**International Journal of Electrical and Computer Engineering (IJECE)**
Vol. 11, No. 5, October 2021, pp. 3996~4007
ISSN: 2088-8708, DOI: 10.11591/ijece.v11i5.pp3996-4007 

# Extended of TEA: A 256 bits block cipher algorithm for image encryption

**Abeer F. Shimal, Baydaa H. Helal, Ashwaq T. Hashim**
Department of Control and Systems Engineering, University of Technology-Iraq, Baghdad, Iraq

**Article Info**

***Article history:***

Received Dec 30, 2020
Revised Apr 7, 2021
Accepted Apr 19, 2021

***Keywords:***

Block cipher
Chaotic map
Cryptography
Image encryption
Polynomial
TEA encryption

**ABSTRACT**

This paper introduces an effective image encryption approach that merges a chaotic map and polynomial with a block cipher. According to this scheme, there are three levels of encryption. In the first level, pixel positions of the image are scuffled into blocks randomly based on a chaotic map. In the second level, the polynomials are constructed by taking N unused pixels from the permuted blocks as polynomial coefficients. Finally, the third level a proposed secret-key block cipher called extended of tiny encryption algorithm (ETEA) is used. The proposed ETEA algorithm increased the block size from 64-bit to 256-bit by using F-function in type three Feistel network design. The key schedule generation is very straightforward through admixture the entire major subjects in the identical manner for every round. The proposed ETEA algorithm is word-oriented, where wholly internal operations are executed on words of 32 bits. So, it is possible to efficiently implement the proposed algorithm on smart cards. The results of the experimental demonstration that the proposed encryption algorithm for all methods are efficient and have high security features through statistical analysis using histograms, correlation, entropy, randomness tests, and the avalanche effect.



***Corresponding Author:***

Ashwaq T. Hashim
Department of Control and Systems Engineering
University of Technology-Iraq
Baghdad, Iraq
Email: 60102@uotechnology.edu.iq

## 1. INTRODUCTION

The block ciphers are symmetric-key which are used for a long time as an essential ciphering element to maintain information security. Though they are designed primarily to provide data confidentiality, diversity allows it to operate such as a major element in the building of many encryption systems, likes generating random numbers and procedures to authenticate messages, stream ciphers and digital signatures. Various block ciphers are offered diverse levels of secrecy, flexibility, and efficiency. Examples of block ciphers existing today are advanced encryption standard (AES), rivest cipher 6 (RC6), tiny encryption algorithm (TEA), Twofish, fast data encipherment algorithm (FEAL), secure and fast encryption routine (SAFER), and international data encryption algorithm (IDEA) which they had the most practical attention [1]. Image encryption contains applications in different domains encompassing internet communication, multimedia systems, medical imaging, military communication and Tele-medicine. Information security holds further significance with the growth in the interchange of information and develops numerous encryption techniques to cipher and decipher images. But there is no lonely ciphering algorithm that will satisfy diverse kinds of images [2]. Due to the features required for nonlinear dynamic systems likes pseudo-

random behavior, sensitivity to initial conditions and ergodicity, chaos-based cryptography offers a novel and effective method for transacting through the headstrong problem of secure image encryption and extremely fast [3].

Cryptography based on chaotic is as yet in its infancy and may not possess a precise parallel to the conceptions and philosophies of conventional cryptography and cryptanalysis techniques. Though chaotic systems and cryptography algorithms possess specific analogous characteristics: Pseudo-random behavior, initial conditions and parameter sensitivity and unstable orbits with long periods, liable on the precision of the numerical implementation. In cryptography, an encryption algorithm has rounds that are led to diffusion and confusion features. Likewise, chaotic system iterations propagate the initial region across the whole phase area [3].

The paper is structured as follows: In section 2 the related works are presented. We described the TEA in Section 3. In section 4, the logistic map is described. The proposed algorithm components are presented in section 5. In section 6, we analyzed the suggested image cipher security and performed the performance evaluation via numerous assessments and results comparisons. Finally, conclusions are presented in section 7.

## 2. RELATED WORKS

The TEA algorithm is mainly populated because of the easiness of application and less exploitation of memory over the whole other algorithms of encryption. Nonetheless, the main concerns in the TEA is utilized the identical keys for all the encryption rounds, which endangers security. That is certainly noticed from the TEA avalanche effect. Furthermore, the cipher and decipher time consuming is high, leading to diminished TEA efficiency [4]. Therefore, for providing an improved security mechanism, researchers in [5] suggested an improved tiny encryption algorithm with embedding (ETEA), a method of data hiding beside the technique of cryptography are employed in this algorithm. The gain of ETEA is that it combines cryptography and steganography. Abdelhalim *et al.* presented the modified of the TEA algorithm (MTEA) [6]. It enhanced the security and power consuming of TEA. The linear feedback shift register (LFSR) is utilized to randomly generate a number to develop the TEA security and energy usage. Rachmawati *et al.* [7] suggested a joint public key and secret key encryption method for securing file transfer. The TEA secret key algorithm is used for maintaining the security of the file while key security is preserved by a public key method LUC based on Lucas function. Nonetheless, this method utilized the same key for all encryption rounds which resulted in security reducing. Novelan *et al*. [8] established an SMS security system for mobile devices by the TEA. This system confirms that the securing messages are ciphered in the key to getting the ciphered SMS message directed to the mobile number destination. Rajesh *et al*. introduced an algorithm named novel tiny symmetric encryption algorithm (NTSA) which develops the TEA security features by more key confusions [4].

To safeguard digital images from illegal users which is done illegitimate duplication and alterations, a diversity of image encryption approaches are suggested. The various thoughts used in the current image encryption techniques. A safe transfer of images is proposed [9] using key-based random flipping (KBRP) and TEA, which provides additional security for images during transfering using image scrambling as well as encrypt images with randomly generated passwords per pixel. Kanagalakshum and Mekala [10] designed a method based on the Blowfish algorithm with improved features. It is used a supplementary key approach to strengthen the security of the image. Huang *et al.* [11] suggested a simple chaotic for encryption of color image which is relied on plaintext related permutation and diffusion for more safty and efficacy. Zhang and Wang [12] introduced the AES remote sensing image encryption algorithm. At first, for time reduction of encryption, the source gathers the values of 16 pixels altogether to form big integers; secondly, the source ciphers big integers by AES and chaotic map; lastly, the ciphered image is resulted from the encrypted big integers. Bas [13] introduced an enhanced approach known “Chaotic Key Based RC6” (CKBRC6) that is employed a logistic map to produce the subkeys for the RC6 rounds. In Ammar *et al*. [14] presented an improved method of Blowfish algorithm for image encryption. At this method the original image is randomly split into many blocks based on a secret key to disassemble the connection between input and processed images subsequently every block is encrypted by traditional Blowfish algorithm. Ashwaq *et al*. [15] proposed a method to combine image compression and image ciphering that is based on chaotic shift keying (CSK). A lossless compression is used, then 3D chaotic maps are performed for encryption. But this method encrypts the plain image at a bit level so it is time-consuming.

## 3. DESCRIPTION OF THE TEA

In cryptography the TEA is a block cipher that operates on 64-bit register, and the key is 128 bit. The TEA is outstanded by its simplicity in description and implementation (usually a little code). It has a Feistel with 64 rounds, typically implemented in pairs termed cycles. The key setup is simple, all round use the same keys. Various multiples of a magic constant are employed to avoid simple attacks based on the symmetry of rounds. The magic constant, 2654435769 or 9E3779B916 is selected to be 232/ϕ, where ϕ is the golden ratio [16]. Figure 1 shows the structure of the TEA algorithm.

The equivalent key problem is the most vulnerable of the TEA algorithm for each key equal to three other keys, which denotes to the active key size, is merely 126 bits [17]. TEA is also susceptible to a related key attack which is required 232 chosen plaintexts under a corresponding key pair, with 232 complexity of time [18].

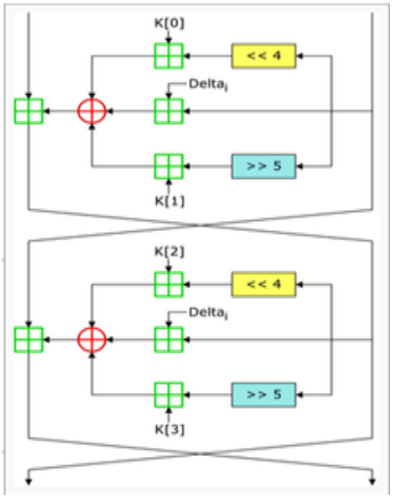



Figure 1. Structure of the TEA algorithm

## 4. LOGISTIC MAP

In dynamic systems, chaos is investigated over a long period. The term chaos means that it is a parachute for various complex conduct solutions to relatively simple and deterministic systems. The logistic map is one of the simplest and most transparent systems that show chaos transmission system [19]. The logistic map is a discrete dynamical system that is given by:

$$x_{n+1} = r\, x_n\, (1 - x_n) \tag{1}$$

For an initial value $0 \leq x_0 \leq 1$ this map creates a sequence of values $x_0, x_1, \ldots, x_n, x_{n+1}$. The r is growth rate is selected to be $0\, r \leq 4$. A bifurcation is a qualitative change in the dynamics that occurs as a system parameter is changed. A bifurcation diagram in Figure 2 shows the possible long-term values that a system variable can have as a function of the system parameter [20].

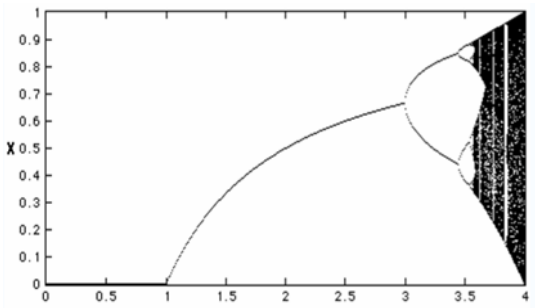



Figure 2. Bifurcation diagram of the logistic map (r between 0 and 4)

## 5. EXTENDED OF TEA (ETEA) ALGORITHM

To dispel the great pixels correlations and raise the value of entropy a scrambling method is introduced to divide the image into N non overlapped blocks using logistic chaotic map. The substituted and transformed image is generated by constructing a polynomial of degree N on generated N blocks. After transformation, the image is passed to the enhanced TEA algorithm and consequently produced the ciphered image. The proposed system combines image scrambling, image transformation and image encryption using various secured and robust techniques. A block diagram of the proposed scheme is shown in Figure 3. Algorithm 1 presents the steps of the proposed scheme.

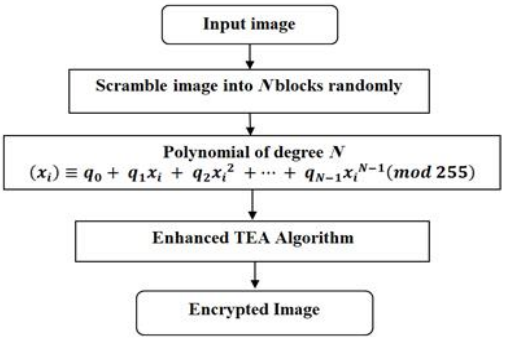



Figure 3. Block diagram of the extended of TEA (ETEA)

Algorithm 1: Extended of TEA (ETEA)

```
Input:   I      // Plain image
         X0, r, // Parameters and Secret Keys of Chaotic map
         N     // number of blocks
Output:  E    // Encrypted image
Step1: Load input image I
Step2: Apply the proposed scrambling image to randomly divide plain image I into N blocks
       using algorithm 2.
Step3: Feed the scrambled blocks to Polynomial of degree N to generate new N transformed
       blocks using algorithm 3.
Step4: Generate the required subkeys for using algorithm 4.
Step5: Combine the transformed N blocks into an image which is fed to the proposed enhanced
       ETEA block cipher
Step6: Output the Encrypted image E
```

### 5.1. Proposed scrambling image based on logistic map

The plain color image can be partitioned into subblocks; each one contained a group of pixels. An increase in the number of blocks resulted in a smaller blocks size, resulting in lower correlation and increased entropy. Then the subblocks are relocated into their new locations. The block size must be small because fewer pixels keep their neighbours as we gain good transformation, and the correlation will be reduced, and therefore it becomes hard to guess the value of any specific pixel from the values of its adjacent.

Algorithm 2: Scrambling image based on logistic map

```
Input:   I  // Plain image
         W, H
         N // number of blocks
         r_min, t_max, num_intrvals
Output:   Blocks  // Scrambled Array N blocks
Step 1: Convert input image I into one dimensional array of length L=W×H
Step 2: Initialize the random generator by srand (time (NULL))
Step 3:  Let r_min = 4.0, r_max = 5.0, num_intervals = 8, r = r_min, b=1
Step 4:  r = r+ (r_max - r_min) / num_intervals
             X0= rand ()  // RAND_MAX
         For i = 1 to L
             Xi= r × Xi-1 (1-Xi-1)
             y = (Xi ×1000) mod N
             ScramSeq[b] = y
              b = b+1
            EndFor i
Step 5: Split the I image into N subblock Blocks depending on generated ScramSeq
```

### 5.2. Image transform based on polynomial

After dividing the plain image into N non-overlapping blocks, then substitute q0, q1, q2, ..., qN−1, which are represented the pixel values from the scrambled image blocks where N is the number of blocks. Finally, the results from the series of polynomial equations are combined in a new transformed image, as illustrated in algorithm 3 and Figure 4.

Algorithm 3: Image transformation based on polynomial

```
Input:  Blocks    // Scrambled Array of N blocks
        N         //  Number of blocks
Output: T         // Transformed image
Step1: Take the first N unused pixels from each block that are generated from a scrambling
image algorithm, then the polynomial is constructed as follows:
```

$$f_j(x_i) = q_0 + q_1 x_i + q_2 x_1^2 + \cdots q_{N-1} x_i^{N-1} (mod\ 255) \quad (2)$$

```
where q0, q1, q2,…, qN-1 are the N unused pixels of the blocks, then evaluate  fj(1), …
fj(N). N is the number of scrambled blocks.
Step2: Repeat Step 1 until there are no more pixels to process.
Step3: The generated pixels are combined into a new transform image T.
```

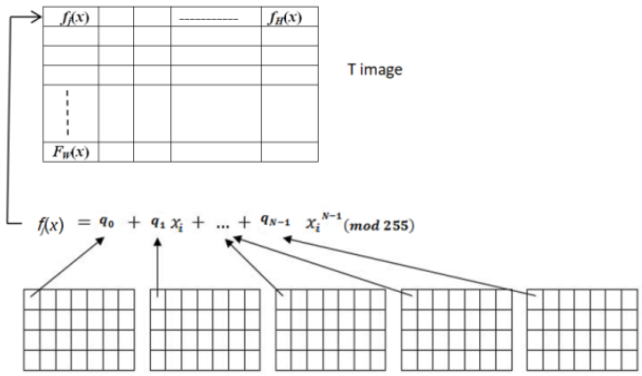



Figure 4. The proposed method of transforming the pixels blocks as polynomial coefficients

The following algorithm 4 steps which are the reveal phase using any *N* transform blocks:

Algorithm 4: Image revealing

```
Input    T   // Transformed image
         N   // Number of blocks
Output   Blocks    // N blocks
Step1: Take the first non-used pixel from each of the N blocks
Step2: Use these N pixels (a subset of {fj(1), fj(2), ..., fj(N−1)} and the Lagrange's
       interpolation to solve for the coefficients q0, .., qN-1 in Eq. (2). The coefficients
       q0, ..., qN-1 are then the corresponding N pixel values of the image blocks.
Step3: Repeat steps 1 and 2 until the entire pixels of the N transformation block are
       processed.
```

### 5.3. Enhanced ETEA algorithm

Numerous encryption algorithms are suggested in recent years for confirming the security of transferred data via the network. A secure algorithm for image encryption is tried to design in this research by employing the features of a chaotic map and the possibility of generating very long length keys. The proposed image encryption scheme is merged with a chaotic map, polynomial and enhanced TEA algorithm. According to this scheme, there are three levels of security. In the first level, pixel positions of the image scuffle into blocks randomly. In the second level, the polynomial is constructed by taking *N* unused pixels from the permuted blocks as polynomial coefficients. Finally, in the third level, an enhanced secret-key block cipher called ETEA (Extended of TEA) is suggested. It is an evolutionary improvement of 64-bit TEA block cipher, which is aimed in designed to investigate the desires of increasing security and improved image encryption performance. The ETEA algorithm increased the block size from 64 bit to 256-bit by using F-function in type three Feistel network design. Figure 5 shows the block diagram of the enhanced TEA algorithm (ETEA).

The key generation's scheduling is very unpretentious by mixing all of the primary material in the same way for each round. The proposed system attempts to generate subkeys that are changed for each round by employing a chaotic map as presented by Algorithm 5. As we noticed from Figures 5 and 6 that each round required six subkeys.

Algorithm 5: Subkey generation based on logistic map

**Input** $X_0$, $a$ // Chaotic parameters and secret keys
$Len$ // The required subkeys (i.e., 384 subkeys)
**Output** $K$ // subkeys
**Step1:** Produce random sequence by Logistic Map
$X_0 = a \times X_0 \hat{} 2$
For i = 1 to $Len \times 6$
$X_i = r \times X_{i-1} (1 - X_{i-1})$
End for
**Step2:** Normalize the Logistic Map X array
$R_{Max} = 32$ , $R_{Min} = 1$
For i = 1 to $Len \times 6$
$K_i = (R_{Max} - R_{Min}) / (R_{Max} - R_{Min}) \times (X_i - R_{Max}) + R_{Max}$
End for

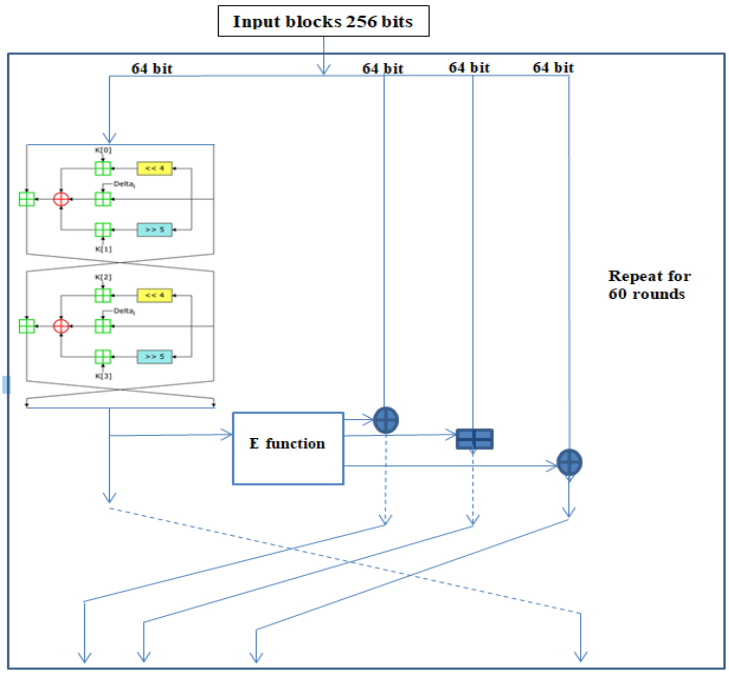



Figure 5. Block diagram of enhanced TEA algorithm (ETEA)

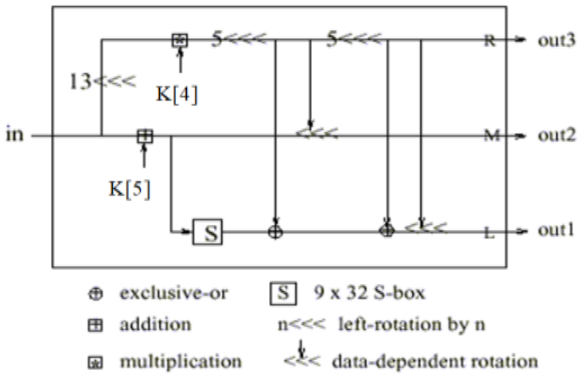



Figure 6. The E function adapted from [21]

The components of the E function are depicted in Figure 6 which is adapted from [21]. The left 64 bits of the input block are expanded using the E function where the output is three 64 bits. The E-function takes as input one data word and uses two more key words to produce three output words. In this function, three temporary variables will be used, denoted below by L, M, and R (for left, middle and right). In the design of the E function, a combination of different operations will be used to maximize the advantages of each. The properties of this function are explained in details in [21].

## 6. EXPERIMENTAL RESULTS

By applying the encryption algorithm pixel by pixel may not lead to a complete secure encrypted image. For example, the image shown in Figure 7 is encrypted by the TEA algorithm directly. From Figure 8, still some information can be inferred from the cipher image so as conclude about the appearance of the original image. To overcome the problem of security issues associated with the TEA algorithm, modification is done by adjusting it. Figure 8(a) is the transformed image; Figure 8(b) is the ciphered image by the proposed system. It is clear that the ciphered image likes noise image and has nothing to do with the plain image. Consequently, the effecting of the encryption algorithm is good.

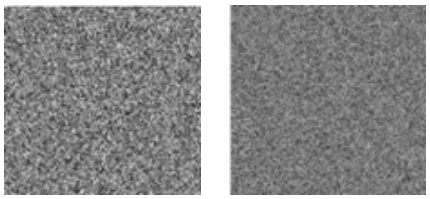
The test images are shown in Figure 9, and the security level is measured in terms of correlation, histograms, and entropy. It can notice that the results in a lower correlation, higher entropy value, and a more uniform histogram over the traditional TEA algorithm. The proposed encryption process can decrease the mutual information among the encrypted image variables, increasing the entropy value. The proposed system maintained a good security level.

Figure 10 shows the histograms of original images and the correlated encryption images by the proposed system. The probability of a histogram is liked by a single peak distribution of all original test images. Whereas the probability distribution of the encrypted images by the proposed system is close to the normalized probability distribution; consequently, the ciphered images are random images like noise.

Figure 11 are shown the results of the correlation distribution map in the horizontal direction for original test images, ciphered by traditional TEA and ciphered images by the proposed system. It can be seen that the original images have a high correlation between adjacent pixels. Thus, a linear relationship is observed, and this correlation is significantly weak while the encrypted images are exhibited strong randomness. This indicates that the proposed algorithm efficiency is good and offered the security level is higher. The proposed system is compared with other researches, as shown in Table 1. Table 2 shows the information entropy of test images, ciphered images by original TEA, and ciphered images by the proposed system. We can see that the information entropies for all ciphered images by the proposed system are very close to 8 bits and have more control.

(a) (b)

Figure 7. Encryption result of TEA; (a) plain image, (b) image ciphered by TEA



(a) (b)

Figure 8. Encryption result of the proposed system; (a) transformed image by proposed transform algorithm, (b) encrypted transformed image by enhanced ETEA algorithm

(a) (b) (c) (d) (f)

Figure 9. Five standard test images sized by 256×256; (a) house, (b) Barbara, (c) Goldhill (e) Lena, (f) lake

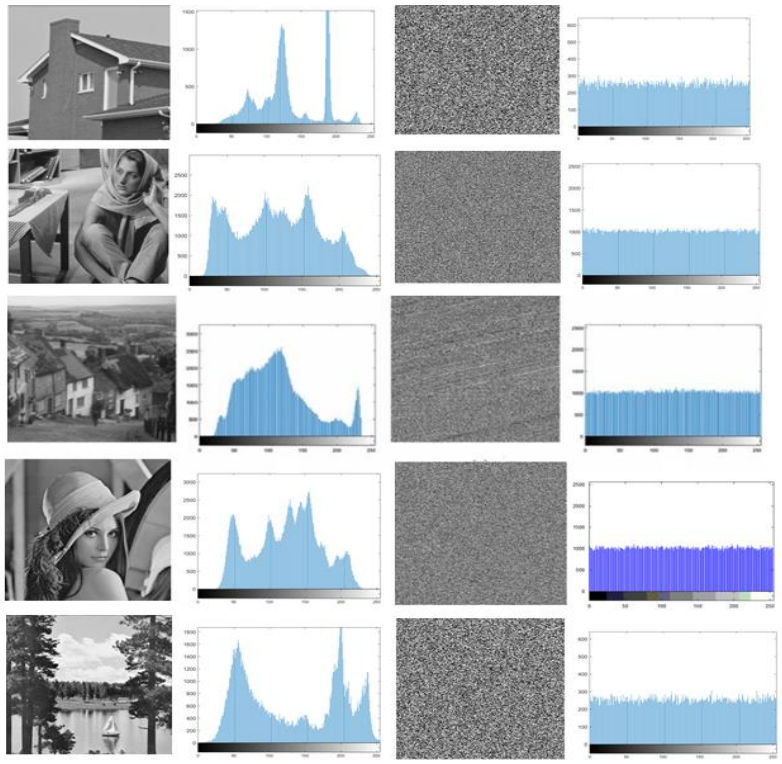



Figure 10. Histogram of image; (a) original test image, (b) histogram of the original test image, (c) encrypted image, (d) encrypted image histogram by extended of TEA (ETEA)

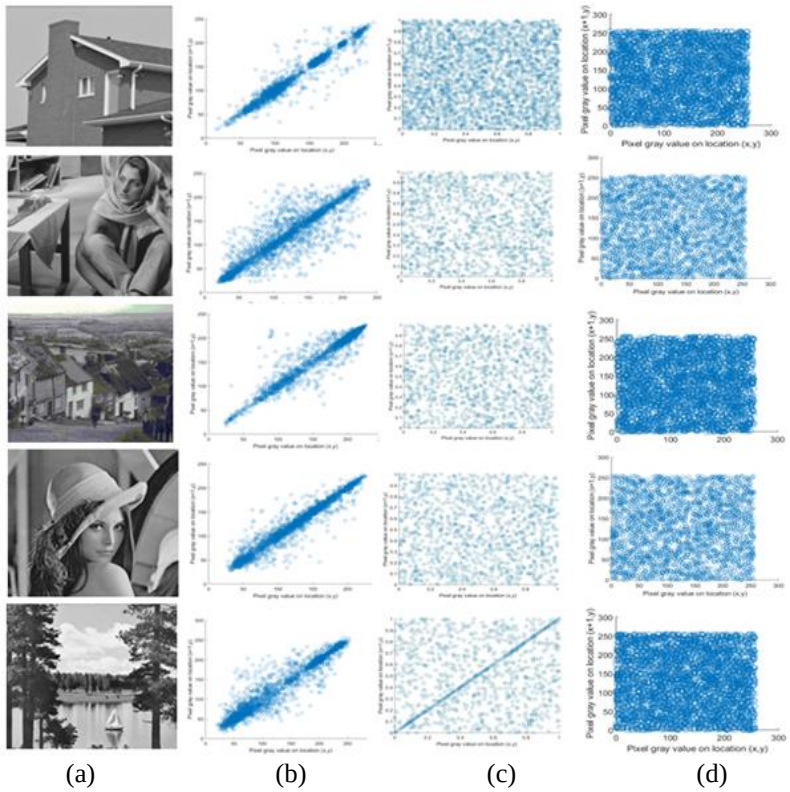



Figure 11. Correlation of image; (a) plain image, (b) correlation of plain test images, (c) horizontal correlation of encrypted image by TEA, (d) horizontal correlation of encrypted image by the proposed system

Table 1. Correlation coefficients of Lena cipher image

| Algorithms | Horizontal | Vertical | Diagonal |
|---|---|---|---|
| Proposed ETEA | −0.003087 | 0.000217 | 0.001344 |
| Ref. [22] | −0.000586 | 0.001391 | −0.004687 |
| Ref. [23] | 0.006034 | 0.012434 | −0.006072 |
| Ref. [24] | 0.001665 | 0.031389 | −0.000633 |

Table 2. Encrypted images entropy

| Images | Original images | TEA | Proposed ETEA |
|---|---|---|---|
| House | 7.7845 | 7.9223 | 7.9987 |
| Barbara | 7.8133 | 7.8933 | 7.9943 |
| Goldhil | 7.7871 | 7.9822 | 7.9987 |
| Lena | 7.7260 | 7.9812 | 7.9968 |
| Lake | 7.6981 | 7.8149 | 7.9899 |

### 6.1. Avalanche effect

When a change in one bit of the plain text or one bit of the key schedule produces a change in many bits of the ciphertext, it is called avalanche effect [25]. A desirable feature of any cryptographic algorithm is that a simple change in either the plaintext or the key must result in a substantial change in the ciphertext. If the changes are small, this may offer a way to reduce the size of the plaintext or keyspace to be examined, thus making the cryptanalysis very effortless. For a cryptographic algorithm to be secure it should exhibit a strong avalanche effect. Hence higher the avalanche value, the higher will be the security. Tabulation of results observed by changing one bit of each block of the ciphered images by original TEA and proposed system are shown in Tables 3 and 4, respectively. The TEA algorithm has the lowest Avalanche effect when compared to the proposed ETEA algorithm. So, it is clear that the ETEA algorithm is more secure than the TEA algorithm.

Table 3. Avalanche effect comparison of TEA algorithm after change one bit in each block of plain image

| Images | Average avalanche effect | |
|---|---|---|
| House | 33 | 51.56 |
| Barbara | 29 | 45.31 |
| Goldhil | 24 | 37.50 |
| Lena | 30 | 46.88 |
| Lake | 31 | 48.44 |
| The average of bits change is | 29.4 | 45.94 |

Table 4. Avalanche effect comparison of proposed ETEA algorithm after change one bit in each block of plain image

| Images | Average avalanche effect | |
|---|---|---|
| House | 143 | 55.86 |
| Barbara | 129 | 50.39 |
| Goldhil | 138 | 53.91 |
| Lena | 140 | 54.69 |
| Lake | 144 | 56.25 |
| The average of bits change is | 137 | 54.22 |

### 6.2. Keyspace

The keyspace of ETEA is $2^{6144}$ (i.e., 64 rounds × 6 keys for each round 16 bits), while the Logistic Map has two independent variables $x_0$ and $r$. Subsequently, $x_0$ and $r$ are double-precision numbers; the entire number of diverse values of $x_0$ and $r$ is more than $10^{14}$. Thus, the keyspace is greater than $10^{14} \times 10^{14} = 10^{28} \approx 2^{93}$. Besides the proposed method for image transformation, $N$ blocks desire to pull the original secret. However, in reconstruction N equations are needed to obtain the $N$ coefficients (actual pixels) $q_1$ to $q_N$ from (2). Thus, to reconstruct the original secret successfully, the only way is to guess one missing block for creating (2). In this case, the probability of guessing the exact solution is then 1/256. Hence for **(**W×H)/N blocks, the possibility of obtaining the correct image $(1/256)^{(W \times H)/N}$. As a result, it is very difficult for the (N-1) block to reconstruct the original secret image. Hence the proposed scheme holds enough confidentiality. The total keyspace of the proposed system is $2^{6237}+(1/256)^{(W \times H)/N}$. The keyspace between the suggested algorithm and other similar encryption algorithms is compared and shown in Table 5. The keyspace size of the proposed system is larger than other related encryption algorithms.

### 6.3. Key sensitivity and randomness analysis

The logistic map is employed to produce a chaotic sequence by using the (1). The sequence is very sensitive to a change in an initial value, where a very small difference of the initial values can cause a large impact on the next values. As illustrated in Figure 12, two signals are generated with initial condition ($X_0$=5 into $X_0$=5.00000000000001) from logistic chaotic generator. Figure 13 shows that the logistic chaos generator exhibits good autocorrelation properties making a call for security applications.

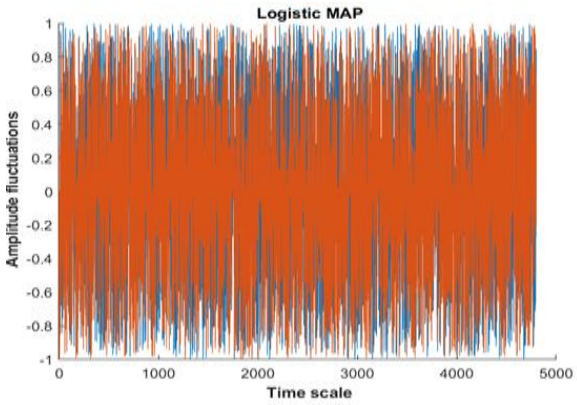



Figure 12. Sensitivity to initial conditions for logistic chaotic generator

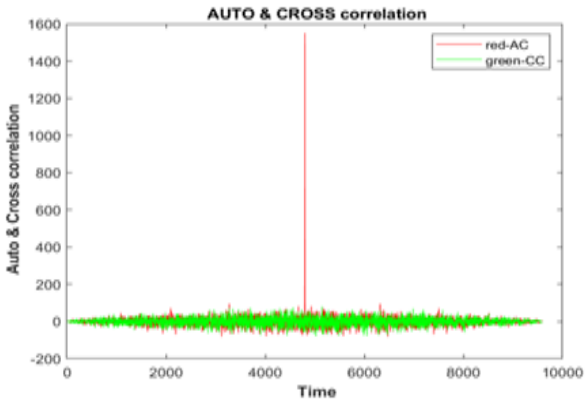



Figure 13. Cross correlation performance for logistic chaos

Table 5. The keyspace comparisons

| Encryption Algorithm | Keyspace |
|---|---|
| Zhu *et al.* [26] | $2^{339}$ |
| Wang *et al.* [27] | $2^{149}$ |
| Guesmi *et al.* [28] | $2^{256}$ |
| Li *et al.* [29] | $2^{299}$ |
| Li *et al.* [30] | $2^{375}$ |
| Curiac *et al.* [31] | $2^{128}$ |
| Curiac *et al.* [32] | $2^{357}$ |
| Ashwaq et al. [33] | $2^{958}$ |
| Proposed ETEA | $2^{6237}$+ (1/ 256) $^{(W \times H)/N}$ |

### 6.4. NPCR and UACI analysis

The number of changing pixel rate (NPCR) and the unified averaged changed intensity (UACI) tests measure the ability of a cryptographic system to withstand a differential attack. The results of NPCR and UACI tests in Table 6. When the NPCR and UACI of the ciphertext are greater than 99.6% and 33.46%, respectively [34], it indicates that the algorithm has good security compared with the traditional TEA algorithm. Thus the values of the proposed algorithm are closer to the theoretical value than the TEA. Hence, the proposed algorithm is powerfully able to resist differential attacks.

Table 6. Comparison of NPER and UACI of encrypted images by TEA algorithm and proposed ETEA

| Image | TEA Algorithm | | Proposed ETEA | |
|---|---|---|---|---|
| | NPCR | UACI | NPCR | UACI |
| House | 97.21 | 32.13 | 99.63 | 33.52 |
| Barbara | 86.55 | 30.34 | 99.60 | 33.47 |
| Goldhill | 87.91 | 30.18 | 99.60 | 33.54 |
| Lena | 98.45 | 32.56 | 99.63 | 33.51 |
| Lake | 88.75 | 31.98 | 99.60 | 33.34 |

## 7. CONCLUSION

A secure, compact, and simple block cipher algorithm is proposed. It offers good performance considerable flexibility. Furthermore, its simplicity will allow analysts to quickly refine and improve our estimates of its security. The suggested system exhibits significantly amended security/performance

compared to the traditional TEA algorithm by gaining the benefit of the potent operations propped in existing computers. The keyspace is large, and thus the exhaustive key search and the matching ciphertext attack are infeasible, consistency in the pixels spreading of the ciphered image. The correlations among adjacent pixels of the ciphered image are very low, and the ciphered images have entropy information very near to the ideal value of 8. The suggested system does not contain weak keys or related keys. The percentage of weak keys must be small enough to make it unlikely that a random key will be chosen. Also, any weak keys must be explicitly recognized; hence they can be disposed of during the key generation process by a chaotic system.

## REFERENCES


[1] C. Burwick *et al.*, "Mars a candidate cipher for AES," *First Advanced Encryption Standard (AES) Conference*, Ventura, CA, 1998, pp. 1-63.

[2] P. P. Dang and P. M. Chau, "Image encryption for secure Internet multimedia applications," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 3, pp. 395-403, 2000, doi: 10.1109/30.883383.

[3] A. Jolfaei, A. Mirghadri, "Image Encryption Using Chaos and Block Cipher," *Computer and Information Science*, vol. 4, no. 1, pp. 172-185, 2011, doi: 10.5539/cis.v4n1p172.

[4] S. Rajesh, Varghese Paul, Varun G. Menon, and Mohammad R. Khosravi, "A Secure and Efficient Lightweight Symmetric Encryption Scheme for Transfer of Text Files between Embedded IoT Devices," *Symmetry*, vol. 11, no. 2, pp.293-314, 2019, doi: 10.3390/sym11020293.

[5] D. Virmani, N. Beniwal, G. Mandal, and S. Talwar, "Tiny Encryption Algorithm with Embedding (ETEA)," *International Journal of Computers & Technology*, vol. 7, no. 1, pp. 1-9, 2013, doi: 10.24297/ijct.v7i1.3479.

[6] M. B. Abdelhalim, M. El-Mahallawy, M. Ayyad, "Design and Implementation of an Encryption Algorithm for use in RFID System," *International Journal of RFID Security and Cryptography (IJRFIDSC)*, vol. 2, no. 1, pp. 51-57, 2013, doi: 10.20533/ijrfidsc.2046.3715.2013.0007

[7] D. Rachmawati, A. Sharif, Jaysilen and M. A. Budiman, "Hybrid Cryptosystem Using Tiny Encryption Algorithm and LUC Algorithm," *IOP Conference Series: Materials Science and Engineering*, vol. 300, 2018, Art. no. 012042.

[8] M. S. Novelan, A. M. Husein, M. Harahap and S. Aisyah, "SMS Security System on Mobile Devices Using Tiny Encryption Algorithm," *IOP Conference Series Journal of Physics: Conference Series*, vol. 1007, no. 012037, 2018, pp. 1-7. doi:10.1088/1742-6596/1007/1/012037.

[9] A. George, M. Riyadh and M. V. Prajitha, "Secure image transferring using KBRP and TEA algorithms," *2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, Coimbatore, India, 2015, pp. 1-5, doi: 10.1109/ICIIECS.2015.7193117.

[10] K. Kanagalakshm and M. Mekala, "Enhanced Blowfish Algorithm for Image Encryption and Decryption with Supplementary Key," *International Journal of Computer Applications*, vol. 146, no. 5, pp. 41-52, 2016, doi: 10.5120/ijca2016910707.

[11] L. Huang, S. Cai, M. Xiao, and X. Xiong, "A Simple Chaotic Map-Based Image Encryption System Using Both Plaintext Related Permutation and Diffusion," *Entropy*, vol. 20, no. 7, pp. 535-555, 2018, doi: 10.3390/e20070535.

[12] X. Zhang and X. Wang, "Remote-Sensing Image Encryption Algorithm Using the Advanced Encryption Standard," *Applied Sciences*, vol. 8, no. 9, pp. 1540-1553, 2018, doi: 10.3390/app8091540.

[13] M. Bas, "Digital Image Encryption using Logistic Chaotic Key-based RC6," *International Journal of Computer Applications*, vol. 182, no. 2, pp. 17-23, 2018, doi: 10.5120/ijca2018917453.

[14] A. H. Jassem, A. T. Hashim and S. A. Ali, "Enhanced Blowfish Algorithm for Image Encryption Based on Chaotic Map," *2019 First International Conference of Computer and Applied Sciences (CAS)*, Baghdad, Iraq, 2019, pp. 232-237, doi: 10.1109/CAS47993.2019.9075747.

[15] Ashwaq T. Hashim and Bahaa D. Jalil, "Color image encryption based on chaotic shit keying with lossless compression," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 6, pp. 5736-5748, 2020, doi: 10.11591/ijece.v10i6.pp5736-5748.

[16] D. Wheeler and R. Needham, "TEA, a tiny encryption algorithm," *Proceedings of the 1995 Fast Software En-CryptionWorkshop*, Leuven, Belgium, 1995, pp. 97-110.

[17] J. Kelsey, B. Schneier, and D. Wagner, "Key-schedule cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES," *Annual International Cryptology Conference-CRYPTO 1996*, vol. 1109. pp. 237-251, 1996.

[18] M. Steil, "17 Mistakes Microsoft Made in the Xbox Security System," *22nd Chaos Communication Congress*, 2005.

[19] S. C. Phatak and S. S. Rao, "Logistic Map: A Possible Random Number Generator," *Mathematics, Physics, Medicine Physical review. E, Statistical physics, plasmas, fluids, and related interdisciplinary topics*, vol. 51, no. 4, pp. 3670-3678, 1993.

[20] S. Iqbal, M. Rafiq Malik, S. Iqbal, and O. Muhammad, "Study of nonlinear dynamics using a logistic map," *LUMS 2nd International Conference on Mathematics and its Applications in Information Technology (LICM08)*, Lahore, 2008, pp. 10-12.

[21] C. Burwick, "MARS-a candidate cipher for AES," *IBM Corporation*, 1999.

[22] X. P. Zhang, Rui Guo, Heng-Wei Chen, Zhong-Meng Zhao, and Jia-Yin Wang, "Efficient image encryption scheme with synchronous substitution and diffusion based on double S-boxes," *Chinese Physics B*, vol. 27, no. 8, 2018, Art. no. 080701, doi: 10.1088/1674-1056/27/8/080701.

[23] X. Wang *et al.*, "S-box based image encryption application using a chaotic system without equilibrium," *Applied Sciences*, vol. 9, no. 4, pp. 781-798, 2019, doi: 10.3390/app9040781.

[24] Ü. Çavuşoğlu, S. Kaçar, I. Pehlivan, and A. Zengin, "Secure image encryption algorithm design using novel chaos-based S-box," *Chaos Solitons Fractals*, vol. 95, pp. 92-101, 2017, doi: 10.1016/j.chaos.2016.12.018.
[25] G. N. Krishnamurthy, V. Ramaswamy, Leela G. H. and Ashalatha M. E., "Performance enhancement of Blowfish and CAST-128 algorithms and Security Analysis of Improved Blowfish Algorithm Using Avalanche Effect," *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 8, no. 3, pp. 244-250, 2008.
[26] Z. Shuqin, C. Zhu and W. Wang, "A New Image Encryption Algorithm Based on Chaos and Secure Hash SHA-256," *Entropy*, vol. 20, no. 9, pp. 716-734, 2018, doi: 10.3390/e20090716
[27] X. Wang, Zhu Xiaoqiang, Wu Xiangjun, and Zhang Yingqian, "Image encryption algorithm based on multiple mixed hash functions and cyclic shift," *Optics and Lasers in Engineering*, vol. 107, pp. 370-379, 2018, doi: 10.1016/j.optlaseng.2017.06.015.
[28] R. Guesmi, M. A. B. Farah, A. Kachouri, and M. Samet, "A novel chaos-based image encryption using DNA sequence operation and secure hash algorithm sha-2," *Nonlinear Dynamics*, vol. 83, pp. 1123-1136, 2016.
[29] S. Li, Guanrong Chen, and Xuanqin Mou, "On the dynamical degradation of digital piecewise linear chaotic maps," *International Journal of Bifurcation and Chaos*, vol. 15, no. 10, pp. 3119-3151, 2005, doi: 10.1142/S0218127405014052
[30] S. Li, G. Chen, K.-W. Wong, X. Mou, and Y. Cai, "Baptista-type chaotic cryptosystems: Problems and countermeasures," *Physics Letters A*, vol. 332, no. 5-6, pp. 368-375, 2004, doi: 10.1016/j.physleta.2004.09.028
[31] D. I. Curiac and C. Volosenc, "Chaotic trajectory design for monitoring an arbitrary number of specified locations using points of interest," *Mathematical Problems in Engineering*, vol. 2012, no. 5, pp. 1-18, 2012, doi: 10.1155/2012/940276.
[32] D.I. Curiac, D. Iercan, O. Dranga, F. Dragan and O. Banias, "Chaos-Based Cryptography: End of the Road?," *The International Conference on Emerging Security Information, Systems, and Technologies (SECUREWARE 2007)*, Valencia, Spain, 2007, pp. 71-76, doi: 10.1109/SECUREWARE.2007.4385313.
[33] A. T. Hashim, A. J. Jassem, and S. A. Ali, "A Novel Design of Blowfish Algorithm for Image Security," *Journal of Physics: Conference Series*, vol. 1818, 2021, Art. no. 012085,.
[34] Y. Wu, J. Noonan and S. Agaian, "NPCR and UACI randomness tests for image encryption," *Cyber Journals: Multidisciplinary, Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT)*, vol. 1, no. 2, pp. 31-38, 2011.