Neural Comput & Applic (2018) 30:3847–3857
DOI 10.1007/s00521-017-2970-3

ORIGINAL ARTICLE

A novel image encryption scheme based on orthogonal matrix, skew tent map, and XOR operation

Jawad Ahmad[1] · Muazzam Ali Khan[2] · Fawad Ahmed[1] · Jan Sher Khan[3]

Received: 25 September 2016 / Accepted: 24 March 2017 /Published online: 27 April 2017

Abstract Content protection is considered as an important issue in today's world. Therefore, encryption of such contents is a challenging task for researchers. They are focusing on protection of valuable data such as image, video, and audio against different attacks from eavesdroppers. In this paper, we proposed an enhanced version of Fawad et al.'s scheme to fulfill essential needs of a secure image encryption algorithm. The proposed cryptosystem is resistant against many attacks like brute force, differential and statistical. To quantify the quality of the proposed scheme, instead of visual inspection, the proposed scheme is analyzed through various tests, such as correlation coefficient, information entropy, Number of Pixel Change Rate (NPCR) and Unified Average Change Intensity (UACI). Simulation results of the presented scheme shows good diffusion characteristics when compared to other traditional schemes.

✉ Jawad Ahmad
jawad.ahmed@hitecuni.edu.pk

Muazzam Ali Khan
muazzamak@ce.ceme.edu.pk

Fawad Ahmed
fawad@hitecuni.edu.pk

Jan Sher Khan
jk26930@mail2.gantep.edu.tr

[1] Department of Electrical Engineering, HITEC University Taxila, Taxila, Pakistan

[2] Department of Computer Engineering, National University of Sciences, Technology, Islamabad, Pakistan

[3] Department of Electrical Engineering, University of Gaziantep, Gaziantep, Turkey

Keywords Image encryption · Security efficiency · Entropy · DCT · NPCR · UACI

1 Introduction

Nowadays, multimedia data such as image, video, and audio is being used in many aspects of daily life. In today's digital world, multimedia data processing, distributing, and storing are being carried out over the Internet. However, the existing IP networks are open and insecure, and the data transmitted can be easily interrupted, intercepted, or modified [1]. Thus, securing multimedia data from eavesdropper became a vital area of research [2]. Nowadays, robust, fast, and reliable security system is a key requirement in many multimedia applications like video conferencing, pay cable TV and medical imaging systems[1, 3, 4]. In recent years, many interesting and novel security technologies have been proposed for multimedia applications that involve images, video, and or audio contents [5–10].

Encryption and digital watermarking are considered two important areas that serve an important role in information security. In encryption, a message is converted into such a form that intruders doest not get any meaningful information from it [11]. In multimedia encryption, data is protected via key, and for correct decryption of that information, a decryption key is required [12]. The encrypted message is called ciphertext while the unencrypted message is called plaintext. Extracting a plaintext back from a ciphertext is known as decryption [11, 13]. In order to protect images from illegal operations and copying, digital watermarking has played a vital role since decades. A digital watermark is an arrangement of characters or code embedded in multimedia data to uniquely recognize its initiator and authorized user [14].

In [15], Liu et al. exploited interesting properties of Piecewise Linear Chaotic Map (PWLCM) for color image encryption. To check the security analysis of the scheme in [15], Liu et al performed only NPCR and UACI tests. However, only these two tests does not prove the security of a color image encryption as discussed in [6–9, 12]. A novel method of confusion and diffusion for images via PWLCM is discussed in [16]. A larger key space was achieved using both PWLCM and Chebyshev map. In [17], permutation of color images were carried out via PWLCM and a higher dimension Chen map was then employed in diffusion stage. The scheme [17] is resistant against various statistical and differential attacks. To resist chosen plaintext attack, Wang et al. proposed a new image encryption scheme [18]. In [18], Wang et al introduced the concept of intermediate parameter for initial conditions. Through this way, initial conditions are strongly dependent on image block and hence can resist plaintext attacks. Three component of color images, i.e. R, G, and B are effectively encrypted in [19]. Wang et al also discussed and carried out the analyses of classical attacks on proposed scheme [19]. Based on the concept of chaotic maps, other related algorithms can be found [20–22]

In recent years, research in multimedia encryption has been focused towards integrating encryption and compression. The basic idea is to encrypt multimedia data in such a way that the encryption overhead is small, and secondly, the encrypted data can be represented in a standard-compliant format. The term that is often used in the literature to describe such encryption schemes is selection encryption or partial encryption. Spanos and Maple [23] introduced the idea of selective encryption in 1995. Encryption and compression has a strong link as pointed out by Claude Shannon in his classical paper "Communication Theory of Secrecy Systems" [24]. Lookabaugh and Sicker [25] have pointed out Shannon's perspective that redundancy in a source can make encryption weak. Shannon suggested that removing redundancy in the source can strengthen the encryption process. The basic idea behind selective encryption is to encrypt selected coefficients from either the intermediate or the final result of a compression system. The coefficients that are not selected are sent unencrypted. If no meaningful information can be deduced from the non-selected coefficients, then the security level of the system is the same as if all the coefficients have been encrypted.

In some scenarios, the quality of encrypted images can be checked through visual test; however, it doest not guarantee security [26]. To quantify the quality and security of an image encryption schemes a number of security parameters can be applied to check the security and efficiency [27–31]. Some of these parameters were applied in the proposed scheme, to check its efficiency.

Weakness in the existing Fawad et al.'s scheme The degree of similarity between two variables can be computed via correlation coefficient [32]. Ideally, zero correlation coefficient value shows that the two images are completely uncorrelated while 1 shows that the images are perfectly related. −1 correlation coefficient demonstrates that the images are negative of each other, between an image and completely uncorrelated image is zero [33, 34]. The mathematical formula for correlation coefficient has been given in [34]. The correlation coefficient (degree of similarity) were tested for original and image encrypted via Fawad et al.'s scheme between two adjacent pixels in all directions. The testing was done by randomly selecting 1000 pairs of two adjacent pixels in all the three directions i.e., (vertical, horizontal, and diagonal direction) from the original and corresponding cipher image. Simulation results for Cameraman and Baboon Girl, and Iris images are shown from Tables 1, 2, 3 and 4, respectively. The correlation coefficient in horizontal direction for Cameraman and Baboon images is 0.9522 and 0.9547, 0.9539 and 0.9593, respectively, which means that image encrypted by Fawad et al.'s scheme has high correlation in horizontal direction .

Self-information about a source can be calculated via entropy. Basically, entropy provide information about a random process itself [35–37]. The mathematical formula for the calculation of entropy is given in [38]. Ideally, entropy of a source that produces 2^8 symbols with equal probability is 8 bits. An encryption scheme is vulnerable to statistical attack if entropy is less than 8 bits [38]. The entropy values obtained for Cameraman and Baboon Girl and Iris images are 7.1455 and 7.1404, 7.1413 and 7.1412, respectively. From information entropy test, it is clear that there is security risk and certain degree of predictability for Fawad et al.'s scheme.

The rest of the paper is organized as: Section 2 demonstrates the at hand scheme that improves a number of security parameters that shall be described in the later part of the paper. Experimental results, comparison and discussion of the proposed scheme with Fawad's [39], Ahmed's [40] and Amir's [41] are presented in Section 3. Conclusion is given in Section 4.

Table 1 Correlation coefficient analysis of two adjacent pixels: Cameraman image

Direction	Plaintext image	Ciphertext image
Horizontal C.C	0.9282	0.9522
Vertical C.C	0.9644	0.0124
Diagonal C.C	0.9116	0.0202

Table 2 Correlation coefficient analysis of two adjacent pixels: Baboon image

Direction	Plaintext image	Ciphertext image
Horizontal C.C	0.7103	0.9547
Vertical C.C	0.5966	0.0611
Diagonal C.C	0.6225	−0.0025

Table 4 Correlation coefficient analysis of two adjacent pixels: Iris image

Direction	Plaintext image	Ciphertext image
Horizontal C.C	0.8931	0.9593
Vertical C.C	0.8156	0.0756
Diagonal C.C	0.9121	−0.0156

2 The proposed Scheme

Some drawbacks in Fawad et al. scheme [39] like correlation in horizontal direction and low entropy values have been found in Section 2. Hence, the existing Fawad et al.'s scheme has been modified to remove the correlation in horizontal direction and as well as the entropy values and diffusion have been increased.

The basic encryption and decryption transformation in Fawad et al.'s scheme is as follows [39]:

1. $C = \Phi_i P$.
   The corresponding decryption transformation will be: $P = \Phi_i^T C = \Phi_i^T \Phi_i P$ where $\Phi_i^T \Phi_i$ = I = Identity matrix.

2. $C = P\Phi_i$.
   The corresponding decryption transformation will be: $P = C\Phi_i^T = P\Phi_i \Phi_i^T$.

Where, C is the ciphertext image, Φ_i is the orthogonal matrix, P is the plaintext image and T is the transpose operator. Flow chat of the proposed image encryption scheme is shown in Fig. 1.

Detail steps of the proposed scheme is outlined as below. Chaotic skew tent map and XOR operations are added to improve the security of Fawad's et al scheme.

Let P_{int} is the initial plaintext image, P_0 is the plaintext image in 1st iteration, S_k be a secret key of 128 bit, respectively. The secret key S_k is only known to the sender. The initial seed κ is generated by bit XOR operation of $H(P_0)$ and S_k, where $H(P_{int})$ represent the hash of P_{int}. The hash of P_{int} can be generated by SHA-3 hashing algorithm. The 256 bit random hash value is generated via SHA-3 hashing algorithm. The initial seed κ is 256 bit which is generated by the sender during encryption process can be easily computed via S_k Without loss of generality, the gray scale images have been considered. The whole encryption process is describes as follows:

Let the size of input plaintext image be $m \times n$ pixels. After the DCT transformation of P_{int}, $\cup_0$ is obtained where $\cup_0$ represents DCT matrix of P_{int}. The size of $\cup_0$ is the same as the size of P_{int} that is $m \times n$. A_0 represents a $S \times S$ partition of $\cup_0$ starting from $\cup_0(0, 0)$, where $\cup_0(0, 0)$ represents the

Table 3 Correlation coefficient analysis of two adjacent pixels: Girl image

Direction	Plaintext image	Ciphertext image
Horizontal C.C	0.9519	0.9539
Vertical C.C	0.9612	0.0312
Diagonal C.C	0.9277	0.0367

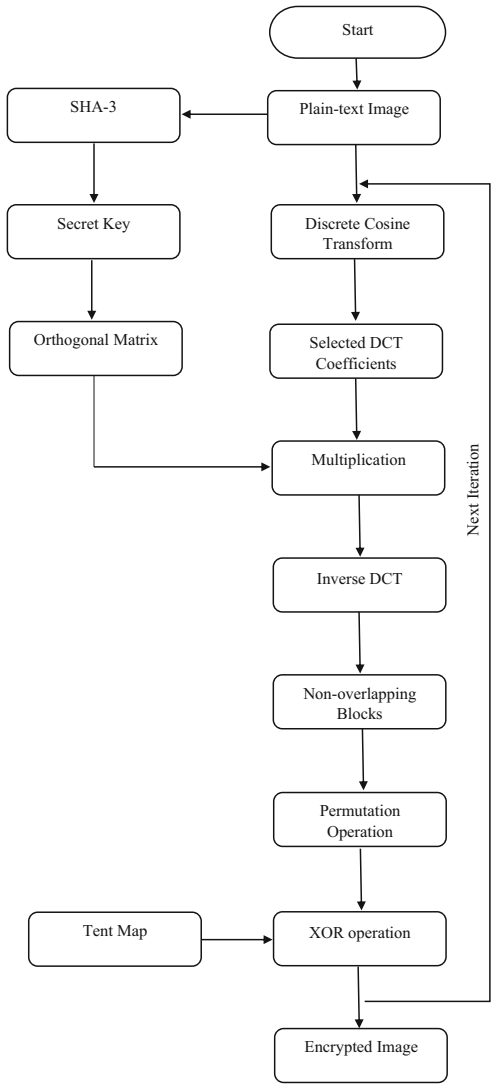
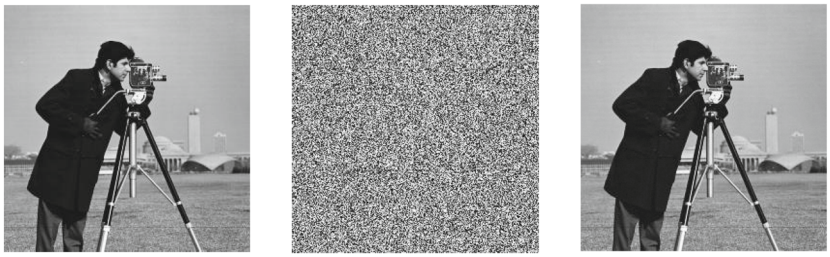


Fig. 1 Flow chart of the proposed scheme based on orthogonal matrix, tent map, and XORed operation

Fig. 2 Encryption and decryption result: Cameraman image



(a) Plaintext Cameraman image. (b) Ciphertext Cameraman image. (c) Decrypted Cameraman image

DCT DC coefficient of $\cup_0$. Total number of iteration are N and begin from 0 up to $N-1$, and i shows the iteration count. The detail steps for iteration are as follows:

Step 1 : Take the DCT of image P_i ; by taking DCT of P_i, $\cup_i$ is obtained.

Step 2 : For each iteration secret key is initialized and secret key is $\kappa_i = \kappa$+i. For generation of Φ_i which is $S \times S$ orthogonal matrix, Gram-Schmidt algorithm is used. The input to Gram-Schmidt algorithm is R_i, where R_i is $S \times S$ random matrix. The secret key κ_i is utilized for the generation of random shifting array ψ_i of size $1 \times Q$.

Step 3 : The orthogonal matrix Φ_i is generated by Gram-Schmidt and it is pre-multiplied with A_i to get $\tilde{A}_i$, where A_i is $S \times S$ partion of $\cup_i$ starting from DCT DC coefficient.

$$\tilde{A}_i = \Phi_i X_i.$$

Step 4 : $\cup_i$ is modified in such a way that DCT partition A_i is replaced with $\tilde{A}_i$ and after modification $\tilde{\cup}_i$ is obtained.

Step 5 : To get $m \times n$ spatial domain image, inverse DCT of $\tilde{\cup}_i$ is taken. and spatial domain image $\ddot{P}_i$ is obtained.

Step 6 : Divide the image $\ddot{P}_i$ into $X \times X$ blocks. Blockwise shifting is carried out by using pseudo-random shifting array ψ_i. The permuted version of $\ddot{P}_i$ is $P_{i+1} = \prec_{\psi_i} (\ddot{P}_i)$, where $\prec_{\psi_i}$ (.) represents the shifting vector ψ_i to perform the shifting.

Step 7 : For each iteration, step 1 to step 6 is repeated.

Step 8 : After last iteration that is Nth iteration, quantization and scaling is done to keep the pixel value between 0 and 255. The resultant image is ciphertext image $\tilde{C}$ of size $m \times n$.
The next two steps are the proposed modification in the existing Fawad et al.'s scheme.

Step 9 : Repeat the skew tent map for X^2 times to get α. Reshape values in a matrix form to get β. Mathematically, the skew tent map $G : [0, 1] \rightarrow [0, 1]$ is given by as:

$$\alpha_{n+1} = G(\alpha_n, p) = \begin{cases} \frac{\alpha_n}{p}, & \text{for } 0 < \alpha_n \leq p \\ \frac{1-\alpha_n}{1-p}, & \text{for } p < \alpha_n < 1 \end{cases} \quad (1)$$

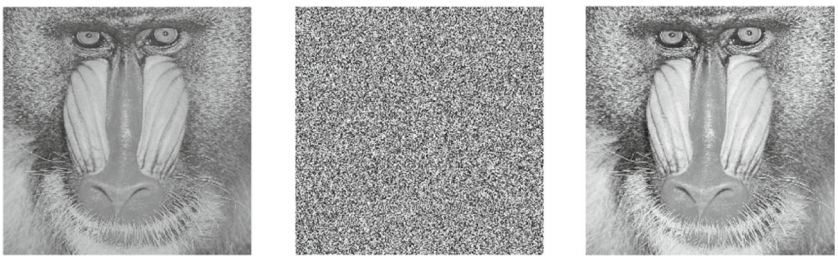
where $p \in (0,1)$ is the positive control parameter and $\alpha_n \in [0,1]$ is the state parameter of the skew tent map.

Step 10 : $\tilde{C}$ is divided into $X \times X$ blocks. β is bitwise XOR with the first block of C_i. The i_{th} block of $\tilde{C}$ is bitwise XOR with $i - 1_{th}$ cipher block of $\tilde{C}$, to obtain cipher image C.
$C_i = E(\tilde{C} \oplus C_{i-1}), C_{-1} = \tilde{C}_0 \oplus \beta$.
Horizontal correlation is removed when images are encrypted via the proposed scheme. Through Steps 9 and 10, the entropy values and diffusion have been increased, which will be discussed in the next section.

2.1 Image decryption algorithm

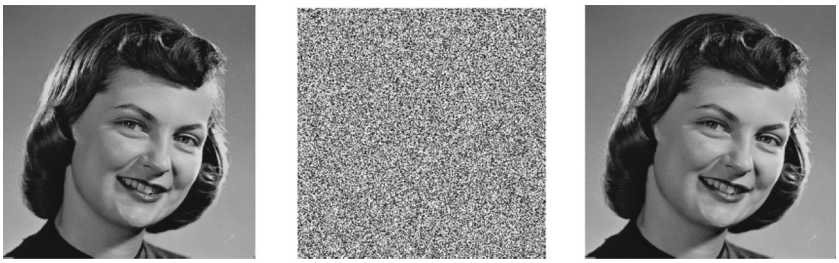
To get the plaintext images from ciphertext images, the decryption algorithm utilizes the secret key κ, Q, N, p,

Fig. 3 Encryption and decryption result: Baboon image



(a) Plaintext Baboon image. (b) Ciphertext Baboon image. (c) Decrypted Baboon image

Fig. 4 Encryption and decryption result: Girl image



(a) Plaintext Girl image. (b) Ciphertext Girl image. (c) Decrypted Girl image

x_0, scaling, and quantization parameters. As decryption is the reverse process of encryption, so all transformation used during the encryption process are implemented in the reverse form. Let $\ddot{C}$ is the received ciphertext image at the decryption side. The transmitted or encrypted image was C, but due to the channel distortion or compression the ciphertext image, C changed to $\ddot{C}$. Let us assume that the channel has no distortion and $C = \ddot{C}$. The effect of noise will be discussed later on. The following describes the decryption procedure as outlined in [39] along with the proposed modification which is shown in step 1.

Step 1 : Iterate skew tent map for X^2 to get α using the initial paramter p and x_0. Reshape α to get $X \times X$ matrix and store the obtained result in β.

Step 2 : C is divided into $X \times X$ blocks. β is bitwise XORed with the 1st block of C. The block of C is bitwise XORed with $(i-1)_{th}$ block of C to obtain $\bar{C}_0$.

Step 3 : Inverse quantization and inverse scaling is implemented to $\bar{C}_0$ to acquire $\breve{C}_0$.

Step 4 : For each iteration, the secret key is initialized to $\kappa_i = \kappa + (N - 1 - i)$. For generation of Φ_i which is an $S \times S$ orthogonal matrix, Gram-Schmidt algorithm is used. The input to the Gram-Schmidt algorithm is R_i, where R_i is $S \times S$ random matrix. The secret key κ_i is utilized to generate random matrix R_i and pseudo-random shift of array ψ_i of size $1 \times Q$.

Step 5 : Divide the image $\breve{C}_i$ into $X \times X$ blocks. Block-wise inverse shift is carried out by using pseudo-random shift sequence ψ_i. The inverse shifted form of $\breve{C}_0$ is expressed by $\prec^{-1}_{\psi_i}(\breve{C}_i)$, where $\prec^{-1}_{\psi_i}(.)$ illustrates the inverse shift function that utilize the shift vector ψ_i.

Step 6 : Δ_i is obtained by taking DCT of $\prec^{-1}_{\psi_i}(\breve{C}_i)$.

Step 7 : Let $\hat{y}_i$ indicates the $S \times S$ partition of Δ_i beginning from $\Delta_i(0,0)$ that is the DCT DC coefficient. The transpose of Φ_i is multiplied by $\hat{y}_i$ to obtain $\bar{y}_i$. $\bar{y}_i = \Phi_i^T \hat{y}_i$.

Step 8 : Δ_i is modified in such a way that the DCT portion of $\hat{y}_i$ is replaced with $\bar{y}_i$ to get modified $\bar{\Delta}_i$.

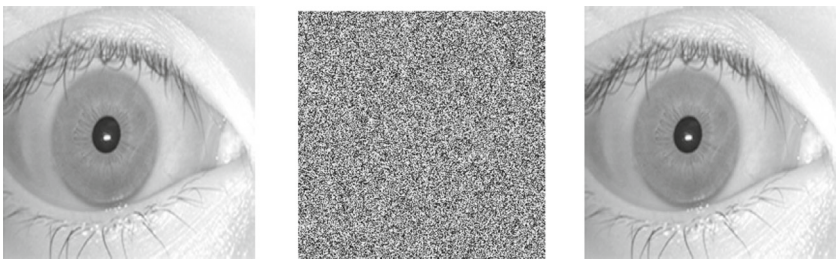
Step 9 : To get $m \times n$ spatial domain image. Inverse DCT of $\bar{\Delta}_i$ is applied to obtain $\breve{C}_{i+1}$, which is the $m \times n$ spatial domain image.

Step 10 : Steps 3 to 8 is repeated for each iteration. After scaling and quantization, P_{dec} is obtained, where P_{dec} is the decrypted image and min $(P_{dec}) = 0$ and max $(P_{dec}) = 255$.

3 Security analysis

In this section, experiments are carried out for Cameramen and Baboon images having a size of 256×256 pixels. In the following sections, experimental results prove the resistance of the at-hand scheme to attacks like brute force attacks, differential attacks, and statistical attacks.

Fig. 5 Encryption and decryption result: Iris image



(a) Plaintext Iris image. (b) Ciphertext Iris image. (c) Decrypted Iris image

Table 5 Correlation coefficient analysis of two adjacent pixels: Cameraman image

Direction	Plain image	[39]	[40]	[41]	Proposed
Horizontal C.C	0.9282	0.9522	0.9120	0.0301	0.0245
Vertical C.C	0.9644	0.0124	0.0738	0.0807	0.0295
Diagonal C.C	0.9116	0.0202	0.4434	0.0228	−0.0319

Table 7 Correlation coefficient analysis of two adjacent pixels: Girl image

Direction	Plain Image	[39]	[40]	[41]	Proposed
Horizontal C.C	0.9519	0.9539	0.9120	0.0301	0.0255
Vertical C.C	0.9612	0.0312	0.0741	0.0807	0.0371
Diagonal C.C	0.9277	0.0367	0.4415	0.0228	0.0356

3.1 Image encryption and decryption

Some images were encrypted by the proposed scheme. Encryption and decryption results are shown from Figs. 2, 3, 4 and 5. The test results show that from ciphertext images, original plaintext images can be recovered. In all the experiments, the iteration count was 4.

3.2 Evaluation and security analysis

This section presents the security and comparison analysis of the proposed scheme with some other traditional schemes. The schemes outlined in [39–41] and the the proposed scheme are analyzed in detail. Mathematical formulas of all security parameters can be found in our previous work [12, 27, 42, 43]

3.2.1 Correlation coefficient analysis

To check the degree of similarity between two adjacent pixels, analysis known as correlation coefficients has been done on both Cameraman and Baboon images. In all (three) dimensions (vertical, horizontal and diagonal) 1000 pairs of two adjacent pixels were selected in random manner. Computation of correlation coefficient was same as in [34]. Tables 5 and 6 depict the correlation coefficients values in all directions. It can be seen from both tables that the correlation coefficients for both ciphertext are nearly zero when the proposed scheme is used. It is clear from Tables 1 and 2 that the proposed modification in Fawad's scheme reduced horizontal correlation. Moreover when compared with other methodologies, the proposed scheme has less correlation values (Tables 7 and 8).

Table 6 Correlation coefficient analysis of two adjacent pixels: Baboon image

Direction	Plain image	[39]	[40]	[41]	Proposed
Horizontal C.C	0.7103	0.9547	0.9137	0.0728	−0.0216
Vertical C.C	0.5699	0.0611	0.2190	0.0695	−0.0512
Diagonal C.C	0.6225	−0.0025	0.0153	0.0121	0.0017

3.2.2 Entropy analysis

The value of entropy for Cameraman and Baboon images are shown in Table 9, which shows that entropy values are near to the ideal value of 8 for the proposed scheme. The at hand scheme is secure against entropy attack when compared with traditional schemes. An attacker cannot predict the ciphertext and there is no security risk with respect to entropy attack.

3.2.3 Encryption quality measurement

By visual inspection it has been shown that the proposed scheme has high encryption quality. This means that ciphertext does not disclose any particulars or fact about the plaintext image. Now the question is how to judge the quality of encryption merely by visual inspection. Numerical results are showed to demonstrate encryption quality of the anticipated scheme. It is needed to show numerically that the modified algorithm has high encryption quality. To check encryption quality numerically, histogram uniformity test has been carried out. For any encryption scheme if the histogram of ciphertext image is uniform that is each gray level is uniformly distributed then the encryption quality is high [44].

The histogram of encrypted images are shown in Figs. 6 and 7. The proposed scheme generates uniform histogram for all encrypted images. It is observed from Figs. 6 and 7 that the histogram of plaintext image and encrypted image is significantly different. Similar results are obtained for Girl and Iris images. This shows the encrypted images bear no statistical similarity with plaintext images. Deviation is another parameter used to judge the quality of encryption

Table 8 Correlation coefficient analysis of two adjacent pixels: Iris image

Direction	Plain Image	[39]	[40]	[41]	Proposed
Horizontal C.C	0.8931	0.9593	0.9211	0.0761	−0.0211
Vertical C.C	0.8156	0.0756	0.2219	0.0678	0.0534
Diagonal C.C	0.9121	−0.0156	0.0143	0.0165	−0.0027

Table 9 Entropy analyses of Fawad's [39], Ahmed's [40], Amir's [41], and the proposed algorithm

Direction of adjacent pixels	Plain image	[39]	[40]	[41]	Proposed
Cameraman	7.1735	6.5676	7.0039	7.6453	7.9455
Baboon	7.4226	6.5558	7.1865	7.7422	7.9120
Girl	7.3275	6.5434	7.1567	7.6343	7.9122
Iris	7.4178	6.5647	7.1564	7.7598	7.9342

algorithm. The encryption quality of an image encryption algorithm can be numerically computed via maximum deviation, irregular deviation, and the uniform histogram deviation [3, 26]. Simulation results for all three parameters are shown in Tables 10, 11, and 12, respectively. The higher value of maximum deviation (D) confirm the robustness of the anticipated algorithm, which means that encrypted image is more deviated from plaintext image. With respect to irregular deviation experimental analysis, the proposed scheme tends to have lower value of I_D, which are actually required for encryption algorithms, as discussed in [3, 26]. If the value of U_D is low, then this indicate the encrypted image is less diverged from ideal assumed histogram [3]. Hence, encryption quality of the presented algorithm is high due to the lower value of U_D when compared to other schemes.

3.2.4 Diffusion characteristics of the proposed scheme

Avalanche effect This test is carried out for the proposed scheme, which is one of the desirable properties for an encryption algorithm [45, 46]. The diffusion characteristic is tested by changing only one bit in the plaintext, that is the plaintext is changed from P to $\bar{P}$ and the corresponding ciphertext is changed from C to $\bar{C}$. The formula for MSE is given in [47]. Simulation results are shown in Table 13. There should be quality difference between the two images if $MSE \geq 30$ dB [48]. From Table 13, quality difference is evident and it shows that the proposed scheme has strong diffusion mechanism.

NPCR and UACI The NPCR [30] test is carried out for the proposed scheme, in order to check the dissimilarity rate of pixels in ciphertext images due to one one pixel change in the plaintext original image . To check the average of these changes, UACI is calculated as in [49–51]. Tests were performed on Cameraman and Baboon images, to identify the impact of a single pixel change on the anticipated scheme. Simulations results are shown in Tables 14 and 15. The values obtained in Tables 14 and 15 are higher than the values obtained in Fawad's [39], Ahmed's [40], and Amir's [41], so the proposed scheme is better. All other schemes indicate very limited sensitivity to minor changes in original images.

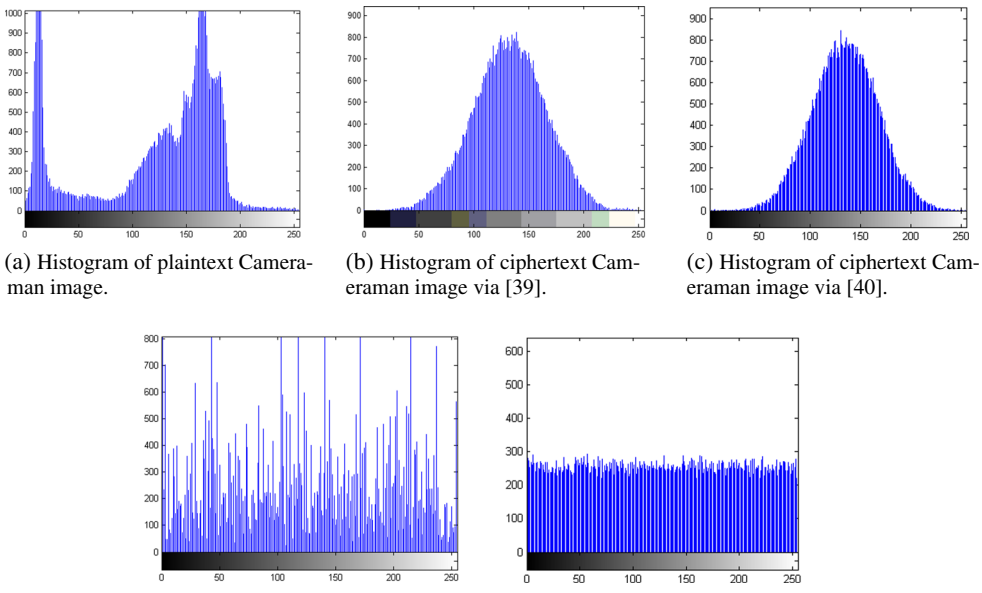


Fig. 6 Histogram demonstration of plaintext and ciphertext: Cameraman images

(a) Histogram of plaintext Cameraman image.

(b) Histogram of ciphertext Cameraman image via [39].

(c) Histogram of ciphertext Cameraman image via [40].

(d) Histogram of ciphertext Cameraman image via [41].

(e) Histogram of ciphertext Cameraman image via the proposed scheme.

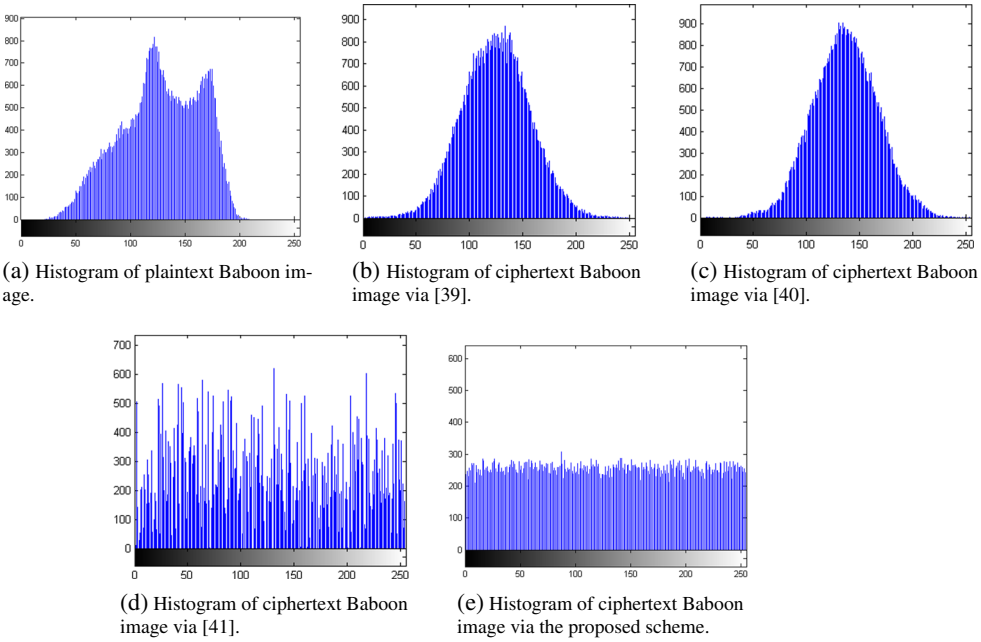


Fig. 7 Histogram demonstration of plaintext and ciphertext Baboon images

(a) Histogram of plaintext Baboon image.

(b) Histogram of ciphertext Baboon image via [39].

(c) Histogram of ciphertext Baboon image via [40].

(d) Histogram of ciphertext Baboon image via [41].

(e) Histogram of ciphertext Baboon image via the proposed scheme.

Table 10 Maximum deviation analyses of Fawad's [39], Ahmed's [40], Amir's [41], and the proposed algorithm

Encrypted image	[39]	[40]	[41]	Proposed
Cameraman	4.1256×10^4	4.9129×10^4	3.8912×10^4	6.1812×10^4
Baboon	3.8120×10^4	1.7652×10^4	5.5129×10^4	6.9678×10^4
Girl	4.3124×10^4	4.8639×10^4	3.9187×10^4	6.1378×10^4
Iris	3.8232×10^4	1.9342×10^4	5.5169×10^4	6.91536×10^4

Table 11 Irregular deviation analyses of Fawad's [39], Ahmed's [40], Amir's [41], and the proposed algorithm

Encrypted image	[39]	[40]	[41]	Proposed
Cameraman	57987	55171	58173	40127
Baboon	58971	75127	59817	51771
Girl	59765	58761	58121	39781
Iris	59796	74656	59796	51445

Table 12 Uniform Histogram deviation analyses of Fawad's [39], Ahmed's [40], Amir's [41], and the proposed algorithm

Encrypted image	[39]	[40]	[41]	Proposed
Cameraman	1.2121	1.1210	0.5504	0.0409
Baboon	1.2223	0.9121	0.4570	0.0512
Girl	1.2022	1.2170	0.5514	0.0591
Iris	1.312	1.1287	0.5112	0.0491

Table 13 MSE results (dB) of Fawad's [39], Ahmed's [40], Amir's [41], and the proposed algorithm

Encrypted image	[39]	[40]	[41]	Proposed
Cameraman	31.7129	32.7121	38.7611	40.5129 dB
Baboon	33.312	33.6120	37.9876	40.4512 dB
Girl	32.8711	32.7651	37.7861	40.8751 dB
Iris	31.9871	32.7819	37.5439	40.7612 dB

Table 14 NPCR results of Fawad's [39], Ahmed's [40], Amir's [41], and the proposed algorithm

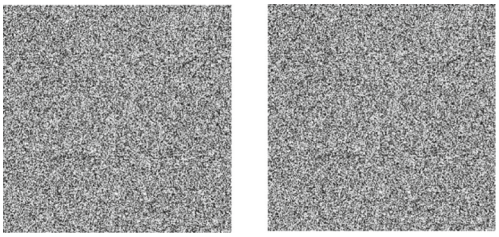
Encrypted image	[39]	[40]	[41]	Proposed
Cameraman	99.1233	99.0541	65.5121	99.6312
Baboon	99.6712	99.1789	66.0128	99.61781
Girl	99.1656	99.0781	65.9871	99.7121
Iris	99.4512	99.1765	65.7651	99.7987

3.2.5 Key space analysis

To test the performance of the proposed scheme against brute force attack, key space analysis was performed.

Exhaustive key search An exhaustive key search requires 2^k operation to succeed, where k is key size in bit. In the proposed scheme, a key size of 128 bits has been used; hence , 2^{128} operations are required for determination of key. In order to predict the key via brute force attack, an attacker requires 10.790283×10^{21} years, if 1000 MIPS computer is employed.

Key sensitivity test To check the key sensitivity of anticipated algorithm, plaintext image was encrypted using two different keys. These keys differ by only one bit. The resultant ciphertext images are C_1 and C_2. The two ciphertext images obtained through the proposed scheme are shown in Fig. 8, but by visual inspection, it is difficult to guess that two ciphertexts are different or same. The same scenarios are found in other schemes as well, so the percentage difference between two ciphertext were calculated for all scheme. Simulation results are highlighted in Table 16. It can be seen from Table 16 that keys which differ by only one bit, the resultant ciphertexts are different, approximately more than 99% for all schemes except Amir's scheme [41]. Generally, these obtained results show that, the all schemes are sensitive towards different keys.



(a) Encrypted Cameraman image using seed = 4.

(b) Encrypted Cameraman image using seed = 5.

Fig. 8 Results of the difference test

3.2.6 Classical attacks

As outlined in [19], classical attacks such as chosen plaintext attack, plaintext-only attack, chosen ciphertext attack, and ciphertext-only attack are most common attacks in cryptography. In such attacks, an intruder has access to the design and working mechanism of an encryption algorithm. In such scenarios, only key is kept secret from eavesdroppers. In these attacks, chosen plaintext is the most powerful attack [19]. If an encryption algorithm resist the chosen plaintext attack, then it is resistant to other attacks as well [19]. In the proposed scheme, if one bit in plaintext changes, the corresponding initial conditions generated via SHA-3 changes and hence orthogonal matrix change. The encrypted image is not only dependent on SHA-3 but also dependent on Tent map initial conditions. With a slight change in Tent map initial conditions, the corresponding ciphertext will be completely different. Hence, the proposed scheme is resistant against ciphertext/plaintext attack.

3.2.7 Time and complexity analysis

Without loss of generality, all images were gray scale with size 256×256. The proposed algorithm was tested on MATLAB R2014 with CPU 2.0 GHZ and 3 GB memory. One can see from Table 17 that the proposed encryption consumes less time as compared with Ahmed's and Amir's schemes. But when compared with Fawad's scheme, the proposed scheme consumes much time. Basically, in the proposed

Table 15 UACI results of Fawad's [39], Ahmed's [40], Amir's [41], and the proposed algorithm

Encrypted image	[39]	[40]	[41]	Proposed
Cameraman	12.4231	13.6121	20.7841	33.6112
Baboon	14.6087	15.7612	20.1671	33.7812
Girl	13.5261	14.5612	19.7812	33.7651
Iris	13.5611	14.8761	19.5612	33.6712

Table 16 Key sensitivty test of Fawad's [39], Ahmed's [40], Amir's [41] and the proposed algorithm

Encrypted image	[39]	[40]	[41]	Proposed
Cameraman	99.0601	99.0616	65.6400	99.3354
Baboon	99.1684	99.1699	65.6534	99.5400
Girl	57974	54912	59348	39342
Iris	59796	74656	59796	49948

Table 17 Processing time (Sec) required for Fawad's [39], Ahmed's [40], Amir's [41], and the proposed algorithm

Encrypted image	[39]	[40]	[41]	Proposed
Cameraman	0.6110	0.8712	0.7110	0.6218
Baboon	0.6217	0.8129	0.7211	0.6331
Girl	0.6120	0.8232	0.7129	0.6311
Iris	0.6003	0.8121	0.7457	0.6127

modified scheme, Tent map and XOR operation were added to achieve higher security.

4 Conclusion

In this paper, we initially investigated the drawbacks in an existing traditional encryption scheme. Then, we proposed an enhanced version of that scheme. The new scheme overcomes many issues that exists in some traditional schemes. To show the strength of the proposed scheme, we evaluate it through different tests such as correlation coefficient, information entropy, deviation, NPCR, UACI, and key sensitivity. These security analyses indicate that our proposed scheme based on skew tent map and XOR operation has advantages over traditional encryption techniques.

Compliance with Ethical Standards

Conflict of interests The authors declare that they have no conflict of interest.

References

1. Jakimoski G, Subbalakshmi K (2008) Cryptanalysis of some multimedia encryption schemes. IEEE Trans Multimed 10(3):330–338
2. Zhang YQ, Wang XY (2014) A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice. Inf Sci 273:329–351
3. Elashry IE (2010) Digital image encryption. MS thesis, Department of computer science and engineering, Faculty of electronic engineering, Menofia University
4. Ahmed J, Hwang SO A fast encryption/decryption scheme for biometric images using multiple chaotic maps. In: IMTIC'15–international multi-topic conference. p 104
5. Zhang YQ, Wang XY (2014) Spatiotemporal chaos in mixed linear–nonlinear coupled logistic map lattice. Physica A: Statistical Mechanics and Its Applications 402:104–118
6. Zeng W, Yu H, Lin C (2006) Multimedia security technologies for digital rights management. Academic Press
7. Zhang YQ, Wang XY (2014) Analysis and improvement of a chaos-based symmetric image encryption scheme using a bit-level permutation. Nonlinear Dyn 77(3):687–698
8. Wang XY, Yang L, Liu R, Kadir A (2010) A chaotic image encryption algorithm based on perceptron model. Nonlinear Dyn 62(3):615–621
9. Zhang YQ, Wang XY (2015) A new image encryption algorithm based on non-adjacent coupled map lattices. Appl Soft Comput 26:10–20
10. Zhang YQ, Wang XY, Liu J, Chi ZL (2016) An image encryption scheme based on the mlncml system using dna sequences. Opt Lasers Eng 82:95–103
11. Schneier B (1996) Applied Cryptography. Wiley, USA
12. Ahmad J (2010) Efficiency analysis and security evaluation of image encryption schemes. computing 23:25
13. Rehman AU, Khan JS, Ahmad J, Hwang SO (2016) A new image encryption scheme based on dynamic s-boxes and chaotic maps. 3D Research 7(1):1–8
14. Chen Y, Chang L (2001) A secure and robust digital watermarking technique by the block cipher rc6 and secure hash algorithm. In: Proceedings of the 2001 international conference on image processing, 2001. IEEE, vol 2, pp 518–521
15. Liu H, Wang X (2010) Color image encryption based on one-time keys and robust chaotic maps. Computers & Mathematics with Applications 59(10):3320–3327
16. Liu H, Wang X et al. (2012) Image encryption using dna complementary rule and chaotic maps. Appl Soft Comput 12(5):1457–1466
17. Liu H, Wang X (2011) Color image encryption using spatial bit-level permutation and high-dimension chaotic system. Opt Commun 284(16):3895–3903
18. Wang X, Liu L, Zhang Y (2015) A novel chaotic block image encryption algorithm based on dynamic random growth technique. Opt Lasers Eng 66:10–18
19. Wang X, Teng L, Qin X (2012) A novel colour image encryption algorithm based on chaos. Signal Process 92(4):1101–1108
20. Wang XY, Yu Q (2009) A block encryption algorithm based on dynamic sequences of multiple chaotic systems. Commun Nonlinear Sci Numer Simul 14(2):574–581
21. Wang X, Luan D (2013) A novel image encryption algorithm using chaos and reversible cellular automata. Commun Nonlinear Sci Numer Simul 18(11):3075–3085
22. Wang XY, Chen F, Wang T (2010) A new compound mode of confusion and diffusion for block encryption of image based on chaos. Commun Nonlinear Sci Numer Simul 15(9):2479–2485
23. Spanos G, Maples T (1995) Performance study of a selective encryption scheme for the security of networked, real-time video. In: icccn, p. 0002, Published by the IEEE computer society.
24. Shannon C (1949) Communication theory of secrecy systems. Bell Syst Tech J 28(4):656–715
25. Lookabaugh T, Sicker D (2004) Selective encryption for consumer applications. IEEE Commun Mag 42(5):124–129
26. Ahmad J, Hwang SO, Ali A (2015) An experimental comparison of chaotic and non-chaotic image encryption schemes. Wirel Pers Commun 84(2):901–918
27. Ahmad J, Hwang SO (2015) Chaos-based diffusion for highly autocorrelated data in encryption algorithms. Nonlinear Dyn 82(4):1839–1850
28. Ahmad J, Hwang SO (2015) A secure image encryption scheme based on chaotic maps and affine transformation. Multimedia Tools and Applications:1–26
29. Khan J, Ahmad J, Hwang SO (2015) An efficient image encryption scheme based on: Henon map, skew tent map and s-box. In: 2015 6th international conference on modeling, simulation, and applied optimization (ICMSAO). IEEE, pp 1–6
30. Bin Younas M, Ahmad J (2014) Comparative analysis of chaotic and non-chaotic image encryption schemes. In: 2014 international conference on emerging technologies (ICET). IEEE, pp 81–86

31. Khan M, Shah T (2015) An efficient chaotic image encryption scheme. Neural Comput & Applic 26(5):1137–1148
32. Elashry I, Allah O, Abbas A, El-Rabaie S, El-Samie F (2009) Homomorphic image encryption. J Electron Imaging 18:033002
33. Hussain I, Shah T, Gondal MA (2012) Image encryption algorithm based on pgl (2, gf (28)) s-boxes and td-ercs chaotic sequence. Nonlinear Dyn 70(1):181–187
34. Elkamchouchi H, Makar M (2005) Measuring encryption quality for bitmap images encrypted with rijndael and kamkar block ciphers. In: NRSC 2005 Proceedings of the 22nd national radio science conference, 2005. IEEE, pp 277–284
35. Mirzaei O, Yaghoobi M, Irani H (2012) A new image encryption method: parallel sub-image encryption with hyper chaos. Nonlinear Dyn 67(1):557–566
36. Wang X, Teng L (2012) An image blocks encryption algorithm based on spatiotemporal chaos. Nonlinear Dyn 67(1):365–371
37. Gray R (2010) Entropy and information theory, Springer Verlag
38. Ahmed H, Kalash H, Allah O (2017) Implementation of RC5 block cipher algorithm for image cryptosystems. Int J Inf Technol 3(4):245–250
39. Ahmed F, Siyal M, Abbas V (2010) A perceptually scalable and jpeg compression tolerant image encryption scheme. In: 2010 4th pacific-rim symposium on image and video technology (PSIVT). IEEE, pp 232–238
40. Ahmed F, Anees A, Abbas VU, Siyal MY (2014) A noisy channel tolerant image encryption scheme. Wirel Pers Commun 77(4):2771–2791
41. Anees A, Siddiqui AM, Ahmed F (2014) Chaotic substitution for highly autocorrelated data in encryption algorithm. Commun Nonlinear Sci Numer Simul 19(9):3106–3118
42. Ahmad J, Khan MA, Hwang SO, Khan JS (2016) A compression sensing and noise-tolerant image encryption scheme based on chaotic maps and orthogonal matrices. Neural Comput & Applic:1–15
43. Khan JS, ur Rehman A, Ahmad J, Habib Z (2015) A new chaos-based secure image encryption scheme using multiple substitution boxes. In: 2015 conference on information assurance and cyber security (CIACS). IEEE, pp 16–21
44. Jolfaei A, Mirghadri A (2010) Survey: image encryption using salsa20. Int J Comput Sci Issues 7(5)
45. Khan MA, Ahmad J, Javaid Q, Saqib NA (2016) An efficient and secure partial image encryption for wireless multimedia sensor networks using discrete wavelet transform, chaotic maps and substitution box. J Mod Opt:1–10
46. Khan JS, Ahmad J, Khan MA (2017) Td-ercs map-based confusion and diffusion of autocorrelated data. Nonlinear Dyn 87(1):93–107
47. Mohamed A, Zaibi G, Kachouri A (2011) Implementation of rc5 and rc6 block ciphers on digital images. In: 2011 8th international multi-conference on systems, signals and devices (SSD). IEEE, pp 1–6
48. Liehuang Z, Wenzhuo L, Lejian L, Hong L (2006) A novel image scrambling algorithm for digital watermarking based on chaotic sequences. Int J Comput Sci Netw Secur 6(8B):125–130
49. Wang X, Wang Q (2014) A novel image encryption algorithm based on dynamic s-boxes constructed by chaos. Nonlinear Dyn 75(3):567–576
50. Ye G, Wong KW (2012) An efficient chaotic image encryption algorithm based on a generalized arnold map. Nonlinear dyn 69(4):2079–2087
51. Mao Y, Chen G (2005) Chaos-based image encryption. Handbook of Geometric Computing:231–265