while the dimension of the field of view is referred to as the picture size. One is able to convert the original picture into a simple image that cannot be seen by anybody who is not permitted to do so if they use a certain method from the field of cryptography and a key. Picture decryption, on the other hand, is the procedure that is analogous to the opposite of image encryption. The number of keys used in encryption and decryption determines the type of calculation used in cryptography. There are two types of cryptographic calculations: secret key algorithms and private key algorithms. Secret key algorithms use only one key parameter to encrypt and decrypt the data, while private key algorithms use two keys [6, 7]. The one before this one is referred to as the symmetric key algorithm, while the one after this one is called the asymmetric algorithm.

2. Image Encryption Terms

During the examination, it was discovered that there are several methods of picture encryption that may be used to ensure the security of these photos. To encrypt an unencrypted picture, the technique necessitates the use of a private key. During the decryption process, the encrypted picture is transformed back into the original image by using the private key. The only distinction between a decryption process and an encryption operation is in their opposing application methods and directions. The relevance of secret keys is paramount in the encryption process. The encryption process employs both a private key and a public key to provide the utmost degree of security [8]. While the private key is known exclusively to the user, the public key is available to anybody who wishes to use it. The encryption and decryption of the images use the same key, which is embedded inside the private key and employed for both operations. When working with a public key, it is necessary to use two separate keys: one for encryption and another for decryption. In this scenario, the encryption key is made available to the general public, but the decryption key is always safeguarded as confidential information [9]. Figure 1 illustrates the schematic representation of the sequential steps that a picture undergoes during encryption.

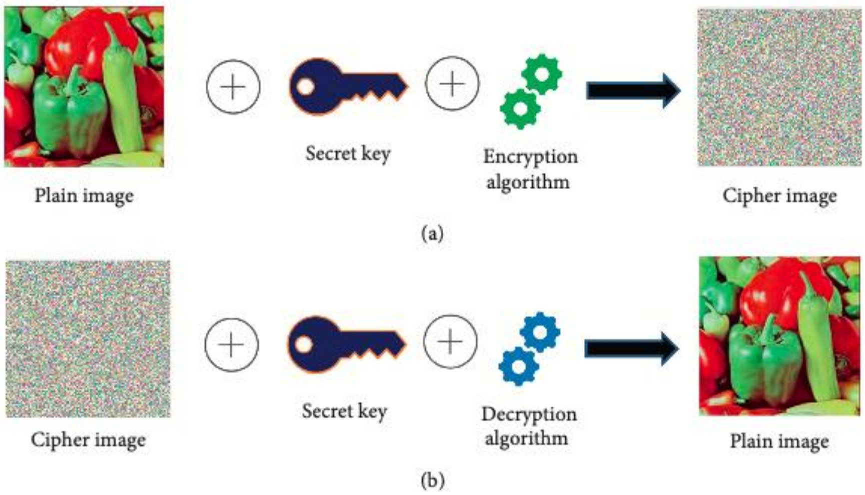

Figure 1. illustrates the overall structure of picture encryption. The encryption procedure is performed at the sender's side. (b) The decryption procedure carried out by the recipient [9].

The following is a brief explanation of some of the fundamental terminology used in encryption.
(i) The uncompressed picture: the image itself is the part that requires protection when it is being sent over a public network. It is often referred to as the input picture or the original image.
(ii) A cipher image is an encrypted and modified version of a plain image, rendering it unreadable.
(iii) Encryption is the procedure of changing a plain picture into an encrypted image by applying an encryption method and a secret key. This process takes a plain image and turns it into a cipher image.
(iv) Decryption: The cipher picture is changed into a plaintext message by the receiver using a decryption method and a secret key. This step takes place after encryption. Decryption is the term used to describe this procedure.
(v) The Key: The key is the most important factor in determining how secure the encryption method is. It may be either numeric or alphabetic in format. Encryption and decryption both require the use of the key in order to successfully complete their respective processes. Always necessary for improved information security is the use of strong keys.

3. Evaluation Parameters

The picture encryption method must first be evaluated since this is an essential step before determining whether or not it is successful. By experimenting with these settings, the many qualities of an image encryption technique may be investigated. The effectiveness of picture encryption may be measured via the use of several evaluation metrics. There are a number of different security methods that may be carried out by attackers in order to break the encryption method and locate the key. Cryptanalysis is the primary method that attackers use to investigate the various encryption methods [10]. As a result of this, it is essential to conceal the statistics of the plaintext as well as the secret key. Employing security and quality assessments are two methods that may be used to evaluate the efficacy of picture encryption. Through the use of peak signal-to-noise ratio, mean square error, and other metrics, the quality analysis evaluates the picture quality of the decrypted images. A statistical analysis, a differential analysis, and a key analysis are all included in the security analyses.

3.1 Differential Analysis

In order to conduct an analysis of the differential attacks, many measures, including the Pixel Change Rate (NPCR) and the Unified Average Changing Intensity (UACI), are used. The differential attack is a method for determining how sensitive the encryption technique is to even the most minute shifts in the plain picture that it is protecting. Attackers often introduce a barely perceptible alteration to the original picture. Encrypt both the original and the updated picture using the same key that you have kept hidden. After that, make an effort to determine the connection between the encrypted versions of the original photographs and the changed versions [11].

3.2 Statistical Analysis

Statistical analysis of a ciphered picture is another method that may be used to break encryption schemes. Histogram Analysis (HA) and Correlation Coefficient (CC) are two methods that are used to demonstrate that an encryption method is resistant to statistical assaults by analyzing the pixels that are next to each other in an encrypted picture. Histograms display the dispersion of pixels at the top of the picture and are used to determine the quantitative attributes of the photographs. The histogram of the isolated picture ought to come as more of a shock to the reader than the graph of the jumbled image. Histograms of normal images are fundamentally not consistent in appearance. Histograms of encrypted photos ought to have a consistent appearance at all times. This indicates that the locations of each pixel are uniformly distributed over the space. It can be seen that the histograms of the cipher text picture and the original photos are quite different from one another [2].

3.3 Noise Attack (NA)

An adversary may inject noise into the encrypted picture in an effort to obscure or obscure important information. Because of this, the intended user is unable to effectively retrieve the original picture once the encryption process has been completed. The attacker includes many types of noise, such as additive noise, Gaussian noise, and Poisson noise, among others, in the encrypted picture [11]. Because of this, an effective method of picture encryption should be able to withstand assaults based on noise.

3.4 Time complexity

The number of instructions that must be carried out in a certain amount of time is referred to as the program's "time complexity." Its manual guess should be attainable by applying all of the executable activities that are included in the collection since the fundamental jobs all have a predetermined amount of time associated with them [12]. This time shows the time that the picture was encrypted as well as unscrambled, and it is recorded by actions that are fundamental to the process. The length of time required to complete the task is determined by a variety of factors, including the design of the system and the picture that was chosen.

4. Image Encryption Approaches

Various strategies for the encryption of images have been created up to this point. After going over the available research, we were able to categorize the methods into several groups, such as spatial, transform, optical, and compressive sensing-based image encryption techniques. Picture Encryption in the Spatial Domain is an example of what is known as a spatial domain technique. This method involves physically modifying the pixels that make up the image. There are several other spatial domain-based picture encryption methods that may be found in the relevant literature. But we have thought about the most well-known methods, such as DNA-based, chaotic-based, elliptic curve-based, fuzzy-based, and Metaheuristics-based methods.

4.1 Image Encryption Using Chaos Methods

Chaotic maps are very relevant in the world of cryptography. These maps are responsible for generating random numbers, which are then utilized as encryption keys. This example arises due to its specific characteristics, such as its ergodicity, its responsiveness to the initial circumstances, and its dynamic and deterministic nature. Various effective iterations of chaotic maps have been used so far. The main classifications used to distinguish chaotic maps are higher-dimensional chaotic maps and one-dimensional chaotic maps. The use of chaotic maps may be advantageous in carrying out the confusion and diffusion processes inherent in the encryption process [9]. There are two methods that may be used to encrypt photos. These processes are not exclusive to chaos, and the tactics may be chaos-based or not, and they can be particular or non-particular. When using chaos-based methodologies, it is crucial to carefully analyze the starting circumstances throughout the planning process. Any alterations to the original state will directly affect the ultimate outcome. Images may be encrypted using chaos-based algorithms, which provide many advantages like easy operation, faster encryption speed, and resistance to attacks [4]. Chaos-based encryption is a versatile method used in various domains such as healthcare, internet communication, military operations, image messaging on cell phones, multimedia systems, medical imaging, telemedicine, security, government documents, and more. These are a few of the areas that may get advantages from this encryption approach. Encryption methods that use chaos are developed by using the phases of confusion and dispersion as its primary components. Figure 1 displays a block diagram illustrating the chaos-based picture encryption method. You may obtain it by clicking on this link. The confusion phase is marked by the rearrangement of the pixel's location, without altering its value in any way. This stage is particularly denoted as the phase of perplexity. The purpose of a diffusion phase is to alter the estimate of every individual pixel that makes up a picture [5].

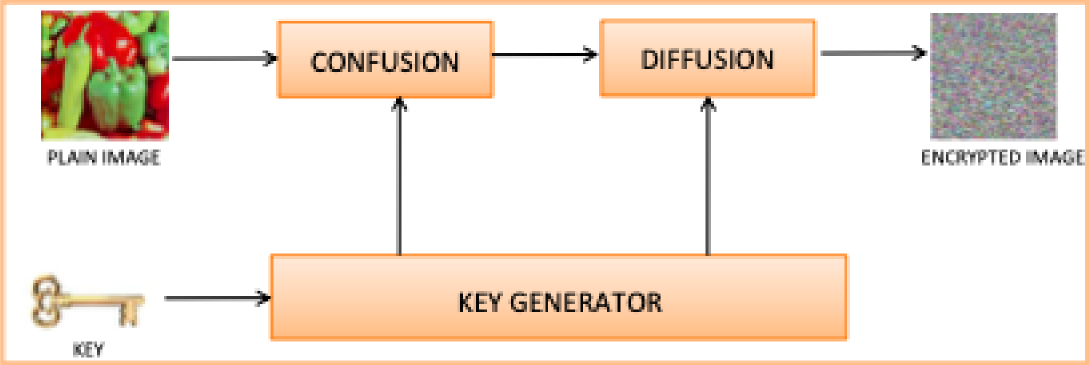

Figure 2. Chaos-based Image Encryption Techniques [10]

In recent years, researchers have been paying particular attention to the close link that exists between chaotic systems and cryptography. Their goal is to develop a chaos-based encryption method that can provide secure image encoding and transmission even when an adversary is present [13]. Consequently, chaotic cryptography may be seen as a combination of chaos theory with the science of encryption, provided that the combination is carried out in a suitable way. The fact that cryptosystems are based on a restricted set of integers, but chaotic systems are based on real numbers, is the most important difference between the two types of systems. Despite the fact that conventional cryptosystems like AES and DES are suitable for the encryption of text, they are not suitable for the encryption of pictures. This is due to the fact that similar images have pixels that contain information that is repeated. Chaos-based encryption methods are able to solve this difficulty by generating random keys that are widely distributed across the cipher pictures. This allows the information contained within the cipher images to be concealed [14]. Nevertheless, these two scientific concepts are very intertwined with one another, and as a consequence, they provide a good combination of enhanced performance, coupled with a high degree of safety, and a variety of practical applications that are of great benefit. The production of pseudo-random numbers for the purpose of producing stream ciphers [15] and block ciphers [16] is one example of these applications. Other examples include secure communications [17], picture encryption [18], and video encryption [19]. Chaotic systems are a collection of dynamical equations that vary over the course of time [20], and time itself may be either discrete or continuous. The notion of chaotic systems refers to this collection of equations. It is a favorable alternative for the construction of cryptosystems because chaotic systems have specific traits like as determinacy, ergodicity, and sensitivity to beginning circumstances. These qualities make chaotic systems an attractive choice. This is because these features are analogous to the confusion and diffusion properties that are necessary in a trustworthy cryptosystem. This is the reason why this is the case. As a consequence of the continual development that has been made in the disciplines of image encryption and cryptanalysis, a number of different chaotic picture encryption algorithms and improved approaches have been introduced. These have the capability to protect against a wide range of potential security threats.

Table 1. Summary of Related Works for Image Encryption-Based Chaotic Map

Ref	Objective	Technique	Remarks
[30]	Suggest the use of finite-time chaos synchronization to provide safe communication in satellite imaging.	Henon map	The system employs chaotic oscillators for encryption, a strong controller for time-delay, and undergoes thorough security analysis.
[31]	A novel hybrid Secure Image Encryption Based on Julia Set of Fractals & 3D Lorentz Map	Lorentz Map	Higher Security, High Sensitivity, Low peak to SNR
[32]	Encryption based image block scrambling for grayscale image	N/A	High Sensitivity
[33]	LSTC map-based bit level for color image encryption	LSTC map	Good key space with good resistant to statistics attacks
[34]	Roulette Cascaded Chaotic System for image encryption	N/A	Good Key Space, Good Key Sensitivity
[35]	Mixed chaotic map for Josephus traversing	N/A	Using the YCbCr color scheme enhances compression.
[36]	Develop a new chaotic image encryption scheme.	Utilizes Josephus traversing and mixed chaotic maps for encryption.	An encryption technique that is effective is able to withstand typical assaults.
[37]	An encryption method-based S-Box and Cellular Automata	Lorenz system	Good against Brute-force attack
[38]	Chaotic image encryption algorithm based on hybrid multi-objective particle swarm optimization and DNA sequence	N/A	Logistic Map, DNA

[39]	Peculiarity of Plaintext DNA Coding for image encryption	Hyper-chaotic Lorenz system	High key space and sensitivity
[40]	Image encryption method using double layer-based DNA and Chaotic map	Hyper-chaotic Lorenz system	High Sensitivity
[41]	Diffusion of pixels with dynamic filtering and permutation-based DNA	5D hyperchaotic system	Higher Security
[42]	A method-based S-Box with chaotic map proposed color image encryption method	piecewise linear chaotic map	Good in key sensitivity and space
[43]	Proposed a method using SHA-512	four-wing chaotic systems and Lorentz systems	Robust for statistical attacks
[44]	Hidden Attractor Chaos and Shuffle technique for image encryption	Hidden Attractor Hyperchaotic System	Higher Security
[45]	Image encryption method-based permutation and substitution	Logistic map	Robust for statistical attacks

A dynamic S-box, a logistic map, and a Lorenz system were all included into the encrypted picture approach that was presented by A. Abdulbaqi and colleagues [21]. This method was based on the integration of these three components. The plain image is permuted using the permutation approach at the beginning of the process. In the subsequent steps, a circular shift of the variable S-box is implemented in order to carry out the replacement process block by block. Following this, the crucial phases are added, and the final picture, which is also referred to as an XOR image, is ultimately formed. After this phase, the key that was produced by the logistic map is combined with the XOR image, and it is then confused. This concludes the process. Several performance metrics, including as entropy, histogram, key space, correlation, NPCR, and UACI, are used in order to evaluate the recommended technique. These measurements serve to highlight the system's resilience to differential and statistical attacks, as well as its success in warding off such attacks. A one-dimensional cosine polynomial (1-DCP) chaotic map was only recently reported by Wang et al. [22] in the area of photo encryption. This has just been done very lately. The solution that has been offered is more favorable than other one-dimensional maps that are already in use because of its uncomplicated structure, which enables a larger key space and reduces the amount of time that is required for processing. In addition, in order to further improve the chaotic characteristics, a different image encryption method known as 1-DCPIE was developed. This system is based on 1-DCP. The sequential permutation was replaced with the parallel permutation instead of the sequential permutation in order to achieve high levels of security while also enhancing the performance of this approach. It was mentioned by Deepa and Sivamangai [23] that a medical image that has been illegally modified makes it more difficult to recognize an ailment that is really there. Since this is the case, it is of the highest need to protect the confidentiality of patients with relation to clinical imaging. On the other hand, the amount of time that is necessary for encryption might potentially bring about a substantial load on the systems that are responsible for medical communication and processing. DNA cryptography and chaos cryptography, according to their assertions, are the most efficient solutions for overcoming this predicament. As part of their study, they presented a few qualitative and quantitative measurements that they had collected from previously done relevant research works in order to illustrate how the specified technologies are able to resolve the tradeoff. These measures were taken from the research works that had been conducted beforehand.

In addition, they outlined many principles that researchers should follow while doing future studies in this field. Yadav and Chaware [24] argue that despite the existence of encryption and concealment techniques, information may still be compromised and copyrights can still be infringed. This is due to the presence of deficiencies in the currently accessible remedies. They began by providing an analysis of the latest breakthroughs in picture encryption techniques. Their research mostly concentrated on collaborative encoding systems, sometimes known as error correction encryption in specific circles. Subsequently, they developed an innovative method that relied on the use of Low-Density Parity-Check (LDPC) code and chaotic maps, while using the capabilities of the Advanced Encryption Standard (AES) and Substitution boxes (S-boxes)[25]. This approach was a groundbreaking innovation that completely transformed the world of encryption. This study [26] describes the chaos-based picture encryption techniques that were proposed and are available online. The idea intends to use an inheritance-based method to improve the connectivity between adjacent pixels. Reenactments demonstrate a security failure that may be used to both interpret the picture and determine the key's location. To address the previously described problem, Knuth intended to substitute the rand work with the logistic map by rearranging the saddle. At this juncture, it is advisable to ascertain the level of security of the proposed computation by simulating a few attacks against it and conducting a review of the resulting consequences. The preservation of pixel entropy in the new calculating approach enhances the system's safety. Moreover, the degree of reduction in the linking coefficient between adjacent pixels in the coded picture was significantly decreased. This resulted in a significant decrease. Chen et al. [27] developed a technique for encrypting images that utilizes a two-dimensional sine map and a Chebyshev map. This approach was devised. The methodology presented is a universal antidegradation method for chaotic maps, enhancing performance even on devices with limited precision. This method enhances the competitiveness of chaotic maps. Xuejing and Zihui [28] suggested using DNA encoding and spatiotemporal chaotic maps to encrypt pictures in their study. After the first phase of converting a simple picture into three DNA matrices using a random encoding approach, the resulting DNA is combined with the original matrix to create a contemporary matrix. Subsequently, the ascent matrix will do various permutations on it to get the encrypted picture. Wang et al. [29] used linked map lattices (CML) together with the DNA method to encrypt the photographs. This action was undertaken with the purpose of safeguarding sensitive personal data. Ismail et al. [30] examined a novel method for encrypting images without any loss of data. This methodology relied on the use of fractional-order and double-humped logistic maps. The technique was created as a result of their research.

Table 2. Summary Obtained Results of Related Works for Image Encryption Based Chaotic Map

Ref	Key space	Key sensitivity	Entropy	Histogram	NPCR	UACI
[31]	10^{210}	Not good	7.9843	good	99.51	N/A
[32]	-	Not good	7.994	Good	99.62	33.90
[33]	26^{912}	Good	7.4434	Not good	99.65	N/A
[34]	-	Not good	7.9915	Good	99.60	33.45
[35]	2^{504}	Good	7.9994	Good	99.60	33.47
[36]	2^{168}	Good	7.5755	Good	99.60	N/A
[37]	2^{429}	Good	7.0951	Good	99.61	N/A
[38]	2^{425}	Not good	7.9970	Good	99.63	30.34
[39]	2^{432}	Good	7.9975	Good	99.62	33.41
[40]	2^{237}	Good	7.9993	Good	99.61	33.45
[41]	2^{100}	Good	7.9971	Good	99.64	31.21
[42]	2^{249}	Good	7.9993	Not good	99.61	33.45

[43]	2^{398}	Good	7.9959	Good	99.62	33.46
[44]	2^{98}	Good	7.9969	Good	99.60	33.47
[45]	2^{327}	Good	7.9983	Good	99.59	33.48
[46]	-	Good	7.9994	Not good	99.62	33.49

4.2 Future Scope

According to what has been gleaned from the existing body of research, the formulation of an effective method for the encryption of images is still a frontier of exploration. The currently available methods for encrypting images have a number of drawbacks, including slow processing speed, insufficient security, insufficient parameter adjustment, and so on. Verification of the picture's integrity and authenticity is very important in the event that the image is altered by a third party while it is being transmitted. This is done to protect the content of the image from being revealed inappropriately. As a result, the development in the near future of a strategy that combines encryption and authentication is something that should be prioritized. In the process of encryption, the amount of key space available is determined by the primary factor that has the most significant influence on the encrypted picture. Image compression is a technique that may be used to strengthen crucial aspects that are lacking. because of the fast progress in the many different uses of multimedia, such as medical and satellite imaging. These applications demand photos with a high resolution; hence, the process of developing image encryption strategies for these applications will require a significant amount of processing resources. Therefore, techniques that employ parallel image encryption may be applied to deal with this problem. There has not yet been sufficient progress made in the field of developing encryption strategies for multimedia data types such as multispectral photographs. When dealing with data of this kind that is multidimensional and multimodal, it is necessary to construct high-dimensional and chaotic systems.

5. Conclusion

The great majority of encryption methods that are now available have been discussed in this work. The focus of the initial survey was on the image encryption algorithms that had already been developed. Nevertheless, the naive algorithm, which involves encrypting the entire multimedia bit series utilizing a standard cipher method, is the most effective method for protecting multimedia data such as images and video. To provide a high level of security, many earlier studies as well as those that are currently being done now focus on developing cryptographic procedures that encrypt just a carefully chosen piece of the image bitstream. A significant number of the systems that were analyzed were only capable of reaching a moderate to low level of safety, and it was possible to build systems under conditions in which partial failure was probable. However, such methods can only provide a semblance of security when applied to particular types of media systems. There have been many different ideas floated for potential solutions to the problem of chaotic networks. The issue was discussed and shown in more detail in the third portion of the survey report. A cryptographic method that is not just speedy but also secure and has been the subject of much research needs to be given priority.

REFERENCES

1. Sharma, B., & Singh, J. (2022). Chaos Based Image Encryption Techniques: A Review. *International Research Journal of Engineering and Technology*.
2. Abdullah, R. M., & Abrahim, A. R. (2022). Review of Image Encryption using Different Techniques. *Academic Journal of Nawroz University (AJNU)*, *11*(3).
3. Zebari, D., Haron, H., & Zeebaree, S. (2017). Security issues in DNA based on data Hiding: A review. *International Journal of Applied Engineering Research*, *12*(24), 0973-4562.

4. Naik, R. B., & Singh, U. (2024). A review on applications of chaotic maps in pseudo-random number generators and encryption. *Annals of Data Science*, *11*(1), 25-50.
5. Yang, C.; Pan, P.; Ding, Q. Image encryption scheme based on mixed chaotic bernoulli measurement matrix block compressive sensing. *Entropy* **2022**, *24*, 273.
6. Zebari, D. A., Zeebaree, D. Q., Saeed, J. N., Zebari, N. A., & Adel, A. Z. (2020). Image steganography based on swarm intelligence algorithms: A survey. *people*, *7*(8), 9.
7. Song, W.; Fu, C.; Zheng, Y.; Cao, L.; Tie, M.; Sham, C.-W. Protection of image ROI using chaos-based encryption and DCNN-based object detection. *Neural Comput. Appl.* **2022**, *34*, 5743–5756.
8. Jubair, M. A., Mostafa, S. A., Zebari, D. A., Hariz, H. M., Abdulsattar, N. F., Hassan, M. H., ... & Alouane, M. T. H. (2022). A QoS aware cluster head selection and hybrid cryptography routing protocol for enhancing efficiency and security of VANETs. *IEEE Access*, *10*, 124792-124804.
9. Zebari, N. A., Zebari, D. A., Zeebaree, D. Q., & Saeed, J. N. (2021). Significant features for steganography techniques using deoxyribonucleic acid: a review. *Indonesian Journal of Electrical Engineering and Computer Science*, *21*(1), 338-347.
10. Kaur, M., & Kumar, V. (2020). A comprehensive review of image encryption techniques. *Archives of Computational Methods in Engineering*, *27*, 15-43.
11. Zia, U., McCartney, M., Scotney, B., Martinez, J., AbuTair, M., Memon, J., & Sajjad, A. (2022). Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains. *International Journal of Information Security*, *21*(4), 917-935.
12. Malik, A., Gupta, S., & Dhall, S. (2020). Analysis of traditional and modern image encryption algorithms under realistic ambiance. *Multimedia Tools and Applications*, *79*(37-38), 27941-27993.
13. Xu, Q.; Chen, X.; Chen, B.; Wu, H.; Li, Z.; Bao, H. Dynamical analysis of an improved FitzHugh-Nagumo neuron model withmultiplier-free implementation. *Nonlinear Dyn.* **2023**, *111*, 8737–8749.
14. Zebari, D. A., Haron, H., Zeebaree, S. R., & Zeebaree, D. Q. (2018, October). Multi-level of DNA encryption technique based on DNA arithmetic and biological operations. In *2018 International Conference on Advanced Science and Engineering (ICOASE)* (pp. 312-317). IEEE.
15. Liu, Z., Wang, Y., Zhao, Y., Zhang, L.Y.: A stream cipher algorithm based on 2d coupled map lattice and partitioned cellular automata. Nonlinear Dyn. **101**(2), 1383–1396 (2020)
16. Kaur, M., Singh, S., Kaur, M., Singh, A., & Singh, D. (2021). A systematic review of metaheuristic-based image encryption techniques. *Archives of computational methods in engineering*, 1-15.
17. Peng, Z., Yu, W., Wang, J., Zhou, Z., Chen, J., Zhong, G.: Secure communication based on microcontroller unit with a novel five-dimensional hyperchaotic system. Arab. J. Sci. Eng., pp. 1–16 (2021)
18. Yang, C.-H.; Weng, C.-Y.; Yang, Y.-Z. TPEIP: Thumbnail preserving encryption based on sum preserving for image privacy. *J. Inf. Secur. Appl.* **2022**, *70*, 103352. Gao, X.; Sun, B.; Cao, Y.; Banerjee, S.; Mou, J. A color image encryption algorithm based on hyperchaotic map and DNA mutation. *Chin. Phys. B* **2022**, *32*, 030501.
19. García-Guerrero, E.; Inzunza-González, E.; López-Bonilla, O.; Cárdenas-Valdez, J.; Tlelo-Cuautle, E. Randomness improvement of chaotic maps for image encryption in a wireless communication scheme using PIC-microcontroller via Zigbee channels. *Chaos Solitons Fractals* **2020**, *133*, 109646.
20. Salih, M. S., & Zeebaree, S. R. (2025). Enhanced Image Encryption Using Pixel-Block Permutation and Multi-Chaotic Maps with DNA-Based Diffusion. *Journal of Soft Computing and Data Mining*, *6*(1), 347-358.
21. Talhaoui, M.Z., Wang, X., Midoun, M.A.: A new one-dimensional cosine polynomial chaotic map and its use in image encryption. The Visual Computer pp. 1–11 (2020)
22. Alsandi, N. S. A., Zebari, D. A., Al-Zebari, A., Ahmed, F. Y., Mohammed, M. A., Albahar, M. A., & Albahr, A. A. (2023). A Multi-Stream Scrambling and DNA Encoding Method Based Image Encryption. *Comput. Syst. Sci. Eng.*, *47*(2), 1321-1347.
23. Yadav, K.; Chaware, T. Review of joint encoding and encryption for image transmission using a chaotic map, ldpc, and aes encryption. In Proceedings of the 6th International Conference on Signal Processing, Computing, and Control (ISPCC), Solan, India, 7–9 October 2021.
24. Noshadian, S., Ebrahimzade, A., & Kazemitabar, S. J. (2020). Breaking a chaotic image encryption algorithm. *Multimedia Tools and Applications*, *79*(35), 25635-25655.
25. Majeed, D. A., Ahmad, H. B., Hani, A. A., Zeebaree, S. R. M., Abdulrahman, S. M., Asaad, R. R., & Sallow, A. B. (2024, September 23). Data analysis and machine learning applications in environmental management. *Jurnal Ilmiah Ilmu Terapan Universitas Jambi*, 8(2).
26. Zebari, D. A., Haron, H., Zeebaree, D. Q., & Zain, A. M. (2019, August). A simultaneous approach for compression and encryption techniques using deoxyribonucleic acid. In *2019 13th International*

Conference on Software, Knowledge, Information Management and Applications (SKIMA) (pp. 1-6). IEEE.

27. Xuejing, K., & Zihui, G. (2020). A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system. *Signal Processing: Image Communication*, *80*, 115670.
28. Wang, X., Wang, Y., Zhu, X., & Luo, C. (2020). A novel chaotic algorithm for image encryption utilizing one-time pad based on pixel level and DNA level. *Optics and Lasers in Engineering*, *125*, 105851.
29. Mohammed, Z. K., Mohammed, M. A., Abdulkareem, K. H., Zebari, D. A., Lakhan, A., Marhoon, H. A., ... & Martinek, R. (2024). A metaverse framework for IoT-based remote patient monitoring and virtual consultations using AES-256 encryption. *Applied Soft Computing*, *158*, 111588.
30. Vaseghi, B., Hashemi, S.S., Mobayen, S. and Fekih, A., 2021. Finite time chaos synchronization in time-delay channel and its application to satellite image encryption in OFDM communication systems. IEEE Access, 9, pp.21332-21344.
31. Masood, F., Ahmad, J., Shah, S. A., Jamal, S. S., & Hussain, I. (2020). A novel hybrid secure image encryption based on julia set of fractals and 3D Lorenz chaotic map. *Entropy*, *22*(3), 274.
32. Rathore, V. and A.K. Pal, An image encryption scheme in bit plane content using Henon map based generated edge map. Multimedia Tools and Applications, 2021. 80(14): p. 22275-22300.
33. Basha, S. M., Mathivanan, P., & Ganesh, A. B. (2022). Bit level color image encryption using Logistic-Sine-Tent-Chebyshev (LSTC) map. *Optik*, *259*, 168956.
34. Wang, X., & Liu, P. (2022). Image encryption based on roulette cascaded chaotic system and alienated image library. *The Visual Computer*, *38*(3), 763-779.
35. Sirichotedumrong, W. and Kiya, H., 2019. Grayscale- based block scrambling image encryption using ycbcr color space for encryption-then-compression systems. APSIPA Transactions on Signal and Information Processing, 8.
36. Wang, X., X. Zhu, and Y. Zhang, An image encryption algorithm based on Josephus traversing and mixed chaotic map. IEEE Access, 2018. 6: p. 23733-23746.
37. Alexan, W., ElBeltagy, M., & Aboshousha, A. (2022). Rgb image encryption through cellular automata, s-box and the lorenz system. *Symmetry*, *14*(3), 443.
38. Wang, X., & Li, Y. (2021). Chaotic image encryption algorithm based on hybrid multi-objective particle swarm optimization and DNA sequence. *Optics and Lasers in Engineering*, *137*, 106393.
39. Kang, Y., Huang, L., He, Y., Xiong, X., Cai, S., & Zhang, H. (2020). On a symmetric image encryption algorithm based on the peculiarity of plaintext DNA coding. *Symmetry*, *12*(9), 1393.
40. Tang, Z., Yin, Z., Wang, R., Wang, X., Yang, J., & Cui, J. (2022). A Double-Layer Image Encryption Scheme Based on Chaotic Maps and DNA Strand Displacement. *Journal of Chemistry*, *2022*, 1-10.
41. Li, T., Shi, J., Li, X., Wu, J., & Pan, F. (2019). Image encryption based on pixel-level diffusion with dynamic filtering and DNA-level permutation with 3D Latin cubes. *Entropy*, *21*(3), 319.
42. Ali, T. S., & Ali, R. (2022). A novel color image encryption scheme based on a new dynamic compound chaotic map and S-box. *Multimedia Tools and Applications*, *81*(15), 20585-20609.
43. Zhou, S., He, P., & Kasabov, N. (2020). A dynamic DNA color image encryption method based on SHA-512. *Entropy*, *22*(10), 1091.
44. Jin, X., Duan, X., Jin, H., & Ma, Y. (2020). A novel hybrid secure image encryption based on the shuffle algorithm and the hidden attractor chaos system. *Entropy*, *22*(6), 640.
45. Arif, J., Khan, M. A., Ghaleb, B., Ahmad, J., Munir, A., Rashid, U., & Al-Dubai, A. Y. (2022). A novel chaotic permutation-substitution image encryption scheme based on logistic map and random substitution. *IEEE Access*, *10*, 12966-12982.