A Random Image Encryption Approach for a Novel Color Image

J. Antonet Navnai Rani[1], X. M. Binisha[2]

[1]*PG Scholar, Department Of Electronics and Communication Engineering, PET Engg. College, Vallioor, India*

[2]*Assistant Professor, Department Of Electronics and Communication Engg., PET Engg. College, Vallioor, India*

***Abstract*: Image encryption has been an attractive research field in recent years. The chaos-based cryptographic algorithms have suggested some new and efficient ways to develop secure image encryption techniques. This chaotic tent map (CTM)-based schemes show some good performances in randomness properties and security level. In this paper, a novel image encryption algorithm by using the combination of the rectangular transform and the CTM principle has been used. It encrypts the three channels of the plain image at the same time and these channel encryptions associate with each other. In addition, by generating the key-streams related to both the secret keys and the plain image, its key-sensitivity has been further improved. The security of the proposed scheme has been verified by security analysis and experimental evaluations, and the results show that many drawbacks of pure CTM-based schemes have been overcome.**

***Keywords*: Chaotic tent map, Rectangular transform, Image encryption, Chaotic cryptography.**

1. Introduction

Steganography is the field of research that utilizes for hiding the secret message in an image. Steganography is the good choice of secure communication. Steganography message can be retrieved by reverse Steganography for which some algorithm is used.

However one problem of Steganography and other visual cryptography techniques is that there can be an eavesdropper Eve between two users, Alice and Bob, and Eve can hijack the message taken from Alice and forward a fake message to Bob. Again it means we need a key to secure the transformation. However if we think of symmetric keys, large keys are no longer going to be suitable for future next generation.

As an important technology to protect digital images, image encryption has become an attractive research area in recent years. Due to some good features of chaotic systems, such as it’s extremely sensitive dependence on initial conditions and control parameters, ergodicity and random-like behaviours, more and more chaos-based image encryption algorithms have been proposed. Different chaos-based schemes use various chaotic systems. A three dimensional (3D) chaotic cat map is used to design a real-time secure symmetric encryption scheme, while the authors proposed a fast image encryption scheme by adopting the 3D chaotic baker maps. In, two chaotic logistic maps with an external secret key are used for its algorithm design. Other alternatives, such as Bernoulli, valley maps and Chen chaotic system can also be found in the literature. On the other hand, the security of chaos based image encryption scheme usually depends on two aspects, namely the permutation and diffusion structures. In the permutation phase, the pixel positions of the image are changed; while in the diffusion phase, the image’s pixel values are changed.

In [17], the author made the initial attempt to adopt chaotic tent maps (CTM) for image encryption algorithm design. The basic idea of this CTM based scheme is to utilize chaotic key-streams, which are generated by chaotic tent maps, to diffuse the plain image pixels by a simple exclusive-or (denoted as _) operation. This system is so simple that its encryption speed is quite fast. As a consequence, it has advantages in dealing with large number of data and lessening redundant information, compared with the conventional image encryption algorithms. But some obvious defects can also be found in this pure CTM-based scheme as follows.

First, this cryptosystem only involves the diffusing phase, and permutation structure has been omitted. Furthermore, when encrypting colour images, this scheme simply encrypts each component of the colour image respectively, which shows no adaptability from encrypting a gray image to a colour one. In addition, as a vulnerability of this scheme, the CTM generated key-streams only relates to the secret keys. All these defects undermine its security level and make it is easy to be attacked by some common methods.

In this work, an improved algorithm, which is based on a rectangular transform (RT)-enhanced CTM system, has been proposed to overcome the defects of the pure CTM-based scheme. In addition to adding a permutation processing, this new scheme generates the key-streams which are not only related to the secret keys but the plain image. In other words, although the secret keys are the same, the key-streams are different when different plain images are encrypted, so that it can effectively resist the known plaintext attack (KPA) and chosen plaintext attack (CPA). As another novel design of this RT-enhance CTM scheme, when encrypting colour images, it encrypts the three channels of the plain image at the same time and these channel encryptions associate with each other. More security and robust can be achieved from these designs.

The remainder of this paper is organized as follows. After briefly reviews the pure CTM-based scheme proposed in [17], in Section II we show its security defects by indicating some well-directed attacking methods. Following this, in Section III, the details of our RT-enhanced CRM algorithm, including encryption and decryption, are described. Some experimental results are given in Section IV. Section V discusses the security of the proposed scheme from different aspects via theoretic analysis, experiment evaluation and performance comparison with other schemes. Finally, we conclude this work by pointing out its practical value in Section VI.

2. Encryption system

Different chaotic systems are employed in confusion and diffusion stages. Also complex chaotic maps are chosen rather than the simple ones to further enhance the complexity of the algorithm and thereby improving the security. The input to the cryptosystem is the plain image which is to be encrypted.

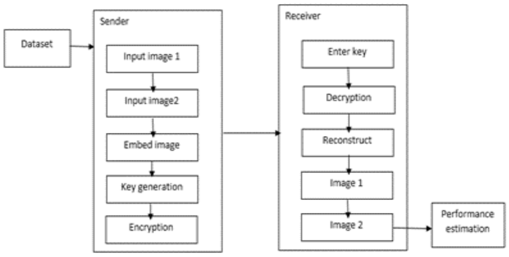


Fig. 1. Block diagram

The cryptosystem consists of two stages. The first stage is the confusion stage and the second one is the diffusion stage. Among the three chaotic dynamic systems namely Lorenz, Chen and LU one is selected by the system parameter which is obtained from the key and it is applied to the digital color image encryption because of higher secrecy of high-dimension chaotic system. The second step of the encryption process is to encrypt the shuffled image by changing its pixel values based on one of the three high-dimensional chaotic systems (Lorenz, Chen and LU). This is referred to as the diffusion stage. The initial conditions and the control parameters used to generate the chaos sequence in both the stages serve as the secret key in the two stages. The resulting image is the Cipher image. Separate key is used for permutation and diffusion stages of the encryption process to improve security of the algorithm.

1) Read the plain image $P_{m\times n\times 3}$, where m and n are the size of the 2D colour image, and we write N = 3mn.
2) Iterate CTM Equation (1) for N times with its control parameter μ and initial value x0 to obtain the chaotic sequence x with the size N.

$$x_{i+1} = \begin{cases} \mu x_i, & \text{if } x_i < 0.5, \\ \mu(1-x_i), & \text{otherwise} \end{cases} \qquad (1)$$

Where, $x_i \in [0, 1]$. Note that when the parameter $\mu \in [0, 2]$ and the initial value $x_0 \in (0, 1)$ the chaotic tent map transforms an interval [0; 1] into itself.

3) Calculate the key stream S1_N by using Equation (2), then reshape S to obtain matrix $M_{m\times n\times 3}$.

$$S = \lfloor x \times 10^{10} \rfloor \bmod 256. \qquad (2)$$

4) Encrypt each pixel of image P by using M with $\oplus$ operation to obtain a cipher image C.

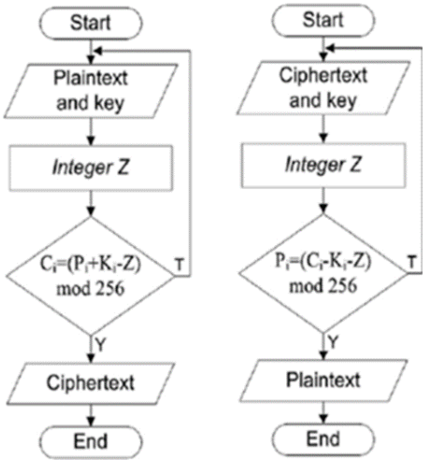


Fig. 2. Encryption and decryption process flow diagram

A. *Review of the pure CTM-based algorithm*

As the pure CTM-based scheme only involves the confusion of the plain image pixels, we summarize its simple encryption steps as follows.

B. *Defects of the pure CTM-based algorithm*

From its processing principle, some defects of its security can be found as follows.

1) Vulnerable to KPA:

The KPA is a kind of attack method, which in based on the condition that the cryptanalyst possesses a serial of plaintext and their corresponding cipher text. For the pure CTM based scheme, let us denote the plaintext as P and its cipher text as C, then matrix $M = P \oplus C$can be obtained. now, if the attacker obtain another unauthorized ciphertext C0, then he can easily reveal its corresponding plaintext P by computing $P' = M \oplus C'$.

2) Vulnerable to CPA:

Different form the KPA, the CPA happens when the cryptanalyst can temporarily use the encryption system. For example, let us choose the plaintext P, which is an all zero matrix, and send it to the pure CTM-based encryption machinery, then its ciphertext C can be obtained. Thus, a matrix $M = P \oplus C$ can be computed to gain some insight of the encryption machinery of this scheme.

3) Other security problems:

In the pure CTM-based algorithm, a chaotic sequence x is obtained by iterating eq. (1) for N times with parameter μ and initial value x0. However, there are several values of x in the start stage may be not chaotic. This give this scheme a potential security risk. In addition, this scheme simply encrypts each component of the colour image respectively, which shows no adaptability from encrypting a gray image to a colour one.

3. RT-enhanced CTM algorithm

As a theory preparation, we first introduce the two dimensional rectangular transform (2D-RT). Actually, the 2D-RT is an extension of the Arnold map and it can directly be used to permutation square images. Mathematically, we describe it as,

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod \begin{pmatrix} m \\ n \end{pmatrix}, \quad (3)$$

Where, (a; b; c; d) are the elements of the transform matrix, (x; y) and (x0; y0) are the position of the original image pixel and the mapped image pixel respectively, while m and n are the height and the width of the plain image, respectively. The 2DRT has an inverse operation when the following condition is met, i.e.

$$\begin{cases} p = \gcd(m, n), \ p_m = p/m, \ p_n = p/n, \\ \gcd(a, p_m) = 1, \ \gcd(d, p_n) = 1, \\ (b \bmod p_m) = 0 \text{ or } (c \bmod p_n) = 0, \\ \gcd(ad - bc, p) = 1. \end{cases} \quad (4)$$

Note that in the Equation (3), (0; 0) is always mapped into (0; 0). In order to avoid this problem, each position (x; y) can be moved to a random shifted position (x + rm; y + rn), where random numbers rm; rn 2 (0; 1). Thus, the improved 2DRT can be expressed as follows.

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} r_m \\ r_n \end{pmatrix} \right] \bmod \begin{pmatrix} m \\ n \end{pmatrix}. \quad (5)$$

And the inverse operation of the improved 2D-RT is expressed as.

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} x' - r_m \\ y' - r_n \end{pmatrix} \bmod \begin{pmatrix} m \\ n \end{pmatrix}. \quad (6)$$

Based on the the CMT given in Equation (1) and (2) and the transforms proposed in (5) and (6), we describe the proposed RT-enhanced CTM algorithm in detail as follows.

Encryption algorithm

Step-1: Choose the secret keys, namely decide values for the set $\{\mu_i; x_{i_0}; a, b, c, d; r_m, r_n; t | i \ 1, 2, 3\}$, where μ_i and x_{i_0} are the control parameters and initial values of the CTM system, respective, while t is the iteration round number for permutation.

Step-2: Read the colour plain image $P_{m \times n \times 3}$ (with notation N = m*n), and denote the three components of P as RP; GP; BP respectively.

Step-3: Stitch the three components RP; GP; BP together to form a gray image $PS_{m \times 3n}$.

Step-4: Permutate the gray image PS by using Equation (5) for t rounds, and get a permutated image as $P_{RT_{m \times 3n}}$.

Step-5: Split the permutated image PRT into three matrices RRTm_n, GRTm_n and BRTm_n, then further convert these three matrices to three 1D vectors Rmn_1;Gmn_1;Bmn_1.

Step-6: Iterate Equation (1) for N+1000 times with the parameters and initial values, respectively, and take the final N values to form three chaotic sequences x1; x2; x3 of length N.

Step-7: Calculate three key-streams Si with xi (where i = 1; 2; 3) by eq. (2).

Step-8: Encrypt R; G; B by using eq. (7) to obtain their corresponding cipher texts R'; G''; B'.

$$\begin{cases} R'(i+1) = ((R(i) + G'_(i) + B'_(i)) \bmod 256) \oplus S_1(i), \\ G'(i+1) = ((G(i) + R'_(i) + B'_(i)) \bmod 256) \oplus S_2(i), \\ B'(i+1) = ((B(i) + R'_(i) + G'_(i)) \bmod 256) \oplus S_3(i), \end{cases} \quad (7)$$

where, i = 1; 2; _ _ _ ;N, while the initial values are

$$R'_0 = (\bar{R} + \delta) \bmod 256, \quad (8)$$
$$G'_0 = (\bar{G} + \delta) \bmod 256, \quad (9)$$
$$B'_0 = (\bar{B} + \delta) \bmod 256. \quad (10)$$

Note in above equations, we used the following definitions, i.e.

$$\bar{R} = \frac{\sum_{i=1}^{i=m} \sum_{j=1}^{j=n} R(i,j)}{m \times n}, \quad (11)$$
$$\bar{G} = \frac{\sum_{i=1}^{i=m} \sum_{j=1}^{j=n} G(i,j)}{m \times n}, \quad (12)$$
$$\bar{B} = \frac{\sum_{i=1}^{i=m} \sum_{j=1}^{j=n} B(i,j)}{m \times n}, \quad (13)$$

And

$$\delta = \lfloor (\bar{P} - \lfloor \bar{P} \rfloor) \times 10^{10} \rfloor \bmod 256. \quad (14)$$

And

$$\bar{P} = \frac{\sum_{i=1}^{i=3} \sum_{j=1}^{j=m} \sum_{k=1}^{k=n} P(i,j,k)}{m \times n \times 3}. \quad (15)$$

Step-9: Reshape three 1D vectors R0; G0; B0 to three matrices $R_{C_{m \times n}}, G_{C_{m \times n}}, B_{C_{m \times n}}$, and use these three components to compose the final colour cipher image C.

4. Decryption system

The decryption system is illustrated in the above figure. The first stage in the decryption process is the diffused image decryption stage. In the encryption process, the pixel value diffusion was carried out with any one of the three chaotic systems. Therefore, in the decryption process to retrieve the original pixel values, again any one of the chaotic system (Lorenz, Chen, Lu) is employed in the first stage of decryption. The first stage of decryption process uses the three dimensional sequence generated by any one of the chaotic system .It is a kind of high-dimensional maps and complex enough. The initial conditions that were used in the encryption process should be used here and this serves as the decryption key for the first stage. Second, in the encryption process, the pixel position permutation was carried out with any one of the chaotic system. The initial conditions and control parameters for generating the chaos-sequence were used as the confusion key. Therefore in the decryption process, the same chaotic systems with same confusion key are used to get the original position of the image. The output of the decryption system gives the original image.

A. Decryption Algorithm

Step-1: Receive the secret keys, i.e.
set $\{\mu_i; x_{i_0}; a, b, c, d; r_m, r_n; t | i = 1, 2, 3\}$
Ste-2: Receive the colour cipher image $C_{m\times n\times 3}$, and denote the three components of C as
C as $R_{C_{m\times n}}, G_{C_{m\times n}}, B_{C_{m\times n}}$, respectively.
Step-3: Iterate Equation (1) for N+1000 times with the parameters and initial values, respectively, and take the final N values to form three chaotic sequences x1; x2; x3 of length N.
Step-4: Calculate three key-streams S1; S2; S3 with x = x1; x2; x3 by eq. (2), respectively.
Step-5: Reshape the three matrices RC, GC and BC to three 1D vectors $R'_{mn\times 1}, G'_{mn\times 1}$, respectively.
Step-6: Inversely diffuse R'; G';B' and obtain three new vectors R; G;B, according to the following equation, i.e.

$$\begin{cases} R(i) = (R'(i+1) \oplus S_1(i) - G'(i) - B'(i)) \bmod 256, \\ G(i) = (G'(i+1) \oplus S_2(i) - R'(i) - B'(i)) \bmod 256, \\ B(i) = (B'(i+1) \oplus S_3(i) - G'(i) - R'(i)) \bmod 256, \end{cases} \tag{16}$$

wherei = 1; 2; _ _ _ ;N.
Step-7: Reshape R; G; B to three matrices
$R_{RT_{m\times n}}, G_{RT_{m\times n}}, B_{RT_{m\times n}}$, then stitch them to form a gray image $P_{RT_{m\times 3n}}$.
Step-8: Inversely permutate the gray image PRT for t rounds with eq. (6) to obtain a un-permutated gray image $P_{S_{m\times n\times 3}}$.
Step-9: Split PS is into three matrices, i.e.
$R_{P_{m\times n}}, G_{P_{m\times n}}, B_{P_{m\times n}}$.
Step-10: Finally, the deciphered colour image P can be composed by whose three channels R_P, G_P, B_P.

We would like to mention that in above encryption progress, each cipher text of plain image is related not only to its plaintext but its former cipher text, and thus a tiny change in any plain image pixel will alter all of the cipher image pixels. Furthermore, in our decryption algorithm, the last pixel value of the decrypted image is unknown because the secret keys do not contain the initial values of R'_0, G'_0 and B'_0. These values should be calculated by pixel values of the plain image.

B. Data Insertion Technique

For each byte of data from the confidential message we interchange 1st bit with 8th bit, 2nd with 7th, 3rd with 6th and 4th with 5th. Then each bit of the bit stream is inserted one after another into the blue and green channels from the beginning to the end. The inserted location of blue and green components (bytes) is determined randomly within 2nd to 8th position a hash function. If the value of the calculated location (by hash function) in blue component and the bit that has to insert are same then '0' is set to the LSB position of that blue component. Otherwise, '1' is set to the LSB position of that blue component. The process is run until the bit stream is finished or the blue components are finished. If the blue components are finished but message bit stream still remained to embed then same embedding process is run on green channel. Embedding into blue channel gets priority as the change of LSBs of the blue channel is not detectable by human eye.

5. Results and Discussion

In order to fully demonstrate the advantages of our algorithm, we choose the standard colour plain image with size 256*256 as the testing subject, which is given in Fig. 3(a) with its histogram. Then embed the secret image into the cover image. After applying the proposed 2D-RT for 5 round, the plain image has been permutated as in Fig. 3(e). Finally, the complete encrypted image and its histogram. As a comparison to the original plain image, the decrypted image and its corresponding histogram are shown in Fig. 3(f) respectively;

The performance was compared using standard parameters, namely, PSNR, MSE. In order to examine whether the proposed encryption algorithm is anti differential, there are two commonly used indexes, namely the number of changing pixel rate (NPCR) and the unified averaged changed intensity (UACI).

Here select JPEG format image as the cover image. The size of the image is 256*256. Then which is the RGB color model image. Then plot the histogram shifting of input image.

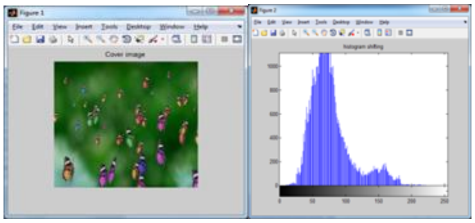


Fig. 3(a). Cover image and histogram shifting

An image is taken as secret data(payload) is set in that image and is passed to the receiver. The receiver can then extract the information from the image using the key provided by the sender.

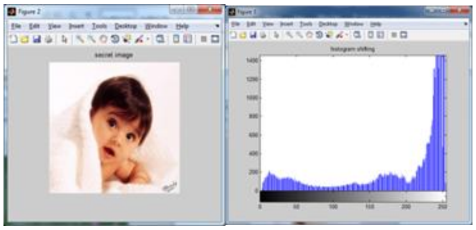


Fig. 3(b). Secret image and histogram shifting

The secret image's LSB bit i.e. least significant bit of some or all of the bytes of an image are changed as per encryption strategy. In 8 bit data, one or two bit of information can be hidden. So increasing or decreasing the value by changing the LSB does not change the appearance of the image much so the resultant stego image looks almost same as the cover image.

Enter the key for concealed the secret data. Here we use 4 bit as the secret key. After enter the secret key encryption process will started. A good encryption algorithm should has a large key space to resist the brute-force attack. Usually, to make a high level security, the key space should be more than 2^100.

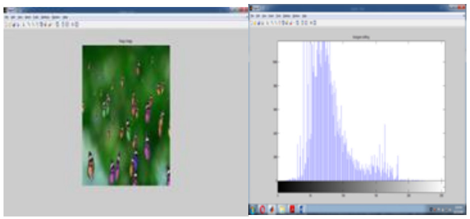
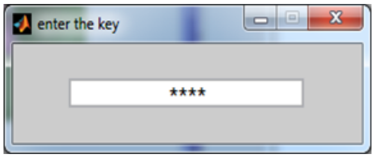


Fig. 3(c). Secret image and histogram shifting



enter the key

****

Fig. 3(d). Secret key for encryption

The 2D-RT is an extension of the Arnold map and it can directly be used to permutation square images. Here separate the rows and columns of the secret image RGB component. Then perform permutation process in each component. Finally together joint RGB component and obtain the encrypted color image.

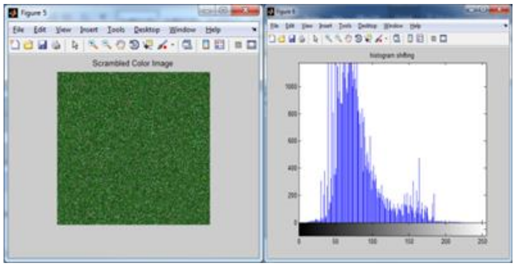


Fig. 3(e). Scrambled image and histogram shifting

After performing encryption process apply secret key in the receiver side for extract the hidden information. It should be same as the receiver side key. If it is wrong we can't extract the hidden information.

Enter the key

asdf

Fig. 3(f). Unscrambled cover image and histogram shifting

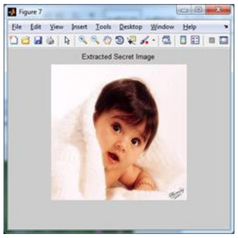


Fig. 3(g). Secret image

In the decrypt phase to detect the positions of the LSB's where the data bits had been embedded we have again used the AND, OR function. In the same order as they are embedded, the bits are extracted from the position when the position of the bits had been specified. At the end of this phase we will obtain the secret image.

6. Quality measures for image

A. *Visual Quality*

The Quality of the reconstructed image is measured in terms of mean square error (MSE) and peak signal to noise ratio (PSNR) ratio. The MSE is often called reconstruction error variance σ_q^2. The MSE between the original image f and the reconstructed image g at decoder is defined as:

$$\text{MSE}= \sigma_q^2 = \frac{1}{N}\sum_{j,k}(f[j,k]-g[j,k])^2$$

Where the sum over j, k denotes the sum over all pixels in the image and N is the number of pixels in each image. From that the peak signal-to-noise ratio is defined as the ratio between signal variance and reconstruction error variance. The PSNR between two images having 8 bits per pixel in terms of decibels (dBs) is given by:

$$\text{PSNR} = 10\log_{10}\left(\frac{255^2}{MSE}\right)$$

Generally when PSNR is 20 dB or greater, then the original and the reconstructed images are virtually indistinguishable by human eyes.

Table 1
PSNR comparison of different images

	Red	Green	Blue
Lena	38.57	39.20	38.14
baboon	37.41	37.38	37.39
barbara	38.79	39.12	38.36
Peppers	36.39	36.26	36.13

B. *Shannon Entropy*

Shannon entropy is usually used to measure the randomness of the gray values of an image. For an 8-bit image, Shannon entropy is defined as,

$$H(m) = -\sum_{i=0}^{255} P(m_i)\log P(m_i), i = 0, 1, \cdots, 255.$$

Where mi represents the ithgray value, while P(mi) is the probability of value mi existing in the image. Obviously, for a 8-bit ideal random image, the entropy is 8, which represents that the image pixel values are completely random. A good image encryption scheme should has a cipher image whose entropy is close enough to 8.

C. *Robustness against differential attack*

Sometimes, attackers make a tiny change in the original plain image, and then encrypts both the original plain image and the changed plain image by the same encryption scheme, and try to find out the relation between plain image and its cipher image by comparing the two encrypted images. We refer to this as differential cryptanalysis. In order to examine whether the proposed encryption algorithm is antidifferential, there are two commonly used indexes, namely the number of changing pixel rate (NPCR) and the unified averaged changed intensity (UACI). Their definitions are as follows.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{m \times n} \times 100\%,$$

$$UACI = \frac{1}{m \times n} \left(\sum_{i,j} \frac{|C(i,j) - C'(i,j)|}{255} \right) \times 100\%,$$

Where m; n are the height and the width of the image, respectively. Here C and C'' are the two encrypted images mentioned above and Di;j is computed as

$$D_{i,j} = \begin{cases} 1, & \text{if } C(i,j) \neq C'(i,j), \\ 0, & \text{if } C(i,j) = C'(i,j). \end{cases}$$

The theoretical values of UACI score is 0:33. And the closer the NPCR score is to 1, the more sensitive the encryption scheme is to the plain image, and the better the scheme resists differential attack.

Table 2
Entropy comparison

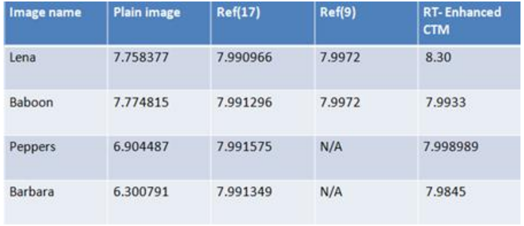
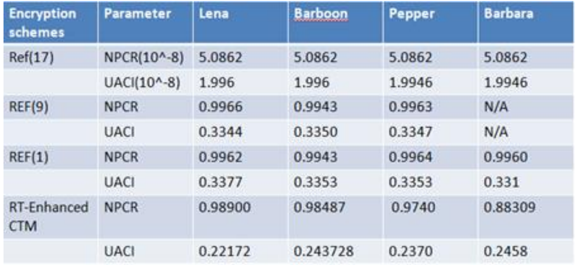


Image name	Plain image	Ref(17)	Ref(9)	RT- Enhanced CTM
Lena	7.758377	7.990966	7.9972	8.30
Baboon	7.774815	7.991296	7.9972	7.9933
Peppers	6.904487	7.991575	N/A	7.998989
Barbara	6.300791	7.991349	N/A	7.9845

Table 3
NPCR and UACI Scores Comparison For Different Encryption Schemes



Encryption schemes	Parameter	Lena	Barboon	Pepper	Barbara
Ref(17)	NPCR(10^-8)	5.0862	5.0862	5.0862	5.0862
	UACI(10^-8)	1.996	1.996	1.9946	1.9946
REF(9)	NPCR	0.9966	0.9943	0.9963	N/A
	UACI	0.3344	0.3350	0.3347	N/A
REF(1)	NPCR	0.9962	0.9943	0.9964	0.9960
	UACI	0.3377	0.3353	0.3353	0.331
RT-Enhanced CTM	NPCR	0.98900	0.98487	0.9740	0.88309
	UACI	0.22172	0.243728	0.2370	0.2458

7. Conclusion and Future scope

In this paper, an image encryption scheme based on RT-enhanced CTM has been proposed. Its security analysis has also be given in detail. Experimental simulation and performance comparison with other systems show that this new scheme has greatly improved the security while still possessing all the merits of the pure CTM-based schemes, which obviously leads some practical value in implementation. This approach results in high quality of the stego image having high PSNR values compared to other methods.

However the disadvantage of the approach is that it is susceptible to noise if spatial domain techniques are used to hide the key. This can be improved if transform domain techniques are used to hide the key. The approach is very simple and the security level can be increased by using standard encryption techniques to encrypt the keys. Discrete Wavelet Transform (DWT) is performed on cover image and the image sub-bands are shuffled by using the key streams generated. Finally, the image frequencies are transformed back to the spatial domain by using inverse DWT (IDWT). The approach shows satisfactory results.

References

[1] X.-J. Tong, M. Zhang, Z. Wang, and J. Ma, "A joint color image encryption and compression scheme based on hyper-chaotic system," Nonlinear Dynamics, vol. 84, no. 4, pp. 2333–2356, 2016.

[2] L. Wang, H. Song, and P. Liu, "A novel hybrid color image encryption algorithm using two complex chaotic systems," Optics and Lasers in Engineering, vol. 77, pp. 118–125, 2016.

[3] P. Praveenkumar, R. Amirtharajan, K. Thenmozhi, and J. B. B. Rayappan, "Triple chaotic image scrambling on rgb–a random image encryption approach," Security and Communication Networks, vol. 8, no. 18, pp. 3335–3345, 2015.

[4] L. Xu, Z. Li, J. Li, and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps," Optics and Lasers in Engineering, vol. 78, pp. 17–25, 2016.

[5] X. Wang and H.-l. Zhang, "A novel image encryption algorithm based on genetic recombination and hyper-chaotic systems," Nonlinear Dynamics, vol. 83, no. 1-2, pp. 333–346, 2016.

[6] M. Khan, T. Shah, and S. I. Batool, "Construction of s-box based on chaotic boolean functions and its application in image encryption," Neural Computing and Applications, vol. 27, no. 3, pp. 677–685, 2016.

[7] Z. Hua and Y. Zhou, "Image encryption using 2d logisticadjusted- sine map," Information Sciences, vol. 339, pp. 237– 253, 2016.

[8] J. Zhang, "An image encryption scheme based on cat map and hyperchaoticlorenz system," in Computational Intelligence & Communication Technology (CICT), 2015 IEEE International Conference on. IEEE, 2015, pp. 78–82.

[9] A. Y. Niyat, M. H. Moattar, and M. N. Torshiz, "Color image encryption based on hybrid hyper-chaotic system and cellular automata," Optics and Lasers in Engineering, vol. 90, pp. 225– 237, 2017.

[10] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3d chaotic cat maps," Chaos, Solitons & Fractals, vol. 21, no. 3, pp. 749–761, 2004.

[11] Y. Mao, G. Chen, and S. Lian, "A novel fast image encryption scheme based on 3d chaotic baker maps," International Journal of Bifurcation and chaos, vol. 14, no. 10, pp. 3613–3624, 2004.

[12] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," Image and vision computing, vol. 24, no. 9, pp. 926–934, 2006.

[13] R. Ye and Y. Ma, "A secure and robust image encryption scheme based on mixture of multiple generalized bernoulli shift maps and arnold maps," International Journal of Computer Network and Information Security, vol. 5, no. 7, p. 21, 2013.

[14] H. Garces and B. C. Flores, "Statistical analysis of bernoulli, logistic, and tent maps with applications to radar signal design," in Defense and Security Symposium. International Society for Optics and Photonics, 2006, pp. 62 100G–62 100G.

[15] T. Papamarkou and A. J. Lawrance, "Nonlinear dynamics of trajectories generated by fully-stretching piecewise linear maps," International Journal of Bifurcation and Chaos, vol. 24, no. 05, p. 1450071, 2014.

[16] F.-G. Jeng, W.-L. Huang, and T.-H. Chen, "Cryptanalysis and improvement of two hyper-chaos-based image encryption schemes," Signal Processing: Image Communication, vol. 34, pp. 45–51, 2015.

[17] C. Li, G. Luo, K. Qin, and C. Li, "An image encryption scheme based on chaotic tent map," Nonlinear Dynamics, vol. 87, no. 1, pp. 127–133, 2017.

[18] S. M. Seyedzadeh and S. Mirzakuchaki, "A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map," Signal Processing, vol. 92, no. 5, pp. 1202–1215, 2012.

[19] P. Zhen, G. Zhao, L. Min, and X. Jin, "Chaos-based image encryption scheme combining dna coding and entropy," Multimedia Tools and Applications, vol. 75, no. 11, pp. 6303–6319, 2016.

[20] Y. Wu, J. P. 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), pp. 31–38, 2011.

[21] Mandal, J.K., Sengupta, M., (2011) "Steganographic Technique Based on Minimum Deviation of Fidelity (STMDF).", Proceedings of Second International Conference on Emerging Applications of Information Technology, IEEE Conference Publications, pp 298 – 301.

[22] Mandal, J.K., Sengupta, M., (2010) "Authentication/Secret Message Transformation through Wavelet Transform based Subband Image Coding (WTSIC)," Proceedings of International Symposium on Electronic System Design, IEEE Conference Publications, pp 225 – 229.

[23] Rubab, S., Younus, M. Improved Image Steganography Technique for Colored Images using Wavelet Transform. International Journal of Computer Applications, Volume 39– No.14, February 2012, 29- 32.

[24] Kapre Bhagyashri, S., Joshi, M.Y. All Frequency Band DWT-SVD Robust Watermarking Technique for Color Images in YUV Color Space. In Proceedings of 2011 IEEE International Conference on Computer Science and Automation Engineering (CSAE), (10-12 June 2011), IEEE Conference Publications, 295 - 299.