Design and Analysis of a High-Efficiency Chaotic Encryption Algorithm for Image Security in ICT Frameworks

Ashok G[1*], Jose Anand A[2]

1. Assistant Professor, Department of Biomedical Engineering, J.N.N Institute of Engineering, Kannigaipair, Uthukottai Taluk, Tiruvallur District, Tamil Nadu 601102, India

2. Professor, Department of Electronics and Communication Engineering, KCG College of Technology, Chennai, Tamil Nadu, India 600097

Abstract:

With millions of people sharing photos over the internet for a variety of personal and professional reasons, secure transfer of images is a challenging topic in the age of communication technology. Encryption algorithms such a cryptographic images contribute to the secure transfer of information about the network. The development of a strong and effective method for medial image encryption is to ensure integrity, change in medical imagery that leads to misdiagnosis to safely and personally prevent patient medical documents and to prevent cyberattacks. Medical image encryption is common in telemedicine, marking secure image transfer extremely important. The dataset includes personal health information about patients. All important information, including medical images, is currently stored on images and communications servers due to growing interest in hospitalization records around the world. This study presented a unique approach to medical image encryption combining triple data encryption algorithms (3DES) and advanced encryption standards (AES) WITH THREE CHAOTIC MAPS (LOGISTIC, Amold Cat, Baker). The BAT optimization algorithm is also used to satisfy the task of key generation. Finally, use the least significant bit (LSB) to hide the encrypted medical images before they are sent to the server via the TCP/IP protocol.

Keywords:
Cryptographic Image, Least significant bit (LBS), Image encryption, chaotic map, triple data encryption standard (3DES), advanced encryption standard (AES), Bat algorithm (BA).

1. Introduction

In the modern digital era, access to the Internet has become one of the most essential human necessities[1].The rapid advancement of digital communication and networking technologies has significantly enhanced data storage capabilities and electronic information exchange[2].However, alongside these developments, ensuring data integrity and network security has become increasingly critical, particularly when dealing with sensitive and private information. Among the vast amount of content transmitted and stored online, digital images constitute a major portion[4]. Consequently, image encryption techniques are widely employed to preserve the authenticity, confidentiality, and integrity of digital images. This requirement becomes even more crucial in the medical domain, where diagnostic images contain highly sensitive patient information.

During the transmission of medical images over public networks, confidentiality must be strictly maintained. If an attacker intercepts and manipulates a medical image, it may lead to incorrect diagnosis and serious clinical consequences[5]. Therefore, protecting medical images against unauthorized access, tampering, and security breaches has become a significant challenge. To address these concerns, robust and secure encryption mechanisms must be implemented to ensure safe transmission while preserving both confidentiality and integrity.

Cryptography, steganography, and watermarking are often used techniques in me dical picture security [6].Cryptography involves the examination of data encoding to avert unauthorized entities from deciphering it. The current popularity of image cryptography can be attributed to the necessity for effective encryption, which demands the management of certain intrinsic features. The fundamental characteristics of images encompass a significant correlation among adjacent pixels, high redundancy, and substantial volume [7]. When implemented directly on images, several text-based encryption algorithms, including AES and DES, prove to be less effective [8]. Among the most prominent and suitable methodologies for image encryption is a chaotic system. This approach secures data through a pixel randomization technique. It possesses numerous inherent advantages, such as sensitivity to control parameters and initial conditions, ergodicity, pseudo randomness, and aperiodicity [9]. Nonetheless, since this method solely scrambles pixel locations and the image's entropy, and despite histogram values remaining unchanged, these two factors are utilized to evaluate the security of image encryption

against statistical attacks [10].
The chaotic system is frequently combined with various methods to enhance image encryption security, including XOR substitution or additional techniques such as El Gamal, compressed sensing, elliptic curves, and DNA coding, among others [11]. Figure 1 illustrates the methods utilized for data encryption, the majority of which were applied in this study.

Derived from the insights of prior investigations, this study introduces a chaotic framework, data obfuscation, and traditional cryptographic techniques with specific enhancements, such as a BA optimization algorithm for key management. The primary aim is to augment the diffusion and permutation processes to ensure that the encryption outcomes exhibit greater resilience to various attacks. Furthermore, the encryption results were evaluated employing a multitude of techniques, including correlation coefficient analysis, histogram examination, MSE, information entropy, avalanche effect, and PSNR. Consequently, the principal contribution of this paper is the provision of diverse chaotic mappings for data encryption and evaluation criteria for image encryption. Ultimately, contemporary challenges are highlighted, alongside a range of potential research avenues that could bridge the gaps in these domains, thereby aiding the efforts of both developers and scholars.
The structure of the paper is organized as follows: Related works are outlined in Section 2. The proposed methodology, encompassing encryption and decryption techniques, is detailed in Section 3. Section 4 includes an analysis of the implementation results concerning medical imagery. Finally, Section 5 presents a summary of the findings.

2.Related Works

This section encompasses the latest chaos-based image encryption methodologies. Numerous image encryption techniques have been proposed, exhibiting variations in robustness and effectiveness. This document introduces methods for encoding images utilizing chaos.
Askar et al. [13] employed chaotic mappings to devise a pseudo-random number generator aimed at formulating a color image encryption and decryption technique. For key generation, this research amalgamates two Logistic maps. The subsequent key is utilized during the processes of obfuscation and dissemination. The confusion phase permutes the pixels of the image, while the diffusion phase

modifies the values of each pixel. The results indicated that this algorithm demonstrated significant accuracy and speed. Bhogal et al. [14] formulated a technique that integrated a chaotic map with AES and evaluated it against the traditional version of AES.This analysis allowed them to explore the influence of the chaotic map on encryption performance. CAT-AES secures data by repeatedly applying Arnold's cat map, unlike conventional AES encryption.The outcomes revealed an enhancement in encryption quality, with the histograms exhibiting greater consistency and the absolute correlation coefficient approaching 0 for several images analyzed post-CAT-AES encryption. Al-Khasawneh et al. [15] suggested an image encryption method founded on multi-chaos. Since a multi-chaotic system underpins the proposed approach, it can effectively address the challenges associated with algorithms reliant on low-dimensional chaotic mappings. Bit and pixel-level permutations are employed to bolster the security of the cryptosystem. Several evaluations were performed to affirm the safety and resilience of the suggested image encryption technique. Gatta and Abd Al-Latief [16] introduced a methodology to protect medical images, which play a crucial role in healthcare facilities. The main aim of this study is to develop a strong encryption method that preserves the integrity of medical treatment and diagnosis while enabling the high-quality, distortion-free reconstruction of the original image from the encrypted format.The experimental results indicate the effectiveness of the proposed approach through various statistical measures and a significant correlation between the original and decrypted images. Kumar et al. [17] proposed an advanced method for encrypting medical images. This technique employs partial discrete cosine transformations, which are resilient to differential, statistical, and brute force attacks, devised via chaotic mappings. The sensitivity of this proposed technique is approximately 10^{12}. In terms of performance, the recommended methodology surpasses numerous cutting-edge algorithms due to its expansive key space of 10^{60}. The results establish a foundation for a range of potential real-time medical applications, including mobile healthcare and wireless networking for medical image protection. Farah et al. [18] introduced a groundbreaking hybrid chaotic map in conjunction with a unique method to improve encryption algorithm efficacy. In terms of unpredictability and sensitivity, the proposed chaotic map outperforms existing chaotic functions. The distinctive mathematical function excels over traditional maps based on its Lyapunov coefficients and entropy metrics. They propose a new image cipher inspired by Shannon's confusion and diffusion

properties. The aim of the optimization procedure is to produce a bijective matrix distinguished by elevated nonlinearity. Yin and Li [19] introduced a medical encryption technique founded on genetic simulated annealing particle swarm optimization (GSAPSO). Experimental results demonstrate that the encryption system effectively disrupts the correlation among adjacent pixels, yielding a cipher text image with a high degree of unpredictability and dispersion. It is resilient against statistical analysis, differential attacks, brute force assaults, and various other threats. Furthermore, it is capable of performing computational tasks and exhibits high encryption efficiency. Yasser et al. [20] proposed a collection of new chaotic maps that utilize discrete wavelet transforms (DWT) and dual chaotic functions to enhance encryption quality and execution. Consequently, the proposed framework circumvented various existing cryptanalysis techniques and cryptographic threats. The dynamic analysis and sampling entropy methods indicated that the proposed map is typically hyper chaotic, showcasing high sensitivity and complexity. Akan et al. [21] introduced an improved methodology for medical image encryption based on a hybrid chaotic permutation technique and a 3D logistic map to safeguard the privacy of patients' medical images during transmission and storage. They implemented a combination of bit-level and block-level pixel scrambling during the confusion phase. The method for image pixel rearrangement involves initially scrambling the image sub-blocks randomly, followed by shuffling individual pixels within each sub-block using the 3D logistic chaotic mapping system. Hashim et al. [22] described a novel approach to securing these images against AES and chaotic system attacks.

The proposed medical image encryption technique employs sophisticated cryptographic foundations to accomplish the following: 1) A substantial key space that makes brute force attempts impractical. 2) Prior to the implementation of the AES method, medical image scrambling offers enhanced security compared to utilizing AES independently. Due to the inadequacy of the conventional image encryption algorithm for authentication purposes, it is being supplanted by a more effective approach. Regarding security, the suggested approach exceeds the current AES algorithm. Chaudhary et al. [23] Conceived and assessed block cipher image encryption and chaos-driven photo encryption techniques. AES is utilized as a block cipher framework, while Arnold cat maps and a logistic map serve as fundamental and integrated chaotic algorithms, respectively.. The Chaos and AES algorithms are

employed for image encryption. The research indicates that the hybrid chaotic map exhibits greater resilience to differential or chosen plaintext attacks due to its elevated NPCR and UACI values. Abdallah and Farhan [24] introduced an innovative image encryption method founded on the principles of confusion and diffusion. The innovative S-confusion Box principle and the diffusion applicator in New IP depend on a multi-chaotic paradigm. This chaotic system is influenced by the initial parameters. When any parameter changes, the substitution and permutation processes are modified. In our methodology, shuffling operations are utilized to augment the distinction between plain and encrypted images. The results from the preceding tables demonstrate that the proposed method is more robust against adversaries attempting to retrieve plain image data. To establish robust encryption against various forms of attacks, Rachmawanto and Zulfiningrum [25] proposed an image encryption process that integrates multiple techniques. These techniques encompass block-based substitution, chaotic hashing, diffusion with logistic maps, scrambling for confusion operations, combined hash functions, and dynamic bit shifting based on Josephus sequences. Based on the experimental results, three categories of images were employed: normal, special, and medical images. It has been evidenced that the proposed encryption methodology is resistant to statistical and differential attacks.

3. Methodology

The proposed framework depicted in Figure 2 intends to enhance the security of medical images due to the delicate nature and confidentiality of the data it encompasses. Consequently, a collection of information security methodologies, including image cryptography and image concealment, has been implemented to achieve this objective, which will be elaborated upon in this section. No predefined dataset was utilized; instead, a selection of random images of varying dimensions was employed. The client acquires a two-dimensional medical image that has been encrypted using the 3DES and LSB algorithms. A key is produced via BAT optimization and AES encryption. The image undergoes encryption utilizing a chaotic map, repeated for N iterations. The secret key formulated by BAT can affect the number of iterations. The TCP/IP protocol enables data transmission between the client and server. All functions are executed in reverse order on the server. Given that medical images contain sensitive and confidential information, the proposed

system aims to enhance security for these types of images. To achieve this, a variety of information security techniques were adopted, including image cryptography and image concealment. This section will discuss these methods in greater detail.

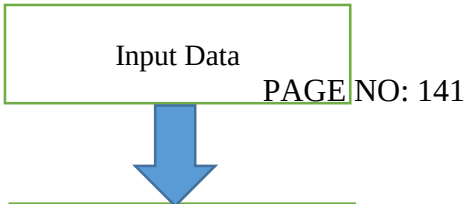
3.1 Optimized Cryptographic Key Generation Using the BAT Algorithm

The Bat Algorithm is a population-oriented metaheuristic derived from the hunting behaviors of bats. Bats utilize bio sonar in darkness to navigate obstacles and locate prey or roosts, allowing them to differentiate among various nearby objects through echoes. Their echolocation abilities enable bats to discern between background obstacles and targets by measuring distance. Bats consistently fly at a random velocity (v_i) at a fixed frequency (f_{min}), although their wavelengths (λ) and amplitudes (A0) may vary based on location (x_i) to pursue prey. The intensity of a bat's pulse can fluctuate significantly. However, Yang theorized that it varies between a substantial positive value (A0) and a minimal constant value (A_{min}). Equations (1), (2), and (3) were calibrated to generate distinct solutions in the simulation by adjusting frequency, amplitude, and pulse rate. A new solution is considered superior to a previous one based on the precision with which the solutions were fine-tuned by modifying amplitude and pulse rate, which is evaluated by proximity to the optimal solution [26].

$$f_i=f_{min}+(f_{max}-f_{min})\beta fi=f_{min}+(f_{max}-f_{min})\beta \quad (1)$$
$$v^t{}_i=v^t-1i+(x^t{}_i-x*)f_iv_i{}^t=v_i{}^t-1+(x_i{}^t-x*)f_i \quad (2)$$
$$x^t{}_i=x^t-1i+v^t{}_ix_i{}^t=x_i{}^t-1+v_i{}^t \quad (3)$$

Where x_i represents the position of the optimal bat within the swarm and β denotes a stochastic vector distributed across the range [0,1]. Figure 3 illustrates the behavior of the bat [27].The key utilized for the 3DES algorithm to encode input data is randomly generated each time using the bat algorithm, thereby significantly complicating the acquisition of the key.

Encryption Phase



Decryption Phase

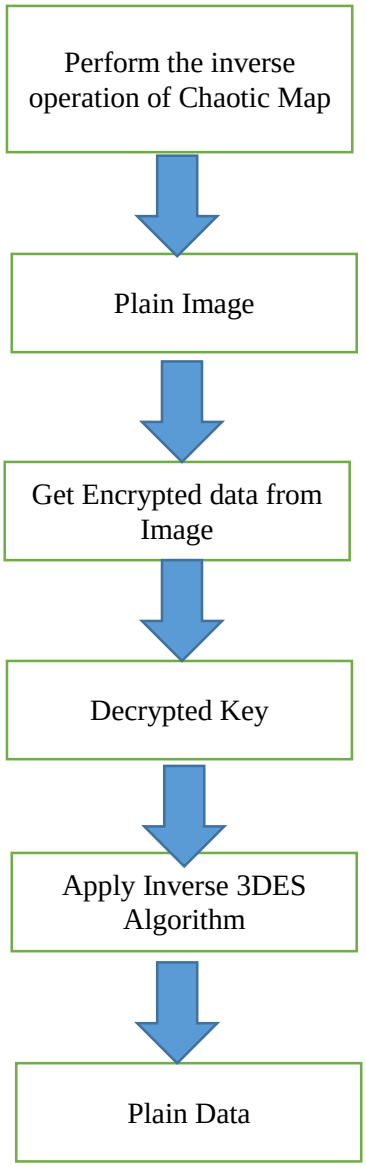


Figure 1,2. An overall diagram of the proposed method

3.2 Encryption of Generated Key Using Advanced Encryption Standard (AES)

NIST advocated for the AES as a contemporary encryption method in 2001 to supplant DES.AES can accommodate any database collection. Through encryption-decryption, the AES algorithm processes 10 iterations for 128-bit keys. After 12 rounds for 192-bit keys and 14 rounds for 256-bit keys, the final cipher text is produced. AES supports a 128-bit information length, which can be divided into four fundamental active blocks. These components are treated as a sequence of bytes,

which are combined to form "the state," a 4 by 4 matrix [28]. The key generated using the bat algorithm in the preceding stage will be utilized to encrypt the patient's data after it has been encrypted with the AES algorithm.

3.3 Securing Data with Triple Data Encryption Standard (3DES)

It was created to address the weaknesses of DES while maintaining the same encryption approach. The 3DES key size is 56 bits. To achieve this, the process is applied three times consecutively, using three unique keys. The total length is 168 bits. TDEA employs three 64-bit DEA keys (K1, K2, and K3) during the encode-decode-encode (EDE) phase [29]. At this stage, the keys generated and encrypted in the prior phases are employed as keys for the conventional 3DES algorithm, where the data input at this phase of the proposed system is encrypted.

3.4 Securing Data with the Triple Data Encryption Standard

In the spatial domain, where a digital image is composed of a matrix of color values and intensity, the Least Significant Bit (LSB) technique is the most prevalent. The LSB method's secret message bits instantaneously substitute the cover image pixels with some or all the LSBs. Due to the modification of the LSB of the host pixels leading to negligible variation in the image, the resulting photograph closely resembles the original image. A grayscale image contains 8 bits per pixel, while a color image possesses 24 bits per pixel, with 8 bits allocated for each color component (RGB) [30]. Data encrypted using LSB technology is concealed in the final phase of the proposed system.

3.5 Encrypt image that contains hiding data by chaotic maps

Three tumultuous mappings are employed to secure the image within which the concealed data is embedded, and the outcomes of these techniques are subsequently evaluated.

3.5.1 Chaotic Dynamics of the Logistic Map

Among these, logistic chaotic mapping stands out as one of the most commonly employed frameworks. The logistic equation was refined by American ecologist May R. Logistic, commonly known as the wormhole model. A suggestion was put forth in 1976.During that period, the relationship between the number of varied insect populations and environmental factors was examined using the logistic equation. It constituted a one-dimensional nonlinear equation that was both significant and fundamental [31]. Eq. (4) is presented in the logistic map:

$y_{n+1}=\mu y_n(1-yn)y_{n+1}=\mu y_n(1-yn)$ (4)

Where, $y0\in(0, 1)$ signifies the chaotic system's initial condition at any moment, and $\mu\in(0, 4)$ is the bifurcation parameter also known as the system parameter. The subsequent state of the system is denoted by y_{n+1}, where n indicates the discrete time. The extent of the control factor dramatically influences the behavior of the logistic map μ [32].

3.5.2 Arnold cat map

The Arnold cat map, a bi-dimensional chaotic framework, was introduced by Vladimir Arnold in 1960. It serves as a fundamental illustration of chaos theory. To establish an NN matrix, an image must be converted into the appropriate number of pixels. In the real interval [0, 1), the coordinates of each pixel are represented by an ordered pair of (X, Y), which is determined by two independent equations (5) and (6) as follows:

$X_{n+1}=X_n+Ay_n(\text{Mod } N)X_{n+1}=X_n+Ay_n(\text{Mod } N)$ (5)
$Y_{n+}1=BX_n+ABY_n(\text{Mod } N)Y_{n+1}=BX_n+ABY_n(\text{Mod } N)$ (6)

Where A, B are two positive integer control parameters, Xn, Yn are the sample coordinates in the N×N matrix, and n=1, 2, 3, N-1. The transformed coordinates following the cat map are denoted by X_{n+1}, Y_{n+1}. The encryption technique is performed via a cat map iteration; following M iterations, there are T positive

integers for which $(X_{n+1}, Y_{n+1})=(X_n, Y_n)$. The variables A and B, in conjunction with the sample matrix dimension (N×N matrix), ascertain the time T [33, 34].

3.5.3 Baker map

The chaotic Baker map is a widely utilized encryption methodology in image processing. It is a permutation-based mechanism that alters pixel coordinates in an NN-dimensional square matrix through the application of a secret key. It assigns a pixel to a bijective mode-positioned pixel. The discretized Baker map can be employed to generate random numbers within a square matrix. B[n1,. . , nk] signifies the discretized map, while the vector [n1,. . . , nk] represents the secret key, Skey. The secret key is selected such that N is the count of data items in a single row, and each integer ni divides N, with n1+. . . +nk=N. Let us assume that Ni = n1+. . . ,+ni. As indicated by Eq (7), the indices (r, s) data item is moved to the indices[35].

$$B(r,s)=Nn_i(r-N_i)+(smod(Nn_i))\cdot n_iN+(s-s(Nn_i))+N_i \ldots\ldots(7)$$

The following steps are taken to accomplish the chaotic permutation:
(1) N rectangles with a width of N_i,n_i are generated, and the NN square matrix is created by partitioning the total number of components N.
(2) Within the permuted rectangle, the components of each rectangle are arranged in a row. Upper triangles are processed first, followed by lower rectangles, moving from left to right. Within each rectangle, the scan progresses upward from the bottomleftcorner[36].

3.5.4 Secure Image Delivery Using TCP/IP Protocol

Transmission Control Protocol (TCP) and Internet Protocol (IP) are two of the most fundamental protocols that make up the TCP/IP protocol suite. TCP/IP, akin to other networking frameworks, is organized in layers. Simple interfaces are employed by layers to interact with those both above and below them. A layer utilizes the services provided by the layer beneath in order to furnish a solution to the layer above [37]. Data is transmitted from the client to the server, where it is processed inversely on the server side to yield encrypted patient information.

3.5.5 Attack types in images

This section introduces some frequent attacks in picture processing [38]:

(1) Cipher text-only

(2) Known-plaintext

(3) Chosen-plaintext

(4) Brute-force

(5) Differential attack

(6) Noise

(7) Occlusion

(8) Entropy

4**.** Interpretation of Experimental Results

The statistical analysis parameters used to assess the efficacy of encryption include Mean Squared Error (MSE), Root Mean Squared Error (RMSE), Normalized Root Mean Squared Error (NRMSE), Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), Information Entropy (IE), Correlation Coefficient, and Execution Time (ET). Table 1 provides specific measurements for several of them [39, 40].A set of medical images was utilized to test the suggested system as shown in Table 2.The Figures 4-9 show the results testing of the three chaotic maps used in this work.

Table 1. A technique for picture encryption evaluation

Metric	Purpose	Calculation Formula	Interpretation
MSE (Mean Squared Error)	Quantifies the average difference between the original and encrypted/decrypted image.	$MSE=MN1\sum i=1M\sum j=1N [P(i,j)-C(i,j)]2$	Lower MSE values suggest minimal distortion; ideally near zero.
PSNR (Peak Signal-to-Noise Ratio)	Compares image fidelity between original and decrypted versions using a logarithmic scale.	$PSNR=10\log_{10}(MSE(2n-1)2)$	Higher PSNR indicates better recovery quality; should be high for effective decryption.
SSIM (Structural Similarity Index)	Evaluates perceived visual similarity by examining structure, contrast, and brightness.	$SSIM(x,y)=[l(x,y)]\alpha\cdot[c(x,y)]\beta\cdot[s(x,y)]\gamma$	SSIM value of 1 indicates identical structure; closer to 1 is better.
IE (Information Entropy)	Measures the level of randomness or data dispersion in an image.	$Entropy=-\sum i=02n-1P(mi)\log2[P(mi)]$	For 8-bit images, values near 8 show high randomness and secure encryption.
ET (Execution Time)	Indicates the total time required to run the encryption or decryption process.	Measured in milliseconds, seconds, or minutes	High Efficiency.

Table 2: Performance Summary of Image Encryption Evaluation Using Chaotic

Maps

MSE	RMSE	NRMSE	Entropy	Correlation	Time to Encrypt (s)	Time to Decrypt (s)
0.0001	0.0102	0.0001	5.4102	0.3907	0.107	0.054
0.0001	0.0110	0.0001	5.4102	0.3907	0.112	0.062
0.0001	0.0127	0.0001	5.4102	0.3907	0.114	0.054
0.0001	0.0130	0.0001	5.9251	0.9999	0.480	0.333
0.0001	0.0138	0.0001	5.9251	0.9999	0.439	0.327
0.0001	0.0136	0.0001	5.9251	0.9999	0.469	0.338
0.0001	0.0138	0.0002	3.1338	0.9999	0.103	0.440
0.0001	0.0142	0.0002	3.1339	0.9999	0.106	0.410
0.0001	0.0139	0.0002	3.1338	0.9999	0.113	0.390
0.0001	0.0140	0.0002	3.9733	0.9999	0.452	0.459
0.0001	0.0139	0.0002	3.9733	0.9999	0.432	0.382
0.0001	0.0138	0.0002	3.9733	0.9999	0.444	0.386
0.0001	0.1047	0.0004	2.7972	0.9999	0.209	0.181
0.0001	0.0137	0.0003	2.7970	0.9999	0.223	0.187
0.0001	0.0136	0.0003	2.7970	0.9999	0.206	0.179
0.0001	0.0139	0.0002	2.5655	0.9999	0.398	0.285
0.0001	0.0130	0.0002	2.5653	0.9999	0.390	0.252
0.0002	0.0147	0.0002	2.5657	0.9999	0.390	0.270

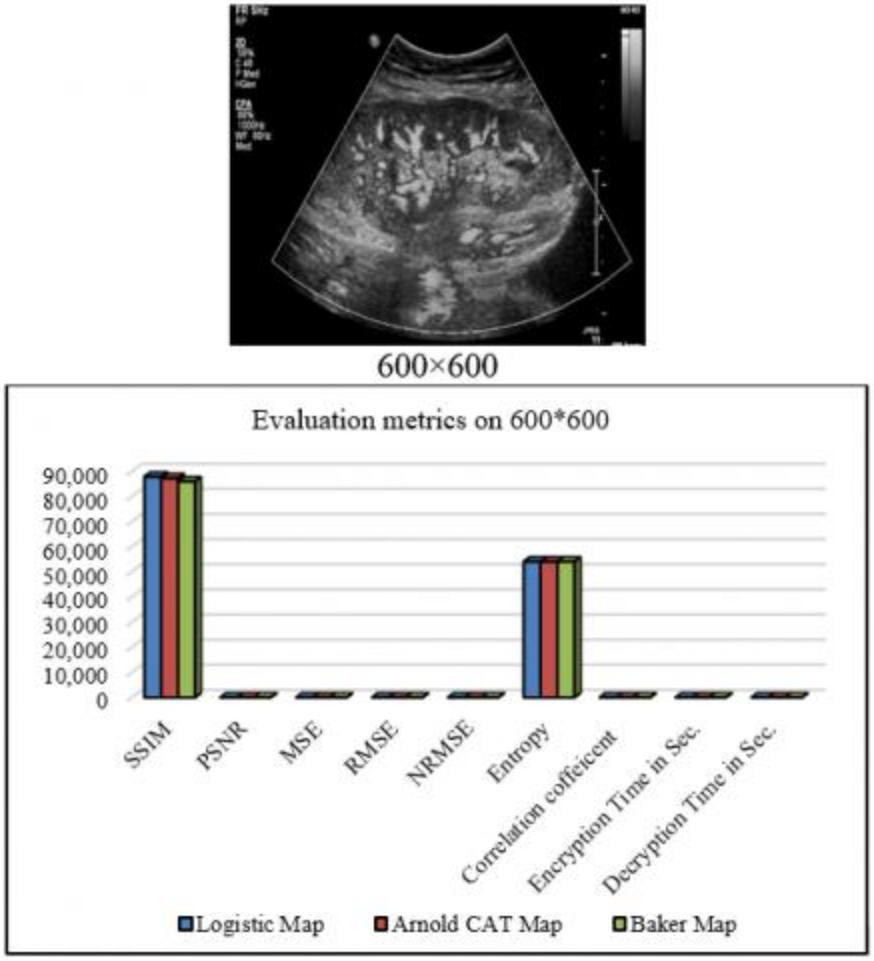


Figure 4. Evaluation metrics on 600*600 image

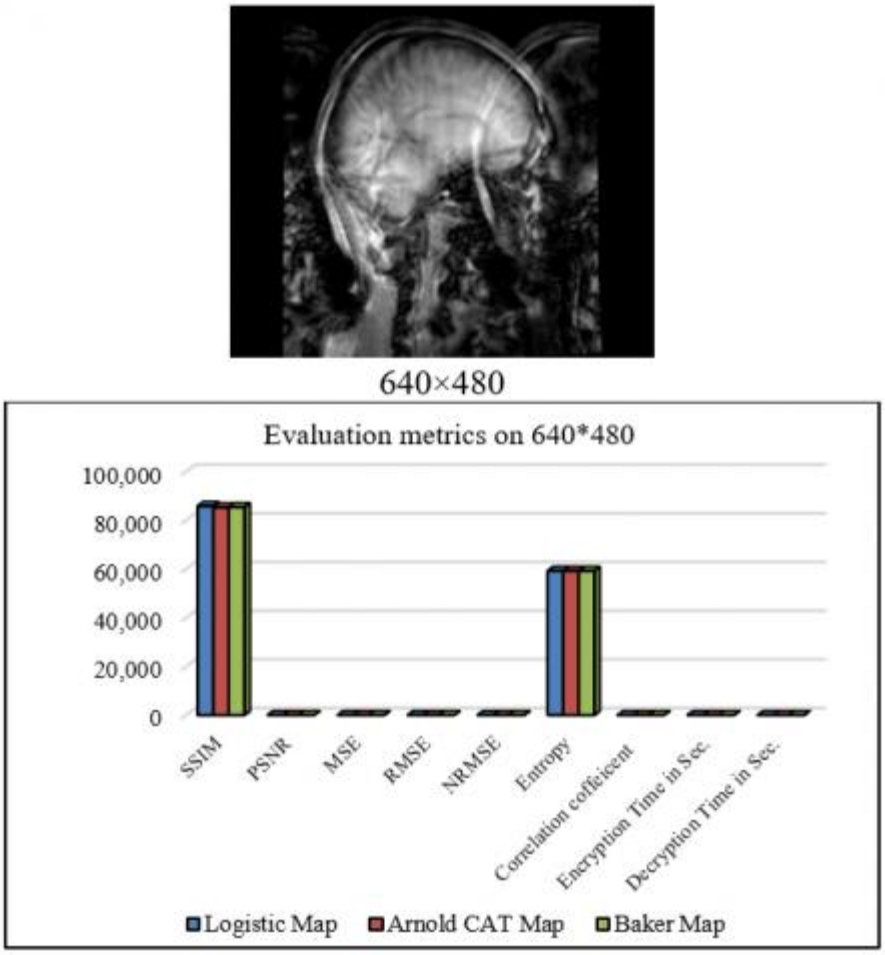


Figure 5. Evaluation metrics on 640*480 image

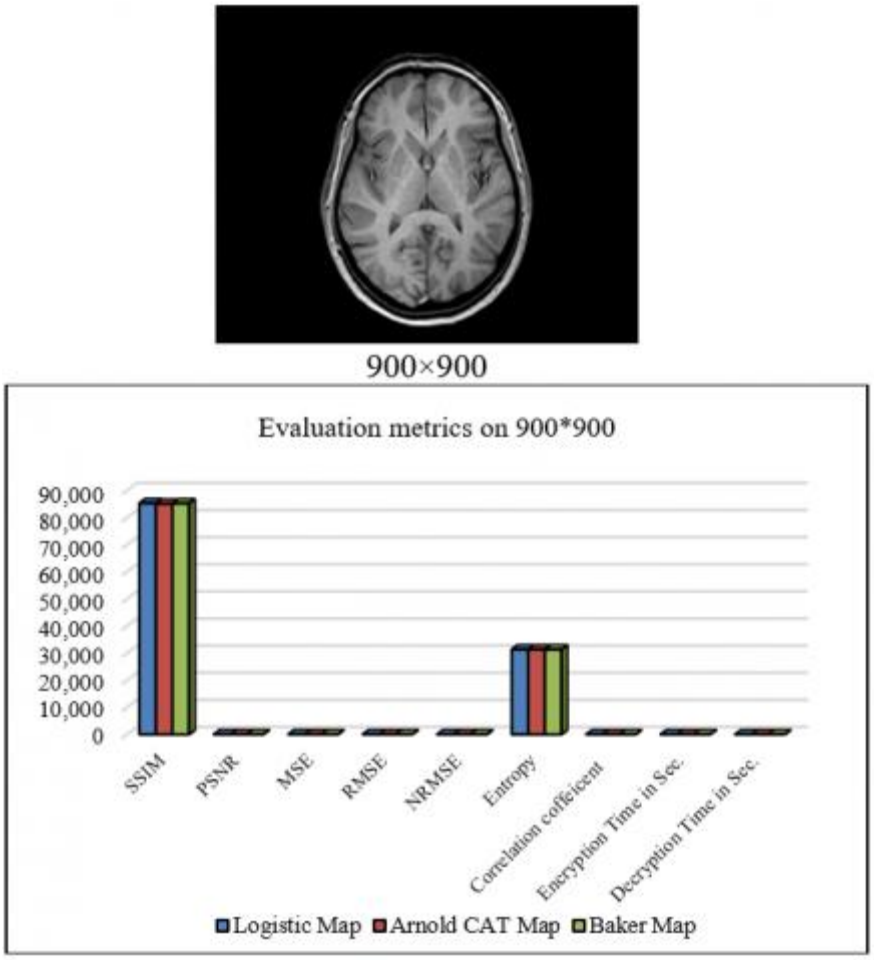


Figure 6. Evaluation metrics on 900*900 image

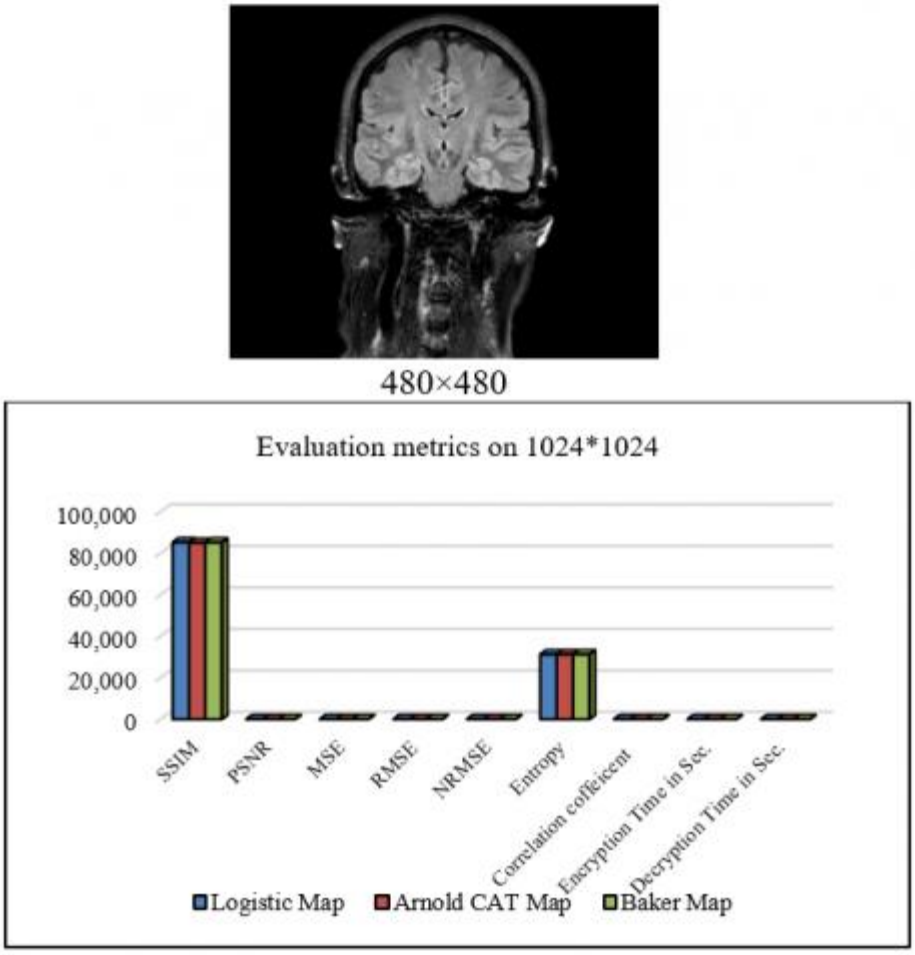


Figure 7. Evaluation metrics on 1024*1024 image

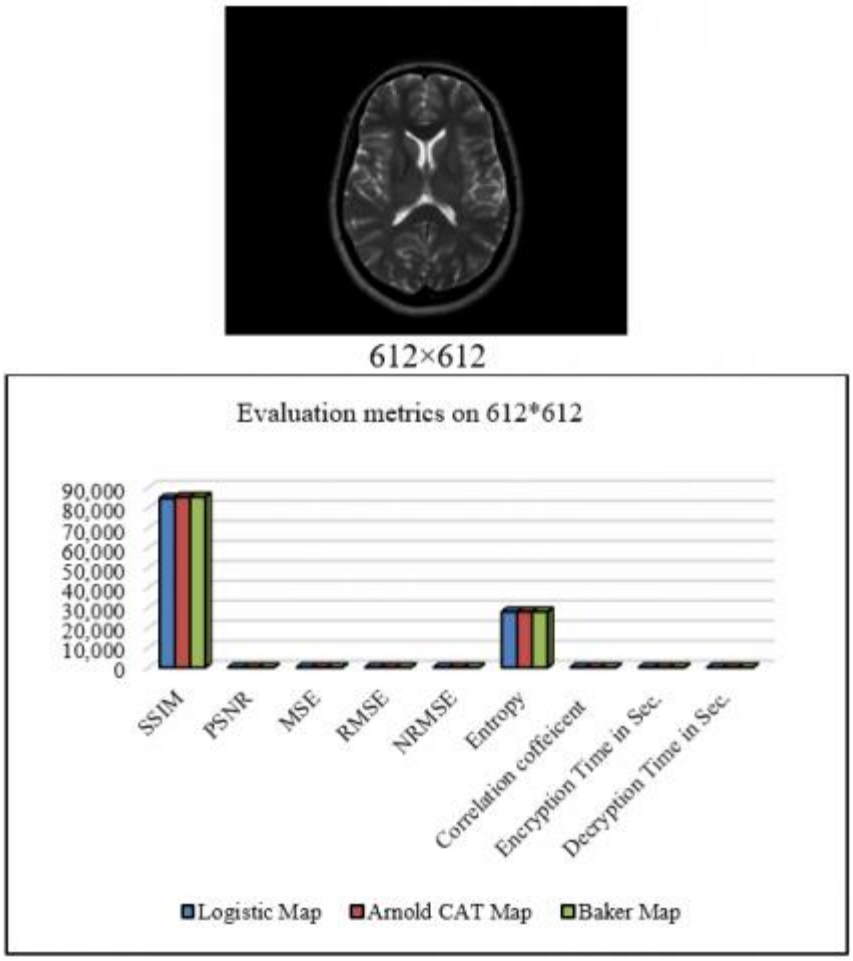


Figure 8. Evaluation metrics on 612*612 image

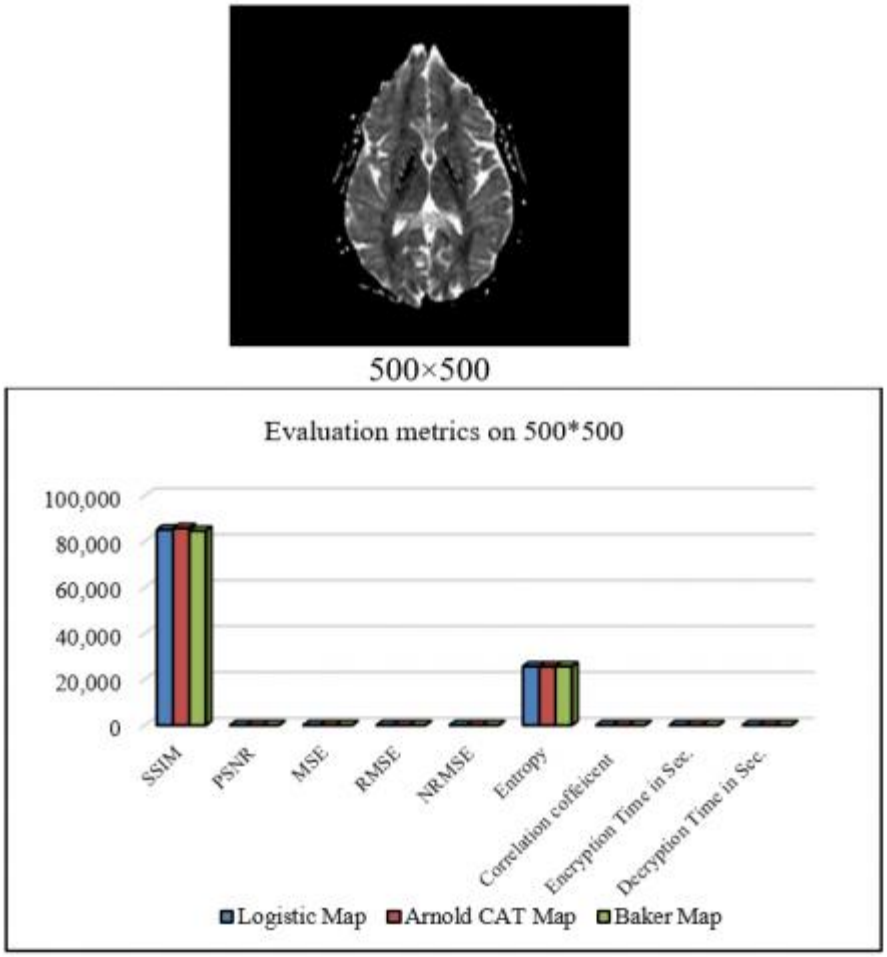


Figure 9. Evaluation metrics on 500*500 image

It is clear from the preceding table and diagrams that, when utilizing the three chaotic maps, the scale values are remarkably comparable and exhibit minimal variation. Employing Arnold's cat map, the highest similarity scale value was 85.5, whereas the minimum value was 84.5. All evaluation results indicated a PSNR of 0.9999 and an MSE of 0.0001, signifying that the image was retrieved with the least conceivable error rate following encoding. This is also applicable to the NRMSE values, which fluctuated between 0.0001 and 0.0002, and the RMSE values, which ranged from 0.0136 to 0.0145. These figures hold equivalent significance to the MSE scale. Ultimately, the entropy values spanned from 3.1338 to 5.925.

Conclusions

Encrypting medical images may potentially resolve various e-health application challenges. These challenges encompass identity theft, data protection, private data transmission, management, and storage of e-health information. This research presented an innovative technique for medical image encryption based on three chaotic mappings (Logistic, Arnold CAT, and Baker) in conjunction with the 3DES and AES algorithms. The BAT optimization framework is additionally utilized for key generation. In the final stage, encrypted medical images are securely embedded using the Least Significant Bit (LSB) technique. This steganographic approach ensures that the presence of the encrypted data remains hidden within a cover medium. Once embedded, the images are transmitted to the server using the TCP/IP protocol, enabling secure and reliable communication over the network. The experiments produced encouraging results in MSE, PSNR, and SSIM, indicating that the image is restored accurately, without any information loss. In terms of collection, entropy results remained within range and did not exceed 8 degrees. Furthermore, in all instances, the execution time was fractions of a second or less. For future endeavors, we recommend employing additional chaotic maps with datasets rather than arbitrarily selected medical images.

Acknowledgment

This document has been prepared solely for scholarly and research objectives, and to support scholars across diverse disciplines and areas of expertise.

References

[1] Alawida, M., Samsudin, A., Teh, J.S., Alkhawaldeh, R.S. (2019). A new hybrid digital chaotic system with applications in image encryption. Signal Processing, 160: 45-58.https://doi.org/10.1155/2020/9597619

[2] Ali, T.S., Ali, R. (2020). A new chaos based color image encryption algorithm using permutation substitution and Boolean operation. Multimedia Tools and Applications, 79(27-28): 19853-19873. https://doi.org/10.1007/s11042-020-08850-5

[3] Arab, A., Rostami, M.J., Ghavami, B. (2019). An image encryption method based on chaos system and AES algorithm. The Journal of Supercomputing, 75: 6663-6682.https://doi.org/10.1007/s11227-019-02878-7

[4] Broumandnia, A. (2019). Designing digital image encryption using 2D and 3D reversible modular chaotic maps. Journal of Information Security and Applications, 47:188-198.https://doi.org/10.1016/j.jisa.2019.05.004

[5] Ghadirli, H.M., Nodehi, A., Enayatifar, R. (2019). An overview of encryption algorithms in color images. Signal Processing, 164: 163-185. https://doi.org/10.1016/j.sigpro.2019.06.010

[6] Ismail, S.M., Said, L.A., Radwan, A.G., Madian, A.H., Abu-Elyazeed, M.F. (2018). Generalized double-humped logistic map-based medical image encryption. Journal of Advanced Research, 10: 85-98. https://doi.org/10.1016/j.jare.2018.01.009

[7] Kamal, S.T., Hosny, K.M., Elgindy, T.M., Darwish, M.M., Fouda, M.M. (2021). A new image encryption algorithm for grey and color medical images. IEEE Access, 9:37855-37865.https://doi.org/10.1109/ACCESS.2021.3063237

[8] Kandar, S., Chaudhuri, D., Bhattacharjee, A., Dhara, B.C. (2019). Image encryption using sequence generated by cyclic group. Journal of Information Security and Applications, 44: 117-129. https://doi.org/10.1016/j.jisa.2018.12.003

[9] Khan, J.S., Kayhan, S.K. (2021). Chaos and compressive sensing based novel image encryption scheme. Journal of Information Security and Applications, 58: 102711.https://doi.org/10.1016/j.jisa.2020.102711

[10] Wang, R., Deng, G.Q., Duan, X.. (2021). An image encryption scheme based on double chaotic cyclic shift and Josephus problem. Journal of Information Security and Applications, 58: 102699. https://doi.org/10.1016/j.jisa.2020.102699

[11] Luo, Y., Ouyang, X., Liu, J., Cao, L. (2019). An image encryption method based on elliptic curve elgamal encryption and chaotic systems. IEEE Access, 7: 38507-38522.https://doi.org/10.1109/ACCESS.2019.2906052

[12] Heo, J., Jeong, J. (2021). Deceptive techniques to hide a compressed video stream for information security. Sensors, 21(21): 7200. https://doi.org/10.3390/s21217200

[13] Askar, S.S., Karawia, A.A., Alshamrani, A. (2015). Image encryption algorithm based on chaotic economic model. Mathematical Problems in Engineering, 2015: 341729.https://doi.org/10.1155/2015/341729

[14] Bhogal, R.S., Li, B., Gale, A., Chen, Y. (2018). Medical image encryption using chaotic map improved advanced encryption standard. IJ Information Technology and Computer Science, 8: 1-10. https://doi.org/10.1155/2022/9363377

[15] Al-Khasawneh, M.A., Shamsuddin, S.M., Hasan, S., Bakar, A.A. (2018). An improved chaotic image encryption algorithm. In 2018 International conference on smart computing and electronic enterprise (ICSCEE), pp. 1-8. https://doi.org/10.1007/s10586-021-03466-2

[16] Gatta, M.T., Abd Al-latief, S.T. (2018). Medical image security using modified chaos-based cryptography approach. In Journal of Physics: Conference Series, 1003(1): 012036. https://doi.org/10.1088/1742-6596/1003/1/012036

[17] Kumar, S., Panna, B., Jha, R.K. (2019). Medical image encryption using fractional discrete cosine transform with chaotic function. Medical & Biological

Engineering & Computing, 57: 2517-2533. https://doi.org/10.1007/s11517-019-02037-3

[18] Farah, M.B., Farah, A., Farah, T. (2020). An image encryption scheme based on a new hybrid chaotic map and optimized substitution box. Nonlinear Dynamics, 99(4): 3041-3064. https://doi.org/10.1007/s11071-019-05413-8

[19] Yin, S., Li, H. (2021). GSAPSO-MQC: medical image encryption based on genetic simulated annealing particle swarm optimization and modified quantum chaos system. Evolutionary Intelligence, 14: 1817-1829. https://doi.org/10.1007/s12065-020-00440-6

[20] Yasser, I., Khalifa, F., Mohamed, M.A., Samrah, A.S. (2020). A new image encryption scheme based on hybrid chaotic maps. Complexity, 2020. https://doi.org/10.1155/2020/9597619

[21] Akan, J.B., Adedokun, E.A., Onuh, G., Umar, A., Nwosu, R.I., Ibrahim, Y. (2020). Medical image encryption scheme based on hybrid chaotic permutation. International Journal of Scientific Research in Computer Science and Engineering, 8(4):97-104.

[22] Hashim, A.T., Jabbar, A.K., Hassan, Q.F. (2021). Medical image encryption based on hybrid AES with chaotic map. In Journal of Physics: Conference Series, 1973(1):012037.https://doi.org/10.1088/1742-6596/1973/1/012037

[23] Chaudhary, N., Shahi, T.B., Neupane, A. (2022). Secure image encryption using chaotic, hybrid chaotic and block cipher approach. Journal of Imaging, 8(6): 167.https://doi.org/10.3390/jimaging8060167

[24] Abdallah, A.A., Farhan, A. (2022). A new image encryption algorithm based on multi chaotic system. Iraqi Journal of Science, 63(1): 324-337. https://doi.org/10.24996/ijs.2022.63.1.31

[25] Rachmawanto, E.H., Zulfiningrum, R. (2022). Medical image cryptosystem using dynamic Josephus sequence and chaotic-hash scrambling. Journal of King

Saud University-Computer and Information Sciences, 34(9): 6818-6828. https://doi.org/10.1016/j.jksuci.2022.04.002

[26] Umar, S.U., Rashid, T.A. (2021). Critical analysis: bat algorithm-based investigation and application on several domains. World Journal of Engineering, 18(4):606-620.https://doi.org/10.1108/WJE-10-2020-0495

[27] Zebari, A.Y., Almufti, S.M., Abdulrahman, C.M. (2020). Bat algorithm (BA): review, applications and modifications. International Journal of Scientific World, 8(1):1-7.https://doi.org/10.14419/ijswv8i1.30120

[28] Smid, M.E. (2021). Development of the advanced encryption standard. Journal of Research of the National Institute of Standards and Technology, 126: 126024. https://doi.org/10.6028/jres.126.024

[29] Sari, C.A., Rachmawanto, E.H., Haryanto, C.A. (2018). Cryptography triple data encryption standard (3DES) for digital image security. Scientific Journal of Informatics, 5(2): 105-117. https://doi.org/10.15294/sjiv5i2.14844

[30] Msallam, M.M. (2020). A development of least significant bit steganography technique. IRAQI Journal of Computers, Communications, Control and Systems Engineering, 20(1): 31-39. https://doi.org/10.33103/uot.ijccce.20.1.4

[31] Rostami, M.J., Shahba, A., Saryazdi, S., Nezamabadi-pour, H. (2017). A novel parallel image encryption with chaotic windows based on logistic map. Computers & Electrical Engineering, 62: 384-400. https://doi.org/10.1016/j.compeleceng.2017.04.004

[32] Ali, T.S., Ali, R. (2022). A novel color image encryption scheme based on a new dynamic compound chaotic map and S-box. Multimedia Tools and Applications, 81(15): 20585-20609. https://doi.org/10.1007/s11042-022-12268-6

[33] Elmacı, D., Baş Çatak, N. (2018). An efficient image encryption algorithm for the period of arnold's CAT map. International Journal of Intelligent Systems and Applications in Engineering, 6(1): 80-84.

https://doi.org/10.18201/ijisae.2018637935

[34] Hariyanto, E., Rahim, R. (2016). Arnold's cat map algorithm in digital image encryption. International Journal of Science and Research (IJSR), 5(10): 1363-1365. https://doi.org/10.21275/ART20162488

[35] Alhumyani, H. (2020). Efficient image cipher based on baker map in the discrete cosine transform. Cybernetics and Information Technologies, 20(1): 68-81. https://doi.org/10.2478/cait-2020-0005

[36] Musanna, F., Kumar, S. (2020). Image encryption using quantum 3-D Baker map and generalized gray code coupled with fractional Chen's chaotic system. Quantum Information Processing, 19: 1-31. https://doi.org/10.1007/s11128-020-02724-3

[37] Pande, A.P., Devane, S.R. (2018). Study and analysis of different TCP variants. In 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), pp. 1-8. https://doi.org/10.1109/ICCUBEA.2018.8697750

[38] Kaur, M., Kumar, V. (2020). A comprehensive review on image encryption techniques. Archives of Computational Methods in Engineering, 27: 15-43. https://doi.org/10.1155/2021/5012496

[39] Priyanka, Singh, A.K. (2023). A survey of image encryption for healthcare applications. Evolutionary Intelligence, 16(3): 801-818. https://doi.org/10.1007/s12065-021-00683-x

[40] Talhaoui, M.Z., Wang, X., Midoun, M.A. (2021). Fast image encryption algorithm with high security level using the Bülban chaotic map. Journal of Real-Time Image Processing, 18: 85-98. https://doi.org/10.1007/s11554-020-00948-1