ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 12, December 2015**

# Multiple Color Images Encryption using Chirikov Standard Map with DWT

**T.Ramashri[1], M.Ashok Kumar[2]**

Professor, Dept. of ECE, SVU College of Engineering, Tirupathi, Andrapradesh, India [1]

M.Tech Student [CS], Dept. of ECE, SVU College of Engineering , Tirupathi, Andrapradesh, India [2]

**ABSTRACT:** An image encryption algorithm to secure three color images simultaneously by combining scrambling with discrete wavelet transform (DWT) is proposed. The three color images to be encrypted are converted to their indexed formats by extracting their color maps, which can be considered as the three components of a color image. These three components are affected each other by scrambling the interims obtained from vertically and horizontally combining the three indexed formats with the help of the chaos-based cyclic shift. The three scrambled components are embedded with the carrier image using DWT. Due to the inherent properties of the chaotic maps, the cipher keys are highly sensitive. Additionally, the cipher image is a single color image instead of three color ones, and is convenient for display, storage and transmission due to the reality property of DWT. Numerical simulations are performed to show the validity of the proposed algorithm.

## I. INTRODUCTION

The past few decades have witnessed the rapid development of the network multimedia, communication and propagation techniques and the exchange of digital information especially images has also greatly increased. Image encryption has become a major task for information security since the issues about illegal data access on Internet are becoming more and more serious. Since optical image encryption system based on double random phase encoding (DPRE) by the Fourier transform was firstly proposed by Refregier and Javidi[1], it has been extended to other optical transform domains[2–10]. With the emergence of color images, color image encryption[11–16]has become an important issue because of the usefulness of the color information in practical applications. The most common method is the multichannel decomposition based on the RGB model or HSI model, however, the complexity and the cost will be increased since multiple channels must be involved during the encryption and transmission processes. A representative method of single-channel color image encryption is based on the digital transformation of the color image to indexed format [16], which is more compact and reliable than the multichannel ones. As a new concept in image encryption field, multiple-image encryption has attracted much attention, which encrypts several different images together. Situ and Zhang[17] firstly employed wavelength multiplexing to realize multiple-image encryption. The qualities of the corresponding decrypted images in the algorithm, however, are not perfect due to the cross-talk effects between images. Subsequently, various multiple-image encryption schemes have been designed [18–28]. The most commonly used for two images is based on the complex function, in which two original images are respectively regarded as the real/amplitude and the imaginary/phase of the complex function. Although it can realize multiple-image encryption through the complex function, it may not be implemented in real time since the encrypted images contain both amplitude information and phase information, which makes it difficult to display, store and transfer. Wang and Zhao [27, 28] proposed the multiple-image encryption method using the phase-truncation and phase retrieval, which makes the cryptosystem nonlinear and the output real-valued. However, the truncated phases as the cipher keys, whose size is the same as the cipher images, need to be transferred to the receivers for decryption, giving rise to increase of the burden of transmission. Besides, the phase-retrieval process is very time consuming.

To display, store and transfer images conveniently, in this paper, we present a new encryption algorithm secure three color images simultaneously by use of scrambling and the discrete wavelet transform (DWT). The encrypted image is a single real-valued color image, which is convenient for display, storage and transmission. Firstly, the three color images to be

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 12, December 2015**

encrypted are separately converted to their indexed formats by extracting their color maps, which can be considered as the three components of a color image. Then two scrambling schemes are implemented to make these three components affect each other by scrambling the interims obtained from vertically and horizontally combining the three indexed formats with the help of the chaos-based cyclic shift. Next, the three scrambled components are embedded in carrier image and transformed with the DWT, in which the generating sequences are determined by the chaotic map. Due to the inherent properties of the chaotic maps, the system is highly sensitive to the cipher keys. Numerical simulation results show the feasibility and the validity of the proposed algorithm. The rest of this paper is organized as follows. Section2reviews the principles of the discrete wavelet transform, the concept of true color and indexed color images, the Chirikov standard chaotic map. The proposed encryption algorithm is also described in Section2. Simulations and discussion are given in Section3. Finally, a brief conclusion is drawn in last section

## II. PRINCIPLES

**i) Discrete wavelet transform**

Sub band coding is based on frequency analysis. Wavelet transform instead is based on the approximation theory. This theory was already used in Fourier expansion coming from the idea that a signal can be expressed as the sum of a series of sines and cosines. However in Fourier analysis only frequency resolution and no time resolution is considered. With Wavelets, both time and frequency variation will be recreated.

The definition of the wavelet transform is:

Where $\alpha_{m,n}$are the wavelet transform coefficients:

**ii) Concept of true and indexed color images**

A true color image can be treated as a three-dimensional (3-D) matrix with each pixel as a triplet corresponding to the values of the primary color components in RGB model, while an indexed color image consists of two 2-D matrices, i.e. an image matrix and a color map matrix. The color map is anM×3 array of class double containing floating-point values in the range [0, 1], whose length M is equal to the numbers of colors it defines. For example, M is 256 for an 8-bit color system. Each row of the color map specifies the red, green and blue components of a single color. An indexed image directly maps the pixel intensity values to the color map values. The color of each image pixel is determined by using the corresponding value of the image matrix as a pointer into color map [24]. After representing an RGB color image with its indexed format, the encryption of the color image can be simplified. Since the color map is uniquely defined for all color images in the same color system and only an indexed image needs to be encrypted, which is straightforward compared with the multichannel encryption. The color image can be retrieved after adding the color map to the decrypted indexed image [16].

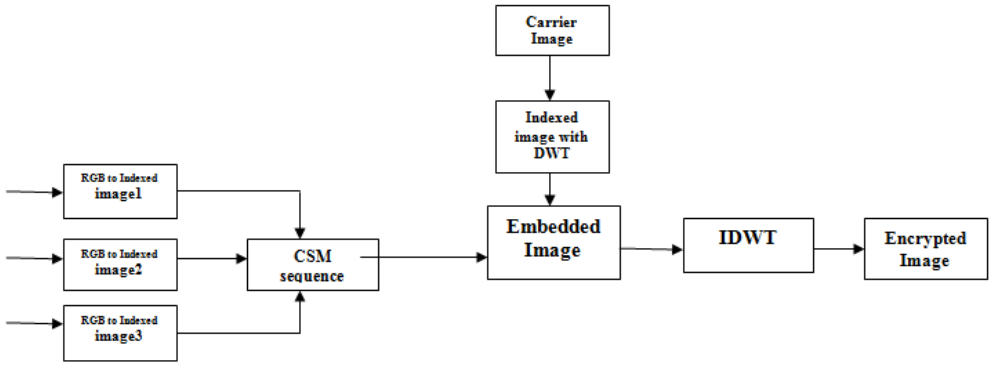



**Fig1:** blockdiagram of encryption algorithm

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 12, December 2015**

### iii) Chirkov standard map

Chirkov standard map(CSM) is an invertible area preserving chaotic map for two canonical dynamic variables from a square with side 2π onto itself i.e.
Where> 0 is the control parameter, and and both take real values in the range [0, 2) for all i. In this paper, the Chirikov standard map will be used twice, which respectively generates the random sequences to be applied to the cyclic shift and the generating sequences.

Where x,y andrepresent the positions of image pixels shifted before and after, respectively. AT is an equal-area transform with periodicity. The period of the transform depends on the size of the image. If an image is scrambled by AT for t times, then the image can be recovered by applying the same AT of (T−t) times, where T is the period. That is, the receiver cannot recover the image correctly without knowing the iteration number t and the period T.

### iv) Description of the encryption algorithm

In the design of three color images encryption, both scrambling and changing pixel values are considered and utilized. Fig. 1gives the flowchart of this proposed encryption algorithm and the details are described as follows:
(1) Generation of indexed color images. Read three color images, and convert these three color images to their indexed formats, which are treated as red, green and blue components of a single color image, respectively.
(2) Cyclic shift. Two scrambling schemes are achieved to make these three components affect each other by scrambling the interims obtained from vertically and horizontally combining the three indexed formats successively, with the help of the chaos-based cyclic shift.

Step 1: Iterate chaotic equation to generate two random sequences of length max{3M+ 1000,N+ 1000}with. Discard the previous 1000 values to avoid the harmful effect and then obtain the sequences x of length 3M and y of length N. Further, two new sequences are generated as:

X=floor (x×) modN, Y=floor (y× ) mod 3M where floor (z) rounds z to the nearest integer toward minus infinity.

Step2: Combine three indexed imagesvertically and get a new matrix F of size 3M×N. Perform the cyclic shift toward the right for each row and the number of shifts is determined by X. After shifting the entire row, do the cyclic shift determined by Y toward the bottom for each column.

Step 3: Decompose the scrambled matrix obtained in Step 2 into three matrices, then combine these three matrices horizontally and get a new matrix of sizeM×3N. Do the same chaos-based cyclic shift for each row and each column of the matrix . Decompose the obtained new matrix into three matricesC1, C2andC3.

(3)The interimsC1, C2andC3are encrypted by the wavelet transform, in which two generating sequences are determined by chaotic sequences for each row and each column. The specific procedures of (i=1, 2, 3) encryption are described as follows:

Step 1: Set the initial values and iterate Eq. (7) max1000+M/2, 1000+N/2 times to get two random sequences. Then select of length and of length and these two sequences are further modified by dividing such that they are distributed in [0,2).

Step 2: Generate two random generating sequences q for the rows and the columns , respectively,

Where m(j) is the values of *i*th state in the random sequence, and L is the length of the random sequence.
Step 3: Set the fractinal orders . Then perform wavelet transforms and corresponding random GS for each row and each column, respectively. The obtained result is denoted as.
The decryption process is the inverse of the above steps. However, in the final step of decryption, the color maps are added to the segregated images to obtain the original RGB images as the outputs.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

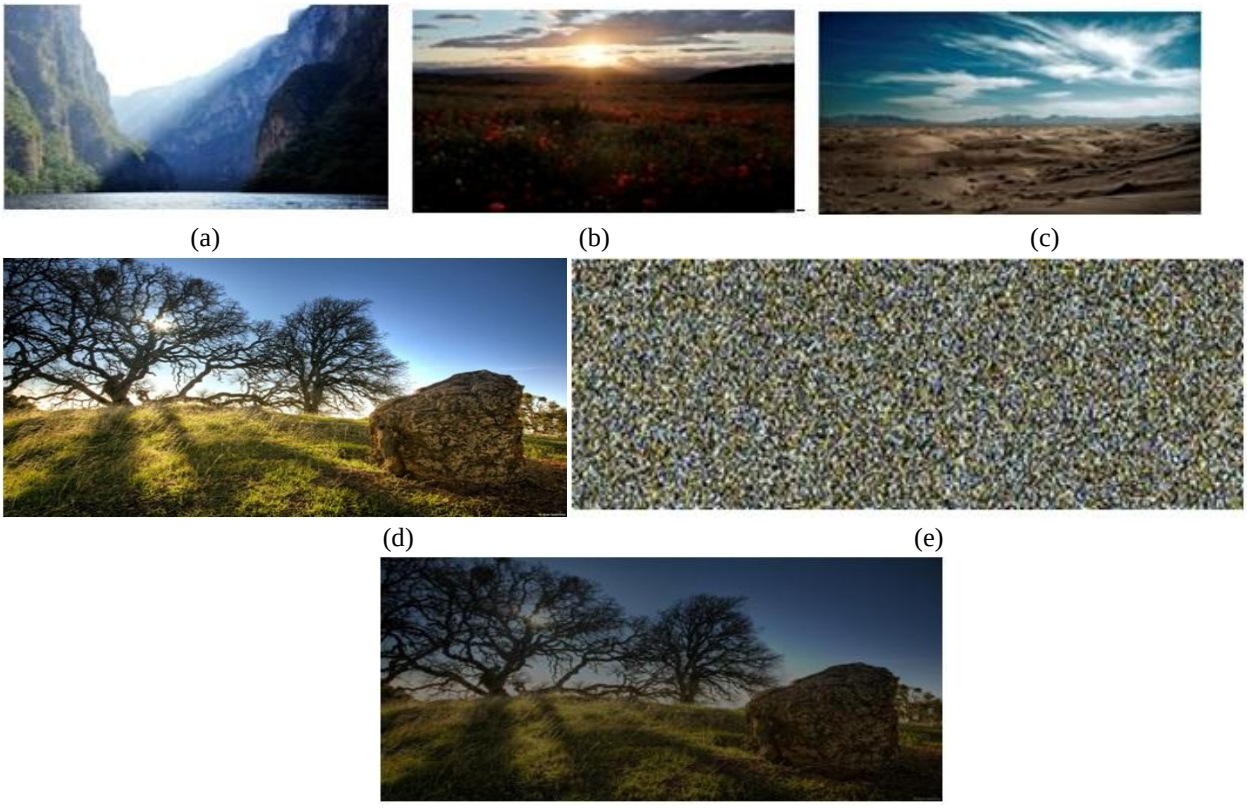
International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 12, December 2015**

### III. SIMULATIONS AND DISCUSSION

Numerical simulations are performed to check the validity of the proposed encryption algorithm. Three typical color images sized 256×256×3 shown in Fig.2(a)–(c) are chosen as the test plaintexts. The initial values and the control parameters of the Chirikov standard map are set as= 0.1234,= 0.2345, =0.4567,= 0.5678 and = 0.3456. The fractional orders and the iteration numbers are set as= 0.6867,= 0.7278 and = 23,= 45 and = 62, respectively. The final cipher color image is displayed in Fig. 2(d). The decrypted images with thecorrect keys are shown in Fig. 2(e)–(g), which demonstrates the lossless decrypted images.



(a) (b) (c)

(d) (e)

(f)

**Fig 2**(a-c): input images, (d): carrier image,(e): scramble image, (f): encrypted images

**i) Key space**

Because of the insensitivity, the fractional orders are not used as the cipher keys. Our encryption algorithm has the following secret keys: (1) given initial values and control parameter ; (2) iteration numbers and . For the initial values and the control parameter of the Chirikov standard map, if the precision is, then the key space will be and the iteration numbers as well, which is large enough to resist the exhaustive attack.

**ii) Correlation**

The correlation between two pixels describes how these are related. If the correlation value is high then these are correlated otherwise uncorrelated. The correlation coefficient is calculated by following Eq. and the results are compiled in tables in simulated result section.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 12, December 2015**

Where () denotes a pair of adjacent pixels, N is the total number of adjacent pixels pairs

,

From Table, one can see clearly that the correlation coefficients and PSNR values of encrypted image are much closer to those in the original images. That is to say, the attacker cannot obtain any information of the original images though statistical analysis.

**iii) Peak signal to noise ratio**

PSNR is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. The PSNR of the fusion result is defined as follows:

PSNR= 20

Here is the maximum componentvalue of the pixels in the encrypted image. Higher the value of the PSNR, better the Performance of the encryption algorithm.

| Set of Images | PSNR | Correlation coefficient |
|---|---|---|
| First set | 63.5695 | 0.7658 |
| Second set | 65.2654 | 0.7854 |
| Third set | 64.8458 | 0.7685 |
| Fourth set | 66.5486 | 0.7864 |
| Fifth set | 64.6548 | 0.7636 |
| Sixth set | 65.2456 | 0.7824 |

Table: PSNR & correlation coefficient values retrieved images

## IV. CONCLUSIONS

We have demonstrated a method to encrypt three color images by use of scrambling and the discrete wavelet transform, which is a kind of encryption with secrecy of pixel values and pixel positions simultaneously. Each color image is firstly converted to its indexed image. The encryption process is only done to their indexed images, due to the color map is uniquely defined for a given color system. During the encryption, two scrambling schemes are achieved to make these three indexed images affect each other by scrambling the interims obtained from vertically and horizontally combining the three indexed formats with the help of the chaos-based cyclic shift. The designed encryption algorithm fully considers the space domain and the frequency domain, so it is more secure than the pure encryption operation based on the DWT. This encryption algorithm makes it convenient to display, store and transfer. The simulation results and discussions demonstrated that this method not only can encrypt and decrypt three color imageseffectively, but also has large key space to resist the exhaustive attack and sensitivity to the keys thanks to the chaotic properties.

## V.FUTURE SCOPE

We can extend the encryption algorithm by using different sizes of colour images and other transforms with different key sensitive parameters.

## REFERENCES

[1] P. Refregier, B. Javidi, Optical image encryption based on input plane and Fourier plane random encoding, Opt. Lett. 20 (1995) 767–769.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 12, December 2015**

[2] G. Unnikrishnan, J. Joseph, K. Singh, Optical encryption by double-random phase encoding in the fractional Fourier domain, Opt. Lett. 25 (2000) 887–889.
[3] S.C. Pei, W.L. Hsue, The multiple-parameter discrete fractional Fourier transform, IEEE Signal Proc. Lett. 13 (2006) 329–332.
[4] Z.J. Liu, S.T. Liu, Random fractional Fourier transform, Opt. Lett. 32 (2007) 2088–2090.
[5] N.R. Zhou, T.J. Dong, J.H. Wu, Novel image encryption algorithm based on multiple-parameterdiscrete fractional random transform, Opt. Commun. 283 (2010) 3037–3042.
[6] L.F. Chen, D.M. Zhao, Optical image encryption based on fractional wavelet transform, Opt. Commun. 254 (2005) 361–367.
[7] D.M. Zhao, X.X. Li, L.F. Chen, Optical image encryption with redefined fractional Hartley transform, Opt. Commun. 281 (2008) 5326–5329.
[8] R. Tao, J. Lang, Y. Wang, The multiple-parameter discrete fractional Hadamard transform, Opt. Commun. 282 (2009) 1531–1535.
[9] J.H. Wu, L. Zhang, N.R. Zhou, Image encryption based on the multiple-order discrete fractional cosine transform, Opt. Commun. 283 (2010) 1720–1725.
[10] N.R. Zhou, Y.X. Wang, L.H. Gong, Novel optical image encryption scheme based on fractional Mellin transform, Opt. Commun. 284 (2011) 3234–3242.
[11] M. Abuturab, Color image security system based on discrete Hartley transform in gyrator transform domain, Opt. Laser Eng. 51 (2013) 3117–3324.
[12] W. Chen, C. Quan, C.J. Tay, Optical color image encryption based on Arnold transform and interference method, Opt. Commun. 282 (2009) 3680–3685.
[13] N.R. Zhou, Y.X. Wang, L.H. Gong, X.B. Chen, Y.X. Yang, Novel color image encryption algorithm based on the reality preserving fractional Mellin transform, Opt. Laser Technol. 44 (2012) 2270–2281.
[14] L.S. Sui, B. Gao, Color image encryption based on gyrator transform and Arnold transform, Opt. Laser Technol. 48 (2013) 530–538.
[15] H. Liu, H. Nan, Color image security system using chaos-based cyclic shift and multiple-order discrete fractional cosine transform, Opt. Laser Technol. 50 (2013) 1–7.
[16] S.Q. Zhang, M.A. Karim, Color image encryption using double random phase encoding, Microw. Opt. Technol. Lett. 21 (1995) 318–323.
[17] G. Situ, J. Zhang, Multiple-image encryption by wavelength multiplexing, Opt. Lett. 30 (2005) 1306–1308.
[18] M.G. Shan, J. Chang, Z. Zhong, B.G. Hao, Double image encryption based on discrete multiple-parameter fractional Fourier transform and chaotic maps, Opt. Commun. 285 (2012) 4227–4234.
[19] Z. Zhong, J. Chang, M.G. Shan, B.G. Hao, Double image encryption using double pixel scrambling de random phase encoding, Opt. Commun. 285 (2012) 584–588.
[20] X.Y. Shi, D.M. Zhao, Y.B. Huang, J.J. Pan, Multiple color images encryption by triplets recombination combining the phase retrieval technique and Arnold transform, Opt. Commun. 306 (2013) 90–98.
[21] H.J. Li, Y.R. Wang, et al., Double-image encryption by using chaos-based local pixel scrambling technique and gyrator transform, Opt. Laser Eng. 51 (2013) 1327–1331.
[22] Z.J. Liu, J. Dai, X. Sun, S.T. Liu, Triple image encryption scheme in Fourier transform domains, Opt. Commun. 282 (2009) 518–522.
[23] X.Y. Liang, X.Y. Su, et al., Key rotation multiplexing for multiple-image optical encryption in the Fresnel domain, Opt. Laser Technol. 43 (2011) 889–894.
[24] M. Joshi, Chandrashahker, K. Singh, Color image encryption and decryption for twin images in fractional Fourier domain, Opt. Commun. 281 (2008) 5713–5720.
[25] J.H. Wu, X.Z. Luo, N.R. Zhou, Four-image encryption method based on spectrum truncation,chaos and the MODFrFT, Opt. Laser Technol. 45 (2013) 571–577
.[26] Y.S. Zhang, D. Xiao, Double optical image encryption using discrete Chirikov standard map and chaos-based fractional random transform, Opt. Laser Eng. 51 (2013) 472–480.
[27] X.G. Wang, D.M. Zhao, Multiple-image encryption based on nonlinear amplitude-truncation and phase-truncation in Fourier domain, Opt. Commun. 284 (2011) 148–152.
[28] X.G. Wang, D.M. Zhao, Double-image self-encoding and hiding based on phasetruncated Fourier transforms and phase retrieval, Opt. Commun. 284 (2011) 4441–4445.
[29] A.W. Lohmann, D. Mendlovic, Z. Zalevsky, R.G. Dorsch, Some important fractional transforms for signal processing, Opt. Commun. 125 (1996) 18–20.
[30] S.C. Pei, M.H. Yeh, The discrete fractional cosine and sine transforms, IEEE Trans.Signal Proc. 49 (2001) 1198–1207.
[31] G. Cariolaro, T. Erseghe, P. Kraniauskas, The fractional discrete cosine transform, IEEE Trans. Signal Proc. 50 (2002) 902–911