Misan Journal of Engineering Sciences ISSN-E: 2957-4250
Vol. 4, No. 1, June 2025 ISSN: 2957-4242

Medical Image Encryption Techniques: A Review

Zainab S.Husamuldeen[1*], Tariq M.Salman[2] and Abbas H.Miry[3]

[1, 2,3] *Department of Electrical Engineering, College of Engineering, University of Mustansiriyah, Baghdad,10052, Iraq*
** Corresponding author E-mail:: zainabsalah4488@uomustansiriyah.edu.iq*

(Received 18 Jan, Revised 21 April, Accepted 9 May)

Abstract: In the majority of hospitals and clinics, doctors currently employ medical images, including brain MRIs, ultrasounds, and X-ray images, to diagnose a variety of severe diseases. Image encryption is critical for safeguarding data confidentiality from fraudulent use and illegal access in eHealth applications. Chaos is an exceptionally powerful cryptographic resource since its inception in image-encryption methods. This work offers a comprehensive overview of the evolution of algorithms for image encryption based on chaos theory, including both symmetric and asymmetric approaches. This research is distinguished from previous review research, which addressed many varied methods of chaos-based image encryption and focused on theoretical aspects only; these techniques could be used in digital medical records of hospital patients and telemedicine communication. This analysis revealed that the most favorable outcomes were presented in the method using the Blum-Goldwasser Cryptosystem (BGC) and Elliptic Curve Cryptography (ECC) with NPCR of 99.6901% and UACI of 33.694%. The review demonstrated that these algorithms offer robust security and intricacy regarding keys. However, certain studies have identified challenges associated with the complexity of keys and the time required for implementation in real-time. The paper suggests that the efficacy of algorithms should be enhanced and evaluated on a broader scale than image types. It begins with a comprehensive introduction to image encryption, which addresses the fundamental concepts. Then, it conducts a thorough examination of chaos-based image encryption, that encompasses a variety of methods and approaches within this field.

Keywords: Chaos, Chaotic Map, Medical Image Encryption, Security, Permutation-Diffusion, Cryptography

1. Introduction

Due to the recent social distancing of the world's population, telemedicine has drawn the interest of academics and industry professionals. Extensive studies have been done on giving medical treatment to patients far from medical professionals. Digital photographs containing sensitive medical data are necessary for diagnosis and decision-making. Images from tests, such as computed tomography (CT) analyses, ultrasounds, X-rays, cerebral imaging, and magnetic resonance imaging (MRI), can hold sensitive and important data for patients and medical facilities [1-7].

Medical records are being widely stolen by hackers and other unapproved parties, who then sell them to merchants on the dark web [8], [9]. The sensitive data was then exploited fraudulently for identity theft. Over the previous ten years, the medical history of the United States (US) has revealed around 3000 breaches, each of which included over 500 compromised sensitive medical records [10], [11]. For instance, a $115 million settlement is shown [12] on account of a breach involving the medical data of 78 million American clients of Anthem, a medical insurance firm [13]. Patient data security is crucial since unauthorized access to such information can have catastrophic consequences [14]. Medical image retention and transfer necessitate confidentiality, legitimacy, and integrity as preconditions [15].

DOI: https://doi.org/10.61263/mjes.v4i1.133

Thankfully, medical images scrambling to meet encryption requirements can use cryptography algorithms to guarantee the necessary security requirements. The main foundation of early image encryption techniques was commercial data encryption technologies [16], [17], including data encryption standards (DES) and advanced encryption standards (AES). These methods, however, have been demonstrated to have poor anti-attack and efficiency levels; these techniques need substantial storage and computing resources, rendering them impractical for encrypting high-volume medical imaging data. These are the challenges and issues encountered by these methods. In the literature, additional sophisticated techniques have been presented to improve encryption efficiency [17-19].

For that reason, possessing a robust encryption mechanism is crucial. The implementation of chaos-based encryption methods ensures the security of picture encryption. Chaotic systems are excellent alternatives for secure encryption due to their ergodicity and highly complex behavior [20]. Picture encryption uses two different varieties of chaotic systems: "one-dimensional" (1D) and "high-dimensional" (HD) chaotic systems [21]. Because of its straightforward design, which maximizes resource efficiency and minimizes key space, the 1D chaotic map seems advantageous. Despite being facility-forceful and complex, HD chaotic maps have many critical spaces [22-24]—Figure 1 types of image encryption schemes.

This paper intends to investigate and assess chaos-based encryption algorithms for medical imaging, comparing their results with regard to NPCR and UACI, as well as for security and efficiency. Organisation of the paper: The other parts of the article are regulated in the following manner: Section 2 compares chaos-based encryption with traditional encryption, Section 3 describes the preceding works featuring a chaotic system, and Section 4 discusses a chaotic system used in image encryption. In Section 5, we first do a literature review that explains work related to image encryption techniques and then summarize it. Section 6 describes the assessment of security then, and Section 7 illustrates the conclusions.

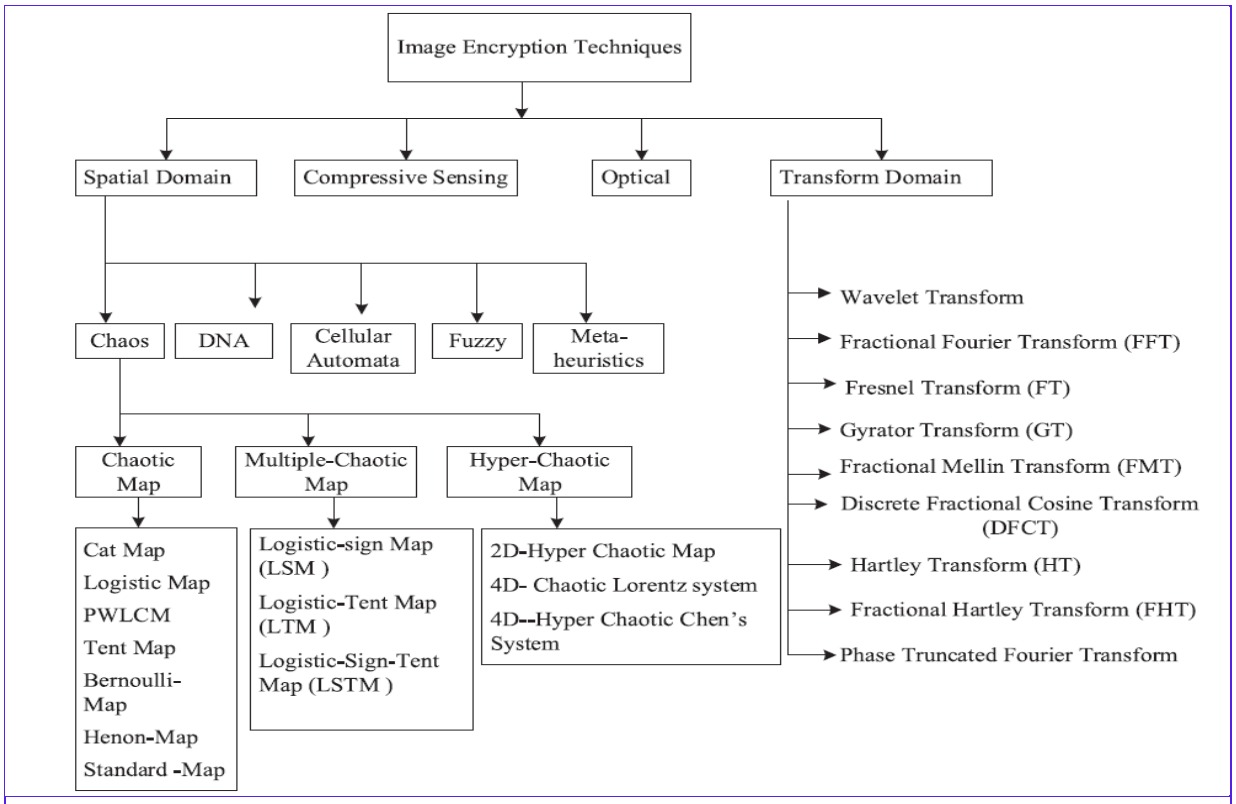

Fig. 1. Types of image encryption schemes (modified from [25]).

2. Comparison of Chaos-Based Encryption and Traditional Encryption

2.1 Mathematical Basis

AES and DES are conventional encryption algorithms that operate on fixed-size data blocks (e.g., 64 or 128 bits) based on linear algebra, logical permutations, and structured substitution and permutation steps [26].

In contrast, chaos-based encryption schemes are based on mathematical chaotic maps containing the Logistic Map, Lorenz System, and Chen Map. They rely on nonlinear dynamical systems. These systems are extremely susceptible to initial conditions and parameters, rendering them appropriate for generating pseudo-random sequences for encryption [27].

2.2 Level of Security

Traditional algorithms, such as AES, are well-established security measures intended to withstand assaults, including brute-force and differential cryptanalysis. Nevertheless, new technologies, such as quantum computation, have led to new [28].

Chaos-based systems offer robust security because chaotic sequences are unpredictable and highly sensitive to initial parameters. However, their security is contingent upon the appropriate selection of chaotic maps and the critical space design [29].

2.3 Performance and Speed

AES is known for its rapidity and efficacy, particularly when enhanced with hardware acceleration. Conversely, chaos-based methodologies sometimes include floating-point calculations and intricate iterations, resulting in diminished performance, especially with large image collections [30].

2.4 Image Encryption Flexibility

Generally, conventional methods treat images as binary sequences, potentially leading to the loss of spatial correlation in image data. By directly integrating pixel positions and values, chaos-based techniques provide greater flexibility, maintain spatial structure, and enhance resistance to assaults [31].

2.5 Standardisation and Mathematical Complexity

Traditional encryption algorithms are mathematically well-studied and standardised, with well-known security proofs (e.g., by NIST). In contrast, chaos-based algorithms are more difficult to analyse and less standardised due to their sensitive dependence on parameters and nonlinearity [32].

2.6 Integration with Artificial Intelligence

Conventional encryption techniques like AES and RSA depend on static key frameworks and inflexible algorithms, complicating their integration with artificial intelligence. Their unchanging nature restricts flexibility in fluid contexts. Conversely, chaos-based encryption solutions provide superior compatibility with AI, enabling neural networks to create or modify keys dynamically, hence improving flexibility and security, particularly in image encryption [33].

3. Overview Of Chaotic Systems

Chaos is a pseudo-random and unexpected behavior seen in a deterministic dynamical system due to its extreme sensitivity to initial conditions and parameters. H. Poincaré's 1913 investigation of the three-object problem served as the foundation for the analysis of chaos theory. The Lorenz equation is the pioneering example of a dissipative system with a chaotic solution to a preordained equation. It was proposed by E. N. Lorenz [34] in 1963 following a number of research studies. Tienyien Li and James A. Yorke [35] originally instituted the word "chaos" to characterize this occurrence in their 1975 work "Period Three Implies Chaos" [36], [37].

3.1 Chaotic Map Theory

Image encryption based on chaos using one-dimensional and multi-dimensional maps. Because of their intricate structure and plenty of parameters, multi-dimensional chaotic maps enhance photo encryption security, but they also make the process more challenging to execute. The first chaotic block cipher algorithm was published by Habutsu et al. in 1991. However, Matthews used chaos to encrypt data for the first time in the late 1980s. Baptista released a disorganized encryption system in 1998. Furthermore, Friedrich said that the image encryption technique should be repeated in two steps in order to get a high-security rank, and diffusion and permutation should be used. A substantial association exists between nearby pixels, and the permutation phase is required to minimize this correlation [38]. Pixel and bit-level permutation techniques are separated into two groups. The diffusion phase is in charge of altering pixel values to prevent the attack and create an oscillating behavior [39]. Almost all ideas for chaos-based image encryption stem from one of two things: (i) the possibility of less computing work than normal encryption, and (ii) concerns about possible security problems when using classical ciphers on pictures [40, 41].

3.2 Brief Types of Chaotic Systems

Discrete chaotic mappings and continuous chaotic systems are the two categories into which chaotic systems can be divided according to how they alter over time. A continuous chaotic system is characterized by dynamical equations that typically comprise an ensemble of differential equations, and in that, dynamic changes occur in the system's status across time. On the other hand, a system with a discrete time evolution of state and an iterative dynamical equation is known as a discrete chaotic map [37]. Below are some examples of discrete chaotic mappings along with their mathematical explanations to help you better understand:
Logistic map [42]:

$$X_{t+1} = f_t(X_n) = pX_t(1 - X_t) \quad (1)$$

Let p ∈ [0, 4] denote a management parameter, $(1-X_t)$ represent the component that constrains the system's growth, and $X_t \in (0, 1)$ signify the state element at time step t. While the parameter ρ falls with in the duration (3.57, 4], the Logistic map displays intricate dynamic behavior, as shown in Figure 2.

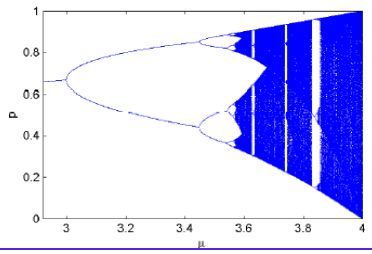

Fig. 2. Chaotic performance of the logistic system (modified from [43]).

Tent map:

$$X_{t+1} = f_t(X_n) = \begin{cases} pX_t, & X_t < \frac{1}{2} \\ pX_t(1 - X_t) & , \quad \frac{1}{2} \leq X_t \end{cases} \tag{2}$$

At time step t, the state variable is denoted as X_t, and the control parameter p is within the interval [0, 2]. The map is divided linearly into a tent-like shape.
Henon map [44]:

$$\begin{cases} X_{t+1} = 1 - aX_t^2 + Y_t \\ Y_{t+1} = b\,X_t \end{cases} \tag{3}$$

A and b represent control parameters, while X_t and Y_t denote the state elements at time step t. The Henon map is a dissipative nonlinear system with intricate dynamics.

The mathematical concept of a discrete chaos map is very simple, enabling ease of implementation and calculation. Nonetheless, its parameter range is often inadequate, and selecting inappropriate settings may rapidly compromise the system's dynamic characteristics.

Below are instances of continuous chaotic systems together with their respective geometric formulations:
Lorenz equation [36]:

$$\begin{cases} \frac{dx}{dt} = \sigma(y - x) \\ \frac{dy}{dt} = \rho x - y - xz \\ \frac{dz}{dt} = xy - \beta z \end{cases} \tag{4}$$

σ stands for the Prandtl number, ρ for the Rayleigh number, and b β for the direction ratio; these are the control parameters. Whereas x, y, and z denote state elements.
Chen system [45]:

$$\begin{cases} \frac{dx}{dt} = a(y - x) \\ \frac{dy}{dt} = (c - a)x - xz + cy\,, \\ \frac{dz}{dt} = xy - bz \end{cases} \tag{5}$$

The management parameters are denoted by the letters A, B, and C, whereas the state variables are named x, y, and z. The Chen system furthermore features two unstable equilibrium points and a chaotic attractor. They have the benefit of offering more flexibility and deeper dynamic behavior. Still, they also have the drawback of requiring more sophisticated mathematical models, higher processing power, and discretization to fit real-world applications [37].

3.3 Tests of Chaotic Behavior

The Lyapunov exponent (LE) and zero-one (0-1) tests evaluate the chaotic nature of a dynamical system.

3.3.1 Lyapunov Exponent

LE Λ quantifies the sensitive dependency on the initial conditions. It describes the average rate at which two nearby paths in the state region diverge or converge, Eq.(6) [46-48].

$$\Lambda = \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \log_2 \frac{X(n)}{X(0)} \tag{6}$$

Where N = 1, 2, 3 is the matching orbit, on the other hand, the starting condition is X (0). It is possible to calculate the LE for specimen locations that are close to the attractor in order to derive an average LE. A chaotic system is one in which at least one of the LE is positive, perhaps more than one. When the Lyapunov Exponents are positive, the system is said to be in a positive state. Exhibits chaos. Sixteen, at which point the LE is negative, the system exhibits periodicity [47]. Moreover, a bifurcation happens when the LE is zero. A greater LE value indicates a more chaotic system [49], [50].

3.3.2. 0-1 Test

The following is a description of the 0-1 test's primary steps [51]:

1. Let D(n) denote a set of one-dimensional data taken at time n, where n = 1, 2, ..., N.
2. Choose R if it is a real, positive number.
3. Determine Q(n) and P(n):

$$P(n) = \sum_{j=1}^{n} D(j)\cos(jR), \tag{7}$$

$$Q(n) = \sum_{j=1}^{n} D(j)\sin(jR) \tag{8}$$

4. Use these steps to calculate the mean square displacement (MSD):

$$\mathrm{MSD(n)} = \lim_{N\to\infty} \frac{1}{N}\sum_{j=1}^{n} [P(j+n) - P(j)]^2 + [Q(j+n) - Q(j)]^2 \tag{9}$$

5. The estimated average growth is

$$K_c = \frac{\log MSD(n)}{\log n} \tag{10}$$

Next, determine the final value of K by computing the middle point of these values. The value of K dictates the system's chaotic nature. When K equals 0, it signifies the system is habitual; however, when the magnitude of K approaches 1, it exhibits chaotic characteristics [49], [52].

4.1 Chaotic System for Image Encryption

An application of image encryption based on computational chaos theory is called chaos-based or chaotic image encryption. This method is quite safe when encrypting photographs before uploading them over public networks and the internet. In order to encrypt the messages, the cryptography researchers worked very hard to develop a reliable and secure random number generator. Edward N. Lorenz discovered chaos theory in 1969. In numerous fields of study, including physics, mathematics, biology, engineering, philosophy, and economics, chaos theory was established in 1970 [53]. Figure 3 displays a permutation diffusion chaotic architecture image encryption.

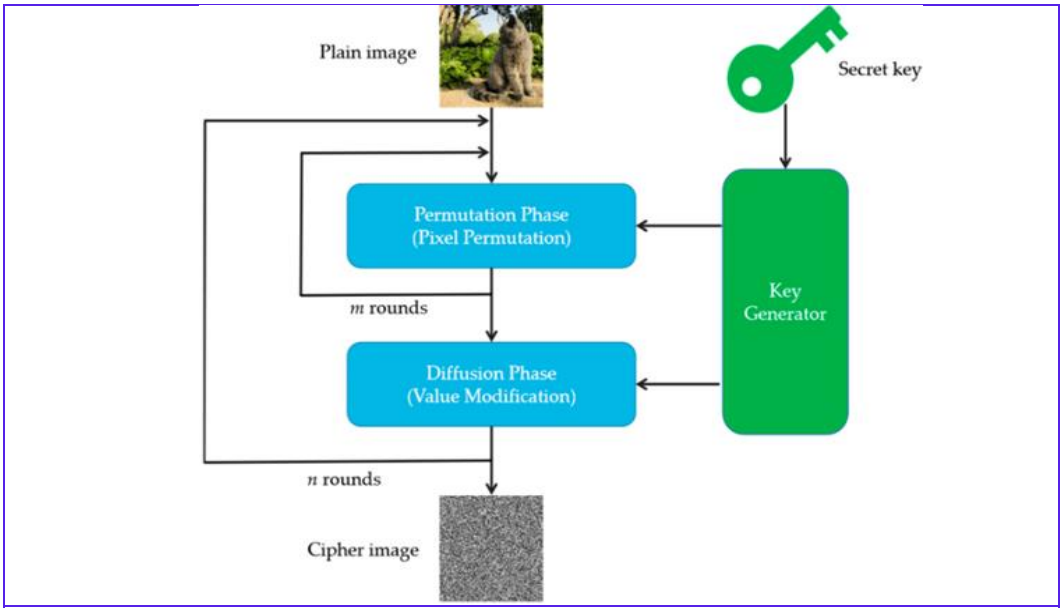

Fig. 3. Permutation–diffusion chaotic architecture image encryption (modified from [37]).

The two primary groups into which encryption techniques can be partitioned are symmetric and asymmetric processes. With symmetric encryption, a single key is necessary to secure an image. In contrast, asymmetric methods require two different keys to be kept [54]. Figure 4 depicts the core process of medical picture encryption. Implementing asymmetric encryption takes longer, but it is better than symmetric encryption [55].

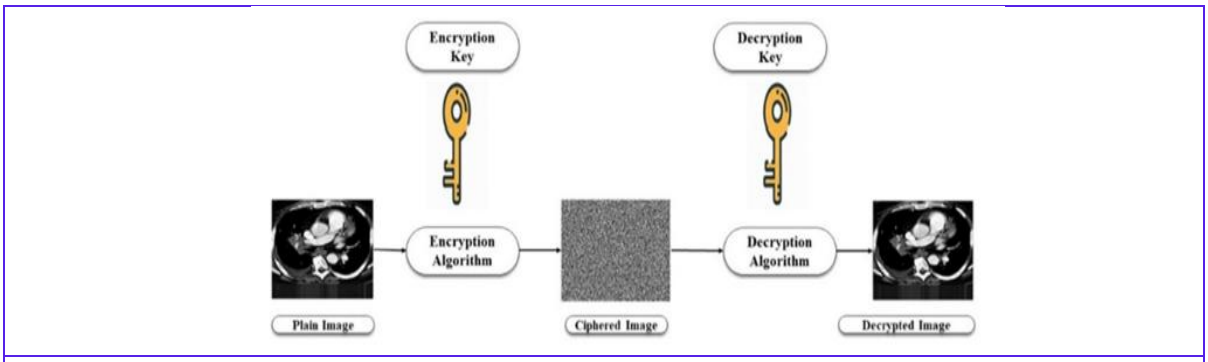

Fig. 4. The fundamental process to achieve the encryption and decryption of medical images (modified from [55])

4.2 Confusion and Diffusion

In his well-known work, "Communication Theory of Secrecy Systems,"[56] Shannon proposed a diffusion and confusion process to create the perfect security system. This proposal's primary objective is to prevent statistical attacks. In image encryption, the expression "diffusion process" refers to the alteration of image pixel values to a degree that effectively diffuses the incidences of these plain image pixels over several cipher image pixel values. This results in a cipher image devoid of statistical features like information entropy or a histogram. To make a statistical attack meaningful, a greater number of cipher images is required.

The location of the picture pixels will be altered during the confusion phase to break the connection between the plain and cipher images. The confusion procedure denotes that the key and the cipher image are not exclusively linked and that every pixel in the cipher image must depend on a key segment [53].

5. Literature Review

Wang Xing-yuan (2013) examined a technique in which the initial image intended for encryption is first rearranged utilizing a one-dimensional logistic map. The motivating system is chosen to be a two-dimensional chaotic system, and a tent map is used in order to ascertain the beginning value for the outcome of the one-dimensional logistic map. Ultimately, following multiple repetitions, the secret key necessary for encryption is obtained. The system attained a UACI of 37.6825% and an NPCR of 99.6537% [57].

Ashutosh Gupta et al. (2015) submitted a picture encryption scheme utilizing a one-dimensional logistic map. The encryption procedure relies on a 256-bit secret key. The system's starting state is established through an external action utilizing the secret key. This encryption design has been shown to improve randomness [58].

Tahir Sajjad Ali et al. (2020) introduced an article encryption method for medical images that satisfies the encryption standards for transmitting confidential medical data. Hybrid cryptography's combining technique makes creating new schemes for encrypting medical pictures easy. It employs elliptic curves and public key cryptography to produce an encrypted secret key. According to the proposed method, medical images are encrypted using chaotic maps and elliptic curves. A single package offers a digital signature, chaotic picture encryption, and a method for exchanging keys. The patient generates a symmetric encryption key with his particular key and the healthcare authority's public key. Then, for medical symmetric picture encryption based on chaos, he uses the hash value of this key. Using the same key, the healthcare authority decrypts the data. The hash value relating to the cipher picture is signed and exchanged to confirm the communication's legitimacy. The NPCR experimental value is 99.6189%, and the UACI experimental value is 33.5643% [13].

Xuehong Wang et al. (2020) proposed an encryption method utilizing chaos during transmission and application. Subsequently, the proposed decryption method facilitates authentication for patients and telemedicine personnel. This method employs the Qi 3-D four-wing chaotic system. The proposed method integrates chaotic dynamics with novel cryptography, yielding more intricate and unpredictable keys than those derived from current cryptographic techniques. The presented method is proven against differential and brute-force attacks utilizing digitized medical images. The original image is converted into a chaotic form impervious to all kinds of assault by thoroughly erasing the pixels using the cat map and diffusing the image's sub-blocks. The study results reveal that the proposed method exhibits superior performance but necessitates increased computational resources for decryption. The experimental evaluation confirmed that the novel encryption strategy improved the security of encrypted images by significantly diminishing the superfluity and correlation of nearby pixels compared to the ACM method. Results from the experiments showed that UACI was 30.3% and NPCR was 99.6% [43].

Chia-Hung Lin et al. (2021) suggested a method for the encryption and decryption of medical images by analyzing intelligent symmetric cryptography using a chaotic map and a quantum-based key generator (KG). The technique of the system is outlined as follows: (1) Generation of arbitrary cipher codes, (2) formulation of an encryptor and a decryptor using gray relational analysis (GRA), and (3) assessment of the decrypted image. Using a hybrid chaotic map and quantum-based KG amplifies chaotic complexity and unpredictability, producing 256 key-space cipher codes for pixel replacement in a two-dimensional image. The cipher codes are formulated using the primary and secondary GRA models to construct an encryptor and a decryptor. The experimental data indicate that UACI is 31.92% and NPCR is 99.45%[59].

Arslan Shafique et al. (2021) introduced a picture encryption system designed to withstand noise, focusing on the encryption of medical images on a bit level instead of a pixel level. This approach utilizes a bit-plane extraction technique, a cubic logistic map, and the Discrete Wavelet Transform (DWT). The proposed work consists of three distinct parts: the image is encrypted in the spatial domain in both the initial and final sections, while the central section focuses on frequency domain encryption utilizing DWT. Furthermore, the proposed encryption method demonstrates UACI and NPCR values surpassing 33% and 99.4%, respectively[60].

Behrouz Vaseghi et al. (2021) developed a unique and efficient finite-time synchronization technique

for chaotic systems, examining its possible use in encrypting medical photographs. In light of this, a rapid, flexible terminal sliding mode tracking controller was devised to effectively synchronize chaotic systems at both the transmitter and receiver ends. The suggested approach was executed using chaotic keys and a combination of chaotic encryption methods, including chaotic MORE and XOR operations, to improve the security of medical image transmission and storage. The fundamental objective of the proposed method was to adequately maintain the retrieved medical image's quality while eliminating all remnants of the original medical image during transfer or storage. The suggested methodology was evaluated by analytical and simulation tests. The findings revealed a rapid convergence rate, strong robustness, and ease of implementation of the presented technique. Moreover, the findings indicated that the proposed cryptosystem exhibited a commendable level of protection against various attacks. The experimental results for UACI are 33.6120%, and NPCR is 99.6281% [61].

Sara T. Kamal et al. (2021) introduced a new technique for encrypting medical images using chaos and image blocks to encrypt color and grayscale images. Image blocks have been introduced as a new way to divide photographs. The image chunks were then irregularly permuted, rotated, and arranged in a zigzag pattern. Next, a disorganized logistic map produces a key to decipher the messy picture. They assessed the efficacy of our suggested method for encrypting medical images by examining their time complexity and security attributes. They analyzed entropy, correlation coefficient, PSNR, keyspace, histogram differential attacks, sensitivity, and additional security metrics. The findings indicated that grayscale and color medical picture encryption attained significant security and performance. They moreover contrasted our strategy with alternative encryption techniques. Regarding encryption, algorithms perform better than the most contemporary encryption techniques. Regarding experimental values, UACI is at 33.4954%, while NPCR is at 99.79% [62].

Marcin Lawnik et al. (2022) proposed a two-step method: initially, the text is transformed to an RGB image, followed by the application of the chosen image encryption technique. The suggested method is illustrated with an example that validates the precision of this text encryption technique and facilitates the secure concealment of textual communication. The computed metrics of entropy, correlation of neighboring pixels, UACI, and NPCR, associated with differential cryptanalysis, in conjunction with MSE, concerning pixel inconsistency analysis, all substantiate this. The system attained an NPCR of 99.40% and a UACI of 33.41% [63].

Ibrahim Yasser et al. (2022) investigated innovative perturbation techniques using chaotic maps. To address the shortcomings of traditional chaos-based confusion and diffusion frameworks, the proposed perturbation-based data encryption is applied throughout both the confusion and diffusion phases. The proposed pipeline framework incorporates supplementary input parameters in addition to a dual-round confusion-diffusion design. Unlike traditional methods, the system includes not only the plain image and secret key but also techniques for encryption using one-time keys. According to the quantitative results, 33.694% and 99.814%, respectively, are the average values of UACI and NPCR.[19].

Sachikanta Dash et al. (2022) present a disordered image encryption method based on shifting (flipping) operations. The proposed technique is uncomplicated, as bit-level permutations utilize simple up-down (UD) and left-right (LR) flipping operations. Moreover, the presented method represents one of the swiftest procedures now accessible in CPU architectures, as the flipping processes do not necessitate continuous time. The proposed methodology initiates with block-based bit-level diffusion operations and subsequently transitions to bit-level permutation operations. The security of the technique is enhanced via diffusion operations and bit-level permutation. In the permutation and diffusion methods, the algorithm's software and hardware efficiency is enhanced by using a certain kind of one-dimensional chaotic map, namely the Piecewise Linear Chaotic Map (PWLCM) system. The method's hash-generated keys also withstand chosen-plaintext and chosen-ciphertext attacks. The simulation results demonstrate the superiority of the suggested method for medical image encryption. The security analysis indicates that the proposed solution has sufficient defenses against all popular security flaws. The experimental values of UACI and NPCR were 33.5065% and 99.69%, respectively [24].

P. Rashmi et al. (2022) proposed Improved Chaos Encryption (ICE), which enhances security by introducing unpredictability. To augment the security of the Lorenz 96 model employed in the chaotic encryption process, the mean energy of the images is calculated and juxtaposed with an adaptive threshold. Due to its heightened sensitivity, Lorenz 96 rendered the chaos encryption process more unpredictable. Median pictures were employed to assess the efficacy of the ICE in image encryption and concealment. The quality of the decrypted and recovered images was evaluated at various embedding rates utilizing the proposed ICE model. The results demonstrate that the presented ICE model has a PSNR value of 104.7 dB, while the LSB-ROI method has a PSNR value of 97.61 dB. For NPCR, the experimental value is 99.62%, while for UACI, it is 33.41% [64].

Haiping Chen et al. (2022) introduced a chaotic system with six dimensions and used random augmentation procedures for the chaotic sequences. Initially, a hyper-chaotic system exhibiting more complex chaotic dynamics was established. Subsequently, the system's unpredictability, chaotic attractor, and Lyapunov exponent spectrum were analyzed. Finally, we use a randomness enhancement operation to produce random sequences. Second, a thumbnail is created by selecting pixels from the original image through image preprocessing; the thumbnail can be manipulated to alter the size of the key space. Thirdly, in order to ensure that the key is unique, the hyper-chaotic system commences with the hash value of the original image. The utmost and minimum pixel values from the respective rows and columns of the thumbnail are used to generate the row and column encryption matrices. The random concatenation of random sequences in a specific order or the comprehensive configuration of random sequences are the components of these two encryption matrices. The Arnold transformation, which employs column and row encryption, is implemented to the original image prior to encryption, resulting in the acquisition of the cipher image. The proposed technique's superior security performance, resilience, and rapid encryption and decryption velocities are demonstrated by the experimental results. For NPCR, the experimental number is 99.5956 percent, while for UACI, it is 33.3997 percent [65].

R. Durga et al. (2022) presented a private blockchain-based chaotic map encryption system for IoT medical settings. Brute force assaults and other Internet of Things attacks can be thwarted by the suggested chaotic application of the blockchain method. All of our thorough experimentation was conducted using standard image data. Correlation coefficients, entropy, NPCR, UACI, and other metrics were calculated in an effort to appraise the strength of the chaotic encryption. We were able to get better outcomes that surpass the current blockchain's processes, which is absurd for inhibiting data leaks and guaranteeing IoT data security. In the future, the Blockchain architecture based on CES for 5G networks can be improved with regard to verifying the security of pictures. NPCR and UACI have experimental values of 99.68% and 33.90%, respectively, to increase the IoT network's efficiency and flexibility [66].

Bassem Abd-El-Atty et al. (2023) presented a distinctive dual-image medical encryption technique utilizing logistic mapping and quantum walks. In the suggested encryption scheme, the two plain images are divided into two separate images: one comprising the high 4 bits of each image and the other containing the low 4 bits. The average values of UACI and NPCR for the tested samples were 33.4659% and 99.6143%, respectively [67].

Ali Akram Abdul-Kareem et al. (2023) presented a novel medical image encryption method by integrating two multidimensional chaotic systems: the Arnold transform, the fast Fourier transform, and the discrete wavelet transform. The medical image is exposed to a discrete wavelet transform prior to the shuffling of subbands with a magic square. Each disordered subband experiences perturbation operations via the implementation of the Uruk 4-D chaotic system. A secondary layer of confusion is introduced in the fast Fourier transform domain with the application of the Arnold transform to enhance unpredictability and randomness. Secret keys derived from the WAM 3D chaotic system are used to produce the final encrypted image. The experimental results for UACI are 33.58%, and NPCR is 99.63% [1].

Tutu Raja Ningthoukhongjam et al. (2024) disclosed an image encryption technique that employs public key encryption, integrating the features of elliptic curve encryption (ECC) and Blum-Goldwasser encryption (BGC). The experimental values obtained for the NPCR and UACI were 99.6901% and

33.5260%, respectively. The overall duration needed for the suggested approach is 0.142 seconds [68].

Ali Abou El Qassime et al. (2024) suggested a ground-breaking hyper-chaotic logistic map that is employed for the first time in biological image encryption. It is distinguished by a high Lyapunov dimension (DL = 2.1886) and its fast synchronization. As evidenced by compelling numerical values, this novel encryption method satisfies the strictest security requirements. It exhibits remarkable resilience against a variety of attacks, particularly against statistical, differential, ciphertext, noisy, and brute force attacks. A correlation coefficient ranging from -1.8319×10^{-4} to 6.6977×10^{-4} and an extensive key space exceeding 2^{298} are observed. This tried-and-true encryption duration guarantees the fastest possible encryption time, roughly 0.3 seconds for 512 × 512 pictures. It was also suggested that adaptive feedback control mode synchronization be used to synchronize this map quickly. Biomedical image encryption has been made faster and more secure by utilizing the new map and its synchronization. Results from the experiments showed that UACI was 33.5438% and NPCR was 99.62% [69].

Saleh Ibrahim et al. (2024) engineered a robust cryptographic framework to improve the encryption efficacy of 12-bit medical images. A pivotal key-dependent 12 × 12 S-box, central to the proposed system, is crucial for enhancing the security and effectiveness of the encryption method. Test results demonstrate that 12x12 S-boxes offer significantly superior confusion and key sensitivity compared to 8x8 S-boxes. The outcome enables the suggested 12×12 S-box-based method to successfully meet all security assessments and handle images with a depth of 12 bits, 3.3% quicker than an 8×8 S-box. Experimental data indicates that the proposed approach can encrypt 12-bit images at an increase reaching 300 MB/s. Moreover, it has been demonstrated that the suggested method can properly manage 8-bit images. Comparative findings illustrate the suggested scheme's superiority over available medical image encryption solutions in terms of efficiency and security. The experimental outputs for UACI were 33.347%, and NPCR was 99.9757% [70].

Xuefang Zhou et al. (2024) presented an image encryption technique based on Rubik's cube matrix and optical chaos in this research. The process of creating an optical device model first produces optical chaos. Second, the image is encrypted bit-by-bit using optical chaos and Rubik's cube matrix for the first encryption. A "U" type encryption method is devised, and various "U" type encryption schemes are chosen for the second encryption run. The encryption of the image is further strengthened by applying the "four-way diffusion" algorithm. The security study results and computer simulations also validate that the ciphertext images can withstand a variety of popular attack techniques, encompasses brute force, differential, and statistical assaults. The paper's suggested algorithm for decimal conversion, "U" encryption, and "quadrangle diffusion" causes the ciphertext image to lose its original features from the plaintext image. This proves the algorithm is suitable for picture encryptions and has good security performance. NPCR and UACI have corresponding experimental values of 99.51% and 33.46% [71].

Table 1: Related Works Summary

Cite	Methodology and Dataset	Key findings	Strengths	Limitations
[57]	A high-dimensional spatial chaotic system and a one-dimensional logistic map	In comparison to UACI, which is 36.6825%, NPCR is 99.6537%	Encrypting just half of the image yields usable results when using Coupled Spatial Chaotic Systems.	Single Image Dataset, Grayscale Image Focus, and Lack of Key Management and Distribution Discussion
[58]	1D Logistic Map	High Security Based on Statistical Tests	the key generator that produces a 256-bit secret key	Limited Experimental Dataset and Lack of Comparative Analysis
[13]	Elliptic curve cryptography (ECC) and chaos-based encryption use the Tent-Logistic-Tent (TLTS) and Henon chaotic maps.	The NPCR is 99.6189%, while the UACI is 33.5643%	Hybrid Cryptographic Approach and Secure and Efficient Signcryption	Computational Complexity and Key Management Challenges
[43]	The chaotic four-wing system of Qi in three dimensions	In comparison to UACI, which is 30.3%, NPCR is 99.6%	Robustness to Noise and Bit-Plane Extraction Technique	Limited Adaptability for Dynamic Environments and Computational Complexity
[59]	The chaotic map and a key generator (KG) that is based on quantum mechanics	In comparison to UACI, which is 31.92%, NPCR is 99.45%	Effectiveness of the proposed encryption method	Computational Complexity
[60]	Discrete Wavelet Transform,	The average UACI is 33% while	Robustness Against Attacks,	Security vs. Processing Time

	Bit-Plane Extraction Method, and Cubic Logistic Map	the average NPCR is 99.4%.	Speed, and Efficiency	
[61]	Using a chaotic cryptosystem and a fast-reaching condition, an adaptive terminal sliding mode tracking technique	The NPCR is 99.6281%, while the UACI is 33.6120%	innovative use of chaotic systems and fast synchronization techniques	narrow dataset for evaluation, lack of real-time and hardware performance testing
[62]	Image blocks and chaos	The NPCR rate is 99.79%, and the UACI rate is 33.4954%.	Versatility and Robust Key Generation	Potential Computational Overhead
[63]	The chosen algorithm for image encryption is applied after the text is turned into an RGB image.	The UACI is 33.41%, whereas the NPCR is 99.40%.	Innovative Approach to Text Encryption	Limited Dataset Diversity and Computational Complexity
[19]	Two novel 2D chaotic maps	The NPCR is 99.814%, while the UACI is 33.694%	Robust defense for digital images and high encryption speeds of approximately 60 MB/s	Susceptibility to future quantum attacks and encrypting more images may impact image restoration due to compression ratios
[24]	Shifting (flipping) operations	UACI is 33.5065%, while NPCR is 99.69%	Low Computational Complexity and Efficiency in Hardware and Software	Limited Focus on Medical Image Types and Lack of Comparison with Other Methods
[64]	Improved Chaos Encryption (ICE)	The efficiency of NPCR is 99.62%, and that of UACI is 33.41%	Enhanced Security via Lorenz 96 Model and High PSNR Values	Computational Complexity
[65]	6-D chaotic system	UACI is 33.3997%, and the NPCR is 99.5956%.	Enhanced Randomness and Fast Encryption	Vulnerability to Specific Attacks
[66]	Blockchain-IoT	In terms of NPCR, it's 99.68%, whereas UACI is 33.90%	Use of Blockchain for Integrity and Efficiency in Resource-Constrained IoT Networks	Memory Constraints
[67]	Logistic mapping and quantum walks	UACI is 33.4659% and NPCR is 99.6143 percent	Effective use of quantum walks and the logistic map	There is a lack of real-time performance evaluation, and no discussion on Key Distribution
[1]	Spatial domain, Fast Fourier Transform (FFT), Distributed Wavelet Transform (DWT)	Compared to UACI, which is 33.58%, NPCR is 99.63%.	Robustness to Noise and Enhanced Security	Complexity
[68]	Two types of cryptography are Blum-Goldwasser and Elliptic Curve Cryptography (ECC).	The NPCR is 99.6901%, and the UACI is 33.694%	Efficient Performance with a total execution time of 0.142 seconds, making it suitable for real-time applications	Susceptibility to Future Quantum Attacks
[69]	Hyper-chaotic logistic map	The UACI is 33.5438%, while the NPCR is 99.62%.	High-Level Security and Strong Resistance to Differential Attacks	Encryption Time
[70]	12 × 12 dynamic S-Box	UACI is 33.347 percent, and the NPCR is 99.9757 percent	Specialized for 12-bit Medical Images and Improved Security	Hardware Requirements
[71]	A technique for encrypting images using optical chaos and a Rubik's cube matrix	NPCR has a success rate of 99.51%, and UACI has a rate of 33.46%	The device proposed for generating optical chaos is relatively simple	Environmental Factors

Upon examining prior research, we identified the following deficiencies:

1) Limited Experimental Dataset.
2) Computational Complexity.
3) Lack of real-time and hardware performance testing.
4) Limited Focus on Medical Image Types (Grayscale Image Focus).
5) Lack of Comparative Analysis.
6) Lack of Key Management and Distribution Discussion.
7) Security vs. Processing Time.
8) Lack of Comparison with Other Methods.
9) Susceptibility to Future Quantum Attacks.
10) Encrypting more images may impact image restoration due to compression ratios.
11) Hardware Requirements.

6. Assessment of Security in Image-Encryption Algorithms

Numerous chaos-based image-encryption algorithms have been suggested, necessitating evaluation methodologies for their functioning, efficiency, security, and other factors. This section presents methods of measuring the efficiency of algorithms that chaotically encrypt images to facilitate the reader's comprehension of the pertinent material [37].

6.1 Evaluation of Image Entropy

In 1949, mathematician Claude E. Shannon introduced a mathematical method to assess how well an image works with a coding technique. The efficacy against entropy assaults is contingent upon the degree of unpredictability present in the encrypted image. A measure of the encrypted image's entropy varies from 0 to 8, as the maximum pixel value, represented in 8-bit binary, is 255. Test results approaching 8 demonstrate the effectiveness of the encryption scheme and the image's substantial unpredictability [1]. Entropy can be computed with the computational equation (11).

$$IE(S) = -\sum P(S) \times log_2 P(S) \tag{11}$$

6.2 Key space

An effective image-encryption scheme must have robust sensitive key, and the key space it occupies must be sufficiently extensive to render brute force attacks unfeasible [37]. A key space exceeding 2^{128} is adequate to thwart brute force attacks.

6.3 Key sensitivity

A chaotic system must be evaluated for qualities that are very sensitive to beginning circumstances before being used for image encryption. Even a little shift in the key might cause the outcome to diverge significantly from what should be expected, which is referred to as key sensitivity [37].

6.4 Histogram

A histogram shows how the values of individual pixels are distributed in an image. In a perfect method, the distribution of pixel values is uniform, and the histogram is also uniform, such that no image information is leaked [37].

6.5 Correlations of Adjacent Pixels

The linear correlation assesses the relationship between adjacent pixels in vertical, horizontal, and diagonal configurations. The formula for Pearson's linear correlation coefficient can be used to determine its value, Eqs. (12).

$$\begin{aligned} r &= \frac{Cov(x,y)}{\sigma_x \sigma_y} \\ \sigma_x &= \sqrt{Var(x)} = \sqrt{\frac{1}{N}\sum_{i=i}^{N}(x_i - E(x))^2}, \\ \sigma_y &= \sqrt{Var(y)} = \sqrt{\frac{1}{N}\sum_{i=i}^{N}(y_i - E(y))^2}, \\ Cov(x,y) &= \frac{1}{N}\sum_{i=i}^{N}(x_i - E(x))(y_i - E(y)), \end{aligned} \tag{12}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \; and \; E(y) = \frac{1}{N}\sum_{i=1}^{N} y_i$$

x and y are adjacent image pixels with dimensions W×H. $|r|$ values near 1 indicate that neighboring pixels are correlated, while r values near 0 indicate that a link between neighboring pixels is absent. The correlation coefficient adheres to the connection r ∈ [-1, 1]. The second case is the preferred variant from the perspective of cryptography [63].

6.6 Mean Squared Error (MSE)

The MSE is determined to assess the discrepancies between the original and decrypted images. The decrypted image quality and the effectiveness of the encryption algorithm are indicated by minor variations in MSE, which should be as low as possible.
The MSE is found to be Eq. (13).

$$MSE = \frac{1}{M \times N}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}\left[f(x,y)_r - f(x,y)_p\right]^2 \quad (13)$$

$f(x,y)_r$ is the decrypted image, and $f(x,y)_p$ is the input image. The dimensions of the images are represented by M and N, respectively, respectively, while x and y represent the pixel coordinates [1].

6.7 Peak Signal to Noise Ratio (PSNR)

The PSNR is considered one of the most suitable metrics for assessing the efficacy of encryption, since it allows the quantification of distortion levels in an image post-encryption. The PSNR measures the degree of similarity between the image and its associated encryption. An appropriate PSNR value for adequate encryption is below 10. Nonetheless, the PSNR between the original image and the post-decryption image approaches infinity. The PSNR is determined by utilizing the following equation (14):

$$PSNR = 20\,log_{10}\left(\frac{K-1}{\sqrt{MSE}}\right) \quad (14)$$

In general, K=2^8, with K representing the maximum possible value for a picture [69].

6.8 Unified average changing intensity (UACI)

UACI is a metric that is frequently employed to compare the quality of an image and assess the difference between the original and processed image. The following equation (15) is used to calculate the degree of change in the average luminance of an image, which is the purpose of UACI:

$$UACI = \frac{1}{P}\left[\sum_{i,j}\frac{|C_1(i,j) - C_2(i,j)|}{M}\right] \times 100\%, \quad (15)$$

$C1$ and $C2$ are the input and encrypted images, respectively, and P is the number of pixels, M is the utmost permissible pixel value in the images [37].

6.9 Number of pixels change rate (NPCR)

NPCR is an index that is typically employed to evaluate the differences between images before and after encryption, and it is used to evaluate image encryption algorithms. NPCR is a method that is intended to assess an encryption algorithm's degree of sensitivity to an image. It is formed in the following manner:

$$NPCR = \sum_{i,j}\frac{d(i,j)}{S} \times 100\%, \quad (16)$$

Let S represent the entire pixel count in the original image, and let d denote a binary array formed as follows:

$$d = \begin{cases} 1 & if\ C_1(i,j) \neq C_2(i,j) \\ 0 & if\ C_1(i,j) = C_2(i,j) \end{cases}, \quad (17)$$

C_1 denotes the input image, whereas $C2$ denotes the image that is protected by encryption [37].

7. Conclusion

Contemporary coding approaches have been developed primarily with the healthcare business in mind. The analysis of modern photo encoding methods is further examined in this work. With so many picture encoding systems currently in use, this paper provides an understandable and thorough taxonomy. Researchers have stressed that image encryption's security, parameterization, and computational performance still require improvement. A summary table of the most often utilized cryptographic methods is provided at the conclusion. Elliptic Curve Cryptography (ECC) can be employed to ensure the confidentiality of telemedicine consultations. This method has improved the NPCR rate to 99.6% and the UACI to 33.694%. There has been a considerable improvement in the use of ECC's strong encryption capabilities in telemedicine. Initially, ECC offers superior security with significantly reduced key sizes compared to other encryption techniques such as RSA. The instantaneous processing and transmission of medical data in telemedicine boosts the efficiency of ECC in terms of computer resources and bandwidth. Secondly, ECC provides a robust defense against cryptographic assaults, including discrete logarithm issues and prime factorization. This renders it ideal for telemedicine systems, which may be utilized to securely send, store, and retrieve medical images and other confidential data. Chaotic maps possess potential as a telemedicine data encryption method; however, additional research, standardization, and practical application are necessary to fully comprehend their benefits and constraints. Telemedicine enhances the security of remote medical care and the secrecy of patient details by applying chaotic systems. A brief table of the most prominent encryption algorithms is shown. Our study will assist future academics in suggesting a suitable encryption technique for the numerous difficulties associated with e-health applications.

Author Contributions: All authors contributed to every aspect of the present investigation.

Funding: This research was conducted without external financial support.

Conflicts of Interest: The authors assert the absence of any conflict of interest.

References

[1] A. A. Abdul-Kareem and W. A. M. Al-Jawher, “A Hybrid Domain Medical Image Encryption Scheme Using URUK and WAM Chaotic Maps with Wavelet - Fourier Transforms,” Journal of Cyber Security and Mobility, vol. 12, no. 4, pp. 435–464, Jun. 2023, doi: 10.13052/jcsm2245-1439.1241.

[2] F. Masood, M. Driss, W. Boulila, J. Ahmad, S. U. Rehman, S. U. Jan, A. Qayyum, W. J. Buchanan. “A Lightweight Chaos-Based Medical Image Encryption Scheme Using Random Shuffling and XOR Operations,” Wireless Personal Communications, May 2021, Published, doi:10.1007/s11277-021-08584-z.

[3] W. El-Shafai, F. Khallaf, E.-S. M. El-Rabaie, and F. E. A. El-Samie, “Robust medical image encryption based on DNA-chaos cryptosystem for secure telemedicine and healthcare applications,” Journal of Ambient Intelligence and Humanized Computing, vol. 12, no.10, pp. 9007–9035, Mar. 2021, doi:10.1007/s12652-020-02597-5.

[4] M. Boussif, N. Aloui, and A. Cherif, “Securing DICOM images by a new encryption algorithm using Arnold transform and Vigenere cipher,” IET Image Processing, vol. 14, no. 6, pp. 1209–1216, Apr. 2020, doi:10.1049/iet-ipr.2019.0042.

[5] A. Pourjabbar Kari, A. Habibizad Navin, A. M. Bidgoli, and M. Mirnia, “A new image encryption scheme based on hybrid chaotic maps,” Multimedia Tools and Applications, vol. 80, no. 2, pp. 2753–2772, Sep. 2020,doi: 10.1007/s11042-020-09648-1.

[6] H. A. Abdullah, H. N. Abdullah, and W. A. Mahmoud Al-Jawher, “A hybrid chaotic map for communication security applications,” International Journal of Communication Systems, vol. 33, no. 4, p. e4236, Nov.2019, doi: 10.1002/dac.4236.

[7] A. B. Joshi, D. Kumar, D. C. Mishra, and V. Guleria, “Colour-image encryption based on 2D discrete wavelet transform and 3D logistic chaotic map,” Journal of Modern Optics, vol. 67, no. 10, pp. 933–949, Jun. 2020, doi 10.1080/09500340.2020.1789233.

[8] CBS News. (Feb. 14, 2019). Hackers are Stealing Millions of Medical Records and selling them on the Dark Web. [Online].Available:https://www.cbsnews.com/news/hackers-stealmedical-records-sell-themon-dark-web

[9] L. Schencker. (Mar. 8, 2019). Hackers Target Health Data: 82% of Hospital Tech Experts Reported 'Significant Security Incident’ in the Last Year. Chicago Tribune.[Online].Available:https://www.chicagotribue.com/business/ct-biz-hospital-databreaches-20190307-story.html

[10] U.S. Department of Health and Human Services (HHS). Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information. Accessed: Feb. 5, 2020. [Online]. Available: https://ocrportal.hhs.gov/ocr/breach/breach-report.jsf

[11] Verizon Enterprise. (2018). 2018 Data Breach Investigations Report. [Online]. Available: https://enterprise.verizon.com/resources/reports/2018/DBIR-2018-Report.pdf

[12] HIPAA Journal. (Aug. 20, 2018). Court Approves Anthem 115 Million Data Breach Settlement. [Online]. Available: https://www.hipaajournal. com/court-approvesanthem-115-million-data-breach settlement/

[13] T. S. Ali and R. Ali, “A Novel Medical Image Signcryption Scheme Using TLTS and Henon Chaotic Map,” IEEE Access, vol. 8, pp. 71974–71992, 2020, doi: 10.1109/ACCESS.2020.2987615.

[14] M. Elhoseny, K. Shankar, S. Lakshmanaprabu, A. Maseleno, and N. Arunkumar, ``Hybrid optimization with cryptography encryption for medical image security in Internet of Things," Neural Comput. Appl. vol. 32, pp. 10979_10993, 2018.

[15] S. Madhu and M. A. Hussain, ``Securing medical images by image encryption using a key image," Int. J. Comput. Appl., vol. 104, no. 3, pp. 30_34, Oct. 2014.

[16] J. Li and H. Liu, “Colour image encryption based on advanced encryption standard algorithm with two-dimensional chaotic map,” IET Inf. Secure, vol. 7, no. 4, pp. 265_270, Dec. 2013.

[17] Q. Zhang and Q. Ding, ``Digital image encryption based on advanced encryption standard (AES)," in Proc. 5th Int. Conf. Instrum. Meas., Com-put., Commun. Control (IMCCC), Sep. 2015, pp. 1218_1221.

[18] N. B. Slimane, K. Bouallegue, and M. Machhout, “Nested chaotic image encryption scheme using two-diffusion process and the secure hash algorithm SHA-1,” in Proc. 4th Int. Conf. Control Eng. Inf. Technol. (CEIT), Dec. 2016, pp. 1_5.

[19] I. Yasser, A. T. Khalil, M. A. Mohamed, A. S. Samra, and F. Khalifa, “A Robust Chaos-Based Technique for Medical Image Encryption,” IEEE Access, vol. 10, pp. 244–257, 2022, doi: 10.1109/ACCESS.2021.3138718.

[20] R. Guesmi, M. A. B. Farah, A. Kachouri , and M. Samet "A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2." Nonlinear Dynamics, vol. 83, pp. 1123-1136, 2016, doi:10.1007/s11071-015-2392-7.

[21] W. Liu, K. Sun, and C. Zhu. "A fast image encryption algorithm based on chaotic map." Optics and Lasers in Engineering, vol.84, 2016, pp. 26-36, doi:10.1016/j.optlaseng.2016.03.019.

[22] K. A. K. Patro, B. Acharya, and V. Nath, "Various dimensional colour image encryption based on non-overlapping block-level diffusion operation." Microsystem Technologies, vol.26, no. 5,2020, pp. 1437-1448, doi:10.1007/s00542-019-04676-w.

[23] X.Wang, S. Wang, Y. Zhang, and K. Guo. "A novel image encryption algorithm based on chaotic shuffling method." Information Security Journal: A Global Perspective, vol. 26, no. 1,2017, pp. 7-16,

[24] S. Dash, S. Padhy, B. Parija, T. Rojashree, and K. A. K. Patro, “A Simple and Fast Medical Image Encryption System Using Chaos-Based Shifting Techniques,” International Journal of Information Security and Privacy, vol. 16, no. 1, 2022, doi: 10.4018/IJISP.303669.

[25] K. N. Singh and A. K. Singh, “Towards Integrating Image Encryption with Compression: A Survey,” ACM Transactions on Multimedia Computing, Communications and Applications, vol. 18, no. 3, Aug. 2022, doi: 10.1145/3498342.

[26] X. Wang, Y. Li, and J. Liu, “A review of traditional encryption schemes,” Journal of Information Security, vol. 11, no. 2, pp. 67–80, 2020.

[27] M. Khan, J. Ahmad, and S. A. Khan, “Chaos-based image encryption: a review,” Multimedia Tools and Applications, vol. 80, pp. 21771–21806, 2021.

[28] W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed., Pearson, 2017.

[29] R. Abirami and N. Marimuthu, “A survey on chaos-based image encryption systems,” Journal of King Saud University – Computer and Information Sciences, vol. 34, no. 6, pp. 2380–2393, 2022.

[30] B. Reddy and S. Varadarajan, “Performance analysis of chaos-based and conventional encryption schemes,” Journal of Information Security, vol. 11, no. 3, pp. 123–134, 2020.

[31] A. A. A. El-Latif, L. Li, and X. Li, “Efficient image encryption scheme based on chaotic maps and permutation-diffusion architecture,” Signal Processing, vol. 143, pp. 122–133, 2019.

[32] K. Nidhal, A. A. Awad, and M. Al-Qutayri, “On the mathematical complexity of chaos-based image encryption schemes,” IEEE Access, vol. 9, pp. 113079–113091, 2021.

[33] Y. Chen, Z. Wang, and T. Zhang, "Chaos-AI hybrid models for secure image transmission," Multimedia Systems, Springer, 2023. [Online]. Available: https://doi.org/10.1007/s00530-023-00985-2

[34] E.N.Lorenz, "Deterministic nonperiodic flow." Journal of Atmospheric Sciences, vol. 20, no. 2,1963,pp.130-141,https://doi.org/10.1175/1520-0469(1963)020<0130:DNF>2.0.CO;2

[35] T.Y. Li And J.A. Yorke, "Period three implies chaos," The theory of chaotic attractors,2004, pp. 77-84.

[36] R. M. May "Simple mathematical models with very complicated dynamics."Nature, vol.261, no.5560,1976, pp. 459-467.

[37] B. Zhang and L. Liu, "Chaos-Based Image Encryption: Review, Application, and Challenges," Jun. 01, 2023, MDPI. doi: 10.3390/math11112585.

[38] Fathi-Vajargah, M. Behrouz, V. Kanafchian, and Alexandrov, "Image encryption based on permutation and substitution using Clifford Chaotic System and logistic map," Journal of Computers, vol. 13, no. 3, pp. 309– 326, 2018.

[39] P. Ping, J. Fan, Y. Mao, F. Xu, and J. Gao, "A Chaos Based Image En- cryption Scheme Using Digit-Level Permutation and Block Diffusion," IEEE Access, vol. 6, pp. 67 581–67 593, 2018.

[40] M. Preishuber, T. Hütter, S. Katzenbeisser, and A. Uhl, "Depreciating Motivation and Empirical Security Analysis of Chaos-based Image and Video Encryption," IEEE Transactions on Information Forensics and Security, pp. 2137–2150, 2018.

[41] B. Sharma and J. Singh, "Chaos Based Image Encryption Techniques: A Review," International Research Journal of Engineering and Technology, 2022, doi: 10.13140/RG.2.2.26235.39204.

[42] J. Leonel Rocha, and A. K. Taha. "Allee's effect bifurcation in generalized logistic maps." International Journal of Bifurcation and Chaos, vol.29, no. 03 2019, pp. 1950039,dol:10.1142/S0218127419500391.

[43] X. Wang and C. Tu, "A chaos-based medical image encryption method," Indonesian Journal of Electrical Engineering and Computer Science, vol. 19, no. 3, pp. 1316–1324, Sep. 2020, doi: 10.11591/ijeecs.v19.i3.pp1316-1324.

[44] M. Amin, O. S. Faragallah, and A. A. Abd El-Latif. "A chaotic block cipher algorithm for image cryptosystems." Communications in Nonlinear Science and Numerical Simulation, vol. 15, no. 11 2010, pp. 3484-3497.dol:10.1016/j.cnsns.2009.12.025.

[45] G. Chen, and T. Ueta, "Yet another chaotic attractor." International Journal of Bifurcation and chaos, vol.9, no. 07,1999, pp. 1465-1466,doi:10.1142/S0218127499001024.

[46] B. M. Tayel , and E. I. AlSaba. "Robust and sensitive method of Lyapunov exponent for heart rate variability." arXiv preprint arXiv:1508.00996 (2015).dol:10.48550/arXiv.1508.00996.

[47] A. Wolf, J. B. Swift, H. L. Swinney, and J. A. Vastano, "Determining Lyapunov exponents from a time series." Physica D: nonlinear phenomena, vol.16, no. 3 1985,pp.285-317,doi:10.1016/0167-

2789(85)90011-9.

[48] R. Kříž "Finding chaos in finnish gdp." International Journal of Automation and Computing, vol.11,2014, pp. 231-240.

[49] H. A. Abdullah, H. N. Abdullah, and W. A. Mahmoud Al-Jawher, "A hybrid chaotic map for communication security applications," International Journal of Communication Systems, vol. 33, no. 4, Mar. 2020, doi: 10.1002/dac.4236.

[50] M. V. Opstall "Quantifying chaos in dynamical systems with Lyapunov exponents." Furman University Electronic Journal of Undergraduate Mathematics 4, no. 1,1998, pp. 1-8.https://scholarexchange.furman.edu/fuejum/vol4/iss1/1

[51] A. G. Georg, and M. Ian. "The 0-1 test for chaos: a review." Chaos Detection and Predictability, Lecture Notes in Physics, Springer, Berlin, Heidelberg ,2016, pp. 221-247.

[52] H. A. Abdullah, and H. N. Abdullah. "A new chaotic map for secure transmission." TELKOMNIKA (Telecommunication Computing Electronics and Control), vol. 16, no. 3 ,2018,pp.1135-1142,doi:10.12928/telkomnika.v16i3.8545.

[53] H. Kolivand, S. F. Hamood, S. Asadianfam, and M. S. Rahim, " Image encryption techniques: A review," Multimedia Tools and Applications,2024, vol. 83, Sep. 01, 2024, Springer. doi: 10.1007/s11042-023-17896-0.

[54] S. Dey, and R. Ghosh, "A review of cryptographic properties of S-boxes with Generation and Analysis of crypto secure S-boxes," Cryptology ePrint Archive (2018).

[55] S. T. Ahmed, D. A. Hammood, R. F. Chisab, A. Al-Naji, and J. Chahl, "Medical Image Encryption: A Comprehensive Review," Aug. 01, 2023, Multidisciplinary Digital Publishing Institute (MDPI). doi: 10.3390/computers12080160.

[56] C.E. Shannon, "Communication theory of secrecy systems." The Bell system technical journal, vol. 28, no. 4,1949,pp.656-715,dol:10.1002/j.1538-7305.1949.tb00928.x.

[57] X. Y. Wang, T. Wang, D. H. Xu, and F. Chen, "A selective image encryption based on couple spatial chaotic systems," Int J Mod Phys B, vol. 28, no. 6, Mar. 2014, doi: 10.1142/S0217979214500234.

[58] A. Gupta and A. Gupta, "Image encryption using chaotic maps," 2015. [Online]. Available: https://www.researchgate.net/publication/280314246

[59] C. H. Lin et al., "Intelligent Symmetric Cryptography with Chaotic Map and Quantum Based Key Generator for Medical Images Infosecurity," IEEE Access, vol. 9, pp. 118624–118639, 2021, doi: 10.1109/ACCESS.2021.3107608.

[60] A. Shafique, J. Ahmed, M. U. Rehman, and M. M. Hazzazi, "Noise-Resistant Image Encryption Scheme for Medical Images in the Chaos and Wavelet Domain," IEEE Access, vol. 9, pp. 59108–59130, 2021, doi: 10.1109/ACCESS.2021.3071535.

[61] B. Vaseghi, S. Mobayen, S. S. Hashemi, and A. Fekih, "Fast Reaching Finite Time synchronization

Approach for Chaotic Systems with Application in Medical Image Encryption," IEEE Access, vol. 9, pp. 25911–25925, 2021, doi: 10.1109/ACCESS.2021.3056037.

[62] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish, and M. M. Fouda, "A new image encryption algorithm for grey and color medical images," IEEE Access, vol. 9, pp. 37855–37865, 2021, doi: 10.1109/ACCESS.2021.3063237.

[63] M. Lawnik, L. Moysis, and C. Volos, "Chaos-Based Cryptography: Text Encryption Using Image Algorithms," Electronics (Switzerland), vol. 11, no. 19, Oct. 2022, doi: 10.3390/electronics11193156.

[64] P. Rashmi, M. C. Supriya, and Q. Hua, "Enhanced Lorenz-Chaotic Encryption Method for Partial Medical Image Encryption and Data Hiding in Big Data Healthcare," Security and Communication Networks, vol.pp.1-9, 2022, doi: 10.1155/2022/9363377.

[65] H. Chen, E. Bai, X. Jiang, and Y. Wu, "A Fast Image Encryption Algorithm Based on Improved 6-D Hyper-Chaotic System," IEEE Access, vol. 10, pp. 116031–116044, 2022, doi: 10.1109/ACCESS.2022.3218668.

[66] R. Durga, E. Poovammal, K. Ramana, R. H. Jhaveri, S. Singh, and B. Yoon, "CES Blocks - A Novel Chaotic Encryption Schemes-Based Blockchain System for an IoT Environment," IEEE Access, vol. 10, pp. 11354–11371, Nov. 2021, doi: 10.1109/ACCESS.2022.3144681.

[67] B. Abd-El-Atty, M. A. El-Affendi, S. A. Chelloug, and A. A. Abd El-Latif, "Double Medical Image Cryptosystem Based on Quantum Walk," IEEE Access, vol. 11, pp. 69164–69176, 2023, doi: 10.1109/ACCESS.2023.3289932.

[68] T. R. Ningthoukhongjam, S. Devi Heisnam, and M. Singh Khumanthem, "Medical Image Encryption Through Chaotic Asymmetric Cryptosystem," IEEE Access, vol. 12, pp. 73879–73888, 2024, doi: 10.1109/ACCESS.2024.3404088.

[69] A. A. El Qassime, H. Nhaila, and L. Bahatti, "Enhancing the Security and Efficiency of Biomedical Image Encryption through a Novel Hyper-Chaotic Logistic Map," International Journal of Intelligent Engineering and Systems, vol. 17, no. 5, pp. 334–349, 2024, doi: 10.22266/ijies2024.1031.27.

[70] S. Ibrahim, A. M. Abbas, A. A. Alharbi, and M. A. Albahar, "A New 12-Bit Chaotic Image Encryption Scheme Using a 12 × 12 Dynamic S-Box," IEEE Access, vol. 12, pp. 37631–37642, 2024, doi: 10.1109/ACCESS.2024.3374218.

[71] X. Zhou, L. Sun, N. Zheng, and W. Chen, "Image encryption algorithm based on optical chaos and Rubik's cube matrix conversion," AIP Adv, vol. 14, no. 8, Aug. 2024, doi: 10.1063/5.0199028.