# A Review on Chaos-based Image Encryption Techniques for Healthcare Applications: Issues and Challenges

**Maddodi B S[1], Dr. S. Koteswari[2], Dr. Ram Bajaj[3], S. Karuna[4]**

[1]Associate professor, Manipal Institute of technology, Mahe, Manipal, India.

[2]Professor, Department of ECE, Pragati Engineering College, Surampalem, Andhra Pradesh.

[3]Chairman, RNB Global University, Bikaner.

[4]Assistant Professor, Department of ECE, Seshadri Rao Gudlavalleru Engineering College, Autonomous Institute, Permanently affiliated to JNTUK, Kakinada, Andhra Pradesh

**ABSTRACT:**

Due to the rapid growth of communications networks, an increased number of multimedia information has been exchanged through unprotected communications. The multimedia data can be in the form of satellite images, images for the military, images for use in medicine, etc. At current time, telemedicine users are using communication networks to transmit various medical data in the form of images. Every single one of these photographs contains private and confidential information. Security of sensitive data is therefore crucial to preventing unauthorised access. Currently, a number of image encryption techniques allow for the extremely secure storage of medical images. Present chaos-based picture encryption techniques offer a high level of security for protecting medical photos. Reviews of several chaos-based image encryption methods for encrypting medical photos are discussed in this paper. The assessment metrics, results, and comparison analysis of various medical picture encryption systems are also presented in this paper. The field's future directions are then addressed.

**KEYWORDS:** security, image encryption, medical images, chaos.

## Introduction

The pace of technological progress during the last few decades has skyrocketed. Information may now be transmitted across the internet more easily because to developments in communications. Digital photographs, movies, and records are just a few examples of the data that is transported instantly around the globe. Telemedicine is the most extraordinary answer to the current healthcare dilemma in the medical industry. Digital medical pictures of internal human organs are utilised for quick diagnosis and effective therapy. Healthcare professionals must manage sensitively since they oversee sensitive patient information due to cybercrimes. The security of patient data is extremely important since unauthorised access to such data might have disastrous consequences. Medical image storage and/or transfer call for validity and integrity as well as confidentiality. Encryption is a popular method for protecting medical images. DES [1], AES [2], and other widely used data protection technologies served as the foundation for early image encryption techniques. However, it has been found that these techniques do not encrypt images as effectively [3][4][5].

Therefore, a strong technique for encrypting medical images will be required. Chaos-based techniques provide a reliable method for medical picture encryption. Chaotic mapping algorithms contain a number of intrinsic characteristics, including ergodicity, mixing characteristics, vulnerability to chaotic factors, and very complicated behaviour. Chaotic systems are a great option for an effective and efficient technique of encryption due to their specific characteristics [6][7][8]. The various kinds of chaos-based processes acquired in picture protection are “one- dimensional” (1D) and “high-dimensional” (HD) [9]. The drawback of chaos-based 1D map is that they contain a limited amount of key space, despite the fact that they appear to be efficient, simple in design, and better resource stewards. Chaotic HD maps have a variety of critical spaces, but they require more resources and are more difficult to create [10] [11]. Some image encryption techniques compromise between speed and security by using a mixture of chaotic 1D and HD maps.

The chaotic image encryption methods are essentially divided into permutation and diffusion phases. During permutation, the pixel coordinates of the actual picture are changed, and during diffusing, pixel-values are altered. The statistics of the ciphertext and the input image are replicated when the encryption method’s permutation step is used alone, making it simple for attackers to launch a statistical assault. Similar to how employing simply the diffusion phase in the encryption process results in higher security than using the permutation process, however the encryption effect is not as powerful. Therefore, being alone during an encryption process is undesirable. Therefore, in order to significantly enhance the encrypting effectiveness and the security of said scheme, researchers were interested in integrating both the transformation phase and the alteration phase in the encryption method [12].

In recent years, medical personnel have used patient data for patient diagnostics by storing and transmitting it. Healthcare personnel must handle sensitive patient information with caution because of cybercrimes. Since unauthorised access to medical data could have disastrous repercussions, patient data security is of the utmost importance. To keep medical data securely safe, a powerful encryption solution is needed, particularly for medical images. Such high security is provided by chaos-based encryption techniques.

This article summarises various chaos-based methods for encrypting medical images and describes them in terms of their means. In certain instances, it provides a thorough analysis of each of the recommended papers. This paper also includes the results of these articles’ evaluations and several traditional performance factors in the evaluation. The comparisons between these articles based on their conclusions are then made.

The remainder of the article is organized in the following manner: Section II discusses the fundamental idea of chaos.

Section III discusses a survey of current medical picture encryption methods. The evaluation metrics and evaluation outcomes for several chaos-based medical picture encryption algorithms are presented in Section IV. This section also includes a comparison of various encryption algorithms depending on their conclusions. Finally, section V brings the article to a close.

## Preliminaries

### A. Chaos Theory

Chaos is defined as “a state of disarray.” The theory of chaos examines the dynamics of complex systems that are very sensitive to their starting conditions. Due to the complexity of these systems, long-term prediction is typically unachievable due to the minor differences in the initial state that lead to such vastly diverse results. Chaos occurs whenever the current approximates the futures while the future is not precisely defined [13].

There is a chaotic activity in several natural systems. Examples of chaotic behaviour include variations in the weather, irregular heartbeats, fluid flow, traffic, and the stock market, among others. Mathematical chaotic models can be used to analyse how these systems behave.

### B. Chaotic Dynamics

A dynamic system must have the following characteristics to be categorised as chaotic [14].

- The chaotic sequence values' randomness. The chaotic sequences created by chaotic maps contain pseudo- random sequence values and are extremely difficult to analyse and predict.
- Sensitive to initial circumstances, which means that slight changes in the starting point can result in mixed results.
- Sensitive to system parameters, which means that small changes in the system parameter can result in distinct chaotic sequences.
- Ergodicity of chaotic signals, i.e., the same distribution of chaotic outcomes by an encryption technique for each plaintext.
- Topological mixing.
- Nonlinear deterministic system.

C. Chaotic Map

Typically, a chaotic map is a discrete map (as opposed to a continuous one) that is sensitive to the beginning conditions (as contrasted to linear systems) but does not diverge to infinite (as contrasted to unstable systems). There is a divergence in the beginning conditions, which are near together. In the dynamical deterministic system, it is the unpredictability. It is expressed as follows in mathematics:

$$Z\mathrm{n}+1 = f(Z\mathrm{n}) \quad (1)$$

where, $0 < Z\mathrm{n} < 1$ and $n = 0,1,2,\cdots$

## Review On Chaos-Based Medical Image Encryption Techniques

This section provides a comprehensive review of several chaos-based picture encryption methods. The entire evaluation is separated into several sections, including reviews of medical image encryption methods that use chaos, combination of chaos and DNA, and hybrid of Chaos, DNA, Transform techniques.

A. Review on Medical Image Encryption Techniques based on Chaos

Many conventional strategies have been employed to protect medical images from attacks, but these techniques are not very effective in encrypting images due to the high redundancy and strong correlation of nearby pixels in images. Some researchers have created selected based encryption algorithms to lessen the correlation and redundancy of pixels [15][16]. A dual watermarking/encryption technology has been used by certain researchers to preserve the authenticity and integrity of photographs [17][18]. The techniques, however, are not appropriate for large amounts of data, such as medical imaging, and they are weak against differential attacks due to this [19].

To address these problems, Cao et al. [19] suggested data encryption that utilized edge maps. Three adaptable components – bit-plane breakdown, chaotic sequence generation, and pixel scrambling – have been used by the technique's creators. The process's use of scrambling modifies both the positions and values of pixels, raising the level of security even higher. The cipher image is especially susceptible to alterations in the normal picture caused by the influence of the bit level diffusion in this process when the plain image is split into multi-bit planes and encrypted using the XOR operation and bit-level dispersion. Hence, the technique is immune to divergent assaults.

Although chaotic 1D maps seem to be efficient, simple in design, and better resource stewards, they have the demerits of having a small amount of key spaces. Hence, Dridi et al.

[20] developed an encryption strategy that mixed the Logistic 1D chaotic map with Perceptron Neural Network (PNN) to obtain the advantages of chaotic 1D maps with larger key space. Because the system has unique properties like a wider parameter scope, fewer regular intervals periods in branching, and a higher key space than a 1D chaotic map, it is more appropriate for use in picture encryption. In [21], Lakshmi et al. proposed another neural assisted encryption scheme for medical image cloud storage. For cloud storage of medical images, this research suggests a Hopfield-governed

image- dependent encryption system. The main advantage of the system lies in the speed of encryption, the proposed scheme takes around 0.5 seconds to encrypt an image while that of [20] takes far more time. The suggested approach is faster and more secure than [20] and is therefore superior. Hua et al. presented another technique in [22] that makes use of pixel adaptation diffusing and faster shuffling. The picture's surroundings are first given a random value, which is then distributed throughout the entire image after two rounds of high-speed scrambled and pixel-adaptive diffusing dynamically mixed pixel positions. The two methods for pixel adaptive diffusion that are accessible are bitwise XOR and modulo arithmetic. The suggested solution is extremely secure and effective.

B. Review on Medical Image Encryption Techniques based on Chaos and deoxyribonucleic acid (DNA)

Ergodicity, mixing qualities, vulnerability to chaotic variables, and highly complicated behaviour are only a few of the intrinsic characteristics of chaotic mapping algorithms. Therefore, chaotic systems satisfy the traditional Shannonrequirements for confusion and diffusion and are suitable for picture encryption. But as stated earlier certain chaos-based cryptosystems have shown low security. To use the advantages provided by the chaotic system many encryption schemes based on chaos and DNA encoding are being developed. The vast parallelism, enormous storage, and low power consumption of DNA computing technology have lately led to its improvement and usage in cryptography. There are numerous image encryption techniques that combine chaos and DNA sequence operations. Studies have shown that DNA technology improves algorithm security and is resistant to chosen-plaintext assaults. Even though the DNA technology-based algorithms have been hampered by the low computer accuracy and use of the poorly chao-based maps. Belazi et al. [23] suggested a healthcare encrypting algorithm utilizing chaotic maps and DNA to solve this issue. The cryptosystem consists of two repetitive phases, which are preceded by a key generation layer which employs the SHA- 256 hash algorithm. Each stage of the encrypted system is composed of block-level permutations, pixel-level replacements, DNA coding, bit-based substitutions, DNA decode, and bit-based dispersion. The logistic-Chebyshev map generates the key stream in bit stage substitutions, whereas the sine-Chebyshev map is employed for the key stream in bit stage dispersion. Implication of two chaotic maps makes the encryption robust and strong and resistant to any known plaintext attacks. Aouissaoui et al. [24] developed another DNA-chaos based encryption algorithm. The creation of keys using the images and its metadata's hash functions constitutes the first stage of the encryption process. The second step is rotating and permuting the medical images' first two MSB bit-planes to remove the black backdrop that results in redundant DNA encoded sequences. The final component is encoding DNA using a dynamically selected DNA rule via a Logistic map. Tent maps and the XOR operation are used to perform dispersion and confusion. The proposed algorithm uses two hash functions instead of one which naturally increases the key space. When PSNR between original and decrypted images after noise attacks were compared with that of [23] the values and stats were significantly better indicating that developed algorithm is robust and resistant to noise attacks when compared with [23].

Using SHA-256, DNA cryptography, and a chaotic map, Akkasaligar et al. [25] built a solution for medical image encryption. The digitalized image's Least Significant Bit (LSB) contains the hash key, which is produced using SHA- 256. Security is added to the image by encoding it using DNA coding principles. Chen's hyper chaotic map is used to randomise the pixels of the encoded DNA matrix. The scrambled pixels of encoded DNA matrix blocks are eventually combined using logical XOR bitwise operation. Since the identical secret message stream are employed to encrypt every plaintext, they may be used to encrypt any secret key when they are found. This is due to the employment of numerous secret code streams by cryptosystems that are separate from the plain image. As a result, attacks employing chosen and known plaintext are more advantageous. To overcome this issue, Guesmi et al. [26] created an analogous approach using hybrid chaotic map and DNA code-based image encryption. Out of the plain picture and the secret hash keys, one-time keys are created using SHA-2. To create the cryptosystem's keys, the plain image's hash value is used. To make the diffusion process stronger, a hybrid chaotic function is employed. DNA XOR is used in confusion step.

C. Review on Medical Image Encryption Techniques based on Chaos, DNA, and Transform Techniques

Banu et al. [27] developed a cryptosystem which suggests encrypting DICOM images using IWT-based chaotic attractors and DNA sequences. The algorithm consists of the following stages: encoding-decoding, permutation- substitution, and complementary. Ravichandran et al. [28] developed a similar system. To safeguard digital medical image, the system reviews an encoding scheme based on IWT combined with chaos and DNA. The recommended work is split into two levels: a diffusion level and a two-stage shuffle level. Row and column shuffling of pixels come after initial block confusion in the initial stage of the shuffling procedure. DNA coding and DNA XOR processes are the foundation of the next step of the diffusion process. The system had an exceptionally large key space and had an NPCR of 99.99. Shafique et al. [29] developed another similar scheme in the frequency domain, a noise-resistant image encryption technique. To encrypt the medical images at the bit level as opposed to the pixel level, they employed bit plane extraction technique, Discrete Wavelet Transform (DWT), and a cubic Logistic map. Three components make up the proposed work; the first and last sections both include spatial domain encryption of the picture. The frequency domain encryption, which uses DWT, is the focus of the proposed algorithm's middle component. It is intended to increase security and shorten processing time of the proposed encryption technique by combining spatial and frequency domain encryption into a single encryption algorithm.

D. Review on Medical Image Encryption Techniques based on Fast Operation of Chaos

The problem with DNA encoding and decoding is that it has extra steps which increases complexity. Additionally, a lot of cryptosystems were overly sequential, took an excessive amount of time to calculate and construct, which dramatically increased complexity and lengthened execution time. To overcome these issues, Gafsi et al. [30] developed a fast medical picture encoding schme using improved chaos. A 256-bit key for the cryptosystem is created using the SHA-256 algorithm. A sophisticated chaos based PRNG is intended to produce an encryption key of excellent quality. The generated key exhibits strong entropy and unpredictability behaviour. Four operations—random pixel position permutations, bit position permutations, S-box pixel replacement, and XOR dispersion – create the encrypted images. To increase security, the encryption can be repeated more times. The following algorithm is fast and easy to understand. Masood et al. [31] suggested another simple cryptosystem to encrypt medical images based on Chen's chaotic system, Brownian motion, and Henon chaotic map. Two-dimensional Henon chaotic maps in the proposed system produce confusion, but Brownian motion and Chen chaotic maps produce diffusion. Like the system of Masood et al. in [31], Akkasaligar et al. in [32] also suggested a similar system using two hyper chaotic map techniques to provide a greater level of security. The confusion-diffusion process of chaos-based scheme is applied to a subset of the pixels in digital medical imaging. To offer very high security, a dual chaotic system's unpredictability is used. Instead of employing a particular one, all DNA-decoding-encoding principles are applied to create distinctive DNA structures and encrypted images. Since the digital medical image's pixels determine which rules of DNA are used, every healthcare picture will have a different structure of DNA. In the suggested system uses selected pixels for encryption using the hyper chaotic maps, the computational time is reduced. The computational time of [31] for a medical image is 1.53 seconds but that of [32] is 0.22 seconds which is faster when compared with [31], since it also involves DNA encoding and two hyper chaotic maps makes it very difficult to decrypt for hackers. Yasser et al. [33] also developed a similar system which also uses two chaotic maps. The suggested approach produced two brand-new chaotic maps that showed powerful chaotic activity. Bifurcation diagrams and Lyapunov exponents, used in dynamic analysis and validation, revealed that suggested maps are hyper chaotic whole, with great sensitivity and complexity. In contrast to algorithms that use one-time keys, the suggested technique uses diffusion and confusion of two-runs and takes additional input factors into account in addition to the original pictures and the secret key. The developed system has the same tests results as that of [31][32] and even the same computational speed as that of [32] but the main advantage over [32] is that this system provides the same result without applying DNA encoding which saves in computational power and makes it more efficient and less complex to imply and understand.

## Comparison Of Some Commonly Used Security Measures

The following is a comparison of various widely used security measures.

A. Key Space Analysis

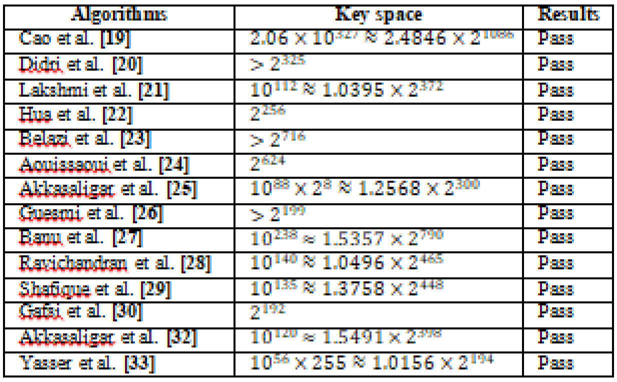
Algorithms' key spaces are their key sets [34][35]. For brute-force resistance, an algorithm's key space must be more than 2128 [36][37]. Results of key space comparisons between several medical image encoding schemes are presented in TABLE I. TABLE I shows that all medical picture encoding methods meet the brute-force attack criteria. The brute-force approach is however strongly resisted by the techniques in [19][23][24][27].

B. Statistical Attack Analysis

Many image encryption techniques employ histogram analysis and neighbouring pixel correlation analysis to analyse the statistical assault.

The graphical method of assessing a statistical assault is called histogram analysis [38]. It displays the distribution of how frequently certain types of valuable pixels occur. Neighboring pixel association measures the association of pixels in images. All medical picture encryption algorithms, successfully resist the statistical assault.

**TABLE I. KEY SPACE COMPARISON RESULTS OF VARIOUS HEALTHCARE IMAGE**



| Algorithms | Key space | Results |
|---|---|---|
| Cao et al. [19] | $2.06 \times 10^{327} \approx 2.4846 \times 2^{1086}$ | Pass |
| Didri et al. [20] | $> 2^{325}$ | Pass |
| Lakshmi et al. [21] | $10^{112} \approx 1.0395 \times 2^{372}$ | Pass |
| Hua et al. [22] | $2^{256}$ | Pass |
| Belazi et al. [23] | $> 2^{716}$ | Pass |
| Aouissaoui et al. [24] | $2^{624}$ | Pass |
| Akkasaligar et al. [25] | $10^{88} \times 2^{8} \approx 1.2568 \times 2^{300}$ | Pass |
| Guesmi et al. [26] | $> 2^{199}$ | Pass |
| Banu et al. [27] | $10^{238} \approx 1.5357 \times 2^{790}$ | Pass |
| Ravichandran et al. [28] | $10^{140} \approx 1.0496 \times 2^{465}$ | Pass |
| Shafique et al. [29] | $10^{135} \approx 1.3758 \times 2^{448}$ | Pass |
| Gafsi et al. [30] | $2^{192}$ | Pass |
| Akkasaligar et al. [32] | $10^{120} \approx 1.5491 \times 2^{398}$ | Pass |
| Yasser et al. [33] | $10^{56} \times 255 \approx 1.0156 \times 2^{194}$ | Pass |

## ENCRYPTION TECHNIQUES

C. Information Entropy Attack Analysis

Entropy is a metric used to quantify the degree of ambiguity associated with individual pixels in an encrypted image. The entropy value of 8 is a universal constant for any encoded image. Less capacity is required to divulge data from the cryptosystem when it rises above 8 [39].

The findings of comparing the information entropy of chaos-based medical image encryption algorithms are presented in TABLE II. The table demonstrates that the entropy of encoded images in all image encryption techniques is nearer to the optimal level, which is 8. This leads to the conclusion that all medical image encryption techniques successfully fend off entropy attacks. The methods in [20][25][32] are less resistant to the entropy attack than other chaos-based medical image encryption schemes.

**TABLE II. INFORMATION ENTROPY COMPARISON RESULTS OF CHAOS- BASED MEDICAL IMAGE ENCRYPTION SCHEMES**

| **Algorithms** | **Imag es** | **Average Entropy** |
|---|---|---|
| Didri et al. **[20]** | Average of 10 Images | 7.9864 |
| Lakshmi et al. **[21]** | Average of 5 Test Images | 7.9926 |
| Hua et al. **[22]** | Average of CipherImages | 7.9977 (8-bit), 7.9994 (16-bit), 7.9981 (24-bit) |

ISSN: 2173-0695

| | | |
|---|---|---|
| Belazi et al. **[23]** | Average of Images | 7.9993 |
| Aouissao et al ui . **[24]** | Average of X-ray, MRI, and US Images | 7.9994 |
| Akkasali et al gar . **[25]** | Average of MRI, CT, X-ray, Ultrasound, ECG | 7.922 |
| Guesmi et al. **[26]** | Avera of 1 ge 2 Image s | 7.997862 |
| Banu et al. **[27]** | Average of Images | 7.998 |
| Ravichandran et al. **[28]** | Average of Images | 15.785 |
| Shafique et al. **[29]** | Average of Images | 7.9983 |
| Gafsi et al. **[30]** | Avera of 1 ge 1 Image s | 8.0000 (Red, Green, and Blue) |
| Masood et al. **[31]** | Average of X, Y, and Z directions | 7.9993 (Chest), 7.9986 (MR), 7.9993 (Brain) |
| Akkasali et al gar . **[32]** | Images | 7.8466 |
| Yasser et al. **[33]** | Average of Images | 7.999 |

D. Differential Attack Analysis

"Number of Pixel Changing Rate" (NPCR) and "Unified Average Changing Intensity" (UACI) are the most oftenly utilised metrics for analysing the differential assault. UACI and NPCR have estimated values of 33.4635% and 99.6094%, respectively [40]. If the UACI and NPCR values are in proximity to or greater than their typical values, any encryption method is said to be resilient to differential assaults.

The UACI and NPCR values of all chaos-focused medical picture encoding schemes are presented in TABLE III. According to the table, all of the performance metrics for the image encoding methods discussed are either extremely close to or higher than their predicted values. This suggests that all picture encryption techniques successfully thwart the differential attack. Comparing the algorithm in [20][22][25][30][32][33] to the other picture encryption schemes, it is very high resistant to differential attack.

**TABLE III. UACI AND NPCR COMPARISONS OF CHAOS-BASED MEDICAL PICTURE ENCODING TECHNIQUES**

| **Algorithms** | **Images** | **Average NPCR** | **Average UACI** |
|---|---|---|---|
| Cao et al. **[19]** | Average of 16 Images | 99.60% | 33.48% |
| Didri et al **[20]** . | Average 8 of Images | 99.8844% | 24.5413% |

| | | | |
|---|---|---|---|
| Lakshmi et al. **[21]** | Average 5 of Test Images | 99.6% | 33.41% |
| Hua et al. **[22]** | Average of 20 Images | 99.9983% | 33.3311% |
| Belazi et al. **[23]** | Average of Images | 99.6173% | 33.4755% |
| Aouissaoui et al. **[24]** | Average of X-ray, MRI, and US Images | 99.6253% | 33.4943% |
| Akkasaligar et al. **[25]** | Average of MRI, CT, X-ray, Ultrasound, ECG | 99.898% | 32.518% |
| Guesmi et al. **[26]** | Average of 12 Images | 99.600124% | 33.459415% |
| Banu et al. **[27]** | Average of Images | 99.68% | 33.47% |
| Ravichandran et al. **[28]** | Average of Images | 99.6067% | 33.47% |
| Shafique et al. **[29]** | Average of 6/5 Images | 99.6453% | 33.4393% |
| Gafsi et al. **[30]** | Average of 8 &11 Images | 99.81543% (R), 99.78057 (G), 99.78593 (B) | 33.90968% (R), 33.87916 (G), 33.85873 (B) |
| Masood et al. **[31]** | Chest ( Average of X, Y, and Z) | 99.63% | 33.60% |
| Akkasaligar et al. **[32]** | Lena | 99.87% | 33.29% |
| Yasser et al. **[33]** | Average of Images | 99.86% | 33.72% |

## Conclusion

This article examines several chaotic algorithms for healthcare picture encryption. Furthermore presented are the evaluation findings from differential attack analysis, information entropy analysis, statistical attack analysis, and key space analysis. The comparisons of various methods are highlighted lastly.

The best alternative for the medical picture encryption algorithm to increase security and speed is rotation-based diffusion-confusion processes. This is so that rotation-based procedures can permute and diffuse the image's pixels quickly.

## References

1. D. Coppersmith, "The Data Encryption Standard (DES) and its strength against attacks," IBM J. Res. Develop., vol. 38, no. 3, pp. 243-250, May 1994.
2. N.F. Pub, "197: Advanced encryption standard (AES)," Federal information processing standards publication, vol. 197, no. 441, pp. 0311, November 2001.
3. H. Gao, Y. Zhang, S. Liang, and D. Li, "A new chaotic algorithm for image encryption," Chaos Soliton Fract., vol. 29, no. 2, pp. 393-399, July 2006.
4. K.A.K. Patro, B. Acharya, and V. Nath, "A secure multi-stage one- round bit-plane permutation operation based chaotic image encryption," Microsyst. Technol., vol. 25, no. 6, pp. 2331-2338, June 2019.
5. D. Sravanthi, K.A.K. Patro, B. Acharya, and M.P.J. Babu, "Simple Permutation and Diffusion Operation Based Image Encryption Using Various One-Dimensional Chaotic Maps: A Comparative Analysis on Security," in Advances in Data and Information Sciences, vol. 94, M. Kolhe, S. Tiwari, M. Trivedi, and K. Mishra, Eds. Springer, Singapore, January 2020, pp. 81-96.
6. 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 Dyn., vol. 83, no. 3, pp. 1123-1136, February 2016.
7. K. Panwar, R.K. Purwar, and A. Jain, "Cryptanalysis and improvement of an image encryption scheme using combination of one-dimensional chaotic maps," J. Electron. Imaging, vol. 27, no. 5, pp. 053037, October 2018.
8. K.A.K. Patro, B. Acharya, and V. Nath, "Secure, Lossless, and Noise- resistive Image Encryption using Chaos, Hyper-chaos, and DNA Sequence Operation," IETE Tech. Rev., vol. 37, no. 3, pp. 223-245, May 2020.
9. W. Liu, K. Sun, and C. Zhu, "A fast image encryption algorithm based on chaotic map," Opt. Laser Eng., vol. 84, pp. 26-36, September 2016.
10. K.A.K. Patro, B. Acharya, and V. Nath, "Various dimensional colour image encryption based on non-overlapping block-level diffusion operation," Microsyst. Technol., vol. 26, pp. 1437-1448, 2020.
11. X. Wang, S. Wang, Y. Zhang, and K. Guo, "A novel image encryption algorithm based on chaotic shuffling method," Inf. Secur. J., vol. 26, no. 1, pp. 7-16, January 2017.
12. [12] Q. Zhang and X. Wei, "RGB Color Image Encryption Method Based on Lorenz Chaotic System and DNA Computation," IETE Tech. Rev., vol. 30, pp. 37–41, September 2013.
13. [13] E. N. Lorenz, "Deterministic nonperiodic flow," J. Atmos.Sci., vol. 20, no. 2, pp. 130–141, March 1963.
14. [14] L. You, E. Yang, and G. Wang, "A novel parallel image encryption algorithm based on hybrid chaotic maps with opencl implementation," Soft Comput., pp. 1–15, January 2020.
15. [15] G. Alvarez, S. Li, and L. Hernandez, "Analysis of security problems in a medical image encryption system," Comput. Biol. Med., vol. 37, no. 3, pp. 424-427, March 2007.
16. [16] K. Martin, R. Lukac, and K.N. Plataniotis, "Efficient encryption of wavelet-based coded color images," Pattern Recognit., vol. 38, no. 7, pp. 1111-1115, July 2005.
17. [17] D. Bouslimi, G. Coatrieux, M. Cozic, and C. Roux, "A joint encryption/watermarking system for verifying the reliability of medical images," IEEE Trans. Inf. Technol. Biomed., vol. 16, pp. 891–899, July 2012.
18. [18] D. Bouslimi, G. Coatrieux, and C. Roux, "A joint encryption/watermarking algorithm for verifying the reliability of medical images: application to echographic images," Comput. Methods Progr. Biomed., vol. 106, pp. 47–54, April 2012.
19. [19] W. Cao, Y. Zhou, C.P. Chen, and L. Xia, "Medical image encryption using edge maps," Signal Process., vol. 132, pp. 96-109, March 2017.

20. [20] M. Dridi, M.A. Hajjaji, B. Bouallegue, and A. Mtibaa, “Cryptography of medical images based on a combination between chaotic and neural network,” IET Image Process., vol. 10, no. 11, pp. 830-839, November 2016.
21. [21] C. Lakshmi, K. Thenmozhi, J.B.B. Rayappan, S. Rajagopalan, R. Amirtharajan, and N. Chidambaram, “Neural-assisted image- dependent encryption scheme for medical image cloud storage,” Neural Comput. Appl., vol. 33, pp. 6671-6684, June 2021
22. [22] Z. Hua, S. Yi, and Y. Zhou, “Medical image encryption using high- speed scrambling and pixel adaptive diffusion,” Signal Process., vol. 144, pp. 134-144, March 2018.
23. [23] A. Belazi, M. Talha, S. Kharbech, and W. Xiang, “Novel medical image encryption scheme based on chaos and DNA encoding,” IEEE Access, vol. 7, pp. 36667-36681, March 2019.
24. [24] I. Aouissaoui, T. Bakir, and A. Sakly, “Robustly correlated key- medical image for DNA-chaos based encryption,” IET Image Process., vol. 15, no. 12, pp. 2770-2786, October 2021.
25. [25] P.T. Akkasaligar and S. Biradar, “Medical image encryption with integrity using DNA and chaotic map,” in Recent Trends in Image Processing and Pattern Recognition, vol. 1036, K. Santosh, and R. Hegadi, Eds. Springer, Singapore, July 2019, pp. 143-153.
26. [26] R. Guesmi, and M.B. Farah, “A new efficient medical image cipher based on hybrid chaotic map and DNA code,” Multimed. Tool Appl., vol. 80, pp. 1925-1944, January 2021.
27. [27] S.A. Banu and R. Amirtharajan, “A robust medical image encryption in dual domain: chaos-DNA-IWT combined approach,” Med. Biol. Eng. Comput., vol. 58, pp. 1445-1458, July 2020.
28. [28] D. Ravichandran, S.A. Banu, B.K. Murthy, V. Balasubramanian, S. Fathima, and R. Amirtharajan, “An efficient medical image encryption
29. using hybrid DNA computing and chaos in transform domain,” Med. Biol. Eng. Comput., vol. 59, pp. 589-605, March 2021.
30. [29] 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, April 2021.
31. [30] M. Gafsi, N. Abbassi, M.A. Hajjaji, J. Malek, and A. Mtibaa, “Improved chaos-based cryptosystem for medical image encryption and decryption,” Sci. Program., pp. 1-22, December 2020.
32. [31] F. Masood, M. Driss, W. Boulila, J. Ahmad, S.U. Rehman, S.U. Jan,
33. Qayyum, and W.J. Buchanan, “A lightweight chaos-based medical image encryption scheme using random shuffling and XOR operations,” Wirel. Pers. Commun., pp. 1-28, November 2022.
34. [32] P.T. Akkasaligar and S. Biradar, “Selective medical image encryption using DNA cryptography,” Inf. Secur. J., vol. 29, no. 2, pp. 91-101, March 2020.
35. [33] 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, December 2021.
36. [34] Y. Li, C. Wang, and H. Chen, “A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation,” Opt. Lasers. Eng., vol. 90, pp. 238-246, March 2017.
37. [35] K.A.K. Patro and B. Acharya, “A simple, secure, and time-efficient bit- plane operated bit-level image encryption scheme using 1-D chaotic maps,”in Innovations in Soft Computing and Information Technology,
38. J. Chattopadhyay, R. Singh, and V. Bhattacherjee, Eds, Springer, Singapore, 2019, pp. 261-278.
39. [36] A. Kulsoom, D. Xiao, and S.A. Abbas, “An efficient and noise resistive selective image encryption scheme for gray images based on chaotic maps and DNA complementary rules,” Multimed. Tools. Appl., vol. 75, no. 1, pp. 1–23, January 2016.
40. [37] D. Sravanthi, K.A.K. Patro, B. Acharya, and S. Majumder, “A secure chaotic image encryption based on bit-plane operation,” in Soft computing in data analytics, vol. 758, J.

Nayak, A. Abraham, B. Krishna, G. Chandra Sekhar, and A. Das, Eds. Springer, Singapore, 2019, pp. 717-726.

41. [38] K.A.K. Patro, B. Acharya, and V. Nath, "Secure multilevel permutation-diffusion based image encryption using chaotic and hyper- chaotic maps," Microsyst. Technol., vol. 25, no. 12, pp.4593-4607, December 2019.
42. [39] K.A.K.Patro, M.P.J.Babu, K.P.Kumar, and B. Acharya, "Dual-Layer DNA-Encoding–Decoding Operation Based Image Encryption Using One-Dimensional Chaotic Map,"in Advances in Data and Information Sciences, vol. 94, M. Kolhe, S. Tiwari, M. Trivedi, and K. Mishra, Eds. Springer, Singapore, January 2020, pp. 67-80.
43. [40] K.A.K. Patro, B. Acharya, and V. Nath, "Secure multilevel permutation-diffusion based image encryption using chaotic and hyper- chaotic maps," Microsyst. Technol., vol. 25, no. 12, pp.4593-4607, December 2019.