Mesopotamian journal of Computer Science
Vol. **(2025)**, 2025, **pp**. 341–354
DOI: https://doi.org/10.58496/MJCSC/2025/22 ;ISSN: 2958-6631
https://mesopotamian.press/journals/index.php/cs

Research Article

Enhanced TEA Algorithm Performance using Affine Transformation and Chaotic Arnold Map

Nada Hussein M. Ali[1], Mays M. Hoobi[1], Sura Abed Sarab Hussien[1,*]

[1]*Department of Computer Science, College of Science, University of Baghdad, Baghdad, Iraq*

ARTICLEINFO

Article History

Received 31 Jul 2025
Revised 3 Sep 2025
Accepted 30 Sep 2025
Published 3 Oct 2025

Keywords

Affine transformation, Arnold map
Keyspace
PSNR
RGB image
TEA

ABSTRACT

In digital images, protecting sensitive visual information against unauthorized access is considered a critical issue; robust encryption methods are the best solution to preserve such information. This paper introduces a model designed to enhance the performance of the Tiny Encryption Algorithm (TEA) in encrypting images. Two approaches have been suggested for the image cipher process as a preprocessing step before applying the Tiny Encryption Algorithm (TEA). The step mentioned earlier aims to de-correlate and weaken adjacent pixel values as a preparation process before the encryption process. The first approach suggests an Affine transformation for image encryption at two layers, utilizing two different key sets for each layer. The dual encryption process achieves high diffusion and confusion properties for the cipher process. The second approach proposed a chaotic Arnold map before the Tiny Encryption Algorithm (TEA) process. Various statistical measures are used, such as Peak Signal to Noise Ratio (PSNR), Structural Similarity Index (SSIM), and Image Quality Index (IQI). For example, the lower PSNR, SSIM, and IQI values indicate better results for test image Lina of the second approach. The obtained results for the previous measures of the second approach are 8.5449, 0.0008, and -0.0061, compared to the first approach, 8.5529, 0.0054, -0.0015, respectively. Moreover, key space and time analysis are used to assess the encryption process. The outcomes show a high-key space ($32{,}768 * 2^{128}$) and a slight encryption time of 130 milliseconds for the first approach and 1862 milliseconds for the second approach.

1. INTRODUCTION

Data security has gained much attention, and in support of the same, cryptographic algorithms have played a major role in maintaining the confidentiality and integrity of sensitive information [1,2]. The encryption method must have an intense and complicated key that unauthorized users cannot easily guess or crack [3]. Among the many lightweight encryption algorithms, the most efficient and with the least computational overhead is the Tiny Encryption Algorithm (TEA). However, traditional implementations for TEA suffer from some drawbacks; such deployments are prone to attacks and continue to be vulnerable to various forms of advanced threats [4]. This study aims to achieve two main objectives: first, improving the robustness of the TEA algorithm by proposing a hybrid model against various attacks as described later. Secondly, to develop a cryptographic model that ensures high security through increased complexity and improved efficiency with reduced execution time, making it well-suited for image encryption applications.

1.1 Tiny Encryption Algorithm (TEA) Concepts

The TEA algorithm is a block cipher that works on a 64-bit register, and the key length is 128 bits. Its explanation and implementation are simple (usually a little code) and have a Feistel structure with 64 rounds, usually done in pairs called cycles. The key setup is easy; all rounds have the same keys [5]. Because TEA is easy to create, it has a quick run time and requires little space for storage [6]. Also, TEA has a 128-bit key, which is split into four parts; this gives 32-bit keyword lengths K[0], K[1], K[2], and K[3], as shown in Figure 1[7].

*Corresponding author. Email: sura.a@sc.uobaghdad.edu.iq

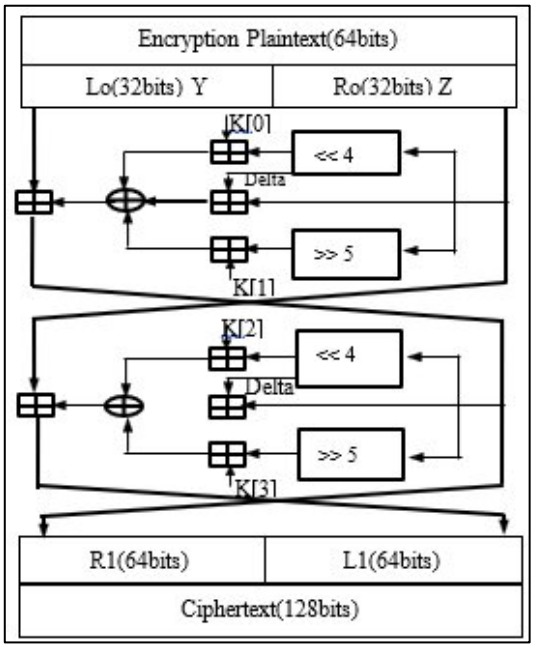


Fig.1: A Single Round TEA with 2 Feistel Operations [7]

1.2 Affine Transformation Principles

An affine transformation is a substitution cipher where each letter in an alphabet is mapped to its numeric equivalent. The encryption process uses a simple mathematical structure, while the decryption process converts back to a letter. Affine transformation is widely used as an encryption algorithm in image and other multimedia file encryption. It is considered a special case of a general monoalphabetic substitution cipher, and it is subjected to frequency cryptanalysis. It carries out many operations such as scaling, truncation, rotation, and translation. In addition, pixel scrambling is also achieved based on an Affine transformation in image encryption. Despite these features, the Affine transformation has weak image encryption and must be improved with other methods [8]. In general, the mathematical structure of the Affine transformation is based on a monoalphabetic substitution cipher, as shown in Equations (1) and (2) [9]:

$$y = (ax + b) mod\ n \qquad (1)$$

$$y^{-} = (a^{-1}\, x + b)\ mod\ n \qquad (2)$$

Where:

- y is the encryption operation.
- $y^{-}$is the decryption operation.
- a and b represents the two encryption keys and is a nonzero value.
- n is the range of the alphabet.

The Affine transformation is similar to other substitution ciphers; it produces identical patterns for plaintext-ciphertext pair characters. Therefore, after one repeated character has been decrypted, the rest of the similar characters can effortlessly be replaced even without any computation or cryptanalysis [10]. Since the affine transformation is used for image encryption in this research, the modular value (n) is 256, depending on the pixel number in each channel.

1.3 Chaotic Arnold Map

Chaos has influenced information security due to its similar and compatible characteristics with information security needs [10]. Chaotic systems are influenced by their initial conditions; even a small alteration to the initial state can have a big effect on the result. Because of its mixing properties and sensitivity to initial conditions and system configurations, chaos theory can be used to build efficient cryptosystems [12].

The Arnold map is a chaotic transformation that can be applied to an image to scramble its pixels and make it hard to identify. Because the Arnold map is area-preserving, the image's overall pixel composition remains unchanged. It does,

however, scramble the pixels, rendering them uncorrelated with their initial locations. The Arnold transform works by taking the pixel coordinates (x, y) and transforming them to a new set of coordinates (x', y') as described in Equation (2) [13]:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} ax & by \\ cx & dy \end{pmatrix} mod\ M \qquad (2)$$

Where a, b, c, and d are integer coefficients that satisfy the condition $ad - bc = 1$. M is the size of the image in pixels. Although the Arnold map is a quick and lightweight encryption technique, it might not offer as much protection as more complicated encryption methods. As a result, it is frequently combined with other encryption methods to improve the security of image encryption software [14].

The rest of the paper is organized as follows: Section 2 introduces the relevant work, and the performance metrics are illustrated in Section 3; then, the main structure of the proposed work is introduced in Section 4. Section 5 clarifies the experimental results of various approaches to the proposed algorithm. Section 6 presents an assessment of the results obtained. Finally, section 7 presents the concluding explanations of the obtained results.

2. RELATED WORK

In [15], they apply the two-dimensional Affine transformations as a generalization of chaotic systems for the image encryption algorithm as a robust technique over an open network against threats. It had been suggested that a random matrix affine cipher combined with a two-dimensional Arnold map be used as a multi-layer color image encryption. This approach for encryption is more secure than when implemented with the regular type used by conventional systems. The system was tested to perform well, with various evaluations known as plaintext attack, chosen plaintext attack, ciphertext-only attack, PRNG characteristics, key sensitivity, differential resistance, and many others. Although the secret keys and their arrangements are highly sensitive for robustness, the key space is limited and may withstand a broad range of brute force attacks.

In [16] presents a lightweight encryption algorithm, "AL-TEA," which is an Alternative TEA algorithm for healthcare images sent over IoT devices. The proposed algorithm uses various encryption keys derived from the source key to overcome the problem of equivalent key issues. The results obtained from the suggested approach were able to achieve quicker encryption speeds and high security with a variety of file image sizes and key sizes. While AL-TEA attempts to fix the equivalent key issue, it's still susceptible to relationships between keys that can lead to key recovery.

In [17] proposes a cryptosystem is proposed that forms the Logistic Sine map by using the Logistic map and the Sine map. Additionally, it implements the Fuzzy concept together with the Hénon map to establish the Fuzzy Hénon map, where both yield secure keys. Furthermore, this system achieves high key sensitivity; even a small change in the keys will bring about significant differences in the encrypted image. The major limitation of the suggested approach is the increasing algorithm cipher time despite integrating multiple chaotic maps and fuzzy logic. Moreover, it is considered not a truly lightweight algorithm and not suitable for resource-constrained environments (e.g., mobile, IoT).

In [18] suggests several types of chaotic maps, like Logistic, Arnold, or Baker, are used with a 3DES algorithm for medical image encryption purposes. Firstly, a preprocessing step is implemented for a specific image, and then the image is encrypted using 3DES. Then, the output image is encrypted using one type of chaotic map. Several evaluation metrics were used to assess the proposed encryption strategy, including Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), and Information Entropy Analysis (IEA). The results of this work achieve a robustness-encrypted image and make a 3-DES algorithm more reliable and have a larger key length. The weakness of using the 3DES algorithm is the limited key space (112 or 168 bits), which makes it vulnerable to brute force. Moreover, the low-dimensional chaos algorithms are 1D or 2D, are considered relatively simple, which leads to predictable patterns in large or high-resolution images.

In [19] suggest a 3D chaotic map is combined with S-box method to encrypt gray and color images. A key generation method has also been proposed based on a novel chaotic map. The ciphering operation is composed of multiple stages, aiming to increase the efficiency and the randomness. Experiments show that the proposed encryption method has a large key space (key $>10^{180}$), and the information entropy performance is superior to 7.999

In [20] introduced an image encryption method was introduced based on a combination of the Lorenz chaotic map, Elliptic Curve Cryptography (ECC), and Genetic Algorithm (GA) for optimization purposes. The Lorenz chaotic map strengthens the confusion property, while ECC gives high security with minimal key sizes. In addition, GA optimizes the performance of cipher image quality, as the overall meaning, the hybrid method is resistant to unauthorized access. The experimental results showed a high degree of complexity security, depending on enhancing the confusion and diffusion property, histogram analysis, and entropy. Various limitations are: computational overhead, GAs may produce different results for the same input, depending on initialization. Moreover, ECC operations on large datasets require modular arithmetic and curve operations that increase the time processing.

The former researchers have mainly focused on TEA as a high-speed encryption algorithm due to its simplicity and constrained resource consumption. The main fixed encryption key structure restricts the overall robustness of the encryption process. Therefore, the use of the same key in all stages of the encryption process is one of the fundamental drawbacks of the TEA algorithm.

The present work addresses this knowledge gap and suggests various strategies to enhance image encryption by incorporating Affine transformation and chaotic techniques. Accordingly, the main contribution of the proposed work is to improve the strength and the randomness of the cipher process for image encryption. This is achieved based on pixel-dependent keys with minimal computation overhead and less execution time, with a high complexity degree. Besides, using a large key space in the present work tries to overcome the problem of brute force attack.

3. Performance Metrics

From the time an image is taken until it is shown to a human viewer, its quality declines. Image quality assessment techniques quantify the degradation of seen images, and considerable efforts have been put into creating objective criteria for image quality [21]. Different metrics are used to evaluate the quality of encrypted images, as described in Table 1.

TABLE I: METRICS QUALITY FOR ENCRYPTED IMAGES

Metric Name	Mathematical Definition	Description	Accepted Values
Mean Square Error [22] [23]	$MSE = \frac{1}{\mathrm{N} * \mathrm{M}} \sum_{\mathrm{i}=1}^{\mathrm{N}} \sum_{\mathrm{j}=1}^{\mathrm{M}} [(\mathrm{x(i,j)} - \mathrm{y(i,j)}]^2$	x and y represent two images, N and M are height and width	Higher
Peak Signal-to-Noise Ratio [24]	$PSNR = 20\ log_{10} = (\frac{255}{MSE})$	For image	Lower
Mean Absolute Error [25]	$MAE = \frac{1}{N} \sum_{i=1}^{n} x_i - y_i\vert$	x and y represent two images	Higher
Structural Similarity Index Matrix [26]	$SSIM(x, y;\theta) = l(x, y)^{\alpha}.\ c(x, y)^{\beta}.\ s(x, y)^{\gamma}$	l(x, y), c(x, y), and s(x, y) represent the luminance, contrast, and structure between the images x and y, and $\theta = (\sigma, \beta, \gamma)^T$	Value varies [0,1]
Image Quality Index [27]	$IQI = \frac{1}{N * M} \sum_{i=1}^{N} \sum_{j=1}^{M} Q_{ij}$ $\mathrm{Q} = \mathrm{luminance} * \mathrm{contrast} * \mathrm{shape}$	where M, N are the image dimensions.	Value varies [-1,1] shows that more noise is suppressed
Correlation Coefficient [28][29]	$CC = \frac{\sum_i^M \sum_j^N (y(i,j) - y^-)(x(i,j) - x^-)}{\sqrt{\sum_i^M \sum_j^N (y(i,j) - y^-)^2} \sqrt{\sum_i^M \sum_j^N (x(i,j) - x^-)}}$	where M, N are the image dimensions. x^-, y^- are source and encrypted images	Lower

4. The Framework of the Proposed Algorithms

To enhance the performance of the TEA for image encryption, two approaches are used to scramble image elements before encrypting to increase the robustness against attacks. Each one of the proposed algorithms is executed in two main layers, the first for the scrambling operation and the second for the encryption process, as explained in the following:

4.1 First Proposed Encryption Algorithm (Affine-TEA)

In cryptography, the Affine transformation is a type of classical substitution cipher. Two main reasons are clarified for choosing the affine transformation in the present work, as a preprocessing stage:

1- It is a lightweight and fast application method, even for large image sizes.
2- It has a very low computational cost, which is ideal for real-time resource-constrained encryption systems.

Combining Affine transformation and TEA for image encryption could be an interesting approach, as both methods have distinct strengths. A robust multi-layer encryption process for color images was used to preserve confidentiality and increase the strength against various attacks with lower processing cost, as shown in Figure 2.

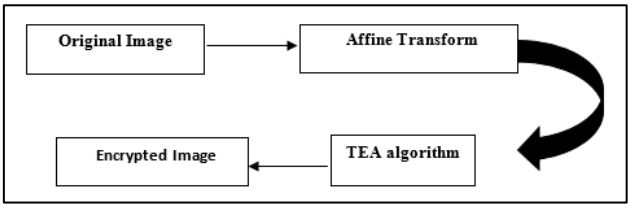


Fig.2: Structure of the first proposed encryption algorithm

The proposed algorithm is divided into two main phases in the encryption process (see Algorithm 1):

- **Phase 1:** The image in this phase is divided into three separate channels: Red, Green, and Blue. Each channel is encrypted using an Affine transformation at two levels. To increase the security and the hardness against attacks, each channel in each level is encrypted with different key sets. Thereafter, in the final step of this phase, the three encrypted channels are merged to reconstruct the cipher image.

- **Phase 2:** The cipher image obtained from Phase 1 is then passed to this phase to be encrypted by the TEA algorithm.

Algorithm (1): Proposed Affine-TEA Algorithm
Input: p-image, and : a- The first key set of **level-1**: Red ($k1, k2$), Green ($k3, k4$), Blue ($k5, k6$) b- The second key sets of **level-2**: Red ($k1^{-}$,$k2^{-}$), Green ($k3^{-}$,$k4^{-}$), Blue ($k5^{-}$,$k6^{-}$)
Output: c-image
Begin **Step1**: Read p-image **Step2:** Separate the p-image into three basic channels: Red, Green, and Blue **Step3**: repeat step4 and step5 for all pixels **Step4**: **level-1;** encrypt with the first set of two keys of Affine transformation for each channel (Eq. 3) **Step5**: **level-2;** the encrypted channel of level-1 is re-encrypted with the second two key sets of Affine transformation for each channel (Eq. 3) **Step6**: Combine all channels to construct the encrypted image (cipher-image) **Step7:** Use the TEA algorithm to encrypt the cipher-image and save the output in the c-image **End**

4.2 Second Proposed Encryption Algorithm (Arnold-TEA)

The present proposed algorithm, the Arnold map, is used with the TEA algorithm to strengthen the encryption process. Using the Arnold map as a preprocessing stage before TEA encryption strengthens the image encryption process. This is achieved by increasing key sensitivity, enhancing confusion/diffusion, and reducing statistical patterns. Figure 3 and Algorithm 2 display the second proposed encryption algorithm, which is composed of two phases:

- **Phase 1:** The image in this phase is scrambled and shuffled pixels to weaken the correlation between image contents. The obtained cipher image in this phase still has some tiding properties between its elements.
- **Phase 2**: Encrypting the image processed in the previous phase using the TEA algorithm to obtain the final encrypted image.

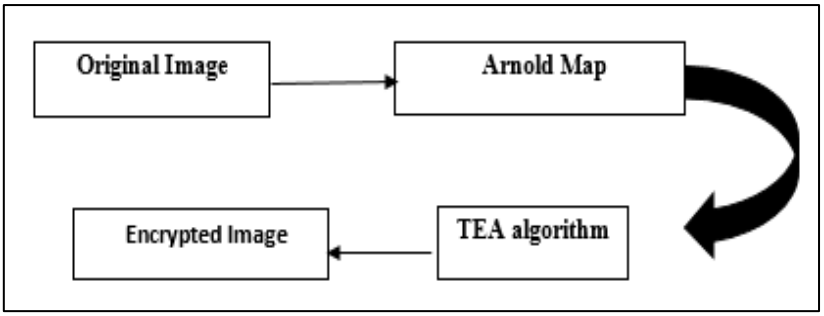


Fig.3: The Second proposed encryption algorithm main structure

Algorithm (2): Proposed Arnold-TEA Algorithm
Input: p-image, N=50
Output: c-image
Begin **Step 1**: Read p-image **Step 2:** for i=1 to N // N is a variable parameter **Step 3:** For individual blocks of pixels in the image, repeat • Arnold map transformation is implemented for the pixel coordinates. • Shuffle the pixels based on the transformed coordinates **Step 4:** End for **Step 5** uses the TEA algorithm to encrypt the cipher image and save the output in the c-image **End**

5. Experiment Results

Several experimental tests are conducted to examine the performance of the proposed encryption algorithms under Windows 11 Home, Processor: Intel(R) Core (TM) i3-1005G1 CPU @ 1.20GHz 1.20 GHz. Random Access Memory (RAM): 8 GB, and Python and C# were used as programming languages. In addition, four test images of size 256*256, Lena, Baboon, Peppers, and Bird, were used to test and evaluate the proposed algorithms, as shown in Figure 4. Three cases are used to demonstrate and analyze the experimental results. The first case is based on standard TEA. The two cases, the proposed algorithms of Affine-TEA and Arnold-TEA, have been implemented to resolve the security issues associated with the TEA algorithm. For all the experimental cases, the TEA key was 128-bit = 1234567890abcdef.

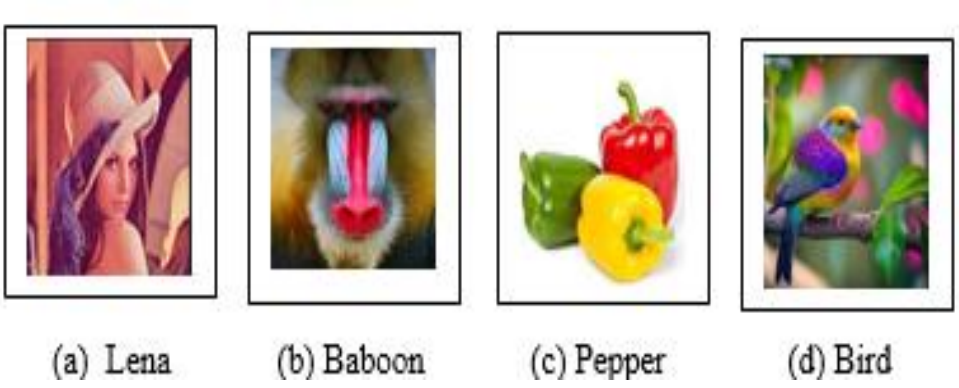
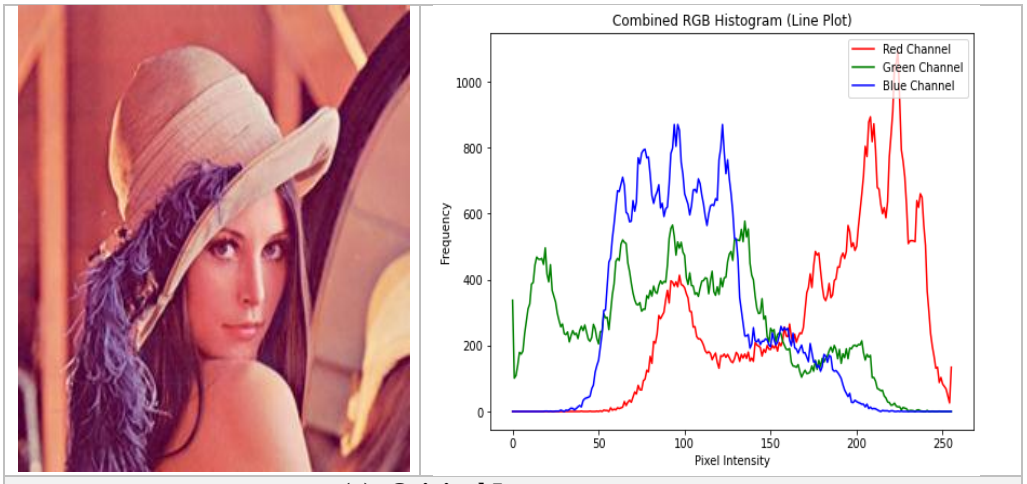


Fig.4: The Four Sample Images used in the Proposed Algorithms

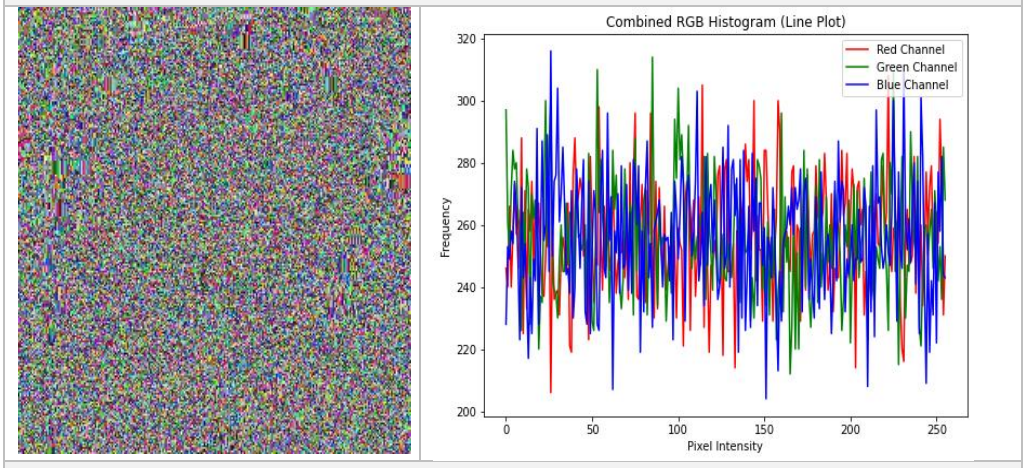
For brevity, only the results for Lina's image will be displayed, while the outcomes of the other images will be demonstrated in the result tables.

5.1 Case1: TEA Algorithm

This case demonstrates the encryption process based on a standard TEA algorithm. Figure 5 shows the pixel intensity distribution and the histogram representation for both the source and encrypted images. The frequency distribution for pixels in each channel in the histogram represents the effect of the encryption process.



(a) Original Image



(b) Encrypted Image using TEA Algorithm

Fig.5: Case1 (Lena encrypted by the TEA algorithm only)

5.1 Case2: Results Analysis for Affine-TEA Algorithm

The encryption process is implemented for each band (Red, Green, Blue) based on Affine transformation in two levels, followed by the TEA algorithm to achieve high privacy. Moreover, to increase the complexity degree, six different sets of key pairs of Affine transformation are used, as shown in Table 2. Each band has two sets, which individually pair at different levels, as demonstrated in Figures 6 and 7, respectively.

TABLE II: SIX PAIRS FOR (A,B) KEYS

Channel	Pair-1 (a,b)	Pair-2 (a,b)
Red	(5,8)	(91,255)
Green	(11,50)	(143,59)
Blue	(3,25)	(131,70)

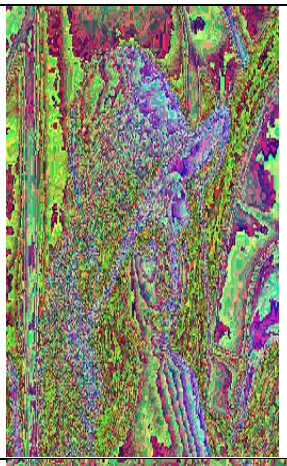
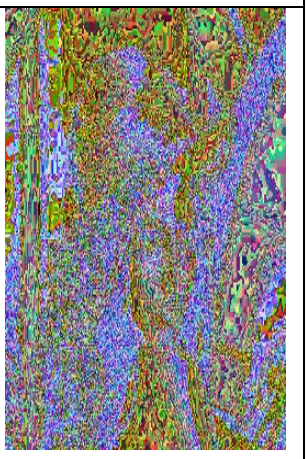
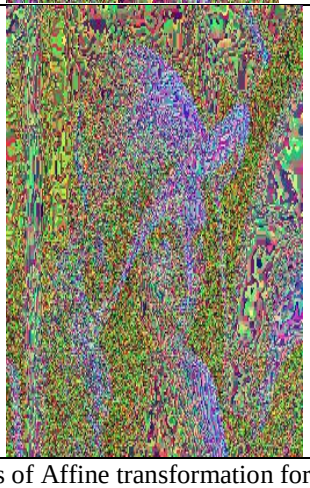
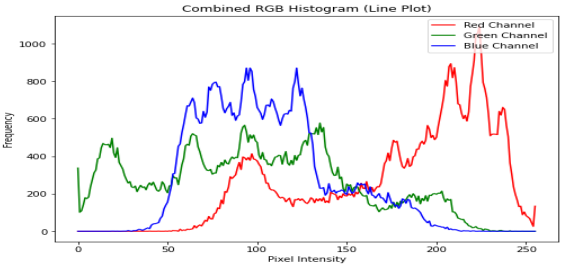
Affine Level no.	Red Channel	Green Channel	Blue Channel
Level-1			
Level-2			

Fig.6: The proposed two levels of Affine transformation for Lina's image

As shown in Figure 6, each channel's first and second levels are permuted and substituted with pixel values for the whole image. At level-1, the first key pair for each channel was used to encrypt the image, and then each encrypted channel was fed into the corresponding channel in level-2, but with a different key set as described in Table 2. The purpose of this step is to preprocess to decorrelate the relation between adjacent pixels within the image. This operation is performed as a nonlinear transformation followed by a linear transformation as described in Equation 1. After applying the above two levels of Affine transformation, the resulting encrypted channels are combined to form the cipher image. Finally, the resulting image is then encrypted using the TEA algorithm as illustrated in Figures 7 and 8.



Original Image

Affine Level no.	Red Channel	Green Channel	Blue Channel

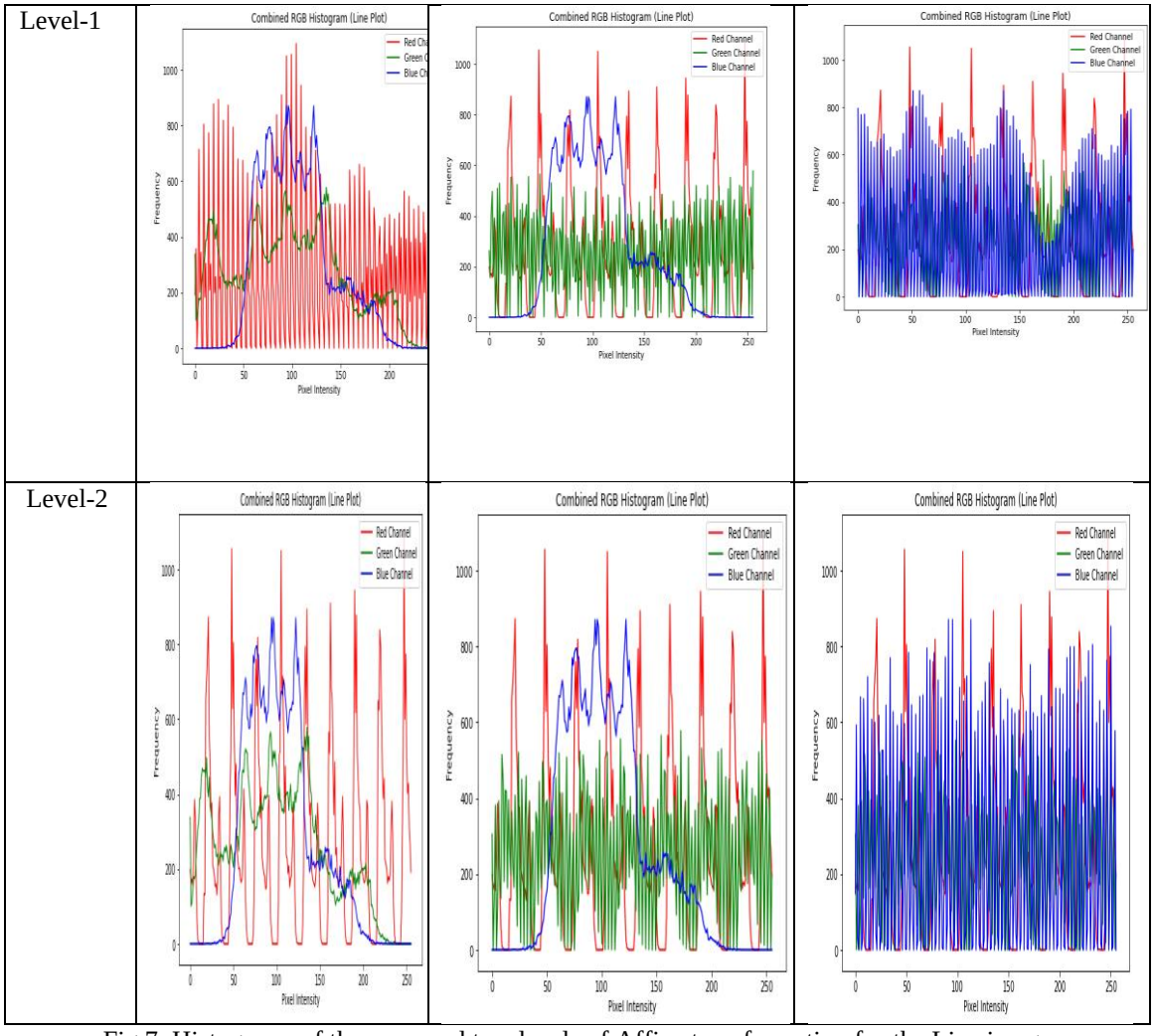
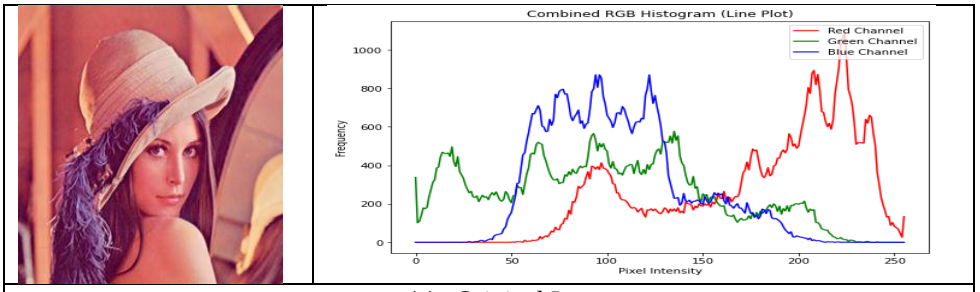
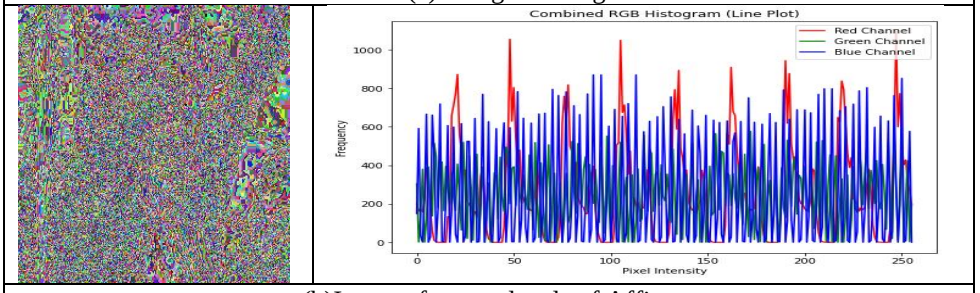


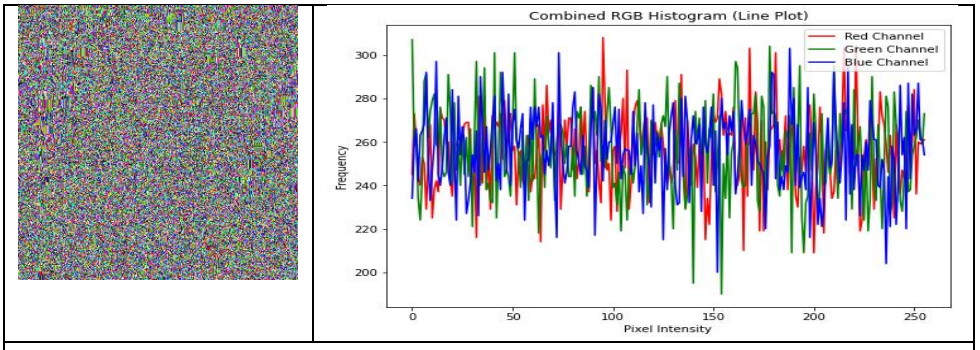
Fig.7: Histograms of the proposed two levels of Affine transformation for the Lina image



(a) Original Image



(b)Image after two levels of Affine

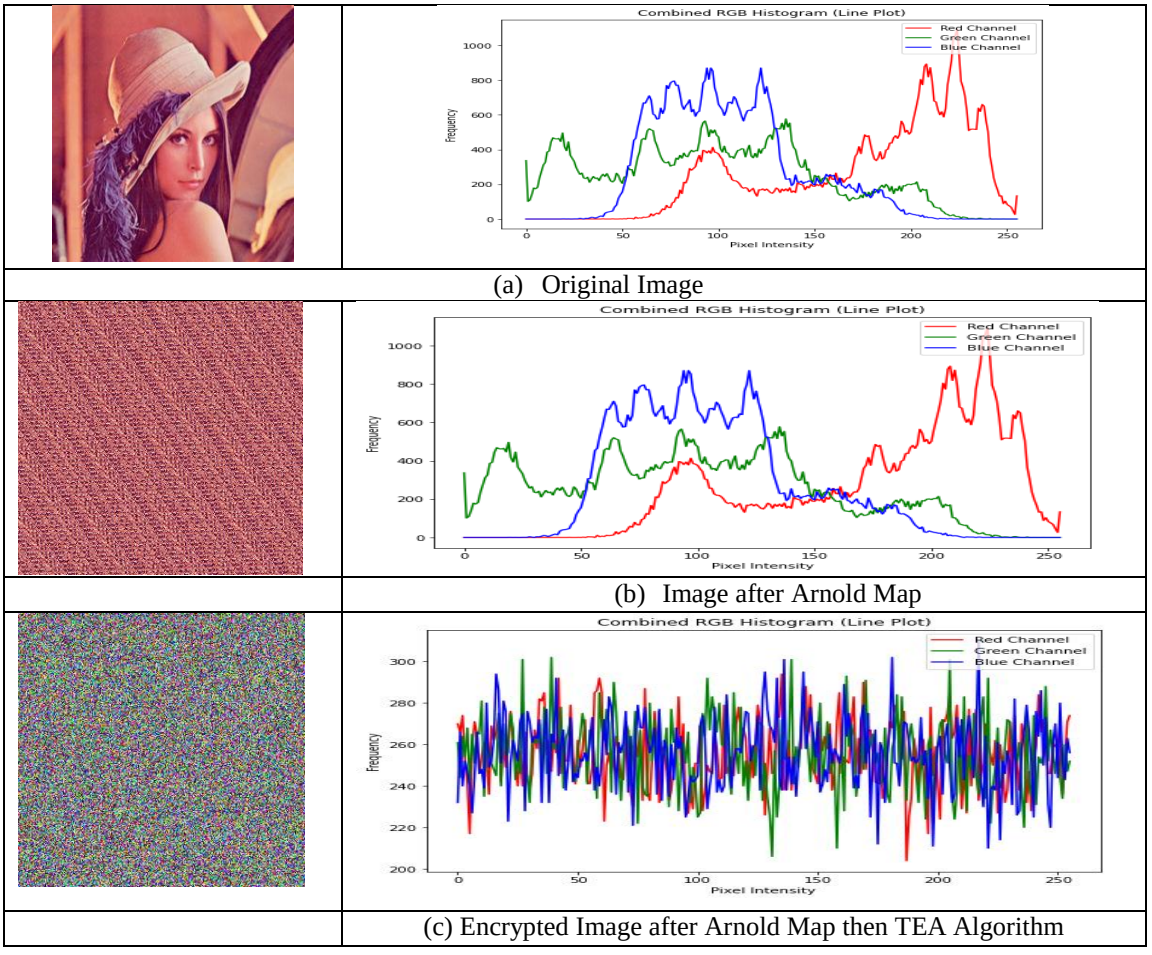


(c) Encrypted Image after using Affine and then the TEA Algorithm

Fig.8: Case-2 (Lena encrypted by Affine-TEA)

5.3 Case3: Results for Arnold-TEA algorithm

In this case, the Arnold map is implemented first and followed by the TEA algorithm. Moreover, Figure 9 depicts graphically the histogram representation for pixel distribution before and after Arnold map implementation. It is noticed from Figure 8 (a and b) that the histograms are similar because the Arnold map works as a permutation process for image pixels.



(a) Original Image

(b) Image after Arnold Map

(c) Encrypted Image after Arnold Map then TEA Algorithm

Fig.9: Histogram representation of Case-3 (Lena encrypted by Arnold-TEA)

6. Security Analysis and Discussion

Different evaluation metrics are used to evaluate the obtained results implemented in three cases, as described in the following:

6.1 Metrics evaluation

As mentioned earlier, four sample images are used to test the proposed algorithms. Five performance metrics are used to evaluate the obtained results: PSNR, SSIM, IQI, and CC; the lower their values, the better. Furthermore, the higher the value for MAE, the better. Tables 3, 4, 5, and 6 display the outcomes for three cases, each using four sample images.

TABLE III: ENCRYPTION PERFORMANCE ASSESSMENTS FOR THREE CASES APPLYING LENA'S IMAGE

Case No.	PSNR	SSIM	IQI	MAE	CC
1	8.5692	0.0095	0.0025	78.0081	0.0048
2	8.5529	0.0054	-0.0015	**78.1106**	0.0038
3	**8.5449**	**0.0008**	**-0.0061**	78.2084	**0.0007**

TABLE IV: ENCRYPTION PERFORMANCE ASSESSMENTS FOR THREE CASES APPLYING THE BABOON IMAGE

Case No.	PSNR	SSIM	IQI	MAE	CC
1	8.0704	0.0166	0.0056	82.2128	0.0021
2	8.0696	0.0135	0.0070	82.3408	-0.0030
3	**8.0527**	**0.0035**	**-0.003063**	**82.3830**	**-0.00897**

TABLE V: ENCRYPTION PERFORMANCE ASSESSMENTS FOR THREE CASES APPLYING THE PEPPER IMAGE

Case No.	PSNR	SSIM	IQI	MAE	CC
1	6.289	0.0872	0.0792	103.9618	0.1182
2	5.8377	0.0132	0.0063	109.4189	-0.0368
3	**5.6845**	**-0.1213**	**-0.1273**	**110.1707**	**-0.4288**

TABLE VI: ENCRYPTION PERFORMANCE ASSESSMENTS FOR THREE CASES APPLYING THE BIRD IMAGE

Case No.	PSNR	SSIM	IQI	MAE	CC
1	8.3973	0.0050	-0.0010	79.4771	-0.0007
2	8.3854	**0.0035**	**-0.0025**	79.3513	-0.0027
3	**8.3826**	**0.0035**	**-0.0025**	**79.5327**	**-0.0077**

It is noticed from the tables above that the outcomes vary depending on image texture and color distribution.

- The PSNR in all cases is <9, indicating very poor quality. Hence, the encrypted image appears visually different and cannot resemble the plaintext image.
- The SSIM scores are near zero and less, which confirms the original image's contents have been almost destroyed. It means no similarity compared to the source image, and there are no visual patterns in the encrypted image.
- The IQI values are near zero, which is considered ideal for encryption and indicates maximum randomness. The Negative values are also acceptable, sometimes even better, since it means the encrypted image is structurally opposite to the original.
- The MAE means the larger the values are better, where case 3 in all test images achieved better performance.
- The CC approved the success of the proposed two approaches since all values are near or less than zero, which indicates no correlation between image pixels in encrypted images.

Moreover, the Arnold map operates iteratively for image pixels. Whereas the Affine transformation task is a stream cipher to rearrange the pixel values within the image. However, one can notice that the obtained results for both proposed methods, Case2 and Case3, are close with a slight difference. Generally, the two proposed methods improved the degree of complexity and increased security compared to the standard TEA algorithm.

6.2 Time Analysis

Time measurement for the cipher process is useful, especially in real-time encryption processes. Since the proposed Affine transformation is a stream cipher process, the encryption time is considered small. The Affine transformation is more efficient in terms of cipher time than the Arnold map, which operates iteratively. Table 7 summarizes the time performance in milliseconds (MS) for the Lena image using the Affine transformation and the Arnold map only as a preprocessing step to enhance the TEA algorithm performance.

TABLE VII: EXECUTION TIME FOR LENA'S IMAGE USING AFFINE AND ARNOLD MAP

Case No.	Method	Time /MS
1	Affine-one level	65
2	Affine-two levels	(65*2)=130
3	Arnold	1862

Observing the results in Table 7, it is clear that the different execution times of the Affine transformation are better compared to the Arnold map as shown in Equation (5).

$$Time\ difference = Arnold\ time - Affine\ time \quad (5)$$

For two levels of Affine transformation, the time difference is 1732 milliseconds, which means that Affine is about 14.3 times faster than Arnold's algorithm. The speed obtained from the Affine transform is because this algorithm is a stream cipher and non-recursive compared to Arnold's algorithm.

6.3 Secret Key Space Analysis

As described in Equations 1 and 2, Affine uses two keys (a *and* b) as a combination of linear transformations and translations to perform the encryption process. The value of a must be co-prime with b to ensure that the cipher is reversible (i.e., there exists an inverse for a). In other words, the Greatest Common Divisor (GCD) between two keys must be 1, as represented in Equation 6:

$$\mathbf{GCD(a, b) = 1} \quad (6)$$

The mathematical key analysis can be explained in the following:

- **For $mod\ n$**: The present work uses a color image for the max value of the pixel is 2^8=256, then n=256.
- **Possible values for key**: to retrieve any encryption value, the decryption process must be reversible, and this is achieved by selecting (a) as a prime value to achieve the relation clarified in Equation 6. Since each channel in the image consists of 256 colors, there are 128 odd numbers between 1 and 255. Thus, there are 128 possible values for the key.
- **Possible values for key b**: The additive key b can be any integer from 0 to 255 (since addition modulo 256 is always reversible regardless of b), as in Equation (7). Thus, there are 256 possible values for b.

  $$b + b^{-1} = 1 \quad (7)$$

  Where b^{-1} is the additive value.
- **Total Number of Possible Key Pairs:** The total number of possible pairs (a, b) is the product of the number of possible values for a and b as explained in Equation (8):

  $$\text{Total key pairs}=128\times256 = 32{,}768 \quad (8)$$

According to NIST, the minimum key length to resist brute-force attacks is 112 bits; therefore, the key space should be larger than 2^{112} to avoid brute-force attacks [3]. Thus, there are 32,768 possible key pairs for the Affine transformation cipher when $n = 256$. In addition, the key space for the TEA algorithm is 2^{128}. Therefore, the total key space for the proposed Affine-TEA algorithm, as described in Equation (9) represents a large key space dimension that resists brute force attack.

$$\text{Total key space}=32{,}768 * 2^{128} \quad (9)$$

7. Conclusions

The integration of either Affine or Arnold maps significantly enhances the performance of the TEA algorithm. The combination of these transformations adds a layer of complexity, improving the overall security of the encryption process. The expected system is highly dependable, realistic, and resilient in a variety of secure communication applications. This is due to several important characteristics of chaotic maps, including sensitivity to initial conditions and control parameters, structure, and attack complexity. The purpose of using two levels of affine transformation is to decorrelate the data,

minimizing patterns and making it more resistant to cryptanalysis. The encryption time of the proposed Affine-TEA algorithm is 14.3 times faster than the Arnold-TEA algorithm. Besides, the key space for the proposed Affine-TEA algorithms is $32{,}768 * 2^{128}$ and it is large enough to resist brute force attacks. The enhanced TEA algorithm introduced in the present work can be effectively applied in various cryptographic scenarios, offering both speed and robustness.

References

[1] S. M. Hameed, Z. H. Ali, G. K. Al-Khafaji, and S. Ahmed, "Chaos-based color image steganography method using 3D cat map," *Iraqi J. Sci.*, vol. 62, no. 9, pp. 3220–3227, 2021, doi: 10.24996/ijs.2021.62.9.34 .

[2] S. G. Mohammed and N. S. Al-Mothafar, "Evaluation of Rijndael algorithm for audio encryption by brute force attack," *J. Eng.*, vol. 30, no. 11, pp. 128–141, 2024, doi: 10.31026/j.eng.2024.11.08 .

[3] N. H. M. Ali, M. M. Hoobi, and D. F. Saffo, "Development of robust and efficient symmetric random keys model based on the Latin square matrix," *Mesopotamian J. Cybersecurity*, vol. 4, no. 3, pp. 203–215, 2024.

[4] M. Rana, Q. Mamun, and R. Islam, "Balancing security and efficiency: A power consumption analysis of a lightweight block cipher," *Electronics*, vol. 13, no. 21, pp. 1–35, 2024, doi: 10.3390/electronics13214325 .

[5] A. F. Shimal, B. H. Helal, and A. T. Hashim, "Extended of TEA (ETEA): A 256 bits block cipher algorithm for image encryption," *Int. J. Electr. Comput. Eng. (IJECE)*, vol. 11, no. 5, pp. 3996–4007, Oct. 2021, doi: 10.11591/ijece.v11i5.pp3996-4007 .

[6] D. Virmani, N. Beniwal, G. Mandal, and S. Talwa, "Enhanced Tiny Encryption Algorithm with Embedding (ETEA)," *Int. J. Comput. Inf. Technol.*, vol. 7, no. 1, pp. 493–499, 2013.

[7] O. R. Oluwade, O. M. Olaniyi, Y. S. Abdulsalam, L. A. Ajao, and F. B. Osang, "ETEASH—An enhanced Tiny Encryption Algorithm for secured smart home," *Covenant J. Informatics Commun. Technol.*, vol. 9, no. 1, pp. 1–15, 2021.

[8] A. N. K. Telem, C. Feudjio, B. Ramakrishnan, H. B. Fotsin, and K. Rajagopal, "A simple image encryption based on binary image affine transformation and zigzag process," *Complexity*, vol. 2022, pp. 1–22, 2022, doi: 10.1155/2022/3865820 .

[9] A. Ihsan and N. Doğan, "Improved affine encryption algorithm for color images using LFSR and XOR encryption," *Multimedia Tools Appl.*, vol. 82, pp. 7621–7637, 2023, doi: 10.1007/s11042-022-13727-w .

[10] J. C. T. Arroyo and A. J. P. Delima, "A keystream-based affine cipher for dynamic encryption," *Int. J. Emerg. Trends Eng. Res.*, vol. 8, no. 7, pp. 2919–2922, 2020, doi: 10.30534/ijeter/2020/06872020 .

[11] M. Khan, S. S. Jamal, M. M. Hazzazi, K. M. Ali, I. Hussain, and M. Asif, "An efficient image encryption scheme based on double affine substitution box and chaotic system," *Integration*, vol. 81, pp. 108–122, 2021, doi: 10.1016/j.vlsi.2021.05.007 .

[12] A. A. Arab, M. J. B. Rostami, and B. Ghavami, "An image encryption algorithm using the combination of chaotic maps," *Optik*, vol. 261, p. 169122, 2022, doi: 10.1016/j.ijleo.2022.169122 .

[13] A. K. Yadav and V. P. Vishwakarma, "An integrated Arnold and Bessel function-based image encryption on blockchain," *Int. J. Adv. Comput. Sci. Appl.*, vol. 15, no. 4, pp. 779–803, 2024, doi: 10.14569/IJACSA.2024.0150482 .

[14] J. Wu, Z. Liu, J. Wang, L. Hu, and S. Liu, "A compact image encryption system based on Arnold," *Multimedia Tools Appl.*, vol. 80, pp. 2647–2661, 2021, doi: 10.1007/s11042-020-09828-z .

[15] S. Sabir and V. Guleria, "Multi-layer color image encryption using random matrix affine cipher, RP2DFrHT and 2D Arnold map," *Multimedia Tools Appl.*, vol. 80, no. 18, pp. 27829–27853, 2021, doi: 10.1007/s11042-021-11003-x .

[16] C. L. Babulal, "AL-TEA: Alternative TEA algorithm for healthcare image in IoT," *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 10, no. 6, pp. 24–30, 2022, doi: 10.17762/ijritcc.v10i6.5620 .

[17] D. E. Mfungo, X. Yongjin, Y. Xian, and X. Wang, "A novel image encryption scheme using chaotic maps and fuzzy numbers for secure transmission of information," *Appl. Sci.*, vol. 13, no. 12, pp. 1–25, 2023, doi: 10.3390/app13127113 .

[18] A. Z. Hussain and M. A. A. Khodher, "Medical image encryption using multi chaotic maps," *TELKOMNIKA Telecommun. Comput. Electron. Control*, vol. 21, no. 3, pp. 556–565, Jun. 2023.

[19] J. Ayad and M. A. Jalil, "Robust color image encryption using 3D chaotic maps and S-box algorithms," *Babylonian J. Netw.*, vol. 2023, pp. 148–161, 2023.

[20] K. Pandey and D. Sharma, "Novel image encryption algorithm utilizing hybrid chaotic maps and elliptic curve cryptography with genetic algorithm," *J. Inf. Secur. Appl.*, vol. 89, p. 103995, 2025, doi: 10.1016/j.jisa.2025.103995 .

[21] Y. Al Najjar, "Comparative analysis of image quality assessment metrics: MSE, PSNR, SSIM, and FSIM," *Int. J. Sci. Res. (IJSR)*, vol. 13, no. 3, pp. 110–114, 2024, doi: 10.21275/SR24302013533 .

[22] S. A. S. Hussien, T. A. S. Hussien, and M. A. Noori, "Proposed algorithm for encrypted data hiding in video stream based on frame random distribution," *Iraqi J. Sci.*, vol. 62, no. 9, pp. 3243–3254, 2021, doi: 10.24996/ijs.2021.62.9.37 .

[23] S. A. Noaman, B. N. Al-din Abed, and A. M. S. Ahmed, "Lossless encoding method based on a mathematical model and mapping pixel technique for healthcare applications," *Iraqi J. Sci.*, vol. 65, no. 12, pp. 7183–7193, 2024, doi: 10.24996/ijs.2024.65.12.32 .

[24] A. N. Ismael, "A comparative study of image enhancement techniques for natural images," *J. Al-Qadisiyah Comput. Sci. Math.*, vol. 14, no. 4, pp. 53–65, 2022, doi: 10.29304/jqcm.2022.14.4.1086 .

[25] S. M. Robeson and C. J. Willmott, "Decomposition of the mean absolute error (MAE) into systematic and unsystematic components," *PLoS ONE*, vol. 18, no. 2, pp. 1–8, 2023, doi: 10.1371/journal.pone.0279774 .

[26] F. Osorio, R. Vallejos, W. Barraza, S. M. Ojeda, and M. A. Landi, "Statistical estimation of the structural similarity index for image quality assessment," *Signal Image Video Process.*, vol. 16, pp. 1035–1042, 2022, doi: 10.1007/s11760-021-02051-9 .

[27] S. M. R. Islam, X. Huang, and K. Le, "Novel image quality index for image quality assessment," in *Proc. Int. Conf. Neural Inf. Process. (ICONIP)*, Berlin, Germany: Springer, 2013, vol. 8228, pp. 549–556.

[28] A. Kaur, L. Kaur, and S. Gupta, "Image recognition using coefficient of correlation and structural SIMilarity index in uncontrolled environment," *Int. J. Comput. Appl.*, vol. 59, no. 5, pp. 1–5, 2012.

[29] J. Ayad, G. Ali, W. Ullah, and W. Robert, "Encryption of color images utilizing cascading 3D chaotic maps with S-box algorithms," *SHIFRA*, vol. 2023, pp. 95–107, 2023.