

Survey Study Image Cryptography System

Fatima Raid Rahman^{1*}, *Baheesa K*², and *May A. Salih*³

¹ Department of Computer Science College of Computer Science and Information Technology, University of Karbala
Karbala, Iraq

² Department of Computer Science College of Computer Science and Information Technology, University of Karbala
Karbala, Iraq

³ Department of Cyber Security, College of Information Technology, University of Babylon, Babylon, Ira

Abstract. Encryption is vital for data security, converting information into an unreadable format to ensure privacy in online communication and sensitive sectors. Advanced encryption balances innovation and security in user-friendly applications. Image encryption employs techniques to protect image data from unauthorized access during transmission or storage, particularly crucial for safeguarding sensitive images in various applications. The goal is to prevent unauthorized access and ensure the safety of associated information. In this paper, I present a study on previous research related to my investigation, which focuses on encryption in general and image encryption in particular. The paper also discusses the methods used, particularly those closely related to my work, involving either SHA-256, MD5, or a combination of both. The review will look at the many strategies and techniques employed, as well as how precisely the task was completed by applying a set of parameters in comparison to earlier studies.

1 INTRODUCTION

In an era dominated by digital communication and information exchange, guaranteeing sensitive data integrity and security, particularly images, has grown to be a top priority. As the reliance on digital imagery continues to grow, the need for robust cryptographic systems becomes increasingly evident. Cryptography is the science of secure communication, using mathematical algorithms to encode data and ensure confidentiality, integrity, and authentication. In image context, it safeguards image data from unauthorized access or manipulation during transmission or storage. Arnold's transformations, blockchain technology, chaotic systems, and DNA encoding have all gained popularity recently important components of many cryptography systems.

Blockchain (BC) is a useful ledger for guaranteeing the quality of data. It has made peer-to-peer interactions among worldwide-decentralized devices easier and enabled "controlling operations" for a variety of decentralized industrial equipment. Blockchain also solves security issues and gives all autonomous systems responsibility and compliance. In industrial settings, a private blockchain has been employed to guarantee security[1].

Chaos-based encryption has attracted a lot of attention because of its fascinating features, which include strong ergodicity, mixing properties, and responsiveness to beginning conditions and parameters, and extremely complex behavior. On the flip side, many encryption schemes that rely on chaos are susceptible to cryptanalysis and unreliable [2]. The Arnold's transformation function possesses key characteristics making it suitable for cryptanalysis, including high ergodicity and image cutting. Nevertheless, it is not suitable for cryptography as it solely alters the pixel positions, leaving their values unchanged. This lack of impact on the image histogram prevents its effective use in cryptographic applications[3].

* Corresponding author: fatimah.raid@s.uokerbala.edu.iq

Because to DNA encryption's extreme low power consumption, high information density, and huge parallelism, it has been a major topic in cryptography research in recent years. Studies reveal that DNA technology not only strengthens cryptosystem defenses but also effectively thwarts chosen-plaintext attacks. The current DNA-based image encryption techniques have many drawbacks despite their benefits. In particular, the principles governing DNA encryption become more predictable when paired with low-dimensional chaotic maps, hence increasing the system's vulnerability. Furthermore, a differential attack might not be able to penetrate the ciphertext image, and the matching key might only be recovered by using a tiny percentage of the known plaintext or ciphertext. To get over these issues, different chaotic sequences for encryption operations are constructed using high-dimensional chaotic maps. The plaintext picture determines the beginning parameters of a chaotic system. As a result, numerous cryptosystems have been created to address these issues [4].

The MD5 message-digest algorithm is easy to implement and generates a unique "fingerprint" or message digest for messages of varying lengths. Hashing algorithms, including MD5, convert any input length to a fixed-length value, the length of which depends on the specific algorithm used. Part of the message digest algorithm family, MD5 was created as an advancement over MD4, its predecessor. The MD hash family's compression function is distinguished by a unified structure that incorporates message expansion and the sequential performance of several related operations, or steps. Typically, there are three to five rounds to these processes [5].

The message dissemination of the message words is enhanced by the MD5 message expansion, which guarantees multiple uses of every message block. Recursive message expansion is employed to improve diffusion, and each step's input maintains a strong association with the initial message. As such, a little change in the message affects many phases and yields a unique hash value or message digest. Bitwise Boolean operations make up an initial operation in MD5. Secondly Addition of integers. Thirdly Bit rotations or shift operations [6].

As a cryptographic hash function, the Secure Hash Algorithm (SHA) is distinguished from MD5 by offering increased security. Password storage and digital signatures are two common uses for it. The 256-bit hash result produced by this hash algorithm is dependent on the input string. The algorithm itself can be segmented into four main parts: 1. Insert Padding Bits: The process begins by adding padding bits to the input string. 2. Add Length Bits: Additional bits representing the length of the original message are appended. 3. Buffer Initialization: Initialization of the buffer is performed as part of the algorithm. 4. Compression Algorithm: The compression algorithm, a crucial step, operates on the padded input to produce the final hash value[6].

By executing these four steps, the SHA algorithm ensures a secure and reliable hashing process, making it suitable for various cryptographic applications.

The SHA-256 algorithm is used to construct the control settings and starting conditions. The 256-bit hash produced by this widely used cryptographic hash algorithm is equal to a 64-digit hexadecimal number. Notably, two photos can differ by just one bit and still provide completely different hash values. This property reinforces the cryptographic strength of SHA-256, making it suitable for use in scenarios where even small changes to the input data should produce noticeably different hash values [7].

Relevant work is included in the second part of the paper's structure. The experimental assessment was covered in the third portion, and the conclusion.

RELATED WORK

The following section explores the latest models specifically designed for image encryption. It provides insights into the workings of these models, detailing their features, strengths, and weaknesses.

Manual Abdullah Alohali et al. demonstrates a blockchain-driven method for picture encryption called BDIE-AOFOLS, which combines fractional-order Lorenz system arithmetic optimization. They have created a brand-new BDIE-AOFOLS method for decoding encrypted color images. To protect images, the BDIE-AOFOLS technique uses three main processes: Optimal key generation, picture encryption, and BC technology. Initially, the images were encrypted using the FOLS technique. After that, to finish the ideal key generation procedure and get the highest PSNR value, AOA was used. Ultimately, BC was used to guarantee security and maintain the photographs' cryptographic pixel values [1].

Nada H. Sharkawy et al. research presents a model designed to keep robust key strength while enhancing picture encryption. The model uses a memristor hyperchaotic system to build the X, Y, Z, and W matrices and creates a key by combining the hash algorithms SHA-256 and MD5. After key production, the source image is subjected to the Arnold transform. The photos are then blended using five chaotic maps. Then, the picture is distributed over three matrices: DNA-encoded, decoded from DNA. Twelve criteria are applied to assess how well the proposed model performs on nine popular images [3].

Ichraf Aouissaoui et al. presents a safe and effective method for encrypting and decrypting medical images that makes use of hash algorithms (SHA-256 and MD5), One-dimensional chaotic maps, particularly those with tents and logistics, and deoxyribonucleic acid (DNA). The method initially generates a highly connected and a sensitive key to

A hash function can be used to achieve the original image to the image and its data. The next steps entail rotating and permuting the medical image's first two Most Significant Bit (MSB) bit plans in order to minimize redundant DNA encoded sequences and lessen the image's black background. Through the logistic map, DNA rules are dynamically selected for each 2-bit pixel value in the third stage, which involves DNA encoding and decoding. Confusion-diffusion is also carried out utilizing the XOR procedure and tent map. Because the system is only used on a small number of benchmark datasets, comprehensive comparisons are challenging, however, the outcomes demonstrate the key space is spacious and sensitivity to minute adjustments [2].

Xingyuan Wang et al. introduce an encryption original image method based on LDCML (Logistic Difference Chaotic Map with Loop) and the sequence that codes for DNA. First, the SHA-256 hash technique and a given key are used to build the basic configurations and values of the LDCML system. Chaotic progression produced by the LDCML(Logistic Difference Chaotic Map with Loop) algorithm initially makes the original image unreadable. To create the matrix that results from the second scrambling, the initial scrambling matrix is transformed into a DNA matrix, DNA-encoded, and then rearranged into a "C" shape. A predefined rule is applied to the related DNA matrix to convert it using the addition of an extra chaotic sequence produced by the LDCML(Logistic Difference Chaotic Map with Loop) system. The DNA matrix from the second scrambling is utilized to diffuse the final encrypted image. Security evaluations and simulation trials show that the algorithm is safe and able to withstand popular attack techniques [8].

Ebrahim Zarei Zefreh offers a unique method of encrypting images that incorporates Hash functions, chaotic systems, and DNA computing in a hybrid design To make sure that a single bit flip in the plain picture or the secret key affects the beginning conditions and regarding chaotic systems' control settings, the method combines SHA256 and MD5 hash obtained from the plain picture and the private key. According to experimental findings, the suggested photo encryption method delivers greater security than five previous sample image encryption schemes and is fast enough for practical application [9].

Prince Waqas Khan and Yungcheol Byun offered an encrypted, permissioned private blockchain system to improve image security. Because the blockchain uses unbreakable cryptography, there are no security vulnerabilities with the Industrial Internet of Things (IIoT). This technique uses the blockchain to securely store an image's cryptographic pixel values, safeguarding the picture data's security and privacy. The recommended photo encryption scheme's resilience to attacks based on differences is evaluated using metrics. The obtained entropy values indicate defense against brute force attacks because they are around the optimal value of eight. The encrypted results demonstrate the scheme's high effectiveness in preventing data leakage and ensuring security. Nonetheless, certain restrictions are still in place, such as those related to transaction speed and processing power. Some IIoT devices, such as sensors that connect, might not have the memory or computing power to function as nodes in a blockchain. Although web services may be able to help with this problem, more research is necessary to get over these obstacles [10].

TABLE 1. Summary of Related Work

Study	Method
M. A. Alohalı et al.[1]	Blockchain-Driven Image Encryption Process with Arithmetic Optimization Algorithm for Security in Emerging Virtual Environments
N. H. Sharkawy et al.[3]	Gray-Scale Image Encryption Using DNA Operations
I. Aouıssaoui et al.[2]	Robustly correlated key-medical image for DNA-chaos based encryption
X. Wang et al.[8]	Image encryption algorithm based on LDCML and DNA coding sequence
E. Z. Zefreh [9]	An image encryption scheme based on a hybrid model of DNA computing, chaotic systems and hash functions
P. W. Khan and Y. Byun [10]	A Blockchain-Based Secure Image Encryption Scheme for the Industrial Internet of Things

2 EXPERIMENTAL EVALUATION

The subsequent sections cover the performance metrics, results of experimental evaluations, and the interpretation of findings in some related works.

2.1 KEY ANALYSIS

Keys for image encryption security are essential for maintaining data confidentiality. Key sensitivity and key space are taken into account when analyzing key strength. The secret key's size reveals the effectiveness of the key space; a higher key space is indicated by a larger secret key. Because of the increased complexity, it is more difficult for adversaries to generate comparable keys in a bigger key space. Key sensitivity is demonstrated when an encryption key change results in the encrypted image becoming unretrievable. Consequently, Good sensitivity and a big key space are traits of an effective encryption algorithm [11].

2.1.1 Analysis Of The Key Spaces

Key space analysis is a critical criterion in the performance assessment of algorithms for image encryption. A robust encryption method should have a large key space and be sensitive to the key value [12]. For the purpose of preventing brute-force attacks, the key space must be greater than 2^{100} [2][3]. In determining the key space, the quantity of variables generated and the probability connected with them are taken into account [3].

Table 2. Comparison of Key Spaces

Study	Key Space
I. Aouissaoui et al. [2]	$2^{624} > 2^{100}$
N. H. Sharkawy et al. [3]	$2^{704} > 2^{100}$
X. Wang et al. [8]	$10^{126} > 2^{100}$
E. Z. Zefreh [9]	$2^{512} > 2^{100}$

2.1.2 A Key Sensitivity Analysis

A strong encryption method ought to respond promptly to changes in its secret key. This shows that the correct decryption of the original image requires the use of a secret key [9]. A significant change in the output should occur with even a small adjustment to the key [2].

2.2 STATISTICAL ATTACKS ANALYSIS

The model's statistical vulnerabilities should be reduced as much as possible. The suggested algorithm's resistance to statistical assaults is assessed through the use of correlation analysis between adjacent pixels in encrypted images, information entropy, and histograms [2]. The degree of security is gauged through various metrics. Together, these metrics help assess how resilient the model is to statistical assaults.

2.2.1 Histogram Analysis

Understanding an image's pixel intensity frequency distribution can be obtained by using a histogram. It is imperative that the encrypted image's histogram differs completely from the original images when it comes to image encryption. Typically, the original image's pixel intensity distribution is non-uniform, while the encrypted image's histogram ought to show a uniform distribution [11]. Consequently, the suggested plan exhibits resistance to statistical analysis intrusions. The analysis of histograms ensures that values are distributed, effectively concealing the original image[3]. Visual uniformity is confirmed through the calculation of histogram variance [2][13], which further substantiates the scheme's effectiveness.

$$var(Z) = \frac{1}{n^2} \sum_{i=1}^n \sum_{j=1}^n \frac{1}{2} (z_i - z_j)^2 \tag{1}$$

In the equation, the histogram values are represented by Z, and the counts of pixels with gray values equal to i and j are indicated by (z_i, z_j). The enciphered image's variation should ideally be less than the cover image's variance in an efficient cryptosystem. An encrypted image's tendency toward smaller histogram variance increases with image homogeneity. The goal of attaining low variation in the encrypted image's histogram—which denotes a more secure and consistent distribution of pixel values—is highlighted by this relationship.

2.2.2 Analysis of Correlation Coefficients (CCA)

The correlation coefficient shows how the pixels in a digital image relate to one another. In the diagonal, horizontal, and vertical dimensions, in simple photographs, neighboring pixels typically exhibit a significant degree of association. To protect against statistical attacks, strong picture encryption ought to greatly lower the relationship between neighboring the cipher image's pixels. Zero is the ideal correlation. The correlation coefficient between two neighboring pixels can be obtained by, this equation is frequently utilized [9][14]:

$$r_{xy} = \frac{cov(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{2}$$

$$cov(x, y) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))(y_i - E(y)) \tag{3}$$

$$D(x) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2 \tag{4}$$

$$E(x) = \frac{1}{N} \sum_{i=1}^N x_i \tag{5}$$

The letters x and y stand for the variance, mean, and gray values of two adjacent pixels, and the covariance are denoted by the letters D(x), cov(x, y), and N, respectively. A correlation coefficient that is nearly 0 indicates that the picture that is encrypted has less connections amongst neighboring pixels, which is the intended result.

Table 3. Comparing CCA with alternative models.

Dataset	Direction	Lena	Cameraman	Peppers
N. H. Sharkawy et al.[3]	H	0.0042	0.0058	-0.0081
	V	0.000049	-0.0111	0.0031
	D	0.0033	-0.0039	-0.0021
X. Wang et al.[8]	H	0.0011	NA	0.0040
	V	0.0013	NA	0.0015
	D	0.0053	NA	0.0018
E. Z. Zefreh [9]	H	-0.0004	-0.0061	0.0049
	V	0.0037	0.0058	0.0099
	D	-0.0378	0.0166	0.0068

Table 4. Comparing the CCA average to different models.

Dataset	Lena	Cameraman	Peppers
N. H. Sharkawy et al.[3]	0.0025	0.0069	0.0044
X. Wang et al.[8]	0.0026	NA	0.0024
E. Z. Zefreh [9]	0.0345	0.0163	0.0072

2.2.3 Analysis of Information Entropy (IE)

Since entropy evaluates the disarray and gray value distribution inside a picture and illuminates the randomness that exists within the system, it is an essential part of a cryptosystem. The greater the level of information entropy, the flatter the distribution of gray pixel values. [15]. The following formula is used to compute entropy:

$$H(x) = - \sum_{i=1}^L p(x_i) \log_2 p(x_i) \quad (6)$$

Where $p(x_i)$ is The chance that the information source x has. The highest entropy value for a grayscale image with 8 bits of depth is 8. As a result, the cryptosystem becomes larger and more random the closer the entropy number approaches 8.

TABLE 5. IE comparison with other models.

Method	IE
<i>M. A. Alohalı et al.[1]</i>	7.9955
<i>I. Aouıssaoui et al.[2]</i>	7.9994
<i>N. H. Sharkawy et al.[3]</i>	7.9971
<i>X. Wang et al.[8]</i>	7.9981
<i>E. Z. Zefreh [9]</i>	7.9993

2.2.4 Peak Signal To Noise Ratio, or PSNR

The pixels with different values in the plain and encrypted images are displayed by the PSNR. A picture with encryption will have a lower PSNR since better image quality is indicated by a higher PSNR number. Less than 10 dB is the ideal PSNR value for an encrypted image [16]. The estimation of PSNR is given by:

$$PSNR = 10 \times \log_{10} \frac{M \times N \times 255^2}{\sum_{m=1}^M \sum_{n=1}^N |(C1(i,j) - C2(i,j))|} \quad (7)$$

The method's quality is guaranteed by the provided PSNR values for different images, which are less than 10 dB. This aligns with the desired characteristic of an encrypted image having a low PSNR.

TABLE 6. PSNR comparison with other models.

Method	PSNR(dB)
<i>I. Aouıssaoui et al.[2]</i>	13.8305
<i>X. Wang et al.[8]</i>	8.6548
<i>E. Z. Zefreh [9]</i>	14.6236

2.2.5 The mean square error, or MSE

It evaluates an image's diffusion properties, especially when applied to an encrypted image. It is anticipated that the theoretical value will exceed 10,000 [3]. The calculation is determined by Equation (17):

$$MSE = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N (I(i,j) - C(i,j))^2 \quad (8)$$

$I(i, j)$ displays the value of the original image's pixels, and $C(i, j)$ displays the value of the encrypted image's pixels, where the dimensions of the image are (M) and (N).

Table. 7. Comparing MSE with alternative models.

Dataset	Lena	Peppers
N. H. Sharkawy et al.[3]	8972	11967
X. Wang et al.[8]	7802	9215

2.3 DIFFERENTIAL ATTACKS ANALYSIS

Differential attack analysis is used to evaluate how a small alterations have been made to the encrypted image is affected by a single pixel in the unadorned picture. This suggests that the original and altered photos must be encrypted using the same secret key. Two frequently used metrics for assessing differential attacks are the number of pixels changing rate (NPCR) and the unified average changing intensity (UACI). These criteria provide insights into how the encryption scheme responds to slight alterations in the input image, contributing to the overall security assessment.

2.3.1 NPCR, or number of pixels changed

The percentage of different pixel numbers between two encrypted images is determined using the Number of Pixel Change Rate (NPCR). A greater NPCR value means that differential assaults can be resisted by the encryption method more successfully [11]. You can use the following formula to calculate NPCR [17]:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{N} \times 100\% \quad (9)$$

Where N is the image's total pixel count and the "Number of pixels that are different" is calculated using the function D(i,j).

$$D(i,j) = \begin{cases} 0 & \text{if } C_1(i,j) = C_2(i,j) \\ 1 & \text{if } C_1(i,j) \neq C_2(i,j) \end{cases} \quad (10)$$

The terms $C_1(i,j)$ and $C_2(i,j)$ stand for the corresponding encrypted versions of the original and altered photos. Meanwhile, $D(i,j)$ demonstrates the difference in values of the pixels between the original encrypted images and their modified versions. The amount of difference in pixel count between the two encrypted photos is the basis for the NPCR computation.

2.3.2 The Unified Average Changing Intensity (UACI) system

The average intensity difference between two encrypted images can be found using the Unified Average Change Intensity (UACI) [11]. It has the following definition [3]:

$$UACI = \sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255 \times N} \times 100\% \quad (11)$$

Where $C_1(i,j)$ and $C_2(i,j)$ show the encrypted photos both before and after the original image's pixel was changed.

Table 8. Comparing NPCR with alternative models.

Dataset	Lena	Cameraman	Baboon	Peppers
N. H. Sharkawy et al.[3]	99.68%	99.61%	99.61%	99.66%
X. Wang et al.[8]	99.59%	NA	NA	99.60%
E. Z. Zefreh [9]	99.61%	99.61%	99.61%	99.60%

Table 9. Comparing UACI with alternative models.

Dataset	Lena	Cameraman	Baboon	Peppers
N. H. Sharkawy et al.[3]	33.57%	33.56%	33.29%	33.29%
X. Wang et al.[8]	33.51%	NA	NA	33.44%
E. Z. Zefreh [9]	33.50%	33.47%	33.47%	33.52%

Table 10. Analyzing recent research articles involves comparing them based on the evaluation measures they used to determine how well spatiotemporal image encryption methods worked.

Ref	Histogram Analysis	CCA	Entropy	PSNR	MSE	NPCR	UACI
[1]	No	Yes	Yes	Yes	Yes	No	No
[2]	Yes	Yes	Yes	Yes	Yes	Yes	Yes
[3]	Yes	Yes	Yes	No	Yes	Yes	Yes
[8]	Yes	Yes	Yes	Yes	Yes	Yes	Yes
[9]	Yes	Yes	Yes	Yes	Yes	Yes	Yes
[10]	Yes	Yes	Yes	No	Yes	Yes	Yes

3 CONCLUSION

All of this research has been studied and this research has used many parameters that measure performance, interpretation of results and results of experimental evaluations. These milestones characterize the quality of work. Correlation Coefficient Analysis (CCA) milestones where the best result [3] was at a rate of 0.0046 and in other milestones such as Information Entropy was [2] the closest to 8 and the value was 7.9994 and so for the rest of the milestones.

REFERENCES

1. M. A. Alohalı *et al.*, “Blockchain-Driven Image Encryption Process with Arithmetic Optimization Algorithm for Security in Emerging Virtual Environments,” *Sustain.*, vol. 15, no. 6, 2023, doi: 10.3390/su15065133.
2. I. Aouissouı, T. Bakır, and A. Sakly, “Robustly correlated key-medical image for DNA-chaos based encryption,” *IET Image Process.*, vol. 15, no. 12, pp. 2770–2786, 2021, doi: 10.1049/ipr2.12261.
3. N. H. Sharkawy, Y. M. Afıfy, W. Gad, and N. Badr, “Gray-Scale Image Encryption Using DNA Operations,” *IEEE Access*, vol. 10, pp. 63004–63019, 2022.
4. Y. Zhang, L. Zhang, Z. Zhong, L. Yu, M. Shan, and Y. Zhao, “Hyperchaotic image encryption using phase-truncated fractional Fourier transform and DNA-level operation,” *Opt. Lasers Eng.*, vol. 143, no. April, p. 106626, 2021, doi: 10.1016/j.optlaseng.2021.106626.
5. R. Rivest, “The MD5 message-digest algorithm,” 1992.
6. V. Mekathoti and B. Nithya, *A Survey on Congestion Control Algorithms of Wireless Body Area Network*, vol. 735 LNEE. 2021.
7. H. Liu and X. Wang, “Color image encryption based on one-time keys and robust chaotic maps,” *Comput. Math. with Appl.*, vol. 59, no. 10, pp. 3320–3327, 2010, doi: 10.1016/j.camwa.2010.03.017.
8. X. Wang, W. Xue, and J. An, “Image encryption algorithm based on LDCML and DNA coding sequence,” *Multimed. Tools Appl.*, vol. 80, no. 1, pp. 591–614, 2021, doi: 10.1007/s11042-020-09688-7.
9. E. Z. Zefreh, “An image encryption scheme based on a hybrid model of DNA computing, chaotic systems and hash functions,” *Multimed. Tools Appl.*, vol. 79, no. 33–34, pp. 24993–25022, 2020, doi: 10.1007/s11042-020-09111-1.
10. P. W. Khan and Y. Byun, “A blockchain-based secure image encryption scheme for the industrial internet of things,” *Entropy*, vol. 22, no. 2, 2020, doi: 10.3390/e22020175.
11. U. Zia *et al.*, “Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains,” *Int. J. Inf. Secur.*, vol. 21, no. 4, pp. 917–935, 2022, doi: 10.1007/s10207-022-00588-5.
12. A. Sonı and A. Kumar Acharya, “A Novel Image Encryption Approach using an Index based Chaos and DNA Encoding and its Performance Analysis,” *Int. J. Comput. Appl.*, vol. 47, no. 23, pp. 1–6, 2012, doi: 10.5120/7493-9944.
13. J. Liu, Y. Ma, S. Li, J. Lian, and X. Zhang, “A new simple chaotic system and its application in medical image encryption,” *Multimed. Tools Appl.*, vol. 77, no. 17, pp. 22787–22808, 2018, doi: 10.1007/s11042-017-5534-8.
14. X. Liu and T. Zhu, “Deep learning for constructing microblog behavior representation to identify social media user’s personality,” *PeerJ Comput. Sci.*, vol. 2016, no. 9, 2016, doi: 10.7717/peerj-cs.81.
15. P. Zhen, G. Zhao, L. Min, and X. Jin, “Chaos-based image encryption scheme combining DNA coding and entropy,” *Multimed. Tools Appl.*, vol. 75, no. 11, pp. 6303–6319, 2016, doi: 10.1007/s11042-015-2573-x.

16. S. Chirakkarottu and S. Mathew, "A novel encryption method for medical images using 2D Zaslavski map and DNA cryptography," *SN Appl. Sci.*, vol. 2, no. 1, 2020, doi: 10.1007/s42452-019-1685-8.
17. A. Belazi and A. A. A. El-latif, "Author ' s Accepted Manuscript," *Signal Processing*, 2016, doi: 10.1016/j.sigpro.2016.03.021.