Transactions on Machine Intelligence 4(2) (2022) 100-108

ISSN Online: 2821-1693

Transactions on Machine Intelligence

Journal Homepage: https://tmachineintelligence.ir/index.php/TMI

Image Encryption Using the TLBO Algorithm and Image Hash

M. Abedzadeh[1], M. J. Rostami[2,*]

[1] Department of Computer Engineering, Faculty of Engineering, Shahid Bahonar University, Kerman, Iran
[2] Assistant Professor, Department of Computer Engineering, Shahid Bahonar University, Kerman, Iran

ARTICLE INFO

Article History:
Received 22 February 2021
Received in revised form 11 April 2021
Accepted 26 June 2021
Available online 27 June 2021

Keywords:
Image Encryption, TLBO Algorithm, Logistic Map, Standard Map, SHA-512

ABSTRACT

An effective encryption algorithm must not only provide fast encryption but also be resistant to various attacks. Chaotic mappings are widely used in image encryption. Furthermore, since the hash of an image produces a distinct output for each image and changes drastically with even a single bit alteration, it can be an ideal candidate for the initial values in chaotic mappings. This paper explores the encryption of images inspired by the Teaching-Learning-Based Optimization (TLBO) algorithm, which is a metaheuristic algorithm. Initially, the image hash is computed using the SHA-512 hash function, and numbers between 0 and 1 are generated based on the obtained hash. The image is then divided into 16 equal parts. In the next step, the pixels of the image are permuted using a specific variant of the standard map proposed in this paper. In each iteration, the part with the best entropy is selected as the teacher. Among the generated values, the one that improves the entropy of that part is chosen, and other parts follow this value. Finally, the pixels of each part are altered using the logistic map. This algorithm offers both adequate execution time and high security.

1. INTRODUCTION

With the advancement of the internet in the digital world, information security has gained significant importance. Image encryption has been a topic of interest with various methods proposed in recent years. Due to the dependency between pixels, symmetric encryption methods such as DES, AES, and IDEA are not commonly used for images, or if they are, they are often combined with other methods [1]. Image encryption generally involves two main phases. The first phase is permutation, where pixel values are not changed but merely rearranged, and the second phase is substitution, where pixel values are altered using chaotic functions or specific formulas. The use of chaotic functions in both phases is common due to their pseudo-random nature [2]. Abdullah et al. proposed a method where the image is divided into four parts, and each part is encrypted separately using multiple pixels from each part through scrambling operations and chaotic logistic mapping [3]. Noshadian et al. introduced an image encryption method using logistic mapping and a modified Noth algorithm, utilizing the parameters of the logistic map as encryption keys. The optimization process of these parameters is accelerated using TLBO and GSA algorithms [4].

* Corresponding Author: mjrostamy@yahoo.com
Assistant Professor, Department of Computer Engineering, Shahid Bahonar University, Kerman, Iran

http://dx.doi.org/10.47176/TMI.2021.100

2. REQUIRED CONCEPTS

2.1. SHA-512 Hash Function

SHA stands for Secure Hash Algorithm. In 2005, security issues in the SHA-1 algorithm were discovered, leading to its compromise and the need for a more secure algorithm. SHA-2 (including SHA-512, SHA-384, SHA-256, SHA-224) is a set of hash functions proposed by the NSA and introduced in 2001 by the National Institute of Standards and Technology (NIST) as a data processing standard. A hash function converts any volume of data into a natural number, typically represented in hexadecimal form. Due to its larger output size, SHA-512 provides higher security compared to other SHA-2 versions. The SHA-512 algorithm combines information in 80 rounds [5]. Figure 1 illustrates a single stage of hashing operations in this algorithm.

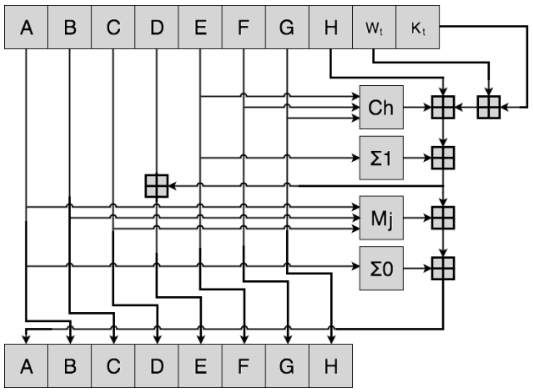

Fig.1. SHA-2 Hash Function Round Process

In the SHA-2 hash function, "Wt" is a 64-bit word derived from the current 512-bit input block, and "Kt" is a 64-bit constant that changes in each round. The SHA-2 algorithm performs several different operations in each round, as expressed in Equation 1:

$$\begin{aligned} Ch\,(E,F,G) &= (E \wedge F) \oplus (\neg E \wedge G) \\ Mj\,(A,B,C) &= (A \wedge B) \oplus (A \wedge C) \oplus (B \wedge C) \\ \Sigma 0(A) &= (A \gg 2) \oplus (E \gg 13) \oplus (A \gg 22) \\ \Sigma 1(E) &= (E \gg 6) \oplus (E \gg 11) \oplus (E \gg 25) \end{aligned} \tag{1}$$

2.2. Standard Map

The standard map, first introduced by Chirikov in 1969, is also known as the Chirikov standard map or the Chirikov-Taylor map. The standard map is generally defined by Equation (2-25) [6]:

$$\begin{aligned} \theta_{n+1} &= \theta_n + K \sin(I_n), \\ I_{n+1} &= I_n + \theta_{n+1}, \end{aligned} \tag{2}$$

where K is a one-dimensional parameter that influences the chaos degree of the standard map. Additionally, I_0 and θ_0 are initialized, and subsequent sequences are generated based on them. A specific case of the standard map used in the proposed method is observed in Equation 3:

$$\begin{aligned} \theta_{n+1} &= \theta_n + I_n - \frac{K}{2\pi}\sin(2\pi\theta_n), \\ I_{n+1} &= I_n - \theta_{n+1} \end{aligned} \tag{3}$$

2.3. Logistic Map

The logistic map is one of the most well-known and simplest chaotic maps, introduced by biologist Robert May in 1976 [7]. It is a one-dimensional map, represented by Equation 4:

$$X_{n+1} = r\, X_n\, (1 - X_n) \tag{4}$$

where X_n is a number between zero and one. The desired values for the parameter r lie within the interval [0,4) to ensure X_n values remain within the (0,1) range. For r ∈ (0,3.57), the map exhibits non-chaotic behavior, while chaotic behavior appears for r ∈ [3.57,4].

2.4. TLBO Algorithm

The Teaching-Learning-Based Optimization (TLBO) algorithm is an intelligent optimization algorithm [8]. Inspired by the teaching and learning process, this method was proposed. A key feature of this algorithm is its minimal parameter dependency, making it advantageous due to having the fewest possible parameters. In TLBO, the population is considered a group of learners or students in a class. A teacher strives to enhance the class's knowledge level, thereby improving students' scores. The best solution (best population member) in each iteration is considered the teacher. The teacher, being a knowledgeable individual, shares their knowledge with the students. Additionally, students learn from mutual interactions, which helps improve their scores.

3. PROPOSED METHOD

In image encryption, due to pixel dependencies, symmetric encryption algorithms used in text cannot be directly applied. The pseudo-random nature of chaotic maps makes them popular in image encryption for pixel shuffling and value alteration. Hash functions are also crucial in encryption due to their bit-sensitivity, where a single bit change drastically alters the output. The proposed method employs the TLBO algorithm, a metaheuristic approach, for image encryption. Additionally, using the image digest, derived from the hash function, the initial candidate values for chaotic maps are generated.

3.1. Candidate Initial Values

Candidate initial values are examined as the initial values for chaotic maps and are derived from the image digest. The image digest computed by SHA-512 comprises 128 hexadecimal digits denoted as $h_0 h_1 \dots h_{127}$. In the proposed method, each channel in a color image has 32 candidate initial values, totaling 96 for color images (32 for grayscale, calculated similarly to the red channel). These values lie within the (0,1) interval. To avoid using zero and one, which nullify all logistic map sequences, normalization is performed to exclude these values. The calculation of these values differs slightly for red, green, and blue channels. For the red channel, the first four digest digits are separated, converted to decimal, and assigned to r0. The next four digits are converted to decimal and assigned to r1, and so on, with the last four digits assigned to r31. The maximum value, FFFF, converts to 16^4-1 in decimal, so numbers are divided by 16^4. To avoid zero, one is added to the numerator and denominator. The 32 candidate initial values for the red channel are calculated using Equation 5:

$$r_i = \frac{hex2dec\,(h_{4i},h_{4i+1},h_{4i+2},h_{4i+3})+1}{16^4+1}\,, i = 0,1,\dots,31 \tag{5}$$

For the green and blue channels, similar calculations are performed with positional adjustments of the digest digits. For the green channel, as shown in Equation 6:

$$g_i = \frac{hex2dec\,(h_{4i+1},h_{4i},h_{4i+3},h_{4i+2})+1}{16^4+1}\,, i = 0,1,\dots,31 \tag{6}$$

For the blue channel, the candidate initial values are calculated according to Equation 7:

$$b_i = \frac{hex2dec\,(h_{4i+3},h_{4i+1},h_{4i},h_{4i+2})+1}{16^4+1}\,, i = 0,1,\dots,31 \tag{7}$$

3.2. Encryption

In the proposed method, there is no difference between encrypting color and grayscale images; the only variation is that the number of initial candidate values in color images is three times that in grayscale images, and encryption is performed separately for each channel. This encryption process consists of seven steps (each channel is processed separately):

1. Step 1: Compute the image digest using the SHA-512 algorithm.

2. Step 2: Using the image digest, generate 32 values for each of the red, green, and blue channels within the range of zero to one, resulting in a total of 96 values (for grayscale images, the first 32 values are used).

3. Step 3: Divide the image into 16 equal parts.

4. Step 4: In each round, the part with the highest entropy becomes the teacher. Using the logistic map (Equation 4) and the initial candidate values, the pixels are altered. The best initial value, which yields the highest entropy, is then introduced to the remaining parts, which are the students.

5. Step 5: The students adopt the best initial value introduced by the teacher as the initial value of the logistic map, and the encryption operation is performed on each of the 16 parts using this initial value.

6. Step 6: The pixels of the entire image are shuffled using the standard map (Equation 3).

7. Step 7: Repeat steps 3 to 6 for ten rounds.

For better understanding, all steps are examined using the 256x256 Lena color image.

In the first step, the image pixels are arranged in a sequential string of numbers (with a space between each pixel), and then the digest of this string is computed using the SHA-512 algorithm. The computed digest of the Lena image is shown below:

45CD26176013C49F334AD7AF2C87E51E774653DF9304A4E257DAD50F3B4A49A

7B9BE8581C3257368D5F7CD210DDB746499FFCE07C109678CF345E17005374050

In the second step, the obtained digest, comprising 128 hexadecimal digits, is used to generate a set of numbers (initial candidate values), as fully explained in section 3-1.

In the third step, the Lena image is divided into 16 equal parts (Figure 2).

Fig.2. Division of the Lena Image into 16 Equal Parts.

In the fourth step, the part with the highest entropy is selected as the teacher. Then, using the logistic map, one of the 32 values is chosen sequentially as the initial value of the logistic map, and the pixels of the selected part are altered (as per Equation 8).

$$X_{n+1} = X_n\, r\, (1 - X_n)$$

$$X_{n+1} = round(X_{n+1} \times 255)$$

$$Pix_{new} = Pix_{old} \oplus X_{n+1} \quad (8)$$

In the fifth step, the initial value that results in the highest entropy is introduced to the remaining parts as the best value, and the students learn from the teacher. Each part is altered separately with the best initial value.

3.3. Key Management

To generate the key to be sent to the receiver for decryption, the following steps are taken:

First, the 512-bit digest obtained from the image hash is required. However, this 512-bit digest is insufficient because it is necessary to know which initial values were used for encryption in each round. Since 32 values are generated for each channel, 5 bits are sufficient to identify each value. In grayscale images, 10 rounds use initial values for each channel, requiring ten 5-bit segments. Combined with the 512-bit digest, the total key length for grayscale images is 562 bits. For color images, there are three channels, resulting in 30 initial values during encryption, each occupying 5 bits, totaling 150 bits. Combined with the image digest, the key length for color images is 662 bits. Therefore, the key length is 562 bits for grayscale images and 662 bits for color images.

The key is structured such that the first 512 bits correspond to the image digest, followed by 5-bit segments that indicate the positions of the initial values. For instance, if bits 513 to 517 are 10110 (which is 22 in decimal), it means that in the first round of the red channel, r_{22} was selected. The next 5-bit segment indicates the chosen number in the second round of the red channel, and so on. Subsequently, values for the green and blue channels follow.

3.4. Decryption

Decryption requires the key, and decryption operations are performed using this key. For grayscale images, 32 values are needed, and for color images, 96 values are needed, as explained in section 3-1. In the red channel, pixel shuffling is first performed using the standard map with initial values $\theta_0 = r_{18}$ and $I_0 = r_{19}$. Once numbers equal to the pixel count are generated, the first pixel moves to the position where the largest value was originally located, the second pixel to the second-largest, and so forth. The number in bits 558 to 562 of the key indicates the value used for encryption in the tenth round of the red channel, thus decryption is done using this value as the initial value of the logistic map. Each of the 16 segments is then individually altered using Equation 8. In the next round of the red channel, pixels are reshuffled using the standard map with initial values θ_0 = r16 and $I_0 = r_{17}$, and the pixel rearrangement is done as in the previous round. The number in bits 553 to 557 of the key is the initial candidate value used for encryption in the ninth round of the red channel, so decryption is performed using this value, and the same steps as the previous round are repeated. This process continues for ten rounds to decrypt the red channel. The green and blue channels are decrypted similarly. In the green channel, the initial values of the standard map in the first round are = g_{18} θ_0 and $I_0 = g_{19}$, and in subsequent rounds, the values are chosen similarly to the red channel, ending with g_0 and g_1 in the final round. The initial values of the logistic function in the first round are in bits 608 to 612, with each subsequent round using the previous 5 bits, continuing until the final round. In the blue channel, the standard map's initial values in the first round are b18 = θ_0 and I_0 = b19, with subsequent rounds using the previous values as in the red and green channels. The initial values of the logistic function in the first round are in bits 658 to 662, and each subsequent round uses the previous 5 bits.

4. RESULTS OF THE PROPOSED METHOD

In this study, results and comparisons were conducted using MATLAB R2019a, and all implementations were carried out on a system with an Intel Core i7-7500U 2.7GHz processor and 8GB of RAM. Figure 3 shows the Baboon, Peppers, color Lena, and grayscale Lena images before encryption, after encryption, and after decryption.

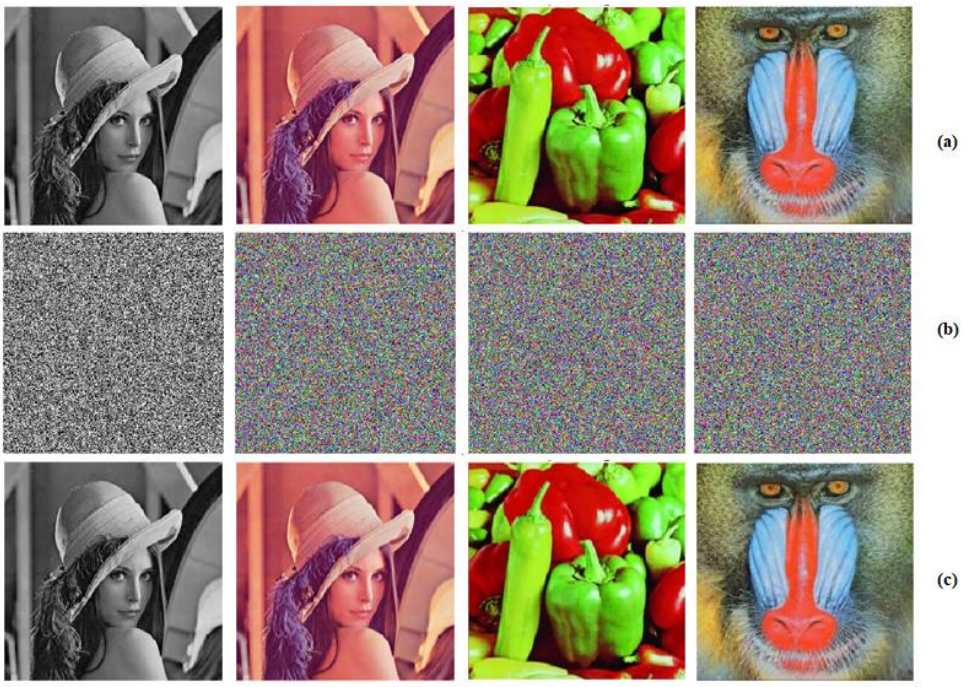

Fig.3. Encryption Results for Various Images (a) Original images; (b) Images encrypted with the proposed algorithm; (c) Decrypted images. (From right to left: Baboon, Peppers, color Lena, and grayscale Lena).

4.1. Visual Analysis

An encryption algorithm is deemed suitable if no information from the original image can be discerned from the encrypted image. Since visual analysis results can vary among viewers, histogram analysis is recommended. Histogram analysis describes the distribution of an image's pixels by the number of observations at each intensity level [9]. The histogram of the grayscale Lena image before and after encryption is shown in Figure 4:

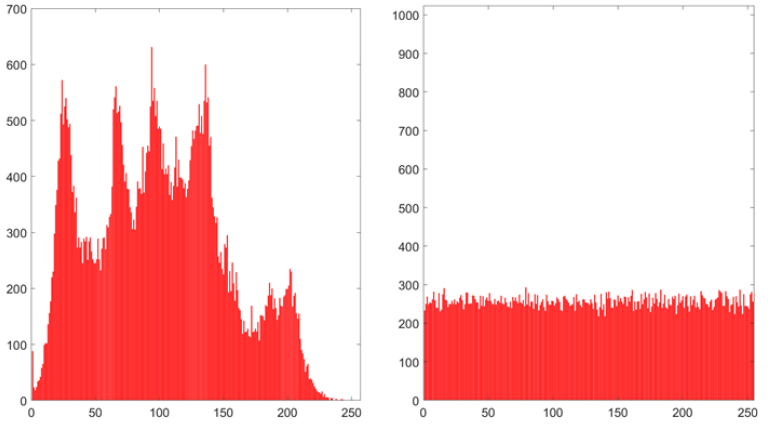

Fig.4. Histogram of the Grayscale Lena Image Before (left) and After Encryption (right).

Additionally, the correlation between pixels before and after encryption is shown in Figure 5. As observed, the proposed method successfully eliminates pixel correlation.

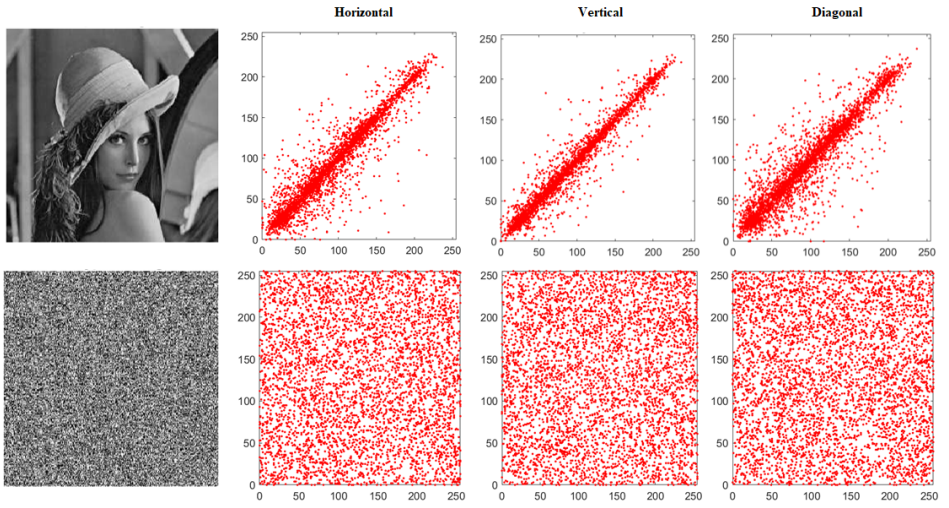

Fig.5. Correlation of Pixels in the Lena Image Before and After Encryption in Horizontal, Vertical, and Diagonal Directions.

4.2. Statistical Analysis

In ordinary images, each pixel is correlated with its vertical, horizontal, and diagonal neighbors. During image encryption, this dependency must be eliminated. The correlation coefficient is a measure used to calculate the correlation of neighboring pixels (horizontal, vertical, and diagonal) and is expressed in Equation 9 [10]:

$$
\begin{aligned}
&r_{xy} = \frac{cov\,(x,y)}{\sqrt{D(x)D(y)}} \\
&E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \\
&D(x) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x_i)\right)^2 \\
&cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x_i)\right)\left(y_i - E(y_i)\right)
\end{aligned}
\tag{9}
$$

where x and y are the values of neighboring pixels, N is the number of pixel pairs, and to ensure the correlation coefficient remains consistent, N equals the total number of pixels so that the correlation of all pixels is examined. cov(x,y) is the covariance, D(x) is the variance, and E(x) is the mean. The closer the correlation coefficient is to zero, the less the dependency between pixels, and the closer it is to 1 or -1, the higher the dependency.

Information entropy is used to determine the randomness of pixel distribution in images. The entropy calculation is given in Equation 10 [11]:

$$
\mathrm{E}_{\mathrm{R/G/B}}(x) = -\sum_{i=0}^{2^n-1} \mathrm{P}(x_i)\log_2 \mathrm{P}(x_i) \tag{10}
$$

where P(xi) is the probability of symbol xi, and n is the number of bits that xi can encompass. In images, pixel values range from [0, 255], represented by up to eight bits, so n = 8. The closer the entropy value is to 8, the better the image encryption.

4.3. Comparison of the Proposed Method

Comparing the proposed method with other methods shows that the proposed method records better results. Table 1 compares the entropy and correlation coefficients of the proposed method with other methods on the grayscale Lena image.

Table 1. Comparison of the Proposed Method with Other Methods on the Grayscale Lena Image.

	Entropy	Correlation coefficient		
		Horizontal	Vertical	Diagonal
Proposed Method	7.9976	0.0047	0.0089	-0.0027
Ref [9]	7.9973	-0.0253	0.0025	0.0090
Ref [10]	7.5899	-0.0428	-0.043	-0.048
Ref [11]	7.9974	0.0095	-0.0195	0.0246

4.4. Execution Time

One advantage of this algorithm is its high speed. The encryption and decryption speeds of the proposed method for 256×256 and 512×512 grayscale and color images are shown in Table 2.

Table 2. Execution Time of the Proposed Algorithm in Seconds.

	Image Dimensions	Decryption Time	Encryption Time
Gray images	256×256	0.1852	0.0407
	512×512	0.6822	0.1918
Color pictures	256×256	0.5663	0.1227
	512×512	0.5831	2.1120

5. CONCLUSION

This paper presents a novel image encryption method inspired by the TLBO algorithm and utilizing standard and logistic maps. Using the SHA-512 hash function, initial candidate values are generated according to the proposed equations, and the encryption process is carried out. A specific case of the standard map is also introduced. The proposed method achieves excellent results in statistical analysis, with outcomes very close to the ideal. Histograms demonstrate that the proposed method can create a uniform distribution, and pixel correlations are entirely eliminated, indicating no dependency between pixels. The proposed method is fast, capable of encrypting and decrypting images quickly. All these features show that the proposed method is highly suitable for image encryption and provides high security.

Transparency Statement

The data supporting this study are available upon reasonable request to the corresponding author, subject to ethical and confidentiality considerations.

Acknowledgments

We would like to express our gratitude to all individuals who contributed to this project.

Declaration of Interest

The authors declare that they have no competing interests.

Funding

This research received no specific grant from any funding agency, commercial, or not-for-profit sectors.

REFERENCES

[1] Li, S., Wang, X., Zhang, J., & Shum, H. (2007). On the design of perceptual MPEG-video encryption algorithms. IEEE Transactions on Circuits and Systems for Video Technology, 17(2), 214-223. https://doi.org/10.1109/TCSVT.2006.888840

[2] Alvarez, G., & Li, S. (2006). Some basic cryptographic requirements for chaos-based cryptosystems. International Journal of Bifurcation and Chaos, 16(8), 2129-2151. https://doi.org/10.1142/S0218127406015970

[3] Abdullah, A. H., Enayatifar, R., & Lee, M. (2012). A hybrid genetic algorithm and chaotic function model for image encryption. AEU - International Journal of Electronics and Communications, 66(10), 806-816. https://doi.org/10.1016/j.aeue.2012.01.015

[4] Noshadian, S., Ebrahimzade, A., & Kazemitabar, S. J. (2018). Optimizing chaos based image encryption. Multimedia Tools and Applications, 77(19), 25569-25590. https://doi.org/10.1007/s11042-018-5807-x

[5] Glabb, R., Imbert, L., Jullien, G., Tisserand, A., & Veyrat-Charvillon, N. (2007). Multi-mode operator for SHA-2 hash functions. Journal of Systems Architecture. https://doi.org/10.1016/j.sysarc.2006.09.006

[6] Chirikov, B. V. (1979). A universal instability of many-dimensional oscillator systems. Physics Reports. https://doi.org/10.1016/0370-1573(79)90023-1

[7] May, R. M. (1976). Simple mathematical models with very complicated dynamics. Nature. https://doi.org/10.1038/261459a0

[8] Rao, R. V., Savsani, V. J., & Vakharia, D. P. (2011). Teaching-learning-based optimization: A novel method for constrained mechanical design optimization problems. Computer-Aided Design. https://doi.org/10.1016/j.cad.2010.12.015

[9] Guesmi, R., & Farah, M. A. B. (2021). A new efficient medical image cipher based on hybrid chaotic map and DNA code. Multimedia Tools and Applications, 80(2), 1925-1944. https://doi.org/10.1007/s11042-020-09672-1

[10] Naz, F., Shah, T., Din, Z., Shah, A., & Qaisar, S. M. (2020). An ASCII based effective and multi-operation image encryption method. Multimedia Tools and Applications, 79(31-32), 22107-22129. https://doi.org/10.1007/s11042-020-08897-4

[11] Abbasi, A. A., Mazinani, M., & Hosseini, R. (2020). Evolutionary-based image encryption using biomolecules operators and non-coupled map lattice. Optik. https://doi.org/10.1016/j.ijleo.2020.164949