A New DWT-Based Random Image Encryption Approach for a Novel Color Image

J. Antonet Navnai Rani[1] X. M.Binisha[2]
[1]PG Scholar [2]Assistant Professor
[1,2]Department of Electronics and Communication Engineering
[1,2]PET Engineering. College, Vallioor, India

Abstract— Image encryption has been an attractive research field in recent years. A new lossless color image encryption algorithm is proposed based on discrete wavelet transform (DWT) and the chaotic tenting map(CTM).The plain-image is first transformed into the frequency domain by DWT. Then the image sub-bands are shuffled by using the key streams generated from CTM and the plain-image. Finally, the image frequencies are transformed back to the spatial domain by using inverse DWT (IDWT). Thus the cipher-image is obtained. The experimental results demonstrate that our presented method is simple, effective, secure and lossless.

Keywords: CTM, IDWT, DWT

I. 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 its 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 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.

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.

Motivated by the above discussions, in this paper, a DWT based lossless encryption algorithm for color images by using CTM is proposed. In our work, the DWT Haar transform is employed. We first convert the plain-image from the spatial domain to the frequency domain by DWT Haar transform. Then key streams are generated from CTM and the plain-image, and used to scramble the image subbands. The resulting cipher-image is obtained via transforming the image frequencies back to the spatial domain. The experimental results demonstrate that our presented method is simple, effective, secure and lossless.

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.

II. Related Work

Survey of existing visible and invisible watermarking techniques is presented here. Both visible and invisible watermarking techniques are implemented either in spatial; domain or transform domain. In spatial domain, watermark is embedded by directly modifying pixel values of cover image. Least Significant Bit insertion is implemented in spatial domain. Thetransform domain watermarking techniques, both cover image and watermark are taken into transform domain and watermark is spread out to entire cover image. Hence these techniques are more secure and more robust [4].

Various transforms like discrete Fourier transform (DFT), discrete Cosine transform (DCT), continuous Wavelet transform(CWT), discrete Wavelet transform (DWT), singular value decomposition(SVD) or combinations of different transform are applied to in transform domain to achieve robustness and perceptual transparency. Common method used for visible image watermarking is compress data of cover image and embed it with given payload into cover image [3][6][7].Another approach is to use spread spectrum method to spread the payload on cover image. One more approach is to implement lossless visible DCT based image presented in [10], while removable visible watermarking for greyscale images is presented in [11]. Many existing visible termarking techniques use binary logo embedding. Invisible watermarking techniques presented in [24-25] are resistant to various image attackswatermarking technique [1]. Reversible visible watermarking and lossless recovery of original images is proposed in [8][9]. Visible watermarking for bitmap images is.

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 .

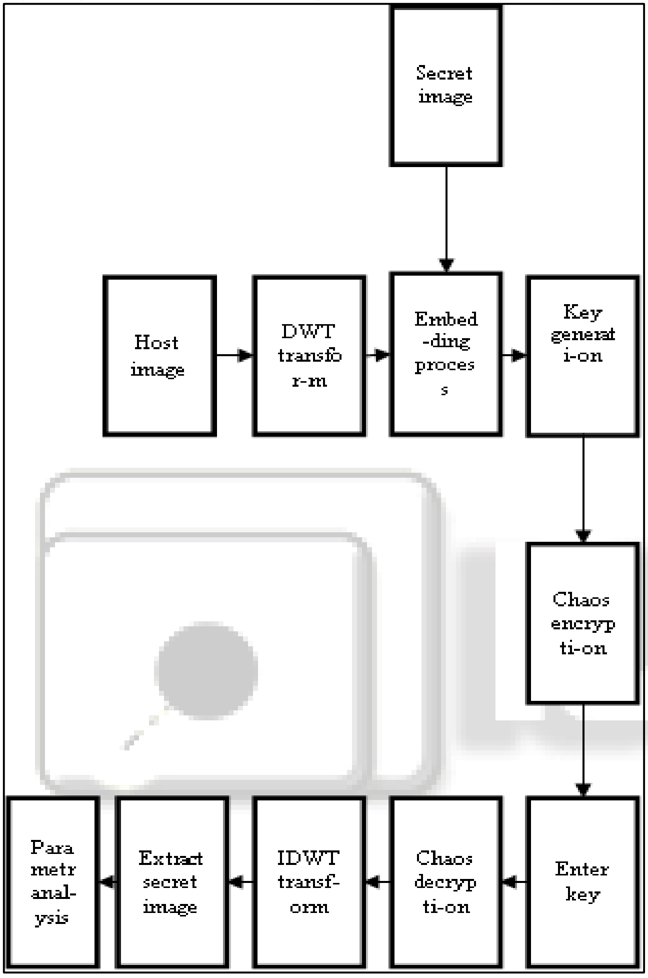


Fig. 1: Block diagram

The 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.

III. Proposed Method

In this paper, a DWT based lossless encryption algorithm for color images by using CMT is proposed. In our work, the DWT Haar transform is employed. First convert the plain-image from the spatial domain to the frequency domain by DWT Haar transform. Then key streams are generated from CMT and the plain-image, and used to scramble the image sub bands.The resulting cipher-image is obtained via transforming the image frequencies back to the spatial domain.

A. *Discrete Wavelet Transform (DWT)*

The DWT represents an image as a sum of wavelet functions, known as wavelets, with different location and scale. It represents the data into a set of high pass (detail) and low pass (approximate) coefficients. The input data is passed through set of low pass and high pass filters. The Daubechies filter coefficients [37] are used for in this work. Filter kernel used for this research work is g 1 1 1 −1i. The output of high pass and low pass filters are down sampled by 2. The output from low pass filter is an approximate coefficient and the output from the high pass filter is a detail coefficient. This procedure is one dimensional (1-D) DWT and Figure 2.10 shows the schematics of this method.

The first level of a DWT decomposition showing each of LL, LH, HL, and HH sub-bands. In order to perform an absolute reconstruction process, the following wavelet equations are required:

$$\{Lo\_D(z)Hi\_D(z) + \ Lo\_R(z)Hi\_R(z)\} = 2$$

$$Lo\_R(z) = z^{-k}Hi\_D(-z)$$

$$Hi\_R(z) = z^{k}Lo\_D(-z)$$

Where $Lo\_(z)$ and $Hi_D(z)$indicate the decomposition wavelet filters, and $Lo\_R(z)$ and $Hi\_R(z)$ represent the reconstruction wavelet filters.
Haar wavelet filters are given in the following equations:

$$Lo\_D(z) = \frac{1}{2}(1 + z^{-1})$$

$$Hi\_D(z) = (z + 1)$$

$$Hi\_R(z) = \frac{1}{2}(z - 1)$$

$$Lo\_R(z) = (z^{-1} - 1)$$

B. *Data Insertion Technique*

Here choose approximation band for hide the secret data.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.

C. RT-Enhanced CTM Algorithm

1) Encryption System

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 permutate nonsquare images. Mathematically, we describe it as

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

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.

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

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.

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

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

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

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.

2) 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.

IV. RESULT 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. 4(a) with its histogram. Apply DWT on cover image shown in Fig. 4(b). 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. 4(d). Finally, the complete encrypted image and its histogram has been given in Fig. 4(e) and Fig. 4(f) respectively. As a comparison to the original plain image, the decrypted image and its corresponding histogram are shown in Fig. 4(g) and Fig. 4(h) respectively
The performance was compared using standard parameters, namely, PSNR, MSE. 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).

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.

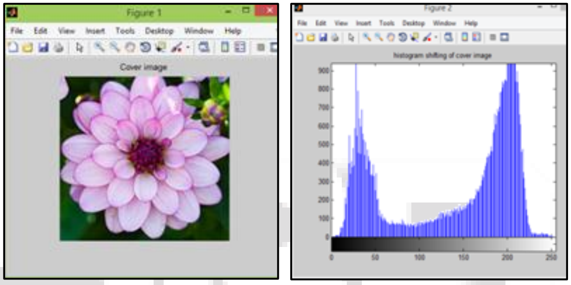


Fig. 4(a): Coverimage and its histogram shifting

After select the cover image apply DWT transformation for split the image into four band using haar wavelet. Then select LL band for hide the secret images.

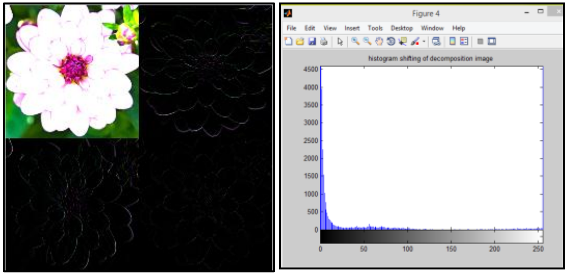


Fig. 4(b): DWT transformation and its histogram shifting

Two images are 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.

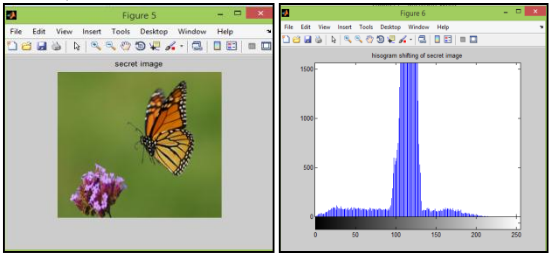


Fig. 4(c): seceret imagesand its histrogram shifting

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.

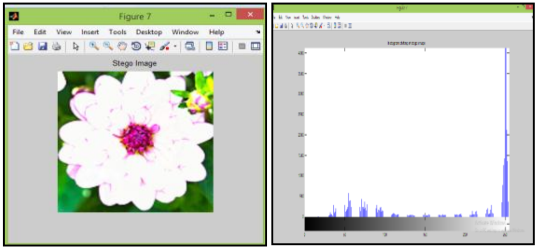
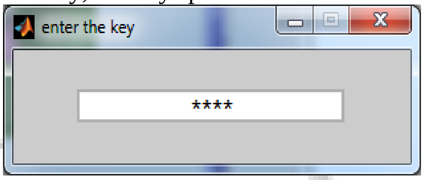


Fig. 4(d): stegoimage and its histogram shifting

A. Secret Key:

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.


enter the key

****

Fig. 4(e):Secret key for encryption

The 2D-RT is an extension of the Arnold map and it can directly be used to permutate nonsquare 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.

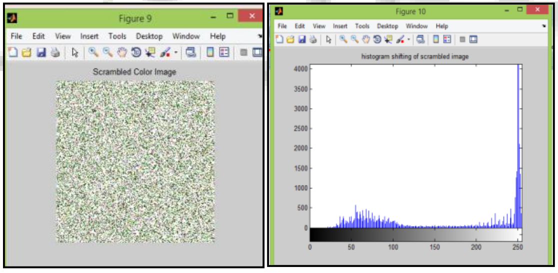
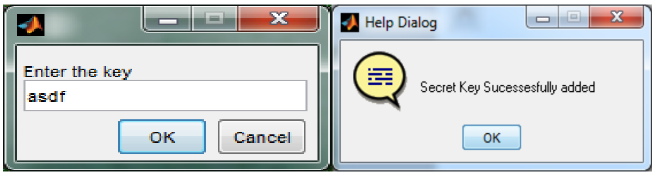


Fig. 4(f): scrambled image and histogram shifting

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


Enter the key

asdf

OK Cancel

Help Dialog

Secret Key Sucessesfully added

OK

Fig. 4(g): secret key for decryption

For decryption process new order of permutation will generated that will perform reverse process of 2D_RT algorithm. Then obtain the decryption of each component of RGB. Finally together joint 3 component and obtain the decryption of stego image.

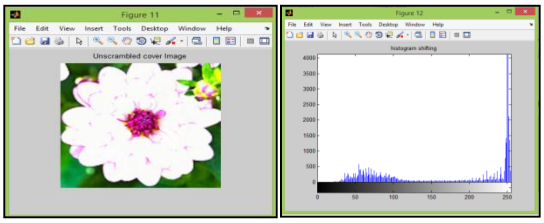


Fig. 4(h): unscrambled cover image and histogram shifting

Apply inverse discrete wavelet transformation process for get the original cover image by using haar wavelet transformation.

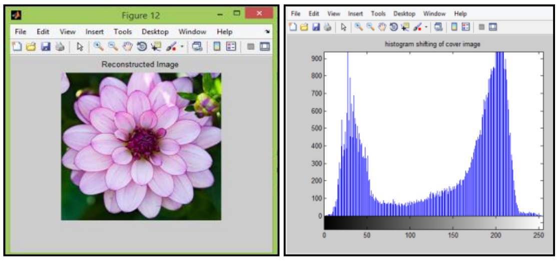


Figure 12
File Edit View Insert Tools Desktop Window Help
Reconstructed Image
histogram shifting of cover image
900
800
700
600
500
400
300
200
100
0
0
50
100
150
200
250

Fig. 4(i): Reconstructed image and its histrogram shifting.

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 .

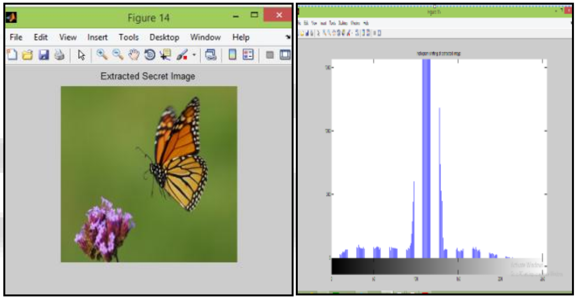


Fig. 4(j): secret images and histogram shifting

B. Quality Measures for Image

1) Visual Quality

The Quality of the reconstructed image is measured interms 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.

	R-Channel	G-Channel	B-Channel
MSE	2.672	5.35	1.67
PSNR	13.903	10.8	15.9008

Table 1: MSE and PSNR values

C. 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 ith gray 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.

D. 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.

Parameters	Values
Entropy	8.58
UACI	0.341
NPCR	0.919

Table 2: Entropy NPCR,UACI scores comparison for different encryption schemes

V. CONCLUSION AND FUTURE WORK

This paper proposes a new lossless color image encryption method based on CTM and DWT. Both CTM and the plain image are employed to generate the key streams, which can enhance the resistance of the cryptosystem against the known-plaintext, chosen-plaintext and chosen-ciphertext attacks. The plain-image is transformed from the spatial domain to the frequency domain via DWT Haar transform. Then use the key streams to shuffle the image sub-bands. The cipher-image can finally be obtained by converting the image frequencies back to the pixel domain. The experimental results show that the proposed encryption scheme is a lossless encryption algorithm and has high security.

The proposed encryption algorithm is robust towards cryptanalysis and also fast making it suitable for real-time encryption and transmission. For future work we have to improve the quality of secret images.

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. 7882.

[9] 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] 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.

[25] Ghoshal, N., Mandal, J.K. A Steganographic Scheme for Color Image Authentication (SSCIA). In Proceedings of International Conference on Recent Trends in Information Technology (ICRTIT 2011), (Madras Institute of Technology, Chennai, India June 03 - 05, 2011), IEEE Conference Publications, 826 – 831.