ORIGINAL RESEARCH ARTICLE UHD JOURNAL OF SCIENCE AND TECHNOLOGY

A Secure Medical Image Transmission System Based on 2D Logistic Map and Diffie–Hellman Key Exchange Mechanisms

Shakhawan H. Wady[1,2], Raghad Z. Yousif[3]

[1]Department of Business Administration, Business College, Charmo University, Chamchamal, Sulaimani, KRG, Iraq, [2]Department of Information Technology, University College of Goizha, Sulaimani, KRG, Iraq, [3]Department of Physics, College of Science, Salahaddin University, Erbil, KRG, Iraq

ABSTRACT

With the tremendous growth of searchable visual media, the content-based medical image retrieval and computer-aided diagnosis systems have become popular in recent years to improve knowledge and provide facilities for radiologists. Medical images transferred throughout public networks demand a mechanism that guarantees image privacy, ownership and source of origin reliability, and image integrity verification. For this reason, secure image retrieval and diagnosis scheme have been given considerable interest due to users' security concerns. This work proposed a secure framework based on a two-dimensional (2D) chaotic map with Diffie–Hellman key exchange protocols to ensure patient information privacy and security. Consequently, from a security and protection perspective, the objective is to provide a privacy procedure for medical image retrieval systems through image encryption technique combined with a secure key exchange procedure to minimize the possibility of secret key interception by an unauthorized person. Simulation results and security analysis show that the suggested technique could protect images with minimal time complexity and a high level of security while also resisting numerous attacks.

Index Terms: Medical Images, Chaotic Map, Diffie–Hellman Key Exchange, Peak Signal-to-Noise Ratio

1. INTRODUCTION

Due to the extensive transmission of medical image data through several communication networks, security concerns have become more and more prominent. The protection of personal information is difficult to guarantee by relying exclusively on access control [1], [2]. Therefore, developing good image security systems have become a focal research topic and attract extensive public and government concerns. An encryption procedure is a mechanism, in which the user transforms the plain text or image into an unintelligible form called a cipher or a cipher image. While decryption is a reverse process of encryption, in which the cipher image is converted back into plain text image (Original image) with the help of a key sequence. Symmetric and asymmetric key encryption techniques are the two important categories of encryption procedures through which the medical images are encrypted and decrypted [3], [4]. The technique of chaos-based image encryption is considered a good candidate for cryptography among numerous approaches for content-based image retrieval (CBIR) and computer-aided diagnosis (CAD) systems on large image collections. In consequence, using the chaos scheme for image encryption and decryption is superior than existing conventional algorithms. Since Fridrich [5], [6] previously recommended a chaos-based encryption mechanism in 1997, chaos-based image encryption algorithms, including the Henon map, Baker map, logistic map, and Arnold cat map, have been applied

Access this article online

DOI:10.21928/uhdjst.v6n2y2022.pp94-104

E-ISSN: 2521-4217
P-ISSN: 2521-4209

Corresponding author's e-mail: shakhawan.hares@charmouniversity.org

Received: 26-04-2022 Accepted: 28-09-2022 Published: 27-10-2022

in numerous literature-based data encryption [7]–[9]. Most chaos-based cryptosystems were starting to use it as a core structure. The Fridrich encryption technique is made up of two layers: A confusion layer that uses the 2-D Baker chaotic map and a diffusion layer.

This work provides a novel security system operation platform to guarantee the safety of the medical images based on chaotic cryptography along with Diffie–Hellman key exchange scheme. The key contribution of this study is to utilize chaotic cryptography to terminate the intelligibility of all the retrieved medical images and applying Diffie–Hellman key exchange protocol to eliminate the need for sending the encryption key into private secure channel. The rest of the paper is organized as follows. Section 2 puts forward a literature review. Section 3 presents a complete architecture overview of the proposed system operation scenario, including sections such as system architecture, encryption and uploading, and downloading and decryption stages. Section 4 discusses the results and analysis. Finally, Section 5 provides the conclusion of the work.

2. LITERATURE REVIEW

In this section, necessary background has been presented on the uses of two-dimensional logistic map and Diffie–Hellman key exchange mechanism in image encryption schemes and literature survey medical image encryption schemes proposed in the literature.

2.1. Two-Dimensional Logistic Map

The two-dimensional logistic map is a discrete dynamic system with a chaotic behavior including less periodic windows in bifurcation diagrams and a larger range of parameters, which are more suitable for cryptography [10], [11]. It has a perfect chaotic property as a traditional logistic algorithm, and it has more complex behavior than one dimensional chaotic behavior. Mathematically, the two-dimensional logistic map is an example for chaotic map, and it can be discretely defined using Equation (1) as follows [12]:

$$2D\ Logistic\ map:$$

$$Z(x,y)=\begin{Bmatrix} x_{i+1}=r(3y_i+1)x_i\ (1-x_i) \\ y_{i+1}=r(3x_{i+1}+1)y_i\ (1-y_i) \end{Bmatrix} \quad (1)$$

Where:

- $Z(x, y)$ is the 2D logistic map
- r is the control parameter (growth rate)
- (x_i, y_i) is the pairwise point at the i^{th} iteration.

The 2D logistic map defined in Equation (1) is more complex than the 1D logistic map, that is, the conventional logistic map is defined in Equation (2), where r is the chaotic behavior control parameter [13].

$$\text{1D Logistic map: } x_{i+1} = rx_i(1-x_i) \quad (2)$$

Fig. 1 shows the 1D logistic map schema, where the horizontal axis is the growth rate which is indicated by the parameter (r) and vertical axis is the population which is indicated by the parameter (x) and the trajectories of every one-dimensional logistics map are shown by the (x) with a fixed (x) as points on Figure.

In this work, 2D logistic map algorithm was performed to encrypt and decrypt the medical images with high security, which facilitates the process of protecting the private information of medical images.

2.2. Diffie–Hellman Key Exchange Mechanism

The Diffie–Hellman key agreement protocol, also known as an exponential key agreement, is a symmetric key exchange protocol which is widely implemented for encryption process, as shown in Fig. 2. The main objective of the Diffie–Hellman procedure is to make it feasible for two or more parties to build and exchange an identical and hidden session key by exchanging information over a public communications channel [14]. The DH key agreement protocol allows two users to produce a shared and symmetric key over an unsecured network.

According to Fig. 2 both parties, that is, client and server, agree on global elements prime P, and generator G which are both publicly available numbers; for instance, they may post the values on their web sites. They keep their respective private keys (X_A and X_G) secret, use modular division, and calculate respectively their shared (public) keys as Y_A and Y_B mathematically. The shared keys can take

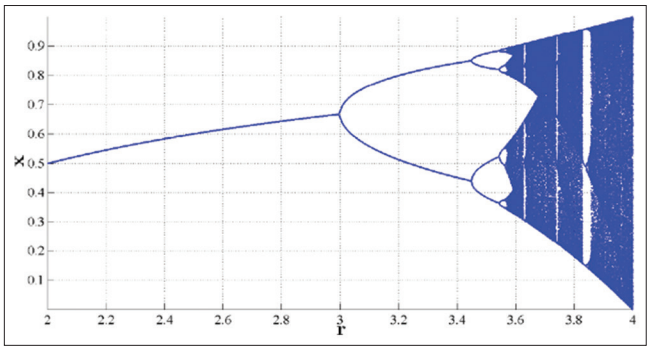

Fig. 1. The bifurcation schema of the 1D logistic map [13].

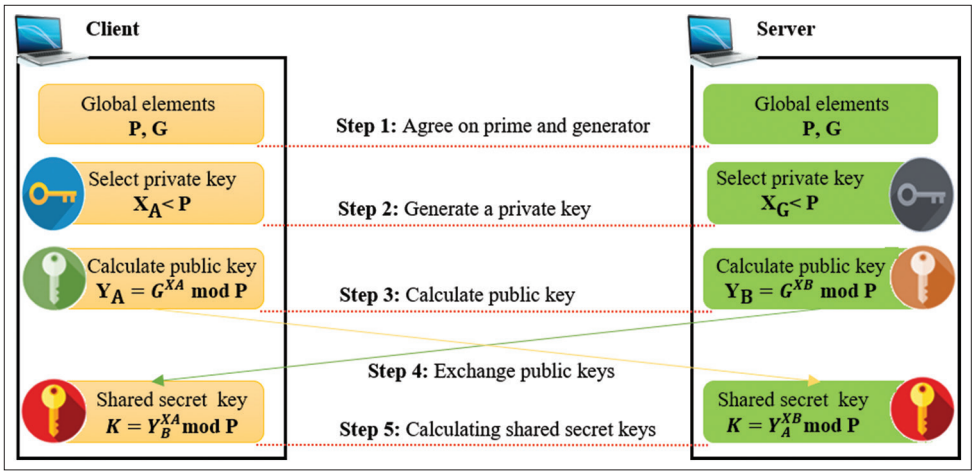

Fig. 2. Diffie–Hellman key exchange authentication procedure [15].

any value between 1 and (P – 1). Both parties exchange their shared keys and calculate the common secret keys value to be used in encrypting the image data which are transmitted over network. DHKE depends on a simple property of modular exponentiations. The mechanism of Diffie–Hellman key that exchanges mathematically is described as follows [15]–[17].

$$\left(G^{XA}\right)m\ o\ d\ P = \left(G^{XB}\right)m\ o\ d\ P \tag{3}$$

Where G, X, A, and P are positive integers. With existing $Y_A = G^A \bmod P$ and $Y_B = G^B \bmod P$, the value of k can be calculated without revealing A or B, which are called secret exponents.

$$K = \left(G^{XB}\right)m\ o\ d\ P \tag{4}$$

In this work, Diffie–Hellman key exchange mechanism was performed to generate and distribute the shared secret key K between the client and server parts. Then, the Diffie–Hellman encryption key K was defined and coded as a 256-bit integer number. In such a way, the encryption key was made to control the pseudo random sequences from the 2D logistic map algorithm for each round.

2.3. Medical Image Encryption Schemes

Protecting patient confidentiality and medical archives are an authorized requirement. Conventional cryptographic approaches are incapable of dealing with the massive quantity of medical image data and its appropriate statistical attributes. Numerous encryption mechanisms for securing medical privacy based on their content have been reported in the related literature. A modern two-dimensional Sine Logistic modulation map (2D-SLMM) which was derived from the logistic and sine maps was provided Hua *et al.* [18] with a broader chaotic spectrum than the traditional sine and chaotic logistic maps. In addition, they combined 2D-SLMM with a chaotic magic transform to establish a new image encryption algorithm (CMT). Simulation results and security analysis show that the proposed algorithm was able to protect images with minimal time complexity and a high level of security while also resisting numerous attacks. In Hua *et al.* [19], the authors addressed a 2D sine chaotification scheme to enhance the complex behavior of current chaotic maps. The authors applied their technique to improve the Henon map and 2D sinus logistics map. A generic medical image encryption system based on a new arrangement of two very powerful concepts, dynamic substitution boxes and chaotic maps, was introduced by Ibrahim *et al.* [20]. Before and after chaotic substitution, the arrangement of S-box substitution was seen to effectively avoid selected plaintext and cipher text attacks.

A two-dimensional of Sine Chaotification Model (2D-SCM) was recommended by Jo *et al.* [21]. The proposed technique can not only considerably improve the complexity of 2D chaotic maps but it can also significantly broaden their chaotic ranges. In Liu *et al.* [22], the authors recommended and implemented an Indistinguishability Under Chosen-Plaintext Attack (IND-CPA) secure CBIR architecture that executed image retrieval on the cloud without the constant interaction of the user. The author addressed a secure CBIR framework based on an Encrypted Difference Histogram (EDH-CBIR) in Liu *et al.* [23]. In that article, the image owner calculated the RGB component order or disorder difference matrices and encrypted them using

value replacement and position scrambling. The encrypted images were subsequently sent to the cloud server, which generated image feature vectors from encrypted difference histograms. To find similar images, image users encrypted the query image in the same way as the image owner did, and the cloud server extracted the query feature vector. To determine the degree of similarity, the Euclidean distance between the query feature vector and the image feature vector was determined.

In Lu *et al.* [24], the authors reported a secure CBIR framework that enables comparison of similarities between encrypted image features, depending on which the secure image retrieval based on content can be achieved. In the system, they focused on security strategies for image features that make a comparison of similarities between protected features. The authors in Sibahee *et al.* [25] developed an effective a lightweight system for content-based browsing over an encrypted image dataset using a Locality Sensitive Hashing (LSH) technique. The LSH index increased the system's expertise and effectiveness, enabling only relevant images to be obtained with a minimum of distance assessments. Vector refining methods were performed for efficient and safe refining of relevant results. The index building process ensured privacy of saved data and trapping doors. In 2017, the author of Gaata and Hantoosh [26] recommended an encrypted CBIR framework with additional improvement for the image retrieval based on features analysis. In this work, the gray level co-occurrence matrix with Haralick features, in combination with color moments, was used to construct the vector feature. In addition, Bloom filter and hash-table for image dataset classification were utilize. A similarity search procedure, based on secure transformation over encrypted cloud images, was presented in Xia *et al.* [27]. In the system, the authorized image client extracted and encrypted the feature vector with a query image to create the cipher text using the secure transformation method. The cipher text was then sent to the cloud to estimate the similarities of the vectors of the transformed feature.

The authors, in Bhagat and Gite [28], published an article on image retrieval for improved authentication using sparse codewords with cryptography. To prevent some form of attack, the Square Quality Control (SQC) encryption algorithm was utilized to the image. Lima *et al.* [29] employed a Cosine Number Transform (CNT) medical image encryption framework for the chosen Galois field. Huang *et al.* [30] implemented an encryption method, which combines chaos and Deoxyribonucleic Acid techniques. To achieve the permutation, substitution, and diffusion needed for encryption, they have performed a scenario of two rounds with six stages. The relatively low encryption speed was the key drawback of their system. The authors, in Hua *et al.* [31], proposed the Medical Image Encryption: Bitwise XOR (MIE-BX), high-speed scraping, random-pixel input, and pixel adaptive diffusion medical image encryption procedure. Their experimental outcomes indicated that the speed of their encryption method can outperform conventional approaches of encryption, such as Advanced Encryption Standard. However, Chen *et al.* [32] pointed out a serious vulnerability in MIE-BX to a reset attack known as the reset attack on Pseudo-Random Number Generator (PRNG). In this attack, the adversary restored the PRNG state to produce the same number of sequences each time.

The authors, in Badr *et al.* [3], introduced the dual authentication mechanism to support an attribute-based encryption (ABE) system that involves multiple parties such as data owners, data users, cloud servers, and authority. The proposed technique provided a safe solution to the problem of sharing significant information such as medical images. In Li *et al.* [33], a healthcare method was introduced by the authors as a new solution to the secure exchange of electronic health information between various entities in separate clouds. The proposed procedure was based on a revocable key policy and ABE algorithms that allowed clients to share encrypted health information on the basis of the data proprietors' and patients' own policy. The research paper in Wu *et al.* [13] applied the 2D logistic map of complicated basin structures and attractors for image encryption. In cryptography, the presented method implemented the classic permutation-substitution network structure; consequently, it ensures both uncertainty and diffusion properties for a protected cipher. In this work, the medical image encryption and decryption were constructed with the proposed system based on a two-dimensional (2D) chaotic map with Diffie–Hellman key exchange protocols to further enhance the security of the proposed system.

3. PROPOSED METHODOLOGY

3.1. System Architecture

In the proposed methodology section, the architecture overview is described, as depicted in Fig. 3. In the proposed framework, encryption and decryption techniques were applied as a force for securing medical images from unauthorized access. A content-based query operation was

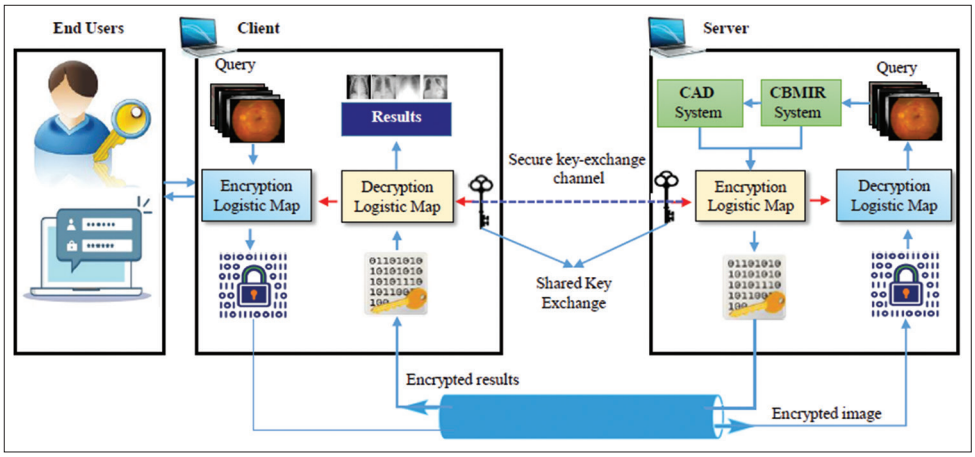

Fig. 3. Architecture overview of the proposed system operation scenario.

initiated from a client side to retrieve the similar medical images and diagnosis result with respect to a query image. Once the query image was chosen as input, 2D logistic map-based Diffie–Hellman key exchange protocol was applied to perform the encryption process for selected query image. After medical images were encrypted, their owner could upload them to the server for conducting the retrieval and classification tasks.

3.2. Encryption and Uploading Stage

First, the authorized users can login using their credentials to login to the proposed system. During this first authentication stage, both credentials are examined by checking the pre-existing dataset. Failure to enter credentials would obstruct the processing of users into additional steps. Now that, a user has registered, and they can start on the client side. On the client side, the query image is selected from a set of test images to carry out the retrieval and diagnosis of medical images. The pseudocode of the encryption procedure using 2D logistic map is shown in Algorithm 1 and the encryption process in the proposed schema involves the following stages:

1. Registering authorized users to access client-side portal
2. Browsing for the query image from the directory of images
3. Calculating the value of the shared secret key (K) between the Client-Server using Diffie–Hellman key exchange protocol
4. Encrypting the query image using the 2D logistic map algorithm with generated Diffie–Hellman key exchange key exchange secret key (Fig. 4).
5. Uploading the encrypted query image data to the server with the shared secret keys (K) value.

Algorithm 1: Pseudocode of image encryption

Input: Plain medical image Pi
Output: Cipher medical image Ci
Step 1: Parameter initialization
Read the original image and convert into a grayscale image
Use the Diffie–Hellman key exchange to generate the secret key (K)
Set Xo, Yo, r, T, F, S, and N
Translate K to map formats
Step 2: Image cipher (encryption)
For i = 1: N
Generate chaotic sequence using 2D logistic map
(e.g., Execute Equation 1)
Compute the 2D logistic permutation (pixel shuffling)
Apply the 2D logistic diffusion (pixel shifting)
Perform the 2D logistic transposition
End
Step 3: Produce cipher image

3.3. Downloading and Decryption Stage

After the client was authenticated by the server with an approved public key, the encrypted data, including the shared secret keys (K) value and medical query image, had to be downloaded and securely stored to the server. On the server side, the encrypted medical query image was directly decrypted using 2D logistic map algorithm and the same shared secret keys (K) from the key that was used for encryption process. The pseudocode of the decryption procedure using 2D logistic map is shown in Algorithm 2. Then, the decrypted image as shown in Fig. 5 was used as a query image to feed into content-based medical image retrieval (CBMIR) and CAD systems for retrieving and classification process of medical images. Following this, the retrieval and diagnosis results were encrypted and transmitted to the client using same procedure. Finally, the client received the returned encrypted results from the server side and performed the decryption process to get the final retrieval

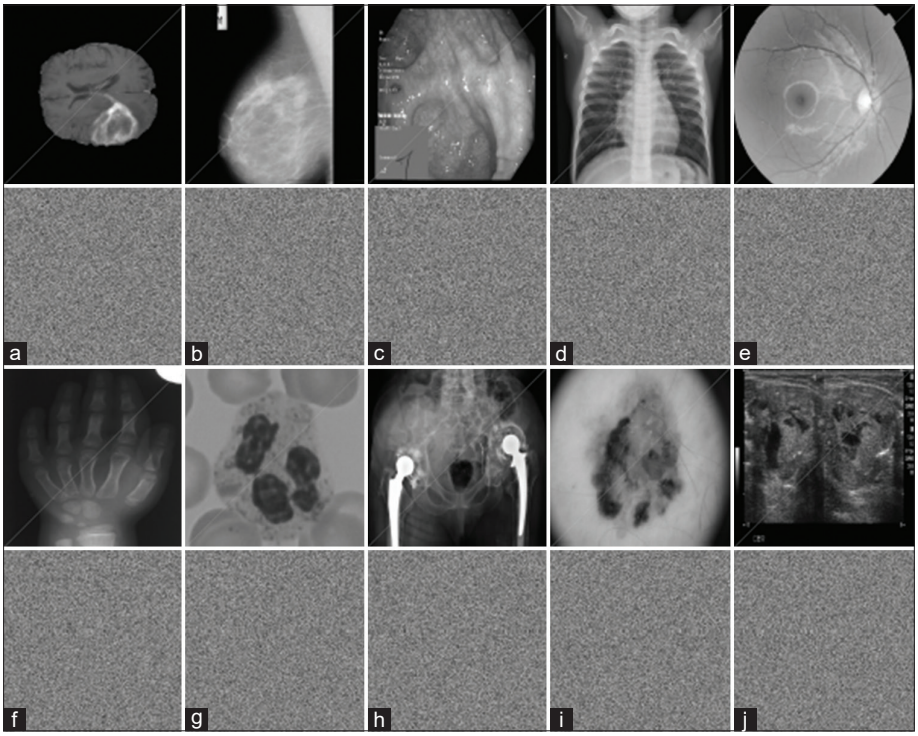

Fig. 4. Medical image encryption using 2D logistic map and Diffie–Hellman key exchange algorithms. original and encrypted medical image: (a) brain tumor; (b) breast mammogram; (c) cecum; (d) chest X-ray; (e) eye fundus; (f) hand X-ray; (g) leukemia; (h) pelvis X-ray; (i) clinical skin; and (j) thyroid images.

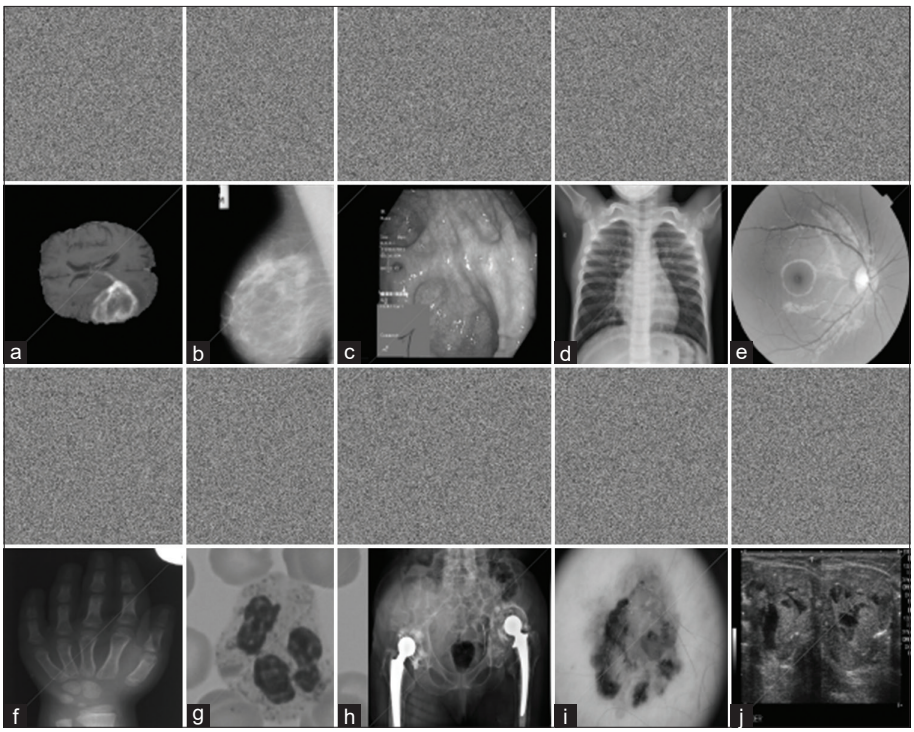

Fig. 5. Medical image decryption using 2D logistic map and Diffie–Hellman key exchange algorithms. encrypted and decrypted medical images: (a) brain tumor; (b) breast mammogram; (c) cecum; (d) chest X-ray; (e) eye fundus; (f) hand X-ray; (g) leukemia; (h) pelvis X-ray; (i) clinical skin; and (j) thyroid images.

and diagnosis results. The GUI of the client side is shown in Fig. 6.

Algorithm 2: Pseudocode of image decryption

Input: Cipher medical image Ci
Output: Decrypted medical image Di
Step 1: Parameter initialization
Read the original image and convert into a grayscale image
Use the Diffie–Hellman key exchange to generate the secret key (K)
Set Xo, Yo, r, T, F, S, and N
Translate K to map formats
Step 2: Image Cipher (Encryption)
For i = 1: N
Generate chaotic sequence using 2D logistic map (e.g., Execute Equation 1)
Perform the 2D logistic transposition
Apply the 2D logistic diffusion (pixel shifting)
Compute the 2D logistic permutation (pixel shuffling)
End
Step 3: Produce decrypted image

3.4. Objective Evaluation

Peak Signal-to-Noise Ratio (PSNR) and Mean Square Error (MSE) are two frequently used evaluation indicators. PSNR calculates the ratio between the maximum signal strength and the noise or distortion strength that affects the quality of the representation. In this paper, PSNR is calculated for the recovered (decrypted) image and original host image. The ratio between these two images is calculated in decibels (dB), where I and K denotes the original host image and recovered (decrypted) image. The PSNR is calculated according to the following equation:

$$PSNR\left(x,y\right)=10\log_{10}\left[\frac{\left[I\right]^2}{MSE}\right] \quad (5)$$

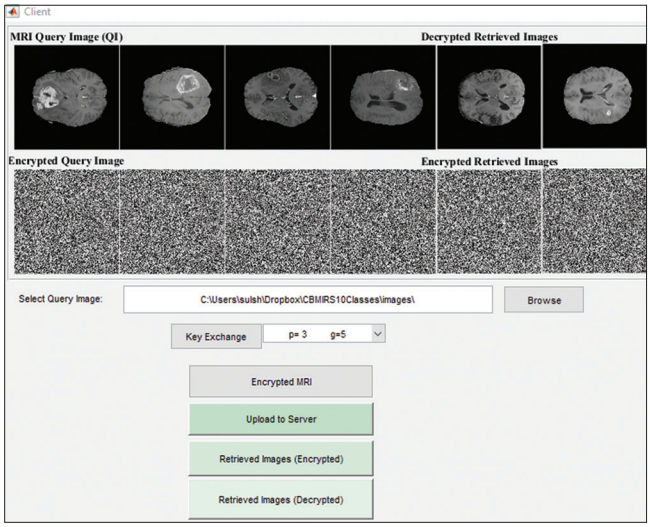

Fig. 6. The GUI of the client-side screen.

where *I* represent the maximum possible value of the pixel in the image (e.g., for a gray-scale image, the maximum value is 255). *MSE* calculates the magnitude of average error between the original image and recovered (decrypted) image. The *MSE* is computed as depicted below:

$$MSE\left(I,K\right)=\frac{1}{m\ n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left(\left[I\left(i,j\right)-\left|K\left(i,j\right)\right|\right]\right)^2 \quad (6)$$

Where:

- $I(i,j)$ denotes the pixel value in the coordinates (i, j) in the image *I* as a reference (original image)
- $K(i,j)$ denotes the pixel value at the coordinates (i, j) of the image *K* as being compared (decrypted image)
- m denotes the image height (in pixels)
- n denotes the image width (in pixels).

4. RESULTS AND ANALYSIS

A secure system for medical image retrieval and diagnosis is the big challenging task in the field of medical image processing. This work proposed a secure framework based on 2D logistic map algorithm along with Diffie–Hellman key exchange scheme for assuring the privacy and security of patient information. In this study, the proposed architecture was implemented in MATLAB 2019 (a) on MacBook Pro machine equipped with a processor of i7 (2.7 GHz Intel Core and 8 GB RAM). A fundamental prerequisite for an effective encryption scheme to avoid statistical attacks is the homogeneity of an encrypted image histogram [34], [35]. The distribution of input images can be represented by image histograms. To gain valuable information regarding the original image, an attacker may analyze the histogram of an encrypted image using attack procedures and statistical analysis of the encrypted image. It is important to guarantee that there are no statistical similarities between both the original image and the encrypted image. The histogram analysis clarifies the distribution of the pixels on an image by plotting the number of pixels at each degree of intensity. A visual analysis of the proposed scheme can be done observing the histograms of the medical images before and after the encryption. For visual inspection, Figs. 7-11 show sample histograms of the encrypted and decrypted medical images generated by the proposed framework for each of the evaluated query images. The histogram of the original medical images (plaintext images) demonstrates how the number of pixels at each gray level is graphically distributed.

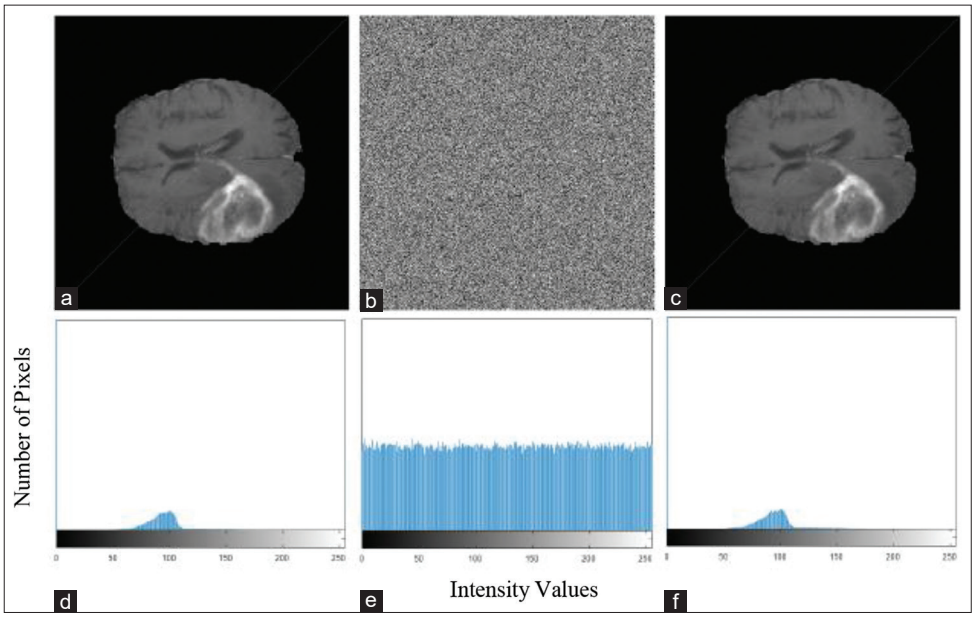

Fig. 7. Two-dimensional logistic map results with Diffie–Hellman on brain tumor image. (a) plaintext; (b) encrypted image; (c) decrypted image; (d) plaintext histogram; (e) encrypted histogram; and (f) decrypted histogram.

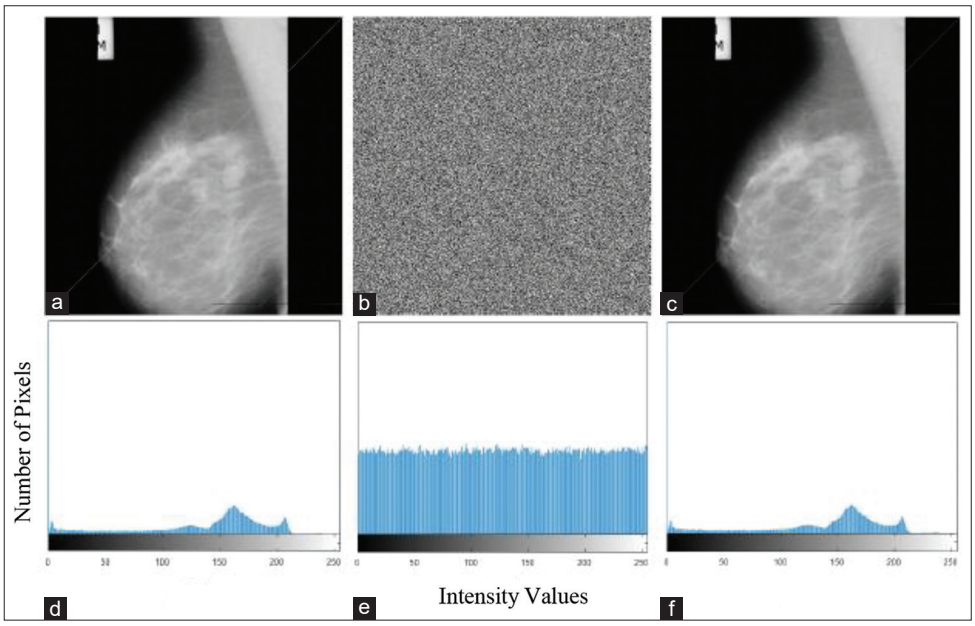

Fig. 8. Two-dimensional logistic map results with Diffie–Hellman on breast mammogram image. (a) plaintext; (b) encrypted image; (c) decrypted image; (d) plaintext histogram; (e) encrypted histogram; and (f) decrypted histogram.

It is evident that the encrypted image (ciphertext images) histogram is almost uniformly distributed, and that it obviously differs from the respective histograms in the original images. The procedure makes statistical attacks difficult, confirming that this evaluation is satisfied by the proposed framework. Therefore, in any statistical attack on the encryption of an image using the proposed technique, the encrypted image does not provide any proof for using. For the purpose of comparison of the recommended procedure, a sample of each different modality of medical (Magnetic Resonance, X-ray, Fundus, Endoscopy, and visible light) images was experienced in the tests. To evaluate the encryption

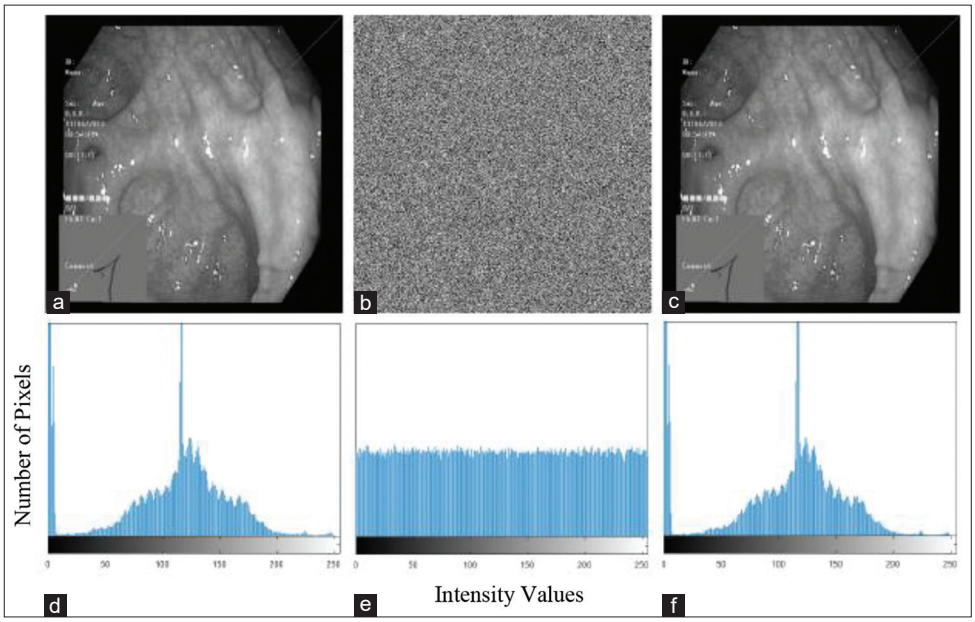

Fig. 9. Two-dimensional logistic map results with Diffie–Hellman on cecum image. (a) plaintext; (b) encrypted image; (c) decrypted image; (d) plaintext histogram; (e) encrypted histogram; and (f) decrypted histogram.

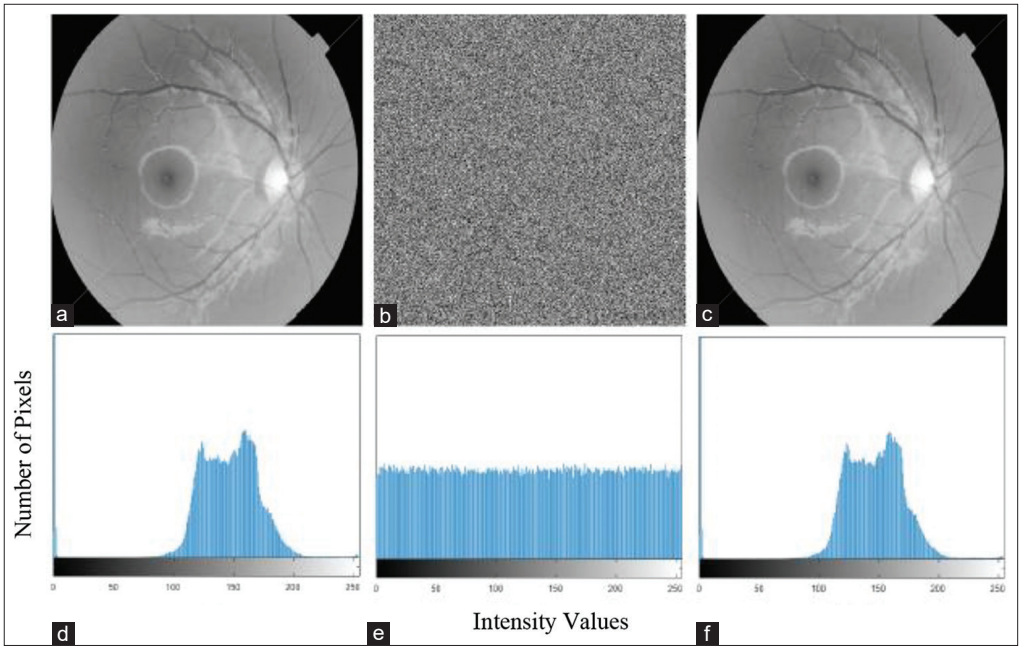

Fig. 10. Two-dimensional logistic map results with Diffie–Hellman on eye fundus image. (a) plaintext; (b) encrypted image; (c) decrypted image; (d) plaintext histogram; (e) encrypted histogram; and (f) decrypted histogram.

performance for different medical image modalities, the originality of the images was compared through their PSNR values. There will be no loss of data in the process which is an additional advantage of the proposed framework. Moreover, the proposed technique results in excellent performance with PSNR of 100% (a PSNR of 100 denotes no significant noise detected between the two images) and an MSE of zero (0) between encrypted and decrypted medical images.

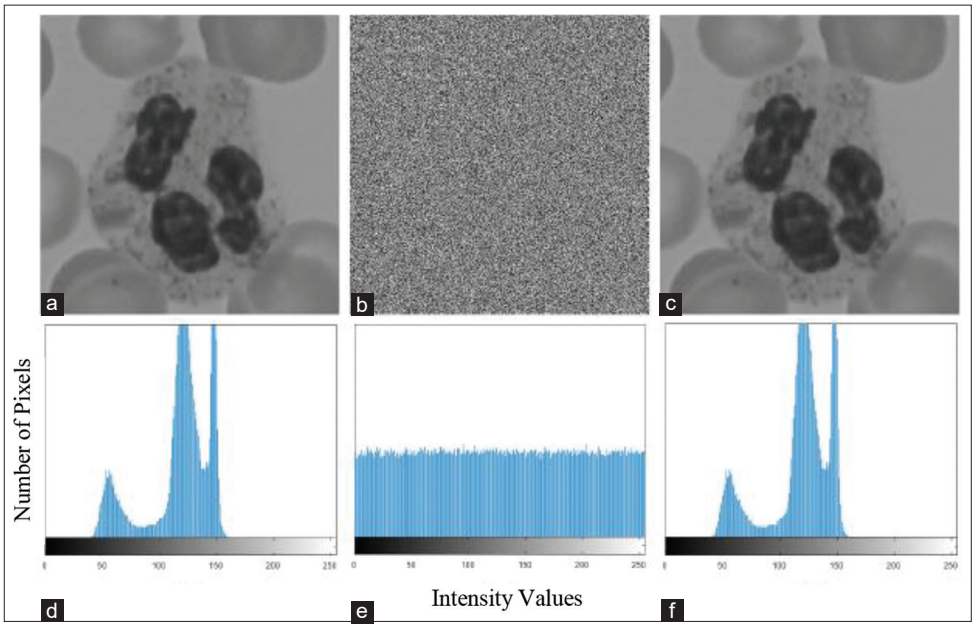

Fig. 11. Two-dimensional logistic map results with Diffie–Hellman on leukemia image. (a) plaintext; (b) encrypted image; (c) decrypted image; (d) plaintext histogram; (e) encrypted histogram; and (f) decrypted histogram.

5. CONCLUSION

Developing a secure medical image retrieval scheme has become an essential requirement for protecting the privacy of patients' medical information. This paper investigated a contemporary mechanism for employing client server to encrypt and exchange critical medical data, helping the user to avoid security risks. To achieve these security requirements, the proposed methodology used different procedures. To further improve the security of the proposed framework, medical image encryption and decryption were constructed based on a two-dimensional (2D) chaotic map with Diffie–Hellman key exchange protocols. The PSNR values were used to compare the image's originality. A further benefit of the proposed approach was that no data would be lost during the process. In addition, the presented approach generated outstanding results, with a PSNR of 100% (no substantial noise between the two images) and an MSE of zero (0) between encrypted and decrypted medical images.

REFERENCES

[1] S. Cheng, L. Wang and A. Du. "Histopathological image retrieval based on asymmetric residual Hash and DNA coding". *IEEE Access*, vol. 7, pp. 101388-101400, 2019.

[2] Z. Xia, L. Lu, T. Qiu, H. J. Shim, X. Chen and B. Jeon. "A privacy-preserving image retrieval based on ac-coefficients and color histograms in cloud environment". *Computers, Materials and Continua*, vol. 58, no. 1, pp. 27-43, 2019.

[3] A. M. Badr, Y. Zhang and H. G. A. Umar. "Dual authentication-based encryption with a delegation system to protect medical data in cloud computing". *Electronics*, vol. 8, no. 2, pp. 171, 2019.

[4] S. M. Farooq, S. M. S. Hussain, S. Kiran and T. S. Ustun. "Certificate based authentication mechanism for PMU communication networks based on IEC 61850-90-5". *Electronics*, vol. 7, p. 370, 2018.

[5] J. Fridrich. *Secure Image Ciphering Based on Chaos*. Final Report for AFRL, New York, 1997.

[6] J. Fridrich. "Symmetric ciphers based on two-dimensional chaotic maps". *International Journal of Bifurcation and Chaos*, vol. 8, no. 6, pp. 1259-1284, 2011.

[7] Z. Hua, Y. Zhou and H. Huang. "Cosine-transform-based chaotic system for image encryption". *Information Sciences*, vol. 480, pp. 403-419, 2019.

[8] J. A. P. Artiles, D. P. B. Chaves and C. "Pimentel. Image encryption using block cipher and chaotic sequences". *Signal Process Image Communication*, vol. 79, pp. 24-31, 2019.

[9] H. Zhu, Y. Zhao and Y. Song. "2D logistic-modulated-sine-coupling-logistic chaotic map for image encryption". *IEEE Access*, vol. 7, pp. 14081-14098, 2019.

[10] 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, no. 3, pp. 1123-1136, 2015.

[11] M. B. Yassein, S. Aljawarneh, E. Qawasmeh, W. Mardini and Y. Khamayseh. "Comprehensive study of symmetric key and asymmetric key encryption algorithms". In: *Proceeding 2017 International Conference on Engineering and Technology ICET*, pp. 1-7, 2017.

[12] R. Hamza, K. Muhammad, A. Kumar and G. "Ramirez-Gonzalez. Hash based encryption for keyframes of diagnostic hysteroscopy". *IEEE Access*, vol. 6, pp. 60160-60170, 2018.

[13] Y. Wu, J. P. Noonan, G. Yang and H. Jin. “Image encryption using the two-dimensional logistic chaotic map”. *Journal of Electronic Imaging*, vol. 21, no. 1, p. 3014, 2012.

[14] A. K. Dhara, S. Mukhopadhyay, A. Dutta, M. Garg and N. Khandelwal. “Content-based image retrieval system for pulmonary nodules: Assisting radiologists in self-learning and diagnosis of lung cancer”. *Journal of Digital Imaging*, vol. 30, no. 1, pp. 63-77, 2017.

[15] S. M. Farooq, S. M. S. Hussain, S. Kiran and T. S. Ustun. “Certificate based authentication mechanism for PMU communication networks based on IEC 61850-90-5”. *Electronics*, vol. 7, no. 12, p. 370, 2018.

[16] A. Chopra. “Comparative analysis of key exchange algorithms in cryptography and its implementation”. *IMS Manthan* (*The Journal Innovations*), vol. 8, no. 2, 2015.

[17] H. Bodur and R. Kara. “Implementing diffie-hellman key exchange method on logical key hierarchy for secure broadcast transmission”. In: *Proceeding 9th International Conference on Computational Intelligence Communications Networks*, *CICN*, pp. 144-147, 2018.

[18] Z. Hua, Y. Zhou, C. M. Pun and C. L. P. Chen. “2D sine logistic modulation map for image encryption”. *Information Sciences*, vol. 297, pp. 80-94, 2015.

[19] Z. Hua, Y. Zhou and B. Bao. “Two-dimensional sine chaotification system with hardware implementation”. *IEEE Transactions on Industrial Informatics*, vol. 16, pp. 887-897, 2020.

[20] S. Ibrahim, H. Alhumyani, M. Masud, S. S. Alshamrani, O. Cheikhrouhou, G. Muhammad and A. M. Abbas. “Framework for efficient medical image encryption using dynamic S-boxes and chaotic maps”. *IEEE Access*, vol. 8, pp. 160433-160449, 2020.

[21] H. J. Jo, S. J. Gotts, R. C. Reynolds, P. A. Bandettini, A. Martin, R. W. Cox and Z. S. Saad. “Effective preprocessing procedures virtually eliminate distance-dependent motion artifacts in resting state FMRI”. *Journal of Applied Mathematics*, vol. 2013, pp. 935154, 2013.

[22] F. Liu, Y. Wang, F. C. Wang, Y. Z. Zhang and J. Lin. “Intelligent and secure content-based image retrieval for mobile users”. *IEEE Access*, vol. 7, pp. 119209-119222, 2019.

[23] D. Liu, J. Shen, Z. Xia and X. Sun. A content-based image retrieval scheme using an encrypted difference histogram in cloud computing. *Informatics*, vol. 8 no. 3, pp. 96, 2017.

[24] W. Lu, A. Varna, A. Swaminathan and M. Wu. “Secure image retrieval through feature protection”. In: *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing*. ICASSP, Taiwan, 2009.

[25] M. A. Al Sibahee, S. Lu, Z. A. Abduljabbar, A. Ibrahim, Z. A. Hussien, K. A. A. Mutlaq and M. A. Hussain. “Efficient encrypted image retrieval in IoT-cloud with multi-user authentication”. *International Journal of Distributed Sensor Networks*, vol. 14, 2018.

[26] M. T. Gaata MT and F. F. Hantoosh. “Encrypted image retrieval system based on features analysis”. *Al-Mustansiriyah Journal of Sciences*, vol. 28, no. 3, pp. 166-173, 2017.

[27] Z. Xia, Y. Zhu, X. Sun and J. Wang. “A similarity search scheme over encrypted cloud images based on secure transformation”. *International Journal of Future Generation Communication and Networking*, vol. 6, no. 6, pp. 71-80, 2013.

[28] M. N. Bhagat and P. B. B. Gite. “Image retrieval using sparse codewords with cryptography for enhanced security”. *IOSR Journal of Computer Engineering*, vol. 16, no. 2, pp. 22-26, 2014.

[29] J. B. Lima, F. Madeiro and F. J. R. Sales. “Encryption of medical images based on the cosine number transform”. *Signal Process Image Communication*, vol. 35, pp. 1-8, 2015.

[30] L. Huang, S. Wang, J. Xiang and Y. Sun. “Chaotic color image encryption scheme using deoxyribonucleic acid (DNA) coding calculations and arithmetic over the galois field”. *Mathematical Problems in Engineering*, vol. 2020, pp. 1-2, 2022.

[31] Z. Hua, S. Yi and Y. Zhou. “Medical image encryption using high-speed scrambling and pixel adaptive diffusion”. *Signal Processing*, vol. 144, pp. 134-144, 2018.

[32] Y. Chen, C. Tang and R. Ye. “Cryptanalysis and improvement of medical image encryption using high-speed scrambling and pixel adaptive diffusion”. *Signal Processing*, vol. 167, pp. 107286, 2020.

[34] M. Li, S. Yu, Y. Zheng, K. Ren and W. Lou. “Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption”. *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, pp. 131-143, 2013.

[35] H. Liu, B. Zhao, J. Zou, L. Huang, Y. Liu. “A lightweight image encryption algorithm based on message passing and chaotic map”. *Security and Communication Networks*, vol. 2004, no. 4, 2020.