Content is available at: CRDEEP Journals
Journal homepage: http://www.crdeepjournal.org/category/journals/ijrem/

International Journal of Research in Engineering and Management
(ISSN: 2456-1029)

Review Paper

A Preliminary Review on Image Encryption Techniques

MD Eqbal Ahmad Shirazi*
Research Scholar in Computer Science Department, Magadh University, Bodhgaya Bihar, India.

ARTICLE DETAILS

Corresponding Author:
Md. Iqbal Ahmad Shirazi

Key words:
Image Encryption Methods, Chaos-Based Image Encryption, Full Encryption Methods, Selective Encryption, Cryptanalysis

ABSTRACT

This paper presents an exhaustive review of research within the field of image encryption techniques. It commences with a general introduction to image encryption, providing an overview of the fundamentals. Subsequently, it explores a comprehensive exploration of chaos-based image encryption, encompassing various methods and approaches within this domain. These methods include full encryption techniques as well as selective encryption strategies, offering insights into their principles and applications. The authors place significant emphasis on surveying prior research contributions, shedding light on noteworthy developments within the field. Additionally, the paper addresses emerging challenges and issues that have arisen as a consequence of these advancements.

1. Introduction

Image encryption, fundamentally defined as the process of transforming a plain image into a coded form that can only be deciphered by its intended recipient[1] has gained increasing importance in response to the growing prevalence of image applications and the transmission of images over the internet and open networks. The critical information embedded within these images necessitates secure protection, making image encryption a vital tool in various domains, including military communications, medical imaging, multimedia systems, and internet communications. [2]While text encryption methods can theoretically be applied to image encryption, practical considerations come into play due to the unique characteristics of images. Images are typically larger in size compared to text, leading to longer encryption and decryption times. Additionally, unlike text, the decrypted image need not be identical to the original, introducing flexibility in image encryption.

The history of cryptography dates back thousands of years, evolving from classical cryptography methods that often involved pen-and-paper techniques to more sophisticated approaches. The development of mechanical and electromechanical devices, such as the Enigma rotor machine in the early twentieth century, marked a significant advancement in cryptography. The subsequent electronic and computational revolutions led to increasingly complex encryption methods. However, these advances in cryptography have paralleled the evolution of cryptanalysis techniques, and methods employed to break encrypted media.

This paper provides an extensive overview of image encryption techniques, focusing on the realm of chaos-based image encryption, which leverages mathematical chaos theory for enhanced security. Chaos-based encryption is particularly well-suited for securing images during transmission over the internet and open networks. It encompasses two primary strat- egies: full encryption and selective encryption. Within this domain, various techniques and approaches are explored, harnessing the power of chaos theory to strengthen encryption algorithms and enhance key security.

* Author can be contacted at: *Research Scholar in Computer Science Department, Magadh University, Bodhgaya Bihar, India.*
Received: 15-3-2024; Sent for Review on: 19-03-2024; Draft sent to Author for corrections: 12-04-2024; Accepted on: 28-04-2024; Online Available from 01-05-2024

Furthermore, this paper delves into the spatial and frequency domain implementations of chaotic-based image encryption methods, offering a comprehensive understanding of their advantages and applications. Throughout the paper, we highlight key image encryption techniques and their contributions to the field.

The structure of this paper is as follows: Sect. 2 provides essential background information to aid in the comprehension of image encryption concepts, along with a review of relevant studies in the field. Section 3 delves into previous studies on image encryption techniques, including a comparative analysis of these approaches. Finally, Sect. 4 presents the overall conclusions drawn from this paper's exploration of image encryption techniques.

2. Cryptography domains

Implementation of a cryptosystem can be done in different domains such as spatial, frequency and hybrid domains. Each of these domains can be explained as follows.

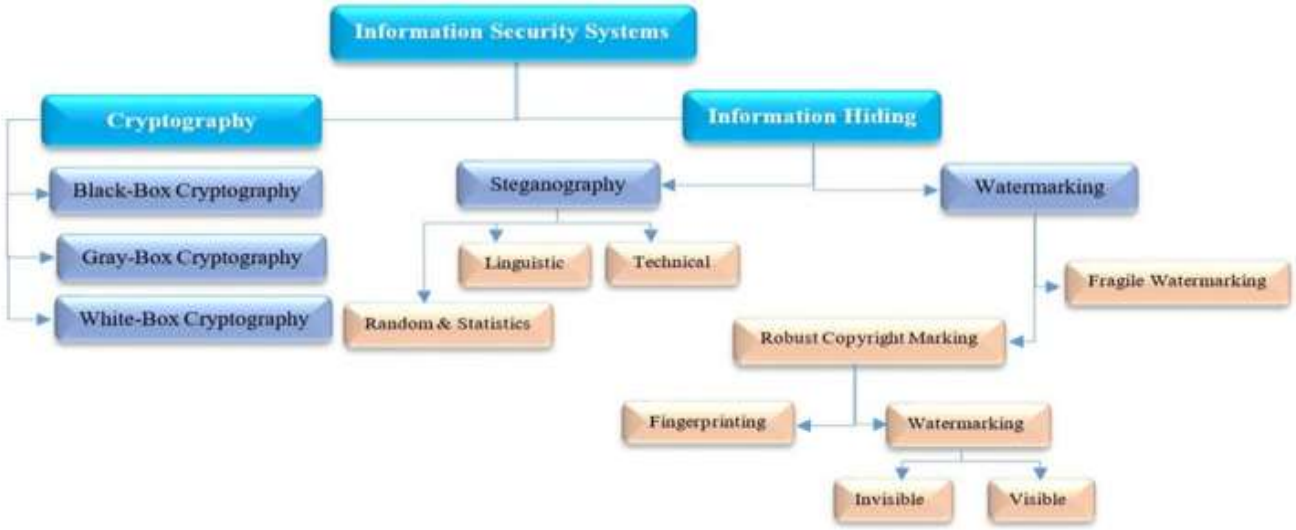

Fig. 1 General classifications for security systems

3. Frequency domain

In frequency domain image analyzed mathematically to series of frequencies, each of these frequencies has two main components which are the amplitude and the phase shift. Any changes in spatial domain image produce an indirect change in its frequency domain repre sentation. The information of the frequency domain is divided into two main components, and these components are high frequency components which represent sharp edges and noise of the plain image while the low frequency component corresponds to the smooth area.

4. Spatial domain

The key cryptosystem, introduced by Habutsu et al.,[3] uses a chaotic-map method to detect statistical attacks and convert text into plain text. It requires a text size of over 73 and a key size of 20 digits. The encryption of text is converted with 2n and sent to the destination. Image encryption is done using scrambling techniques, which mark different points in the original images using an irregular number generator and seeds. The 2-D method, introduced by Bourbakis and Alexopoulos, uses a 1-D list to convert images using different letters of the SCAN language. This method does not use the clamping method but consumes more resources. The distortion of images for encryption purposes was developed by Kuo, adding phase spectra technique to disorder plain images using different key sizes. However, this method does not have compression for images. Pressure and encryption techniques have been used for image encryption, with quadtree and SCAN ling being the most effective.

The encryption algorithm balances certain invertible untidy two-dimensional maps to build new symmetric square encryption plans. The unravelling Algorithm-based encryption of images uses the structure of VLSI, turbulent paired grouping, Lorenz Scientific, and the disorderly Algorithm. These systems provide maximum security when properly used. The piecewise direct-disorderly guide (PWLCM) is proposed in the turbulent cryptosystem by Rhouma et al.,[4] using three vectors to change images into shading and a skew tent. The stage space uses 256 comparisons for accurate and compatible security, with a minimum key length of 1093 and a randomness of 7.9551, indicating minimum disclosure of encrypted information.

Abugharsa et al.[5] proposed a strategy for image encryption that uses filtering lines and segments of the image, which is classified into 3*3 pixels of squares. This method performs better but has low consistency in image scrambling. Image encryption is a useful response to achieving privacy and is more suitable for common images. Zhang and Xiao[6] proposed a novel image encryption arrangement centered on rotation grid bit-level change and square dispersion. Choi et al.[7] proposed an ARX model-based image encryption framework using addition, rotation, and XOR to achieve confusion and diffusion for plain images. Bashir et al. proposed a 4-D chaotic image encryption technique based on dynamic state variables to increase security and effectiveness of chaos-based methods. Kulsoom et al.[8] proposed a new image encryption algorithm based on stream cryptography and uses DNA complementary rules in addition to one-dimensional chaotic map. Kar et al. [9]proposed a bit-plane image encryption method for chaotic, cubic, and quadratic maps, based on permutation, diffusion, and pixel randomization processes. Gu et al.[10] proposed a chaotic-cipher-based packet body encryption algorithm for JPEG2000 images, using bitwise XOR and cyclic rotation operation for a 2-byte block encryption process. Enayatifar et al. [11]proposed an image encryption method based on chaotic map and deoxyribonucleic acid (DNA), converting two-dimensional plain images into one-dimensional arrays, implementing pixel permutation and diffusion simultaneously to reduce sending time.

5. Hybrid domain

The proposed wavelet change and disordered guide for image encryption have been proposed, using wavelet decay for low recurrence sub-band data and XOR for high recurrence data. The Arnold scrambling technique is used for repeated wavelet images, but the execution time is 0.266 seconds. El-Latif et al. propose a mix of direct input move enlists (LFSR) and tumultuous frameworks in half and half spaces, which minimizes image output using dim light and applies cryptographic operations. This technique is suitable for fixed applications and requires an entropy estimation of 7.999 seconds.

Another image compression-encryption half and half algorithm is proposed, which acknowledges pressure and encryption simultaneously, allowing the key to be easily disseminated, stored, or retained. The algorithm uses the spatial space and change area for image encryption, low-pass sub-band coefficients for image discrete wavelet transform (DWT) decay, and dim-scale light for encryption. The algorithm uses a long key size, which can resist animal constraints and differential attacks. The proposed algorithm has attractive encryption capabilities, making it suitable for various applications.

6. Chaos-based image encryption

Chaos-based or chaotic image encryption is an implementation of image encryption depending on mathematical chaos theory. This encryption technique is very safe to encrypt images before the transferring over internet and open networks. The cryptography research- ers made great efforts to obtain a secure and efficient random number generator to encrypt the messages. Chaos theory was discovered in 1969 by Edward N. Lorenz. By 1970, chaos theory has established in many research areas such as physics, mathematic, biology, engi- neering, philosophy, and economics. Because there is no common acceptable mathematical definition for chaos, it can be said the dynamical system is chaotic if it has the following properties:

- It must be topologically mixed.
- It must be very sensitive to initial conditions and control parameters.
- The periodic orbit of the dynamical chaotic system must be dense.

The topologically mixing property is to ensure the chaotic map ergodicity; this means if the state space is partitioned into regions with finite numbers, all map orbits will pass through all of these regions. The sensitivity to the initial conditions and control parameters means any light changes in these inputs should produce output with significant differences. Since the 1990s, researchers in the cryptography field have noticed that there is a close relationship between cryptography and chaos. The difference between chaos and cryptography is chaos is useful in a continuous field while a cryptosystem is implemented in a finite system. Although the cryptosystem and chaos are closely related, many chaos proper- ties such as sensitivity to initial conditions and mixing, actually match with the cryptography properties. Table 1 illustrates the coincide between chaos and cryptography.

7. Image encryption techniques

Recently there have been two main strategies for image encryption which are full encryption and selective encryption. Considering the chaotic encryption which will improve the encryption algorithm by multifaceted encryption techniques in addition to the secret key. Also, there are many chaotic-based image encryption methods implemented in the spatial space while there is another implemented in the frequency domain.

7.1 Full encryption methods

Information protection is the most important issue in the image encryption field. The trade- off between the secrecy of the encrypted image and the time cost has occupied the mind of image encryption researchers. These issues have been distinguished between many techniques implemented in spatial, frequency and hybrid domains in a full image encryption

framework. In full encryption, the used techniques implement the encryption for all image pixels, and there is no priority between the parts of these images for the encryption process. Also, the cipher image has equivalent criteria for all image parts or segments.

7.2 Selective encryption

They completely layered the technique of images, scrambling using the procedures of the standard image and video content which is based on the protection plans. The specified encryption is the procedure for encoding a piece of an object into the bit stream. It includes encoding only a subset of the information. In this manner, specific encryption is every so often called halfway encryption. A basic feature of the specified encryption is the encryption of information about an object that is converted into a bit stream that can decode the encrypted objects using standard decoders. Both scrambled and decoded bits of the layered bit stream may be exactly decoded and appear. Consequently, particular encryption is furthermore suggested as design reliable encryption. With the limit specified encryption, various objectives can be proficient. The specified encryption framework not at all like the full encryption methodology, encodes simply significant districts in the provided image. The principle estimation of the particular/ specified encryption procedure provides computational and other security necessities without tradeoffs [12]. The positive conditions about the specified encryption technique are essentially continuous applications-based, which protect the basic and colossal measure of information turns out to be perhaps the most vital element.

The incomplete image encryption methods are resolved from the way toward isolating the information into perceptually sensitive and obtuse information centred on acknowledgement. Here, we exhibit writing works that tended to the focal essential of an incomplete encryption arrangement, which is that the scrambled district must be free of the decoded ranges. In this way, the proposed plots in the written work will be investigated in the subsequent exchanges that will explore the preface of their proposed approaches. Some- thing else, the proposed procedures of the existing works will be done which is biased on the introduction of the associations between the scrambled and decoded pixels [13]. The incomplete encryption plans show various existing work tries in this characterization to wrap all spaces to be particular, spatial, recurrence, and half-breed. In the following ranges, we will investigate different existing systems from the state-of-the-art studies that are based on the spaces and encryption approaches used. For example, piece and stream Figure.

7.3 Random key generating

The main issue in the random function is the key, which reflects how to start generating random numbers from the beginning without repetition. The random key is considered the first step to start generating other numbers in the series. A key is used to encrypt and decrypt whatever data is being encrypted /decrypted. A program used to generate keys is called a key generator. The secret key is mandatory for encryption algorithms and the success of encryption depends on it, even though it is considered more important than the encryption algorithm itself, this is because of three reasons which are: The encrypted message cannot be decrypted without knowing the correct secret key, brute-force can be hander by increasing the key space size, and encryption with strong key is difficult to be attack and vice versa. The used keys should be absolutely independent of the content of the plain text and the using of different keys lead to producing different cipher text for the same plain text. This can be achieved only by using the correct key. The secret key is divided into a public key algorithm and a private key algorithm. The public key algorithm or asymmetric encryption algorithm uses one key for the encryption process which is called the public key while the second key is used for the decryption process. The public key will be distributed to all net- work users while the decryption key or private key is only owned by the related recipient. In a symmetric key encryption algorithm, the key used in the encryption process is the same key used in the decryption process. Therefore, it is known only by the sender and receiver and it should be maintained. The sensitive issue for the symmetric key is that it should be always secret. Thus, it should be highly protected and shared securely. The implementation of a symmetric key is broadly used in the image encryption field. Figure 2 explains the encryption and decryption process in symmetric and asymmetric encryption algorithms. The public key algorithms need more complex computations; therefore, it is not preferred in the field of multimedia protection.

The key generating methods can be described by the traditional encryption algorithms such as AES, RC4, and RC5. Random number generation is the generation of a sequence of numbers or symbols that cannot be reasonably predicted better than by a random chance, usually through a random- number generator. The distribution of random keys reflects the behaviour of the generated random numbers. The chaotic maps are unpredictable sequences of real numbers which can be normalized to be between 0 and 1. A distribution of values cluster around an aver- age (referred to as the “mean”) is known as a “normal” distribution or it can also be called the Gaussian distribution. In terms of entropy, the quality of image encryption is commonly measured by the information entropy over the cipher text image. The expression of the degree of uncertainty in a system can be measured by the information entropy parameter [14]. Sometimes entropy is defined as the degree of randomness or disorder in the system, therefore information entropy is suitable for use in the evaluation of image encryption systems.

Information entropy indicates the distribution of colors in an image and a good ciphered image is an image with an equal distribution of color values or gray values in grayscale images. According to Stoyanov and Kordov [15] they consider the following assumptions:

"Let us consider that there are 256 values of the information source in red, green, blue, *and grey colors of the image with the same probability. We can get the perfect entropy H(X) = 8, corresponding to a truly random sample".*
The differential analysis is another issue in the field of image encryption. In differential analysis, the cryptanalysis may make a slight change (e.g., modify only one pixel) of the encrypted image, and then observe the change in the result. In this way, he may be able to find out a meaningful relationship between the plain- image and the cipher-image. If one minor change in the plain-image can cause a significant change in the cipher-image, with respect to diffusion and confusion, then this differential attack would become very inefficient and practically useless.

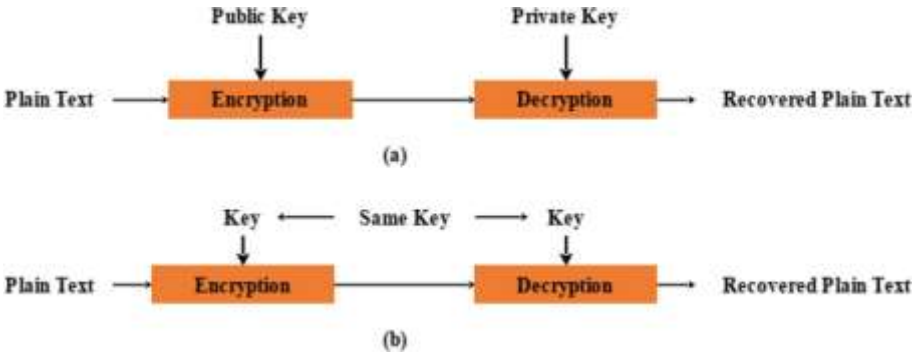

Fig. 2 Encryption key types (**a**) asymmetric key (**b**) symmetric key

8. Random key generating in AES algorithm

Advance Encryption Standard (AES) is a block symmetric cipher designed to be used instead of Data Encryption Standard (DES) and it is adopted for encrypting data in many applications. It has a variable key length of 128,192 or 256 bits and the size of the encrypted data block is 128 bits, the encryption process is within 10, 12, or 14 rounds which depends on the key size. AES encryption algorithm is flexible and fast for the block cipher, it can be implemented in various models such as; CBC, ECB, OFB, CFB and CTR. They work in certain operation modes as a stream cipher. In AES algorithm the key used for encryption is the same used for decryption, and it only accepts block size of 128 bits, therefore AES is considered a symmetric block cipher. There are three versions of the AES algorithm (AES-128, AES-192 and AES 256) each one of these versions has its own name which is driven from the used key size. In addition, the number of needed rounds to implement this encryption algorithm depends on the key size i.e. if the key size is 128 the number of rounds is 10 while for key sizes 192 and 256 the rounds number is 12 and 14 respectively. Figure 3 demonstrates the operation of AES encryption algorithm.

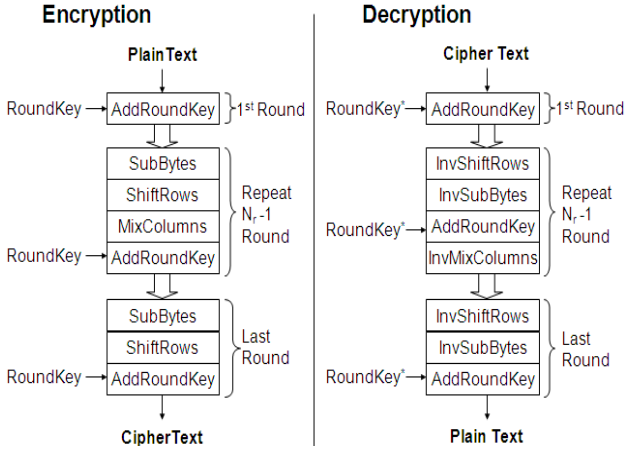

Fig. 3 General flowchart of AES encryption algorithm [16]

are encrypted in this method while four different patterns are used to rescan the insensitive blocks. Based on the importance, and by using edge detection technique each block is classified into significant or insignificant classes. To reduce the computational cost and to maximize the protection for sensitive information this algorithm applies different security levels for each block class. The small predictability level will prevent the attacker from snapping off any information about the cipher

image.

9. Secret key of RC5 and RC6 algorithms

RC5 is considered a parameterized encryption algorithm, RC5 is flexible in both security level and performance characteristics, because in this encryption algorithm, all of the number of rounds, block size, and key size are variables. Simplicity is the most important feature of RC5 and the encryption process is based on three operations: addition, exclusive-or and rotation. Simplicity in design and simplicity in analysis is provided by the RC5 design. In addition, heavy use of the rotations of data-dependent is another characteristic feature in the encryption, and this is very useful in the hindering of linear and differential attacks. Rivest [17] is the official name of the RC5 stream cipher, it is more efficient and more use- able in real-time fields and based on random permutation implementations. According to a different analysis, the period number of the cipher is more than 100. Due to their absolute performance RC4 and RC5 becomes a member of the cryptographic community. The basic flow process of RC5 is shown in Fig. 4.

A partial and fast image encryption technique was proposed by Sasidharan and Philip [18] this technique is based on DWT and RC4 stream cipher. In this technique, the image is converted into a frequency domain using DWT and the approximation matrix (low frequency band) was used to protect the critical image information by implementing RC4 algorithm, the rest image information is shuffled by the using of shuffle algorithm. An XOR operator is implemented between the low-frequency band component and the RC4

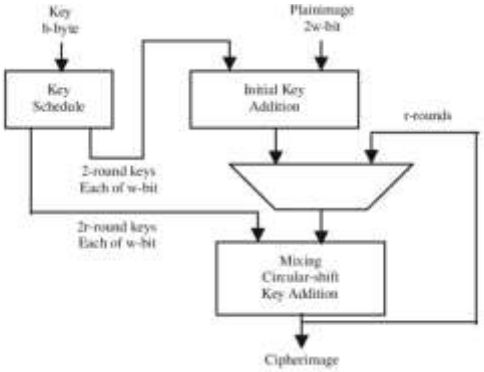

Fig. 4 General block diagram for RC5 algorithm

key stream. Two issues were achieved by implementing this technique, which are reducing the required time by encrypting part of the image and increasing the security by shuffling the rest image. Faragallah [19] use RC5 to encrypt the images by extracting the image header and dividing the image data into 16-bit blocks. RC5 is performed on all 16-bit blocks sequentially until the end of the bit stream of image data. The secret key is developed as n random binary word sequence which consists of three simple algorithms (initialization, mixing and conversion). Table 2 shows a summary of the key space size for AES, RC4 and RC5 encryption Algorithms.

Other researchers suggest their own random generators such as Jallouli et al., [20] pro- posed a new pseudo-random number generator based on three chaotic maps Skewtent, Piece Wise Linear Chaotic (PWLCM) and Logistic maps, these maps are weakly coupled and implemented with a finite precision. A chaotic multiplexing technique is also included. The proposed pseudo-random number generator is achieved by iterating three chaotic maps which are Skewtent, PWLCM and Logistic maps by coupling them weakly with a coupling matrix. Also, a technique of chaotic multiplexing is used. The proposed pseudo-random number generator uses three initial conditions (one for each map) also the control parameters for the used maps and coupling matrix must be specified. All of the initial conditions and control parameters are initiated by the use of the Linux kernel.

New pseudo-random number generator algorithm proposed by Hanis et al., [21] the new key is generated by using a novel modified convolution and chaotic mapping technique. First of all, the initial condition and control parameters for the logistic map are specified to generate two random sequences, after that a convolution process is implemented on these two generated sequences to produce a new random sequence. The convolution is done on the binary sequences; therefore, it can be said the process is a binary convolution.

The distribution of random keys reflects the behaviour of the generated random numbers. The chaotic maps are unpredictable sequences of real numbers which can be normalized to be between 0 and 1. A distribution of values cluster around an average (referred to as the “mean”) is known as a “normal” distribution or it can also be called the Gaussian distribution.

10. Cryptanalysis

Cryptanalysis can be defined as a technique used by attackers or hackers to break coded data without prior knowledge about the used key. Cryptanalysis is derived from the Greek word kryptós which means "hidden" and the word analýein which means "to untie" or "to loose". It is used to decrypt the cipher information by analysing the flow in the used algorithm to understand the hidden aspect included in the system.

Friedrich Kasiski is considered the first one who broke the Vigenere cipher during World War I. Before that, the Vigenere cipher was used for about two centuries to communicate securely. To hander the cryptanalysis attacks asymmetric cipher was introduced in the last decades. In this type of cryptography, there are two keys (private and public keys) and the key increased dramatically as in 1980 the key space was 150 digits then early in the twenty-first century the key space increased to 700 digits. After the end of the world war, all governments had their own agency or cryptographer team that was responsible for the decoding of cipher messages by implementing the cryptanalysis methods.

11. Some of the techniques used in image encryption

Two chaotic maps are used in some works. The chaotic logistic map is modified to be more suitable to the proposed method. Sensitive Logistic Maps (SLM) and Hénon Maps in addition to additive white Gaussian noise are used in the proposed confusion method while in the diffusion method, the Bernoulli map is modified to Extended Bernoulli Map (EBM) and Tinkerbell, Burger, Ricker maps are used to obtain random sequences with better criteria. The following sections explain the chaotic maps and additive white Gaussian noise used in the proposed framework.

- Chaotic logistic map
- Hénon map
- Additive white gaussian noise (AWGN)
- Bernoulli map
- Tinkerbell map
- Burgers map
- Ricker map

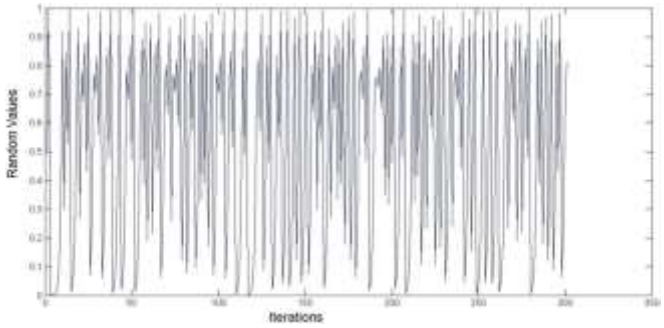

Fig. 4 The behavior of logistic map

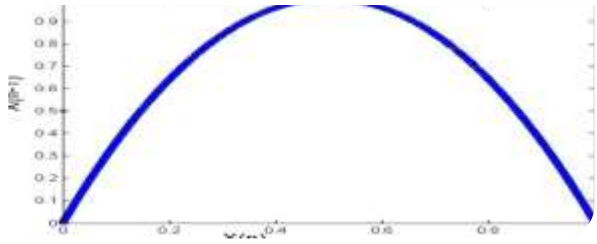

Fig. 5 The cobweb diagram of the logistic map. The previous studies on image encryption techniques

While we acknowledge that there have been previous reviews on image encryption techniques, it's important to note that our paper takes a unique and innovative approach to this subject matter. In addition to referencing and building upon the existing works presented in our study stands out by introducing a novel classification framework. We categorize the reviewed papers

based on several critical factors, including the domain, methodology, dataset utilized, performance metrics, and the valuable insights and remarks provided by the original authors. This approach allows us to provide a comprehensive and differentiated perspective on the state of image encryption techniques. Several traditional image encryption techniques will be summarized in this section, this discussion will focus on the full image encryption frameworks. As mentioned earlier full image encryption type divided into spatial, frequency and hybrid domains and in This addition will enhance the validity and reliability of our findings, ultimately contributing to a more comprehensive review of the selected encryption methods.

12. The previous studies on image encryption techniques

While we acknowledge that there have been previous reviews on image encryption techniques, it's important to note that our paper takes a unique and innovative approach to this subject matter. In addition to referencing and building upon the existing works presented in [22,23], and [24], our study stands out by introducing a novel classification framework. We categorize the reviewed papers based on several critical factors, including the domain, methodology, dataset utilized, performance metrics, and the valuable insights and remarks provided by the original authors. This approach allows us to provide a comprehensive and differentiated perspective on the state of image encryption techniques. Several traditional image encryption techniques will be summarized in this section, this discussion will focus on the full image encryption frameworks. As mentioned earlier full image encryption type divided into spatial, frequency and hybrid domains will be summa- rized to show brief explanation for are summarized as hybrid techniques. This addition will enhance the validity and reliability of our findings, ultimately contributing to a more comprehensive review of the selected encryption methods.

13. Conclusion

In this comprehensive review, we have explored a wide array of image encryption techniques, each designed to safeguard sensitive image data from unauthorized access and ensure its confidentiality and integrity. These techniques span various domains, including spatial, frequency, and hybrid domains, each offering unique advantages and challenges. In the spatial domain, we observed innovative approaches that utilize chaotic maps block shuffling, pixel substitution, and advanced encryption algorithms such as AES. These techniques excel in terms of speed, resistance to statistical attacks, and key sensitivity, making them suitable for real-time applications. Furthermore, they offer robust protection against brute-force attacks, ensuring the security of encrypted images.

Frequency domain techniques introduced rotations, phase masks, and affine transforms to achieve image encryption. Notable characteristics of these methods include fast encryption speeds, high security levels, and the use of transformation parameters as encryption keys. These techniques exhibit key sensitivity and resistance to various forms of attacks, solidifying their efficacy in safeguarding image data.

Hybrid domain techniques combined the strengths of both spatial and frequency domains, employing methods such as Discrete Wavelet Transform (DWT), S-box encryption, Arnold diffusion, and logistic map permutation. The advantages of these techniques include fast encryption processes, acceptable key spaces, and high-security levels. They exhibit robustness against differential and entropy-based attacks, making them valuable choices for image encryption.

Our review also highlighted the importance of selecting an appropriate dataset for evaluating the performance of these encryption techniques. The SIPI dataset, with its diverse range of image specifications, proved to be a valuable resource for assessing the quality and effectiveness of the encryption methods discussed in this paper.

In conclusion, image encryption is a vital component of data security in today's digi- tal age. The techniques presented here demonstrate a rich landscape of methods and approaches to protect sensitive image data from unauthorized access and malicious attacks. The choice of encryption method should be carefully tailored to the specific requirements of the application, ensuring a balance between security and computational efficiency. As technology continues to advance, the field of image encryption will evolve further, and researchers will continue to innovate to meet the growing demands for image data security. The findings presented in this review provide a valuable resource for researchers, practitioners, and decision-makers seeking to implement effective image encryption solutions in various domains. The ongoing pursuit of stronger, more efficient, and highly secure image encryption techniques remains essential to safeguarding the confidentiality and integrity of valuable visual data in an increasingly interconnected world.

14. Funding

This paper received no specific grant from any funding agency in the public, commercial, or not- for-profit sectors. Data availability Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

15. Conflict of interest

We certify that there is no actual or potential conflict of interest in relation to this manuscript.

16. References

1.Divya V, Sudha S, Resmy V (2012) Simple and secure image encryption. Int J Comput Sci Issues (IJCSI) 9(6):286
2. Pakshwar R, Trivedi VK, Richhariya V (2013) A survey on different image encryption and decryption techniques. Int J Comput Sci Inform Technol 4(1):113–116
3. Habutsu T, Nishio Y, Sasase I, Mori S (1991) A secret key cryptosystem by iterating a chaotic map. In Advances in Cryptology—EUROCRYPT'91: Workshop on the theory and application of cryptographic techniques Brighton, UK, April 8–11, 1991, Proceedings 10. Springer, Berlin, Heidelberg, pp 127–140
4. Rhouma R, Arroyo D, Belghith S (2009) A new color image cryptosystem based on a piecewise linear chaotic map. In 2009 6th International Multi-Conference on Systems, Signals and Devices. IEEE pp 1–6
5. Abugharsa AB, Almangush H (2011) A new image encryption approach using block-based on shifted algorithm. Int J Comput Sci Netw Secur (IJCSNS) 11(12):123–130
6. Zhang Y, Xiao D (2014) An image encryption scheme based on rotation matrix bit-level permutation and block diffusion. Commun Nonlinear Sci Numer Simul 19(1):74–82
7. Choi J et al (2016) A fast ARX model-based image encryption scheme. Multimed Tools Appl 75(22):14685–14706
8. Kulsoom A, Xiao D, Abbas SA (2016) An efficient and noise resistive selective image encryption scheme for gray images based on chaotic maps and DNA complementary rules. Multimed Tools Appl 75(1):1–23
9. Kar M et al (2016) Bit-plane encrypted image cryptosystem using chaotic, quadratic, and cubic maps. IETE Tech Rev 33(6):651–661
10. Gu G et al (2016) A chaotic-cipher-based packet body encryption algorithm for JPEG2000 images. Signal Process: Image Communication 40:52–64
11.. Enayatifar R et al (2017) Image encryption using a synchronous permutation-diffusion technique. Opt Lasers Eng 90:146–154
12. Chen J-X et al (2015) Analysis and improvement of a double-image encryption scheme using pixel scrambling technique in gyrator domains. Opt Lasers Eng 66:1–9
13. Suresh V, Madhavan CV (2012) Image encryption with space-filling curves. Def Sci J 62(1):46
14. Shannon CE (1949) Communication theory of secrecy systems. Bell Syst Tech J 28(4):656–715
15. Stoyanov B, Kordov K (2015) Image encryption using Chebyshev map and rotation equation. Entropy 17(4):2117–2139
16. Duta CL, Michiu G, Stoica S, Gheorghe L (2013) Accelerating encryption algorithms using parallelism. In 2013 19th international conference on control systems and computer science. IEEE pp 549–554
17. Rivest RL (1994) The RC5 encryption algorithm. In: International workshop on fast software encryption. Springer, Berlin, Heidelberg, pp 86–96
18. Sasidharan S, Philip DS (2011) A fast partial image encryption scheme with wavelet transform and RC4. Int J Adv Eng Technol 1(4):322
19. Faragallah OS (2011) Digital image encryption based on the RC5 block cipher algorithm. Sens Imaging: An International Journal 12(3):73–94
20. Jallouli O, et al. (2016) An efficient pseudo chaotic number generator based on coupling and multiplexing techniques. in International Conference on Emerging Security Information, Systems and Technologies (SECUR WAR E 2016)
21. Hanis S, Amutha R (2018) Double image compression and encryption scheme using logistic mapped convolution and cellular automata. Multimed Tools Appl 77(6):6897–6912
22. Kaur M, Kumar V (2020) A comprehensive review on image encryption techniques. Arch Comput Methods Eng 27:15–43
23. Abdullah RM, Abrahim AR (2022) Review of image encryption using different techniques. Acad J Nawroz Univ 11(3):170–177
24. Sajitha A, Rekh AS (2022) Review on various image encryption schemes. Mater Today: Proceedings 58:529–534