Efficient Image Encryption Using DNA Encoding Rules and Modular Arithmetic Operation

Farhana Shirin Chowdhury[1], Kingshuk Dhar[2]

Abstract

In today's dynamic world, we rely heavily on online communication for day-to-day communication. Confidentiality becomes essential when sending digital data, including images. One of the best ways to ensure secrecy is through picture encryption. In this context, we propose a novel technique for image encryption that combines DNA encoding rules and modular arithmetic operation. In our proposed method, the position of each pixel is first changed by applying a modular arithmetic operation to the current position of each pixel of the host image using a secret key. Then, the image is split into non-overlapping blocks following the circular shift operation. The pixel values of each pixel in each block are then modified by using logical operations to the current pixel value and DNA encoding rules. Extensive testing has been done to validate the effectiveness of this approach. It is evident from statistical and differential analysis that our suggested system offers robust defense against different kinds of attacks, such as histogram attacks, correlation-based attacks, chosen plaintext and known plain text attacks, and so on. Furthermore, our technique outperforms other well-known systems in some critical aspects, thereby demonstrating its potential to advance the field of image encryption significantly.

KeyWords: *Chaotic Map, DNA Encoding, Confusion, Diffusion, Arithmetic, Modular.*

1. Introduction

In today's day-to-day communication, we are greatly dependent on the Internet. Since technology and industry emerged extensively, much multimedia data in text, image, audio, and video are transmitted over the networks. However, these data can be tempered, accessed unauthorizedly, and have ownership issues. Therefore, solutions are introduced to deal with these issues, such as watermarking (Yeung et al., 1997), cryptography, and authentication algorithms (Muhammad et al., 2018).

1. *Associate Professor*
Department of Computer Science and Engineering
Premier University, Chittagong, Bangladesh.
Email: fshirin2007@gmail.com

2. *Assistant Professor*
Department of Computer Science and Engineering
Premier University
Email: kingshuk2018@gmail.com

Image watermarking embeds watermark data into the host image (Yeung et al., 1997), whereas image cryptography aims to encrypt images using secret code by applying different cryptographic algorithms (Satish et al., 2019).

Cryptographic methods can be done in two ways: permutation and diffusion. In permutation, also known as scrambling, the pixel position of the image is changed (Min et al., 2013). Meanwhile, in diffusion, another value changes the pixel's value (Kengnou Telem et al., 2022).

In recent years, chaotic systems have played an important role in image encryption. The spatial qualities of chaos systems are high sensitivity in initial condition, ergodicity, pseudo-randomness, and determination. These requirements are crucial for image encryption. In a chaos-based cryptosystem, confusion and diffusion processes are performed jointly (Zhang et al., 2011). Fig. 1 shows an overview of its architecture.

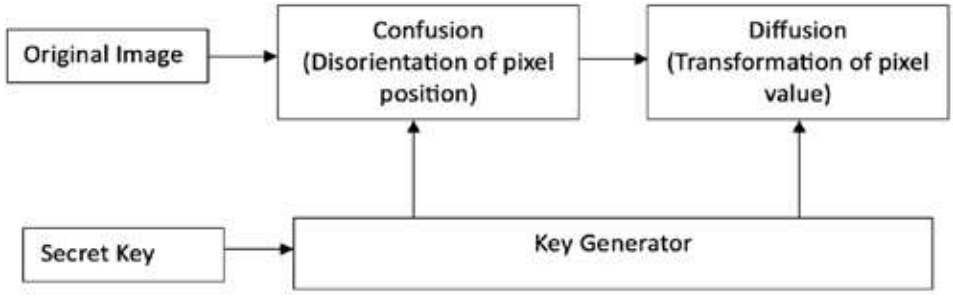


Figure 1. Overview of Chaotic System.

In permutation, the pixel positions are changed first, then in diffusion, the pixel values are changed. Both in permutation and diffusion, a secret key is used to ensure the security of the process.

A digital image has several properties: correlation between adjacent pixels, redundancy of image information, and large data capacities. All these properties should be accountable for encrypting an image.

Most image encryption techniques use complex steps that increase the computational overhead (Kengnou Telem et al. 2022; Wang et al., 2017).). The primary purpose of this research is to propose a simple yet well-defined image-scrambling method. For this purpose, a chaotic-based image encryption

method is proposed. The proposed system changes the pixel position by applying modular arithmetic operation. Finally, the diffusion process is carried out by imposing DNA rules on dividend blocks to reduce the computational overhead.

Our paper is organized into five sections. The second section expands on some previous work, while the third thoroughly discusses the proposed strategy. Section 4, the second-to-last element, summarizes the evaluation of the proposed method. Finally, Section 5 concludes with some final thoughts.

2. Related works

Asymmetric and symmetric encryption are the two categories of conventional image encryption methods. A single secret or private key is used for encryption and decryption in symmetric encryption. Conversely, asymmetric encryption methods require the public key to encrypt the data and the private key to decrypt the data. These methods for image encryption employ several algorithms, including DES, AES, RSA, TDEA, and others (Blakley et al.,1979; Wang et al., 2014; Barker et al., 2017). However, because of their large storage capacity, great redundancy, and significant correlation between neighboring pixels, these techniques are ineffective for encrypting such digital images.

An algorithm is designed employing scrambling to be different from traditional techniques of hiding data in the image. The primary idea of this method is to flip the host image's pixel location. Arnold Transformation (AT) is one of the most widely used scrambling techniques (Min et al., 2013). The periodicity issue is this method's primary flaw. That means one can get the original image after executing a few iterations in the jumbled image. Using no additional bandwidth, (Van De Ville et al., 2004) presented an effective image encryption method. This method's drawback is that the decrypted image is not fully recovered, and the scrambled image is not fully scrambled. In (Satish et al., 2019), a modified Arnold Transformation is applied. The images are disoriented into two levels, and the iteration process is performed alternatively in pixels and blocks. The disadvantage of this method is that the overall performance is not satisfactory. (Chang et al., 2009) proposed a magic-square scrambling method in a grayscale image. In this process, the least significant bits are replaced by each block. The drawback of this method is that the magic squares are not performed well in the even order.

In (Wong et al., 2008), a chaotic-based image encryption is proposed where diffusion is performed by add and shift basis. The disadvantage of this scheme is that the NPCR and UACI value is achieved after some iterations of confusion and diffusion. Also, the cross-correlation value is not quite well. Block-based image encryption using the Playfair matrix is proposed (Albahrani et al., 2020). The authors used a 16x16 modified Playfair matrix as a key in this paper. The main drawback of the algorithm is that the block size is fixed, and the time complexity is high. (Wang et al. 2017) suggested a novel encryption method based on DNA encoding. This proposed system first generates a key image by randomly applying one of the eight DNA codes to the original image. After that, the host image and key are encoded to generate a cipher image. The main flaw of this algorithm is that the encoding procedure takes too many computational steps to generate a cipher image. Also, the cross-correlation value is not suitable for this method. (Liu et al., 2012) suggested a DNA complementary and chaotic map-based image encryption method. Every pixel in this investigation is encoded by DNA coding and then transformed into a base pair using the piecewise linear chaotic map. The disadvantage of this scheme is that the overall performance, such as NPCR value, UACI value, and information entropy, is not quite good. An affine transformation and zigzag process are performed to a binary image in (Kengnou Telem et al. 2022). In order to cause confusion and dissemination, the secret key in this study is produced from a binary image and paired with another key. This approach performed successfully exclusively in biomedical photos. A bi-modular architecture was proposed by (Boriga et al., 2014). It involves the use of a random permutation to shuffle picture places and a newly developed XOR operation to modify pixel values. An image encryption method is suggested to enhance diffusion performance and overall security (Eslami et al., 2013). (Alkhonaini et al., 2024) presented a technique that combines reversible cellular automata (RCA) and two-way chaotic maps to increase key sensitivity and broaden the key space. (Sun et al. 2023) present a new cryptosystem that combines random signal insertion with a 6D hyperchaotic system. To enhance the dynamic performance of the system, random signals are repeatedly added to the system variables. The system's initial values are generated as the sum of all plaintext pixel values, ensuring that the simple image and the cryptosystem have a close link.

3. Proposed method

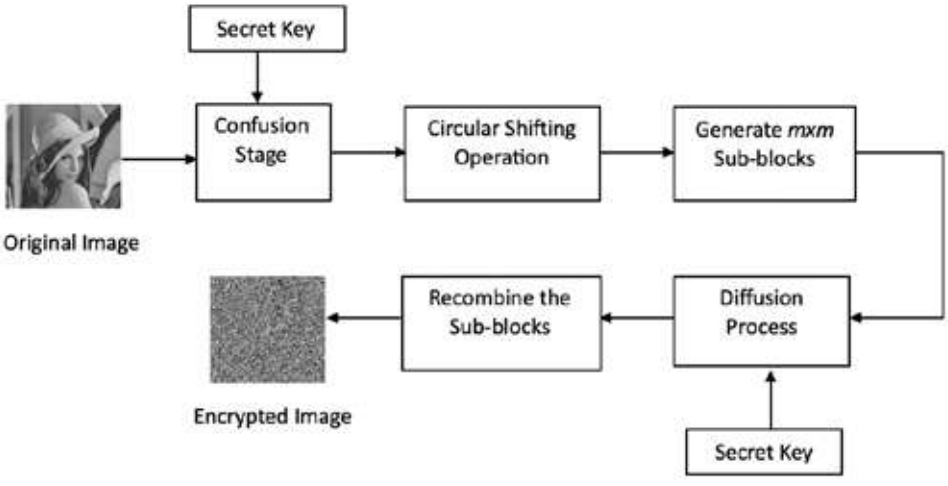


Figure 2. Encryption Process of Proposed Method.

We suggested a simple yet good image encryption method in our proposed system. The whole process is described in Fig. 2. The whole process is elaborated in the following:

Step 1: At first, the pixel position of the whole image is scrambled using the equation (1):

$$a'(x', y') = (a(x, y) * key) \bmod 256 \quad (1)$$

In this case, $a'(x', y')$ is the new location of the scrambled image following the application of a modulus operation to the multiplied position of the plain image. (x, y) is the pixel position of the original image. The value selected at random is the key.

Step 2: After that, circular shift operation is applied to the scrambled image using equation (2):

$$a'' = a'_{(x'+c_v)+mod\ X,\ (y'+c_h)+mod\ Y} \quad (2)$$

Here, a'' is the translated image. Pixels are shifted c_v and c_h along *the* x- and y-axes, respectively.

Step 3: In this third step, the scrambled image a'' is divided into M *number of* non-overlapping L blocks with the size of $m \times m$, where m represents the row and column size and $L = \{L_1, L_2, \ldots, L_M\}$.

Step 4: The four chemical bases Adenine (A), Thymine (T), Cytosine (C), and Guanine (G) in the DNA double helix always produce "base pairs" by bonding with the same recipient. Cytosine is always paired with Guanine, and Adenine pairs with Thymine. According to DNA rules, A, T, C, and G complement each other (Liu et al., 2012)—only eight out of 4!=24 different coding types meet these complementary rules. Any eight-bit pixel value in a grayscale image can be encoded into a nucleotide string by using the four-acid base T, C, G, and A to represent the binary values 00, 01, 10, and 11, respectively (Liu et al., 2012). For instance, if a pixel value has a grayscale value of 228, its four 2-bit nucleotides, "AGCT," can be used to represent its binary value, 11100100. Such 8 combinations are represented in Table 1. In this step, we encode our pixel values using these rules, as explained in equation (3).

$$L_i(p, q) = g \oplus (g \ mod \ 8) \quad (3)$$

Here, $L_i\ (p, q)$ is the modified pixel value in the i number sub-block, and $i = \{1, 2, 3, \ldots, M\}$, the L_i block's pixel value is denoted by g in the (p, q) position. Here, we first apply the modulus operation to the pixel value g. The reminder of this operation is used to determine rule no. For example, if the reminder is 7, we use rule no 7, which is "CGAT," and its binary and decimal representation is 01101100 and 108, respectively. After that, we XOR the pixel value g with this decimal value. Moreover, in this way, we change each pixel value of each image block L_i.

Step 5: Finally, we merge all the sub-blocks L and obtain a new encoded image E.

Table 1
Complementary Coding Combinations

Rule	Rule 0	Rule 1	Rule 2	Rule 3	Rule 4	Rule 5	Rule 6	Rule 7
00	A	A	G	G	T	C	G	C
01	G	G	A	A	C	T	C	G
10	T	C	T	C	A	A	A	A
11	C	T	C	T	G	G	T	T

4. Performance Analysis of Proposed Method

Figure 3. Original Grayscale Image.

In this segment, the effectiveness of the suggested encryption method is analyzed. A comparative analysis of the suggested and other recent methods is also studied. The projected approach is executed using MATLAB R2024a software on a computer equipped with a Core i5 processor and 16 GB of random-access memory. The USC-SIPI image dataset (The USC-SIPI Image Database) is used to collect the experimental images. Digitalized images are gathered and utilized for research purposes in the USC-SIPI image database. The images are varied into sizes 1024x1024, 512x512 and 256x256. Each pixel is represented by 8 bits/pixel for black and white images, whereas for color

images, this representation would be 24 bits/pixels. The host images Lena, Mandrill, and Peppers, which are shown in Fig. 3, are used for assessment. The simulation uses the original grayscale host image 256 × 256. It consists of 8 x 8 non-overlapping blocks throughout the entire image. A sample of 8 x 8 sub-block is shown in Fig.4.

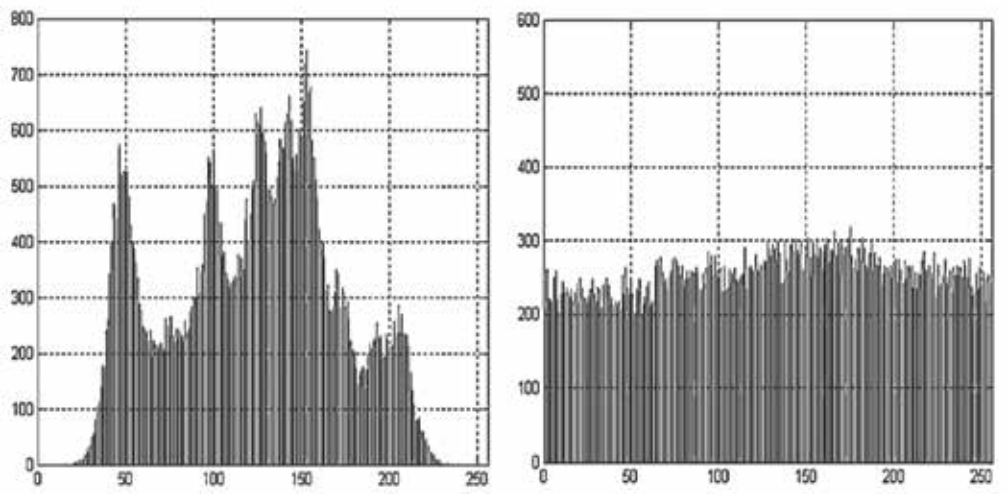
Figure 4. Sample of 8x8 Non-Overlapping Sub-block.

4.1 Histogram Analysis

Figure 5 displays both the original and encrypted images generated with the suggested technique. The original and encrypted images' histogram analysis is displayed in Fig. 6. The number of pixels on each gray level is shown via a histogram. If the histogram of cipher image is smoother, then it represents that the suggested approach is more effective. The illustration shows that the color bands and the cipher image's histogram are equally distributed. As a result, studying the histogram yields no statistically meaningful information about the original image.

(a) (b)

Figure 5. (a) Original Image; (b) Encrypted Image using Proposed Method.



(a) (b)

Figure 6. (a) Histogram of Lena; (b) Histogram of Encrypted Lena.

4.2 Correlation Coefficient (CC)

A few metrices are considered to check the performances of any encryption method. Correlation coefficient, is in the class of theses evaluation matrices. To measure, the similarities between two images, is the function of correlation coefficient (CC). If the encipher image is distorted due to the applying encryption method, the CC value will reach its lowest point. And hence, this encryption method is considered as an efficient method. The CC value is 1 if the main image and scrambled image resemblance same. Whereas, it is -1 if the cipher image is inverse to its main image. The correlation value is literally 0 if the encipher image is highly uncorrelated to its main image. The calculation of the correlation coefficient can be as follows:

$$CC = \frac{cov\ (x, y)}{\sqrt{var\ (a) \times \sqrt{var\ (a^{'})}}}$$

$$var\ (a) = \frac{1}{Y}\sum_{x=1}^{Y}(a_x\ - E\ (a_x))^2$$

$$cov\ \left(a, a^{'}\right) = \frac{1}{Y}\sum_{x=1}^{Y}(a_x\ - E(a))\left(a_x^{'}\ - E(a^{'})\right) \quad (3)$$

Where *a'* is the enciphered image of its key image *a*, *var(a)* and *var(a')* are the variance at a pixel value of image *a* and *a'* respectively, both *E(a)* and *E(a')* is the mean value of a_x and a'_x correspondingly. Co-variance between *a* and *a'* is denoted as *cov(a, a').* Table 2 shows the values of correlation coefficients in three directions of the adjacent two pixels of the original image and cipher image. As described before, if the CC value is nearly 0, the cipher image is highly uncorrelated to its original image. Moreover, Table 2 shows that since the CC value is almost 0 in all three directions, the encrypted image is dissimilar to its original image. Also, on the basis of CC value, a comparison is shown between the proposed method and other state-of-art methods in Table 3. From the table, it can be concluded that the proposed framework is more effective than the other state-of-the-art methods in hiding the content of the original image, as the values in all three directions are nearly zero.

Table 2
Correlation Coefficients of Different Images in Three Directions

Image	Direction	Plain Image	Encrypted Image
Mandrill	Horizontal	0.75615	0.0007316
	Diagonal	0.63109	0.0004132
	Vertical	0.95491	0.0005120
Peppers	Horizontal	0.97403	-0.000571
	Diagonal	0.95317	0.000257
	Vertical	0.98112	0.000391
Lena	Horizontal	0.94185	0.0007141
	Diagonal	0.94457	0.0001796
	Vertical	0.95120	0.0006629

Table 3
Correlation Coefficients of Different Methods and Our Proposed Method

Methods	Direction	Cipher Image
(Wang et al., 2017)	Horizontal	-0.00330
	Diagonal	-0.00720
	Vertical	0.00790
(Boriga et al., 2014)	Horizontal	-0.00570
	Diagonal	0.00261
	Vertical	-0.00142
(Eslami et al., 2013)	Horizontal	0.008067
	Diagonal	0.001945
	Vertical	0.008530
Our Proposed Method	Horizontal	0.00071
	Diagonal	0.00017
	Vertical	0.00066

4.3 Information Entropy (IE)

Information entropy measures uncertainty or randomness in an image. For encrypted images, entropy quantifies the degree of randomness in the pixel values, which ideally should be uniformly distributed in a well-encrypted image. A higher entropy value indicates more randomness, which correlates with better encryption quality. The general formula of information entropy for an encrypted image is derived as:

$$H = -\sum_{x=1}^{n} p(x_i) \log_2 p(x_i) \quad (4)$$

Here, $P(x_i)$ is the probability of occurrence of each pixel value x_i, and n is the total number of possible pixel values.

The optimum entropy value for a full cipher image should be 8 or more like it.

Table 4 shows the value of information entropy of several encrypted images. The entropy value obtained by the proposed technique is closely comparable to the actual value 8. Table 5 shows the comparative entropy analysis of conventional and our proposed methods. And from the analysis, we found that the entropy value is slightly better than (Wang et al., 2017) and far better than (Boriga et al., 2014).

Table 4
Entropy Test of Various Cipher Images

Methods	Cipher Image
Mandrill	7.9973
Peppers	7.9932
Lena	7.9975

Table 5
Comparative Entropy Analysis of Recent Methods and Our Proposed Method

Methods	Cipher Image
(Wang et al., 2017)	7.99750
(Boriga et al., 2014)	7.27181
Our Proposed Method	7.99752

4.4 Differential Analysis

The tests for universal average change intensity (UACI) and number of pixels change rate (NPCR) can also be used to evaluate the scrambling method security [(Zhang et al., 2011). Several pixels affected in the enciphered image by changing a random pixel in the main image are defined by NPCR. Assume $a(x, y)$ and $a'(x', y')$ are the pixel values of the original and encrypted pictures, indicated by a and a' in the x^{th} row and y^{th} column, respectively. The calculation of NPCR can be expressed as follows:

$$NPCR = \frac{\sum_{x,y} D(x,y)}{X \times Y} \times 100\% \quad (5)$$

where,

$$D(x,y) = \begin{cases} 0, if\ a(x,y) = a'(x',y') \\ 1, if\ a(x,y) \neq a'(x',y') \end{cases} \quad (6)$$

A significantly elevated NPCR score indicates that a modification in pixel value has a substantial effect on the overall appearance of the image. The estimated critical value for this test exceeds 99% (Liu et al., 2012).

The average intensity difference between two images, commonly known as original and encipher images, can be calculated by the UACI indicator. This evaluator can be assessed as follows:

$$UACI = \frac{1}{X \times Y} \sum_{x,y} \frac{a(x,y) - a\prime(x,y)}{255} \times 100\% \quad (7)$$

The estimated analytical value of UACI must be above 33% (Liu et al., 2012).

Table 6 shows the analysis of NPCR and UACI values of different encrypted images. Also, Table 7 shows the differential analysis of the proposed method and state-of-the-art methods. Based on the comparison results, the proposed method outperforms the recent encrypting methods for NPCR and UACI.

Table 6
NPCR and UACI Analysis of Our Proposed Method

Encrypted Images	NPCR (%)	UACI (%)
Mandrill	99.0169	33.37
Peppers	99.6478	33.51
Lena	99.6667	33.55

Table 7
Comparison Between Recent Methods and Our Proposed Method in terms of NPCR and UACI

Methods	NPCR (%)	UACI (%)
(Wang et al., 2017)	99.60	33.45
(Boriga et al., 2014)	99.22	33.12
(Eslami et al., 2013)	99.65	33.33
Our Proposed Method	99.66	33.55

4.5 Key Space Analysis

Any brute-force assault should be rendered ineffective by the length of the key space (Kengnou Telem et al., 2022). In our proposed system, we use two keys: in pixel position changing, we use a 128-bit long key. From 128 bits, we get 2^{128} different key combinations of secret keys. In the diffusion stage, we use 8-bit DNA rules. From these 8 bits, we also get 2^8 distinctive arrangements of rules. The search space consists of 256 x 256 = 65,536 possible combinations, with a frequency of 1/256 = 0.0039. Therefore, from the key space and search space analysis, we can conclude that our proposed system is robust against brute-force attacks.

5 Conclusion

This paper proposes a simple, well-structured, chaotic map-based image encryption method. In our system, we scramble the pixel position of the original by applying a modular arithmetic operation, and for changing the pixel value, we use DNA rules. The effectiveness of this method has been validated through various tests. Both statistical and differential analysis demonstrate that our proposed scheme offers robust protection against statistical and differential attacks. Additionally, a comparison with other well-known schemes reveals that our method outdoes them in several aspects.

A significant limitation in our image encryption technique is the requirement to transmit the coding rules to the receiver. This creates a security breach since the encrypted image's confidentiality depends on the key's secrecy. If the key is intercepted or disclosed during transmission, the encryption is rendered ineffective, allowing unauthorized parties to decrypt the image. Furthermore, the process of securely transmitting the key introduces additional complexity and overhead, potentially reducing the overall efficiency of the encryption system.

In the future, we intend to overcome the limitation of transmitting encryption keys in image encryption techniques by focusing on the development of a more secure and efficient key management system.

References

Albahrani, E. A., Maryoosh, A. A., & Lafta, S. H. (2020). Block image encryption based on modified Playfair and chaotic system. *Journal of Information Security and Applications, 51*, 102445.

Alkhonaini, M. A., Gemeay, E., Zeki Mahmood, F. M., Ayari, M., Alenizi, F. A., & Lee, S. (2024). A new encryption algorithm for image data based on two-way chaotic maps and iterative cellular automata. *Scientific Reports, 14*(1), 16701.

Barker, E., & Mouha, N. (2017). *Recommendation for the Triple Data Encryption Algorithm (TDEA) block cipher* (NIST Special Publication No. 800-67 Rev. 2). National Institute of Standards and Technology.

Blakley, G. R., & Borosh, I. (1979). Rivest–Shamir–Adleman public key cryptosystems do not always conceal messages. *Computers & Mathematics with Applications, 5*(3), 169–178.

Boriga, R. E., Dăscălescu, A. C., & Diaconu, A. V. (2014). A new fast image encryption scheme based on 2D chaotic maps. *IAENG International Journal of Computer Science, 41*(4), 249–258.

Chang, C. C., Kieu, T. D., Wang, Z. H., & Li, M. C. (2009, August). An image authentication scheme using magic square. In *Proceedings of the 2nd IEEE International Conference on Computer Science and Information Technology* (pp. 1–4). IEEE.

Eslami, Z., & Bakhshandeh, A. (2013). An improvement over an image encryption method based on total shuffling. *Optics Communications, 286*, 51–55.

Kengnou Telem, A. N., Feudjio, C., Ramakrishnan, B., Fotsin, H. B., & Rajagopal, K. (2022). A simple image encryption based on binary image affine transformation and zigzag process. *Complexity, 2022*, Article 3865820.

Liu, H., & Wang, X. (2012). Image encryption using DNA complementary rule and chaotic maps. *Applied Soft Computing, 12*(5), 1457–1466.

Min, L., Ting, L., & Yu-jie, H. (2013, November). Arnold transform–based image scrambling method. In *Proceedings of the 3rd International Conference on Multimedia Technology (ICMT-13)* (pp. 1302–1309). Atlantis Press.

Muhammad, K., Sajjad, M., Mehmood, I., Rho, S., & Baik, S. W. (2018). Image steganography using uncorrelated color space and its application for the security of visual contents in online social networks. *Future Generation Computer Systems, 86*, 951–960.

Satish, A., Prasad, E. V., Tejasvi, R., Swapna, P., & Vijayarajan, R. (2019, April). Image scrambling through two-level Arnold transform. In *Proceedings of the Alliance International Conference on Artificial Intelligence and Machine Learning (AICAAM)*.

Sun, S. (2023). A new image encryption scheme based on 6D hyperchaotic system and random signal insertion. *IEEE Access, 11*, 1–12.

University of Southern California Signal and Image Processing Institute. (n.d.). *The USC-SIPI image database*. http://sipi.usc.edu/database/

Van De Ville, D., Philips, W., Van de Walle, R., & Lemahieu, I. (2004). Image scrambling without bandwidth expansion. *IEEE Transactions on Circuits and Systems for Video Technology, 14*(6), 892–897.

Wang, X., & Liu, C. (2017). A novel and effective image encryption algorithm based on chaos and DNA encoding. *Multimedia Tools and Applications, 76*, 6229–6245.

Wang, X., & Wang, Q. (2014). A novel image encryption algorithm based on dynamic S-boxes constructed by chaos. *Nonlinear Dynamics, 75*, 567–576.

Wang, X., & Xu, D. (2014). Image encryption using genetic operators and intertwining logistic map. *Nonlinear Dynamics, 78*, 2975–2984.

Wong, K. W., Kwok, B. S. H., & Law, W. S. (2008). A fast image encryption scheme based on chaotic standard map. *Physics Letters A, 372*(15), 2645–2652.

Yeung, M. M., & Mintzer, F. (1997, October). An invisible watermarking technique for image verification. In *Proceedings of the International Conference on Image Processing* (Vol. 2, pp. 680–683). IEEE.

Zhang, G., & Liu, Q. (2011). A novel image encryption method based on total shuffling scheme. *Optics Communications, 284*(12), 2775–2780.