New CA based image encryption-scaling scheme using wavelet transform

Bala Suyambu Jeyaram
Department of Mathematics, IIT Madras
Chennai, Tamil Nadu-600036, India

and

Rama Raghavan
Department of Mathematics, IIT Madras
Chennai, Tamil Nadu-600036, India

ABSTRACT

The wide use of digital images leads to the necessity of securing them when they enter into an insecure channel. Image cryptography plays a vital role in the modern communication. In this paper we propose a new image encryption scaling scheme, which will do both, image scaling and encryption. Cellular automata is used for key generation and wavelet transformation is used for image scaling. Encryption has been done in two steps: one before wavelet transformation and another one after the wavelet transformation. Performance evaluation results clearly show that the proposed method is better in all aspects.

Keywords:

Elementary cellular automata (ECA), wavelet transformation, image scaling, image encryption and decryption.

1. Introduction

Nowadays images are widely used in the communication networks. Even though the computer network has been largely developed, this development is not achieved fully without passive and active attacks. Secure ways of storing and transmitting the images have become the need of the hour. Image cryptography helps to achieve these requirements. The randomness in the encryption method and the size of the encrypted image can be the important parameters as far as the strength of the algorithm and the speed of transmission are concerned. The method of generating pure random numbers is always an open problem. Because of this, researchers are getting motivated to develop new methods to generate good random numbers. Cellular automata(CA) with its simple implementation nature, unpredictability, parallelism and homogeneity are found as very good tools for generating random numbers. Starting from Wolframe [1, 2] many researchers have worked in CA based cryptography. Due to high data redundancy and capacity, images have to be compressed before transmission to increase the speed and reduce the storage place. So the study on image compression has been increased tremendously. There are two types of image compression: lossy and lossless. In lossless compression, we can recover the original image, whereas in the lossy compression, we can recover only similar image of the original image, in which some data would be lost. Each compression type has its own field of applications. In [3, 4, 5, 6, 7], some techniques on image compression have been proposed with good performance on compression. But these methods cannot take care of secrecy and integrity of the travelling images in the communication channel. In the recent years, it is essential to carry out both encryption and compression of the images for secure and fast transmission. A number of image encryption and compression schemes have been proposed [8, 9, 10]. Wavelets [11, 12, 13] are used in signal and image processing as well as in its analysis applications. Several researchers have worked on applications of wavelets in image cryptography[14, 15]. Since wavelet based compressions are generally lossy compressions, they can not be directly used for encryption purpose. At the same time wavelet transformation gives the scaled version of the original image in its approximation coefficients. We can get back the original image using inverse wavelet transform along with its detail coefficients. In [16], we have proposed an image encryption scheme for RGB color images using ECA for key generation and GF(2^8) for encryption and decryption. In [16], we have not dealt with image scaling and the pixel intensity distribution of the encrypted images are not following uniform distribution. In this paper we have proposed a new encryption step along with the encryption step in [16], which fairly produces the uniform distribution in the pixel intensities of the encrypted images. This paper is organized as follows. Section 2 describes the basics of Cellular Automata; section 3 presents some basics of wavelet transformations; Section 4 describes the proposed encryption scheme; In section 5 we present some experimental results and security analyses are given in section 6. Concluding remarks are given in section 7.

2. Cellular Automata

A Cellular Automaton is a mathematical model of a system with discrete inputs and outputs. A cellular automaton (CA) is a finite state machine with infinite, regular lattices that change the states synchronously, according to a local rule. Binary state automaton takes only the states 0 and 1. Elementary Cellular Automata is a one dimensional, binary state CA that uses the nearest neighbors to determine their next state. If a neighborhood has 3 states then there are 2^8=256 elementary CA. The cell i is denoted by (i) and the state of the cell (i) at time t is denoted as S_i^t. The neighborhood of radius r is defined for each cell (i) is defined as $N(i) = ((i-r), .., (i-1), (i), (i+1), .., (i+r))$. The state S_i^{t+1} of the cell i at time $t+1$ depends only on states of its neighborhood at time t i.e., $S_i^{t+1} = f(N(i))$ where f is the transition function, called a rule. When there are n number of states in a neighborhood, the number of rules can be expressed as 2^{2^n}. CA's are classified into two ways in terms of the number of rules used to update the cells. If the same rule is used to update the cells, then the CA is called uniform, in contrast if different rules are used to update the cells, then the CA is called non-uniform. An evolution of rule 30 is given in Figure 1.

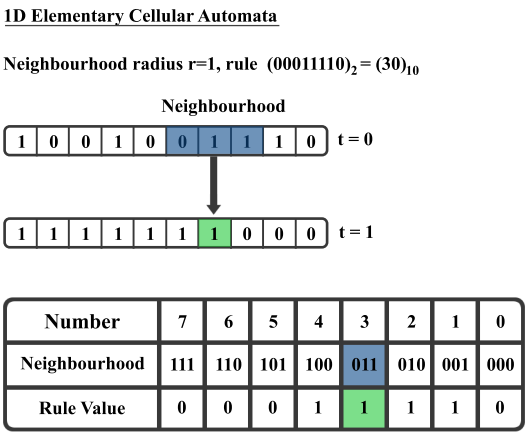

Fig. 1. Example of an evolution of Rule 30

3. Wavelet Transformation

The wavelet transformation W(s,t) of a signal f(x) in terms of an orthonormal basis formed by a mother wavelet family is defined as, $W(s,t) = \int_{-\infty}^{\infty} f(x) \frac{1}{\sqrt{s}} \psi^*(\frac{x-t}{s}) dx; s > 0$, where t corresponds to the translation of the mother wavelet function and s corresponds to the scaling of the mother wavelet. When digital images are to be viewed or processed at multiple resolutions, the discrete wavelet transformation (DWT) is the mathematical tool of choice. Discrete Fourier Transform defined by two straightforward equations that resolve around a single pair of transformation kernals, where as the Discrete Wavelet Transform refers to a class of transformations that differ not only by transformation kernels but also by the nature of these functions and in the way they are applied. We cannot write a single equation for a DWT that completely describes all since it encompasses a variety of unique but related transformations. A transform kernel pair as set of parameters that defines the pair can characterize DWT. The various transforms are related by the fact that their expression functions are small waves of varying frequency and limited duration. The kernel can be represented as these separable 2-D wavelets.
$\psi^H(x,y) = \psi(x)\phi(y)$
$\psi^V(x,y) = \phi(x)\psi(y)$
$\psi^D(x,y) = \psi(x)\psi(y)$, where $\psi^H(x,y)$, $\psi^V(x,y)$ and $\psi^D(x,y)$ are called horizontal, vertical and diagonal wavelets, respectively and one separable 2-D scalling function $\phi(x,y) = \phi(x)\phi(y)$, Each of these 2-D functions is the product of two 1-D real, square integrable scaling and wavelet functions $\phi_{i,j}(x) = 2^{j/2}\phi(2^j x - k)$ and $\psi_{i,j}(x) = 2^{j/2}\psi(2^j x - k)$, where the translation parameter k determines the position of these 1-D functions along the X-axis, the scaling parameter j determines their width-how broad or narrow they are along X and $2^{j/2}$ controls their height or amplitude. The associated expression functions are binary scaling and integer translates of the mother wavelet $\psi(x) = \psi_{0,0}(x)$ and scaling function $\phi(x) = \phi_{0,0}(x)$. The wavelet decomposition of an image is used to analyze the image in low and high frequencies with different resolutions. This information can be used to compress the images.Figure 2 shows the first level approximation,horizontal,vertical and diagonal details of lena image.

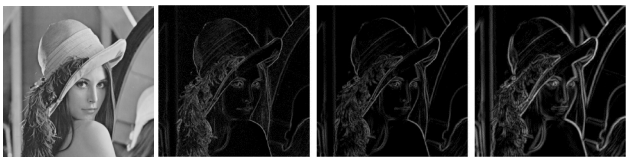

Fig. 2. First level decomposition of lena image

4. Proposed Image Encryption Scheme

In [16] we proposed an encryption method for RGB color images as well as gray scale images. Algorithm 1 given below is proposed in [16].Let P be a gray scale image of size MxN, and Q be the encrypted image encrypted by Algorithm 1 [16].
Algorithm 1:
Input:
1. Plain Image P of size MxN.
2. Key Image K of size MxN.
Output: Encrypted Image Q of size MxN.

Step 1: Input the plain image P to the algorithm.
Step 2: Input the Key Image K.
Step 3: Change the values of the pixels in P to 1 wherever the value is 0.
Step 4: Consider each pixel values of K and P as elements in GF(2^8). Perform the multiplication operation in GF(2^8) between the corresponding elements in P and in the key image K to get the encrypted image Q.
$Q(i,j) = P(i,j) \odot K(i,j)$, where $\odot$ is the element wise multiplication in GF(2^8).
Construct the matrix K_{in} from the matrix K by replacing the elements of K with its multiplicative inverse in GF(2^8).This matrix K_{in} is used as the inverse key image for the decryption in the receiver side. So the original image can be found using the following operations.
$P(i,j) = C(i,j) \odot K_{in}(i,j)$, where $\odot$ is the element wise multiplication in GF(2^8).

Now this Q is considered as the input of the proposed method. Algorithm 2 describes the over all encryption scheme of the proposed method.

Algorithm 2:
Input:
1. Encrypted image Q of size MxN (Output from Algorithm 1)
2. Key image K2 of size M/2 x N/2.
Output: Encrypted image C of size M/2 x N/2.

Step 1: Input the image Q of size MxN.
Step 2: Fix the wavelet for wavelet transformation.
Step 3: Decompose Q using wavelet transformation and get the approximation coefficient matrix QA of Q.
Step 4: Generate the key image K2 of size M/2 x N/2 using ECA as in [16]
Step 5: Do element wise Exclusive OR operation between QA and K2.
Step 6: The resultant M/2xN/2 matrix is the encrypted image C.
Encrypt the plain image P using the key K1 of size MxN as in [16] and get the intermediate encrypted image Q. Decompose Q using wavelet transformation and get C and S. Extract the approximation coefficient matrix QA of Q. Get the encrypted image C using the key K2 as follows:
$C(i,j) = QA(i,j) \oplus K2(i,j)\ \forall\ 1 \leq i \leq M/2$ and $\forall\ 1 \leq i \leq N/2$, In the receiver side the decrypted image can be got as follows: $QA(i,j) = C(i,j) \oplus K2(i,j)\ \forall\ 1 \leq i \leq M/2$ and $\forall\ 1 \leq i \leq N/2$, where $\oplus$ is the element wise Exclusive OR operation. After getting QA, using C and S by applying wavelet reconstruction method we will get back Q. From Q by applying the decryption process described in [16], we will get back the original image P.

5. Simulation Results

Different Gray scale images are used to test the performance of the proposed method. In this paper we have given the test results on Lena images. Figures in 3(a),(b) and (c) show the original, scaled and encrypted as well as decrypted images of the proposed method. This clearly shows the definitive difference between the original and the scaled encrypted images. Figures in 3 (d) and (e) show the encrypted images of the Lena by [16] and by the proposed method. When compare to the existing method, the newly proposed method gives not only a perfectly encrypted image but in addition causes size reduction of the image which helps in increasing the transmission speed.

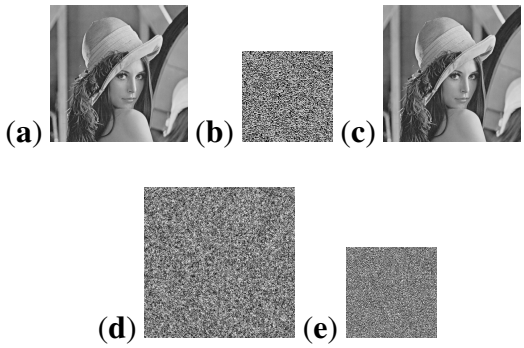

Fig. 3. (a) Original Lena image (b) Encrypted lena image (c)Decrypted lena image (d)Encrypted lena image by existing method (e)Encrypted lena image by proposed method

6. Security Analysis

In this section we carry out the performance analysis of the proposed scheme. We provide: key space analysis, histogram analysis, correlation analysis, key sensitivity analysis. All the experiments are performed on a personal computer with an 3.1 GHz Intel Core Quad Core i5 Processor, 4 GB RAM and 1 TB hard disc with apple i mac operating system.

Key Space Analysis

The key space of a strong encryption algorithm should be very large to make the brute force attack ineffective. Since the proposed method is the extension of the existing method [16], the key space includes the space for both the methods. The key space size of the existing method for a 256x256 gray scale image is 2^{2066} when we fix the third parameter as 1024. The seed to generate M/2xN/2 key image for the proposed method can take 2^{8^N} possible values and the wavelet decomposition vector C as well as the corresponding book keeping matrix S. Excluding C and S, the over all key space size of the newly proposed method for a 256x256 gray scale image is 2^{2066}x2^{2048}=2^{4114}, which is considerably very large to make the brute force attack very hard. This is very larger than the existing system's key space size.

Histogram Analysis

Histogram is the gray value distribution graph, which shows the pixel distribution of an image. If each gray value of the encrypted image has equal probability, then the encryption method is more robust against statistical attack and differential attack. This can be easily checked by the histogram of the encrypted image. That means the histogram of an encrypted image should be uniform for a well encrypted image. Figures 4(a) represent the original Lena image and its histogram chart respy. Figures in 4(b) represent the encrypted Lena of the existing system and its histogram chart respectively. Figures in 4(c) represent the encrypted Lena of the proposed method and its histogram chart respy. It is clear from the figures that the gray value of the encryption image is fairly uniform and significantly different from the gray value distribution of the plain image. And they show that the gray value distribution of the newly proposed method is more fairly uniform than the gray value distribution of the existing method. So this will not provide any hint to perform statistical and differential attacks on the proposed image encryption and compression scheme.

Key Sensitivity Analysis

This section shows the key sensitivity of both encryption key as well as the decryption key. Figure 5 (b) is the encrypted lena image with key K1 and (c) is the encrypted Lena image with key K2. Figure 5(d) shows that the difference between (b) and (c). This clearly shows that the wrong encryption key leads to entirely different image with good difference. Next we encrypted the original Lena image with the encryption key K1 and decrypted with another key K2, which fails to get back the original image. Figures 6(a),(b),(c) show this analysis. From this we can conclude that the proposed scheme is sensitive to both encryption as well as decryption keys.

Correlation Analysis

Plain image and imperfectly encrypted images have correlation between the adjacent pixels, which makes statistical attack possible. We have tested the correlation between horizontally

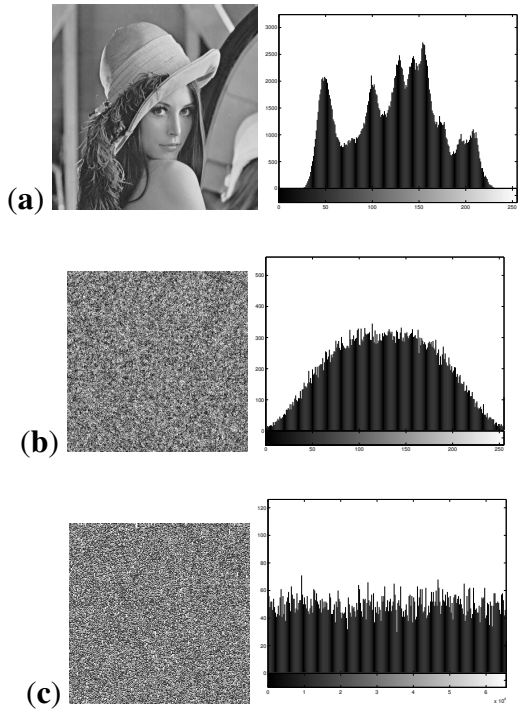

Fig. 4. (a) Original Lena image and its Histogram. (b) Encrypted Lena image and its Histogram in existing system. (c) Encrypted Lena image and its Histogram in proposed system.

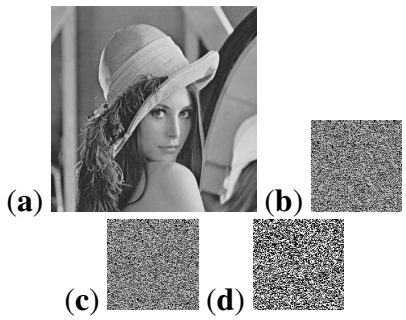

Fig. 5. (a) Original Lena Image. (b) Encrypted image of (a) with key K1. (c) Encrypted image of (a) with key K2. (d) Image difference between (b) and (c).

adjacent pixels, vertically adjacent pixels and diagonally adjacent pixels, to show the diffusion effect of our scheme. We have randomly selected 2000 pairs of adjacent pixels from the plain image and the encrypted image. We have plotted the distribution graph of two horizontally, vertically and diagonally adjacent pixels of the plain image and encrypted image in figure 4. This figure clearly shows that the pixels in the encrypted image are highly uncorrelated. We have also calculated the correlation coefficient of adjacent pixels of the plain image and the encrypted image by the Eqs. (1),(2),(3) and (4). Table 1 shows that the correlation coefficients of two horizontally adjacent pixels, vertically adjacent pixels and diagonally adjacent pixels of original lena image and encrypted image.This confirms that the adjacent pixels in the plain images are strongly correlated where as the adjacent pixels in the encrypted images are weakly correlated. Figure 7 illustrates the

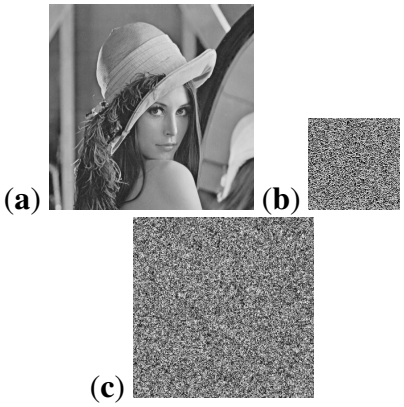

Fig. 6. (a) Original Lena image. (b) Encrypted image of (a) with key K. (c) Decrypted image of (b) with key K3.

correlation distribution of the horizontal adjacent pixels, vertical adjacent pixels and diagonal adjacent pixels of the plain and the corresponding encrypted images using the proposed method. This shows that the encrypted images are very weakly correlated.

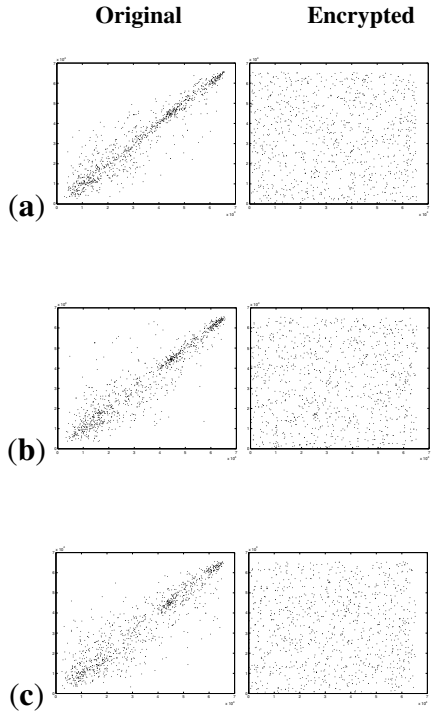

Fig. 7. Correlation Distribution of the pairs of adjacent pixels: (a)Horizontal. (b) Vertical. (c) Diagonal

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{1}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}((x_i - E(x))^2 \tag{2}$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \quad (3)$$

$$\gamma_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (4)$$

Table 1: Correlation coefficients for adjacent pixels between original and encrypted images.

	Horizontal	Vertical	Diagonal
Original Lena Image	0.9385	0.9313	0.8965
Encrypted Lena Image	-0.0216	0.0273	0.0154

Pixel Randomness

Pixels in the perfectly encrypted images are independent identically distributed(i.i.d.) with equal probabilities. Perfectly encrypted images should be indistinguishable with random like images. So it is essential to check the pixel randomness in an encrypted images. Yue Wu et. al., proposed a new test for image randomness in [17]. This is a quality evaluation test for both image shuffling and encryption using pixel differences. Image randomness is encoded within a non-local feature computed from the patchwise difference of a pair of pixels. Patchwise distance of a prescribed configuration is defined below.

The Patchwise Distance: Given a patch configuration P and two distinctive pixels y_l and y_k, their patchwise distance is defined as the average of L^1 norms of corresponding pixelwise distance as shown in equation 5.

$$\rho^P_{l,k} = \sum_{j\in P} \|y_{l+j} - y_{k+j}\|/|P| \quad (5)$$

By simply using the uniform pixel distribution, the random variable of pixel difference distribution for perfectly encrypted images $\varrho^e_{l,k}$ follows the triangular distribution

$$Pr(\varrho^e_{l,k} = d) = \begin{cases} 1/L & \text{, if d=0} \\ 2(L-d)/L^2 & \text{, if d} \in \text{[1,L-1]} \end{cases} \quad (6)$$

with the following mean and variance.

$$\mu_{\varrho^e} = (L^2-1)/(3L) \ and \ \sigma^2_{\varrho^e} = (L^2-1)(L^2+2)/(18L^2) \quad (7)$$

Theoretical numerical values of μ_{ρ^e} and σ_{ρ^e} of binary, 8-bit gray scale, 16-bit gray scale images and the critical values of both the local as well as the global hypothesis tests are given in [17]. Randomness of the encrypted images of our newly proposed encryption method are tested using the algorithm given in [17].

The scores of the two different encrypted Lena images by two different keys K_1 and K_2 are given in the figure 8. The score tells the number of times the image succeed the test in 100 trials.

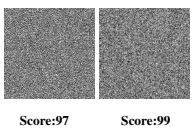

Fig. 8. Encrypted Lena images by two different Keys

7. Conclusion

In this paper, we have proposed a new image encryption scaling scheme with Cellular Automata and Wavelet transformation. In this scheme we have used ECA to generate good random key image and wavelet transformation to carry out image scaling. These two tools together have made a strong encryption-scaling scheme. We have analyzed the proposed scheme by carry out different performance analyses tests to demonstrate the security and strength of the proposed method. Wavelet transformation is used here for image scaling to reduce the size of the image. Our next work is to design a new image cryptosystem for lossless image compression with better randomness in the encryption.

1. REFERENCES

[1] S. Wolfram, Cryptography with Cellular Automata, in advances in cryptology: Crypto '85 proceedings, Lecture notes in Computer Science, vol. 218. Springer; 1986 p.429-32.

[2] S. Wolfram, Theory and Applications of Cellular Automata, Advanced series on complex systems-Volume 1.

[3] Rafael C. Gonzalez and Richard E. Woods, Digital Image Processing, 2nd Edition, Pearson Education 2004.

[4] Bryan Usevitch, "A Tutorial on Modern Lossy Wavelet Image Compression: Foundation of JPEG 2000", IEEE Signal Processing Magazine, 2001.

[5] DONOHO D. Compressed sensing [J], IEEE Transactions on Information Theory, 2006, 52(4): 1289-1306.

[6] S. Singh, V. Kumar, H. K. Verma, " DWT-DCT hybrid scheme for medical image compression", Journal of Medical Engineering and Technology, Volume 31, Issue 2, pp.109-122, March 2007.

[7] Macarena Boix, Begona Canto, Wavelet Transform application to the compression of images, Elsevier, Mathematical and Computer Modelling 52 (2010), 1265-1270.

[8] Debayan Goswami, Naushad Rahman, Jayanta Biswas, Anshu Koul, Rigya Lama Tamang, Dr. A. K. Bhattacharjee, "A Discrete Wavelet Transform based Cryptographic Algorithm", International Journal of Computer Science and Network Security, Volume 11, Number 4, April 2011.

[9] Ch.Samson, V. U. K. Sastry, A Novel Image Encryption Supported by Compression Using Multilevel Wavelet Transform, International Journal of Advansed Computer Science and Applications, Volume 3, Number 9, 2012.

[10] Xiping He, Qionghua Zhang, Image Encryption Based on Chaotic Modulation of Wavelet Coefficients, 2008 Congress on Image and Signal Processing, May 2008, Sanya, Hainan, China.

[11] Robi Polikar, The Wavelet Tutorial, "http://users.rowan.edu/ polikar/WAVELETS/WTtutorial.html"

[12] K. P. Soman, K. I. Ramachandran, Insight into Wavelets from theory to practice, Second Edition, PHI, 2006.

[13] Jatan K. Modi, Sachin P. Nanavati, Amit S. Phadke, Prasanta K. Panigrahi, "Wavelet Transforms- Application to Data Analysis-I", Resonance, Nov.2004.

[14] Zhu Yu Zhou Zhe Yang Haibing Pan Wenjie Zhang Yunpeng, A Chaos-Based Image Encryption Algorithm Using Wavelet Transform, ICACC 2010 IEEE,pp.217-222.

[15] Juan M Vilardy, J. Useche, C. O. Torres and L. Mattos, Image encryption using the fractional wavelet transform, Journal of Physics: Conference Series 274 (2011) 012047.

[16] Bala Suyambu Jeyaram, Rama Raghavan, Krishna Shankara Narayanan, New CA based key generation for a robust RGB color image encryption scheme, International Journal of Computer Applications (0975-8887), Volume 80, Number 7, October-2013.

[17] Yue Wu, Sos Agaian and Joseph P. Noonan, "A novel method of testing image randomness with applications to image shuffling and encryption" proc. SPIE 8755, Mobile Multimedia/Image Processing, Security and Applications, 2013.