New CA based Key Generation for a Robust RGB Color Image Encryption Scheme

Bala Suyambu Jeyaram
Research Scholar
Department of Mathematics
IIT Madras, Tamil Nadu, India

Rama Raghavan
Professor
Department of Mathematics
IIT Madras, Tamil Nadu, India

Krishna Shankara Narayanan
Associate Professor
Department of Computer Science
IIT Bombay, Maharastra, India

ABSTRACT

In the past few years, study of securing the digital images has increased tremendously and several encryption algorithms based on Cellular Automata have been proposed to protect the digital images against different cryptographic attacks. This paper proposes a novel pixel based encryption scheme based on Cellular Automata and Galois Field. Here the random key image has been generated using 1D Cellular Automata and for the encryption purpose GF (2^8) is used. The encryption is done on pixel values of the RGB components separately. Since this cryptosystem uses only logic operations for both key generation and GF (2^8) operations, it requires minimized computational resources and the execution speed is also high. Experimental results exhibit the confusion and diffusion properties of the proposed system. The correlation analysis shows that the proposed scheme has zero correlation amongst adjacent pixels (horizontal, vertical, diagonal).

Keywords:

Elementary Cellular Automata(ECA), Galois Field, RGB color image, random key, image encryption and decryption.

1. INTRODUCTION

These are the days of digital revolution and usage of digital data in different forms especially images has increased tremendously in various domains. It is essential to emphasize, secure digital communication networks with the requirements of secrecy and integrity of the travelling information. Storage and distribution of digital images securely over the networks has become the need of the hour. So the researchers are getting motivated to develop new techniques to achieve these challenges. Encryption is the main technique to protect the digital data. Image encryption has applications in computer networks, medical imaging, telemedicine, military communications and in multimedia. Image encryption has additional requirements due to its size, redundancy and real time applications. Digital images in the sender side are transformed into an unrecognized form using a key for encrypting them. Most of the conventional methods are process-intensive and they will consume more time for encrypting images. Strength of an encryption algorithm mainly rely on the randomness of the key. Generating pure random number is always cumbersome. Cellular automata due to its easy hardware and software implementation, parallelism and homogeneity as well as the unpredictability are good tool for generating random keys. Wolfram first proposed the idea of using CA in cryptography[1, 2], following that many researchers have contributed their works in cryptology using CA[3, 4, 5, 6, 7]. Cellular automata is also being used largely in image cryptography [8, 9], visual cryptography [10, 11, 12] and in image processing [13, 14]. Image cryptography is being done by other methods also[15, 16, 17]. In [17], a chaos based image encryption method has been proposed. The key image has been genereated from a given initial key image using the same encryption method several times to produce randomness in the key image. Apart from the encryption of the original image, key image also undergo the same procedure several times. Every time the key generation process takes more than double the time of an encryption.
This can be reduced using a good random number generator to generate the key image directly. We have overcome this problem using cellular automata and we have come up with a better random key image generator scheme.In this paper a new image cryptosystem has been proposed. CA is used for key generation and GF(2^8) is used for encryption purpose. Computer simulation is performed for confusion and diffusion properties and for other tests. The remaining of this paper is organized as follows. Section 2 describes the basics of Cellular Automata. Section 3 presents the proposed algorithm. Section 4 presents the key generation process. Section 5 describes the experimental results and security analyses are given in section 6. Concluding remarks are given in section 7.

2. CELLULAR AUTOMATA

A Cellular Automaton (CA) is an infinite, regular lattice of simple finite state machines that change their states synchronously, according to a local update rule that specifies the new state of each cell based on the old states of its neighbors. At a particular time each cell in the binary state CA will be in a state 0 or 1 in the simplest case. One-dimensional, binary state CA that use the nearest neighbors to determine their next state are called elementary cellular automata. There are only 2^8 = 256 elementary CA, and it is quite remarkable that one of them is computationally universal. 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.

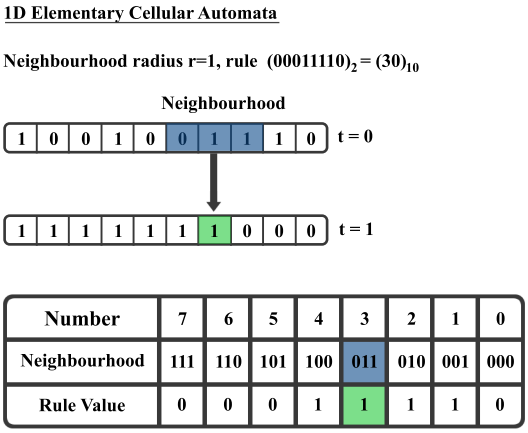

Fig. 1. Example of an evolution of Rule 30

3. IMAGE ENCRYPTION SCHEME

The proposed image encryption algorithm is based on GF(2^8) operations and it generates a high quality pseudo random key image of same size as plain image using CA. An image is represented as a matrix of positive integers. Intensity range of an image depends on the number of bits need to represent a pixel. An 8-bit gray scale image has 256 gray levels. Generally the pixels in an RGB color image represented with 24 bits. Each pixel consists of R(Red), G(Green), B(Blue) components and each R,G and B component is represented by 8-bits. So each color component has 256 values between 0 and 255. Each pixel together with its components represent a color. For example (0, 0, 0) represents a black color pixel where as (255, 255, 255) represents a white color pixel. The basic idea of the proposed method is to change the RGB values of a pixel seperatly using the key image. The operations required in encryption and decryption as well as in key generation consumes less computational time. Algorithm 1 explains the encryption scheme. Galois Field known as finite field, refers to a field in which there exists finitely many elements. It is particularly useful in translating computer data as they are represented in binary forms. That is, computer data consist of combination of two numbers, 0 and 1, which are the components in Galois field whose base field is Z_2. Representing data as a vector in a Galois Field allows mathematical operations to transform data easily and effectively. Since each byte of data is represented as a vector in a finite field, encryption and decryption using mathematical arithmetic is very straight forward and is easily manipulable. Since every element in the field GF(2^8) can be expressed as a 8-bit vector, it is used for our encryption process. Every pixel in the R, G and B components of the plain color image and every pixel in the key image are considered as elements in GF(2^8); then the encryption and decryption are performed.

Algorithm 1:
Input: 1. Plain Image P of size MxN.
2. Key Image K of size MxN.
Output: Encrypted Image C of size MxN.

Step 1: Input the plain image P to the algorithm.
Step 2: Input the Key Image K.
Step 3: For each pixel of P get the RGB components.
Step 4: Change the RGB values of the pixels in P to 1 wherever the value is 0.
Step 5: Consider each pixel values of K and each RGB values of P as elements in GF(2^8). Perform the multiplication operation in GF(2^8) between the corresponding elements in each RGB components and the key image K.
Step 6: Concatenate the encrypted RGB components to get the encrypted image.
Let P(r), P(g), P(b) be the RGB components of P and C(r), C(g), C(b) be the RGB components of the encrypted image. The encrypted image is generated using the following operations.
$C(r) = P(r) \odot K$
$C(g) = P(g) \odot K$
$C(b) = P(b) \odot K$, 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.
$P(r) = C(r) \odot K_{in}$
$P(g) = C(g) \odot K_{in}$
$P(b) = C(b) \odot K_{in}$, where $\odot$ is the element wise multiplication in GF(2^8). Figure 2 explains the proposed method pictorially. To strengthen the proposed method, one can use different key to encrypt different components.

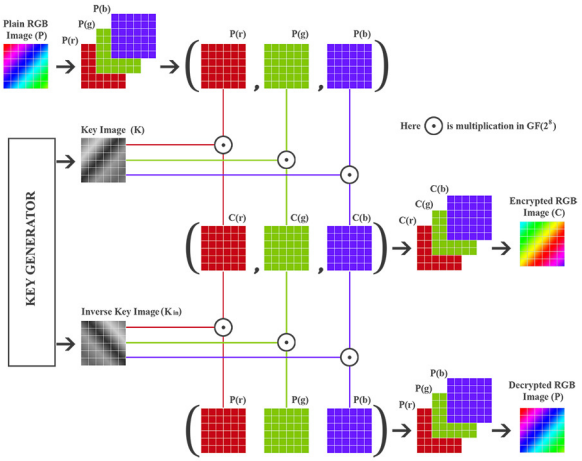

Fig. 2. Proposed encryption and decryption Process

4. KEY GENERATION:

It is well known that the encryption algorithms are not considered as secret parameter where as the key is. So the key should be strong

enough to break. To make the attackers enter into an exhaustive search in the key space, the key should be random. This will lead to the computational infeasible situation when the key space is large enough. In this section, a new key generation algorithm has been proposed to generate high quality pseudo random numbers. Cellular automata due to its unpredictability, is a good source to generate pseudo random numbers.

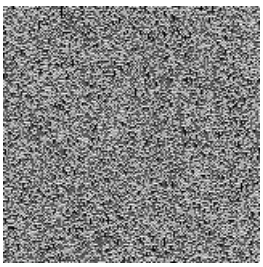

Fig. 3. A key image generated by proposed method

To generate the key for a plain image of size MxN, a pseudo random number of size Nx8 is used. This is used as the seed for generating high quality random key image for our encryption method. Considering this seed as the initial state of the ECA, the consecutive evolutions are performed using a chosen rule. Any consecutive M number of evolutions are taken for the key image, which is a matrix of size Mx(Nx8). This matrix is now resized to MxN matrix (8-bits in each position) and is used as the key image. Figure 3 shows a key image which is generated by our proposed method.

5. EXPERIMENTAL RESULTS

This section details the simulations which are conducted to test various properties of the proposed method. RGB color images are used for visual testing. Figure 4 shows these test images: Lena, Car along with their encrypted images using the proposed method. This figure clearly shows that there is perceptual difference between the original images and their encrypted images.

Fig. 4. (a) Original Lena and its encrypted image. (b) Original car and its encrypted image.

We have used Number of Pixels Change Rate (NPCR) to measure the amount of difference between the encrypted images and the original images. NPCR gives the percentage of different pixels between the two images. Let P(i, j) and C(i, j) be the pixel values of plain and encrypted images P and C at the ith row and the jth column position respectively. Equation 1 gives the mathematical expression of the NPCR measure.

$$NPCR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{M \times N} \times 100\% \quad (1)$$

Where $D(i,j) = 0$ when $P(i,j) = C(i,j)$ otherwise $D(i,j) = 1$. NPCR values should be as large as possible to approach the performance of an ideal image encryption method. NPCR values between plain and encrypted images of of Lena and car images are calculated using equation 1 and found 0.9944 and 0.9947 respectively. In all the cases the values are very close to unity. Percentage values of the NPCR measure is directly proportional to the amount of changes in the pixel values between the two images.

6. SECURITY ANALYSIS

Security is an essential tool in cryptology. A strong image encryption scheme should resist various kinds of attacks such as known plain text attack, cipher text only attack, brute force attack and statistical analysis attack. This section presents the key space analysis and statistical analysis on the proposed image cryptosystem against different attacks.

6.1 Key Space Analysis

A secure image encryption algorithm should have large key space to make the brute force attack computationally infeasible. Theoretically the proposed method can include an infinite key space due to the third parameter of the key triplet (seed, rule, R_{min}). For an 8 bit RGB color image of size MxNx3, the seed can take 2^{8N} possible values and ECA rule can take 2^{2^3} possible values. With these two parameters, the key space size is 2^{8N} x 2^{2^3} keys. The third parameter has no limit as it specifies the starting number of ECA evolutions, i.e. it can be as large as possible. So one can easily see that the size of the key space can be considerably large when R_{min} value is large. As an example, consider an RGB image of size $256 \times 256 \times 3$, so the seed size is 256×8 bits, rule size is 2^8 and by taking R_{min}=1024, the key space size is equal to $2^{256\times8}$ x 256 x $1024 = 2^{2066}$. For the large image and with the large R_{min} value the size of the key space will be very large. So the key space is large enough for exhaustive search in brute force attack. Size of the key space will be tremendously increased when different keys are used for different components.

6.2 Confusion property:

Confusion means making the key and the cipher text as irrelevant as possible. Attackers will not be able to get the key from the cipher text. Histogram is a graph between the pixel values and the number of pixels in an image. Histograms of the original test images and their corresponding encrypted images are shown in Figures 5 and 6. The histograms of the encrypted images are almost similar regardless of the plain images and at the same time the histograms of the encrypted images greatly differ from those of the plain images. These results clearly establish the confusion property of the proposed method.

6.3 Diffusion Property

Diffusion refers to making the relationship between the plaintext and the ciphertext as complex as possible. This tells that the small change in the plain text or in the key will make significant change

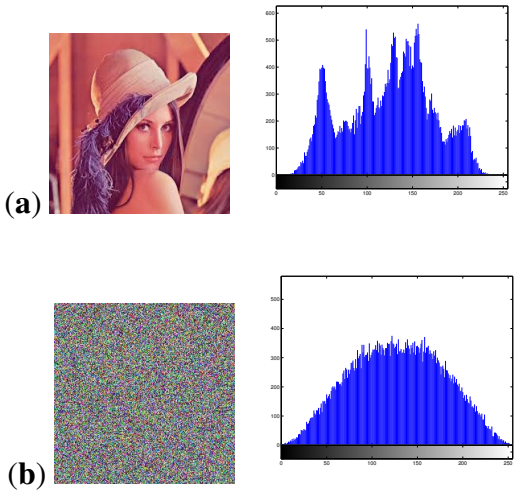

Fig. 5. (a) Original Lena image and its Histogram. (b) Encrypted Lena image and its Histogram.

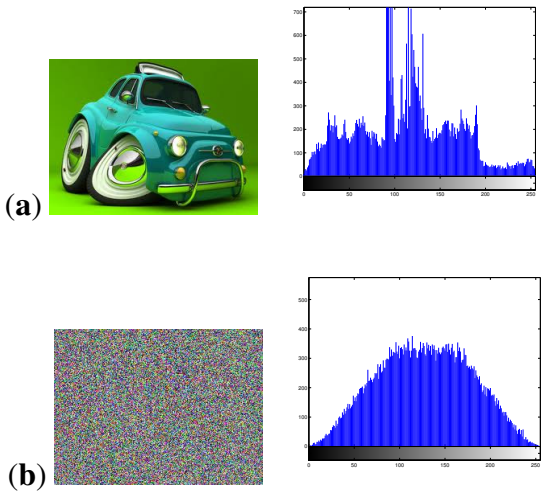

Fig. 6. (a) Original car image and its Histogram. (b) Encrypted car image and its Histogram.

in the cipher text. This property can be exhibited by the key sensitivity test. This means that any small change in the key lead to a significant change in the encrypted or decrypted images. We have performed two tests to illustrate the key sensitivity of our method. The first test is to show the change in the encryption process. The original image P is encrypted using the key K1= (seed1, rule1, $R_{min}1$) and the same image is encrypted using another key K2 which differs in any one of the parameters in K1. Figure 7 Shows the original image and their encrypted image using two different keys K1 and K2 as well as the difference between the encrypted images. It clearly shows that the image encrypted by the key K1 differs largely from the image encrypted by the key K2.
The second one shows the key sensitivity in the decryption process. This has been tested by changing one parameter at a time. Let the plain image P be encrypted using the key K = (seed, rule, R_{min}) to get the encrypted image E. This image E is decrypted using three different keys K1, K2 and K3 separately by changing one parameter in K and by keeping the other two unchange. The experimental results are given in Figure 9. This shows that a small change in any one parameter in the key triplet does not succeed to get the plain image. Figure 8 shows the strength of the proposed method when the related images are encrypted using the same key. Figure 8(a) and 8(c) are related Lena images, figure 8(b) and 8(d) are their encrypted images using the same key. Figure 8(e) shows their difference visually. This clearly shows that the encryption of the related images are not related.

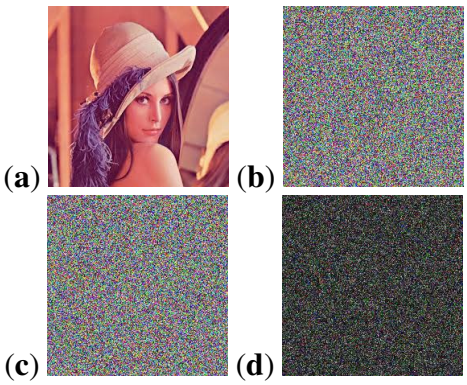

Fig. 7. (a) Original Lena Image. (b) Encrypted image of (a) with key K1. (c) Encrypted image of (a) with key K2. (d) Image difference between (b) and (c).

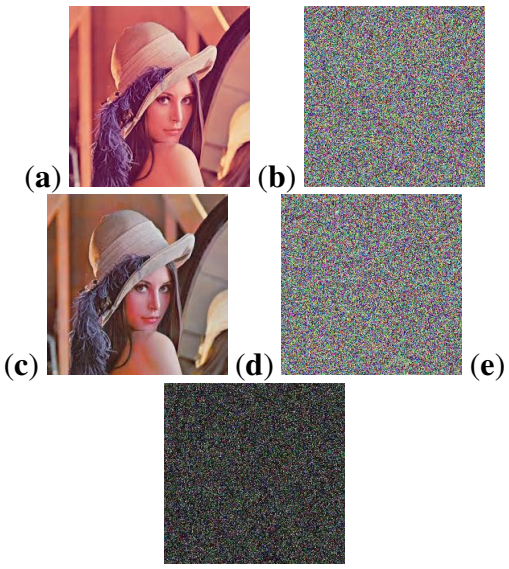

Fig. 8. (a) Original Lena1 image. (b) Encrypted image (a) with key K. (c) Original Lena2 image. (d) Encrypted image (c) with key K. (e) Image difference between (b) and (d).

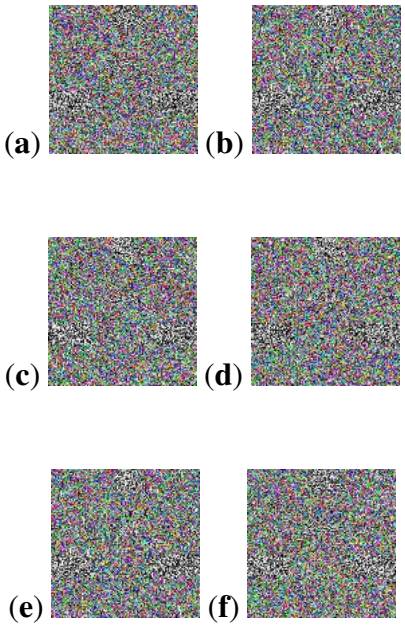

Fig. 9. (a) Encrypted image with K1=(seed1, rule1, $R_{min}1$). (b) Decrypted image with K2=(seed2, rule1, $R_{min}1$). (c) Encrypted image with K1=(seed1, rule1, $R_{min}1$). (d) Decrypted image with K2=(seed1, rule2, $R_{min}1$). (e) Encrypted image with K1=(seed1, rule1, $R_{min}1$). (f) Decrypted image with K2=(seed1, rule1, $R_{min}2$).

6.4 Statistical Analysis

The statistical analysis has been done to demonstrate the high quality confusion and diffusion properties of the proposed system. This has been done by the test on the correlations of adjacent pixels in the encrypted image. Lena and car images are used to perform this test. Generally,pixels chosen arbitrarily from an image will be strongly correlated with its adjacent pixels either in horizontal, vertical or diagonal. A secure image cryptosystem should always produce encrypted images having low correlation between adjacent pixels. 1000 random pairs of adjacent pixels have been chosen horizontally, vertically and diagonally from the plain and encrypted images. The correlation coefficient has been computed between two adjacent pixels using the equation 5.

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

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}((x_i - E(x))^2 \tag{3}$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{4}$$

$$\gamma_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{5}$$

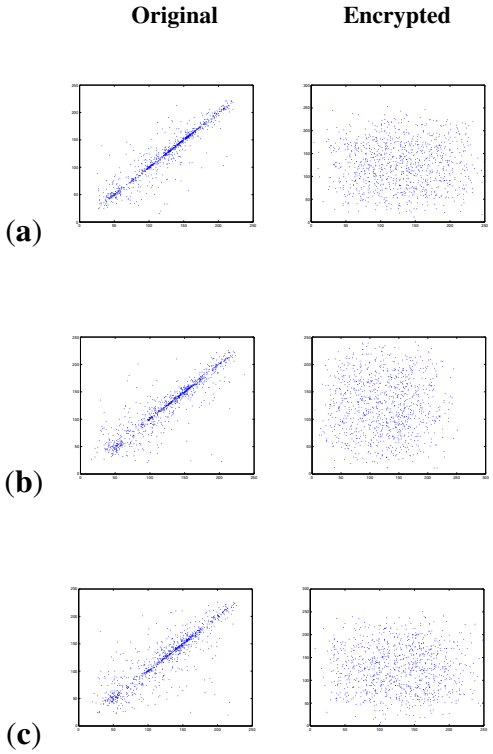

Fig. 10. Correlation Distribution of the pairs of adjacent pixels: (a)Horizontal. (b) Vertical. (c) Diagonal

Table [1] gives the correlation coefficient values of adjacent pixels in the RGB components along horizontal, vertical and diagonal directions of the plain and encrypted images. 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 10 illustrates the correlation distribution of the horizontal adjacent pixels of the R components, vertical adjacent pixels of the G components and diagonal adjacent pixels of the B components of the plain and the corresponding encrypted images using the proposed method. We can clearly see that the encrypted images are very weakly correlated.

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

	Horizontal	Vertical	Diagonal
Original Lena Image	0.9614	0.9287	0.9118
Encrypted Lena Image	-0.0199	-0.0212	0.0245
Original car Image	0.8891	0.9217	0.8532
Encrypted car Image	-0.0010	0.0068	-0.0064

7. CONCLUSION

In this paper, a simple image encryption method is proposed which is highly secured due to its key generation using cellular automata. Some rules of ECA are able to produce high quality pseudo random numbers, which are used for the key generation process and this makes the proposed method a strong one. The method of key generation proposed in this paper is novel and substantially different from any of the existing key generation techniques. It is also ensured that the key is more secure and rigit. Numerical results of our experiments demonstrate the robustness of the method against different attacks. The simple operations involved in encryption and decryption process make it easy in both software and hardware implementations which makes this scheme suitable for real time applications.

8. 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] Chen RJ, Lai JL, Image security system using recursive cellular automata substitution, Pattern Recognition 2007; 40(5): 1621-31.

[4] Jun Jin, An image encryption based on elementary cellular automata, Optics and Lasers in Engineering 50 (2012) 1836-1843.

[5] S. Nandi, B. K. Kar, P. P. Chaudhuri, Theory and applications of cellular automata in cryptography, IEEE Transactions on computers 43(1994) 1346-1357.

[6] J. Kari, Cryptosystems based on reversible cellular automata, Personal communication,1992.

[7] P. Guan, Cellular automata public key cryptosystem, Complex system. 1(1987) 51-56.

[8] F. Maleki, A. Mohades, S. Mehdi Hashemi, M. E. Shiri, An Image Encryption System by Cellular Automata with Memory, The Third International Conference on Availability, Reliability and Security, IEEE Computer Society, 2008.

[9] Chen Rong-Jian, Horng Shi-Jinn. Novel SCAN and 2-D Von Neumann cellular automata. Signal Process: Image Commun, 2010;25(6): 413-26.

[10] F. Seredynski, P. Bouvry, A. Y. Zomaya, Cellular automata computations and secret key cryptography, Parallel Computing 30 (2004) 753-766.

[11] Jin Jun, Wu Zhi-Hong, A secret image sharing based on neighborhood configurations of 2D-Cellular automata, Optics and Lasers in Technology. 2012; 44(3): 538-48.

[12] Eslami Z, Razzaghi SH, Ahmadabadi J, Secret image sharing based on cellular automata and stegnography, Pattern Recognition 2010; 43(1): 397-404.

[13] Rosin Paul L, Image Processing using 3-state cellular automata, Comput.Vis. Image Understand. 2010; 114(7): 790-802.

[14] Cappellari L, Milani S, Cruz-Reyes C, Calvagno G. Resolution scalable image coding with reversible cellular automata. IEEE Trans Image Process 2011; 20(5): 1461-8.

[15] Chen. G,Mao Y,Chui CK, Asymmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons and Fractals 2004; 21: 749-61

[16] K. Loukhaoukha, J. Y. Chouinard, A. Berdai, A secure Image Encryption Algorithm Based on Rubik's Cube Principle, Hundawi Publishing Corporation, Journal of Electrical and Computer Engineering, Volume 2012, Article ID 173931, 13 pages.

[17] N. A. Al-Romema, A. S. Mashat, I. AlBidewi, New Chaos-Based Image Encryption Scheme for RGB Components of Color Image.,Computer Science and Engineering 2012, 2(5): 77-85.