**Contemporary Engineering Sciences, Vol. 8, 2015, no. 35, 1693 - 1701**
**HIKARI Ltd, www.m-hikari.com**
**http://dx.doi.org/10.12988/ces.2015.510285**

# Color Image Encryption by Cellular Automata

**José Cruz Martínez Perales**

Instituto Politécnico Nacional
Escuela Superior de Cómputo
Av. Juan de Dios Batíz, esq. Miguel Othón de Mendizábal
Ciudad de México 07738, México

**Abstract**

This paper presents a proposed cryptosystem to encrypt color images using cellular automata. A reversible cellular automaton has the characteristic of being able to return in the evolution of the automata, and is therefore, that in this paper are used to generate a symmetric key used to encrypt images.

**Keywords:** Cryptosystem, encryption image, cellular automata, symmetric key

# 1. Introduction

Due to the high technology boom that has been developed in the computer field, the need arises to safely protect the information transmitted through the network. In this way computer algorithms have been developed whose aim is to encrypt and decrypt information that send by a channel of information, the development of these computational algorithms are known as cryptosystems. The main problem that have attacked the developing cryptosystems is to encrypt and decrypt textual information, but the problem of development of cryptosystems is more extensive, ranging from encryption and decryption of text information, sound, images, etc. [1, 2, 3, 4].

Algorithms such as AES and DES are widely used to encrypt information. Both algorithms were developed in the United States, on the other hand, the DES algorithm came to be used effectively, however, certain details are found in the design algorithm as the fact of having a key length relatively short, in addition to this algorithm was exposed to intense analysis of brute force to find the key, This motivated the development of cryptosystems, born the concept of block cryptosystems such as the AES [5, 6, 7].

On the other hand, cellular automatas are mathematical tools that were considered outside the development of cryptosystems, but, its effectiveness has been applied to the encrypted and decode information [8, 9].

In this paper is presented a proposed cryptosystem implemented with reversible cellular automata with memory, applied to process images of any size in both dimensions and number of pixels and the generation of a variable key size providing greater security to our information.

# 2. Cellular automata

Then comes the definition of what a cellular automaton is.

A cellular automaton is a reticulated represent a discrete dynamical system which is composed of a finite number of objects called cells, which are defined by a finite number of states.

Mathematically a cellular automaton is defined as $LA = (\mathcal{C}, \mathcal{S}, \mathcal{V}, f)$, where:

- $C$, it is the cell space formed by $n$ cells.
- $S$, is the set of states that can take each of the cells of the space $S = \mathbb{Z}_c$
- $V$, the neighborhood is defined by $|V| = m$, where $m$ is the number of neighbors for each cell $i$; then $V = \{a_0 ... a_m \}$.
- $f$, is the local transition function of the automaton of each cell defined by $f = S^m \rightarrow S$ that defines the evolution of the automaton with respect to a neighborhood. Where $a_i^{t+1} = f(a_{i0}^t .........a_{im}^t)$ that defines us the next evolution of a cell with respect to its vicinity at the current time.

# 3. Proposed method

## a. Image encryption

As a first step we have to define a key, which we will turn to their representation in binary and will be taken as the seed of our pseudo-random bit, with which we will create three matrices of $mxn$ size where $m$ is the width of the image $n$ it is long. The matrix created will be filled by our pseudorandom bit generator. Therefore we use the rule 45 of linear cellular automata. Rule 45 is presented below:

| Rule 45 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 |
|---|---|---|---|---|---|---|---|---|
| | 111 | 110 | 101 | 100 | 011 | 010 | 001 | 000 |

We should mention that the images have three color components (RGB) which are each represented by a two dimensional matrix of size m$xn$. With values from 0 to 255 which represent the color at each pixel.

Already generated pseudo-random matrices our proceed to implement the function XOR of each of our pseudo-random matrices with each of the image components, which will get an encryption process.

Later we will separate each of our components of our image into 2 equal parts of size $\frac{m}{2}xn$. Which represent configurations $C^0$ and $C^1$ of the cellular automaton.

Our local transition function to evolve our next state time depends on evolution rule based on the Moore neighborhood and is obtained as follows:

For each character in the string is taken the ASCII numerical representation for obtain the evolution rule $k$, which will get its eight-bit binary representation.

| Position Caracter | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| | $\lambda_{-1,-1}$ | $\lambda_{-1,0}$ | $\lambda_{-1,1}$ | $\lambda_{0,-1}$ | $\lambda_{0,1}$ | $\lambda_{1,-1}$ | $\lambda_{1,0}$ | $\lambda_{1,1}$ |

| | | |
|---|---|---|
| $\lambda_{1,-1}$ | $\lambda_{1,0}$ | $\lambda_{1,1}$ |
| $\lambda_{0,-1}$ | 0 | $\lambda_{0,1}$ |
| $\lambda_{-1,-1}$ | $\lambda_{-1,0}$ | $\lambda_{-1,1}$ |

Thus our transition function is:

$$a_{i,j}^{t+1} = \sum_{\alpha=-1}^{1} \sum_{\beta=-1}^{1} a_{i+\alpha,j+\beta^{\lambda},\alpha,\beta}^{t}$$

Where:

- $0 \leq i \leq m-1$ and $0 \leq j \leq n-1$, with periodic boundary conditions.
- $a^t_{i,j}$, it represents a cell at time $t$.
- $\lambda$, is the rule evolution of cellular automata calculated from the user-defined key.

As the cell space is finite, you must set boundary conditions to define the evolution of the cellular automaton. For the implemented algorithm are considered periodic boundary conditions where $i \equiv j(modn)$ then $a^t_i = a^t_j$.

For obtaining the following cell configurations $C^0, C^1...C^{k+1}$ cellular automata are used with memory, that is, means using the obtained configurations above, in this case used for each evolution its above configuration, and the function used is as follows:

$$C^{t+1+l} = F_l(C^{t+l}) + C^{t-1+l}mod(256)$$

Where:

- $0 \leq l \leq k-1$ and $0 \leq j \leq k-1$, number of letters in the key.
- $C^t$, configuration is obtained in time $t$.
- $l$, is the transition function in time $t$.
- $n$, is the size of our network from which we get our rules of evolution of cellular automata.
- $F_l$, is the transition function at time $t$.

After obtaining all the configurations, encrypted image is created with the union of the last two configurations obtained $C^k$ and $C^{k+1}$.

### b. Decoded image

To decode a picture must separate the image components into two parts for obtain the settings $\overline{C^0}$ and $\overline{C^1}$. After the rules of evolution are obtained of the key to decrypt and make use of reversible cellular automaton following:

$$C^{t+1} = -F_{k-1-l}(C^t) + C^{t-1}mod(256)$$

Thus the settings were obtained $\overline{C^0}, \overline{C^1}...\overline{C^{k+1}}$ where $\overline{C^{k+1}}$ is the decoded image.

Subsequently, three pseudo-random matrices are generated from bit conversion to our key and proceed to apply the function XOR of each pseudo-random matrices with each of the image components, whereby an encryption process is obtained.

### c. Testings and Results

**Test 1.** For the test an image size of 666x296 was used that containing the word ”PRUEBA”. In Figure 1 shows the results obtained to encrypt and decrypt the image with AES and DES algorithms used, in 1-a) and 1-e) the original image are displayed after applying the AES and DES respectively, It shows that the image stands still in both cases. In 1-c) and 1-g) the histograms of the images are shown encrypted with AES and DES respectively and as noted, these peaks have information indicating predominant colors in the image encrypted. In 1-d) and 1-h) the original images are displayed to decode the encrypted images.

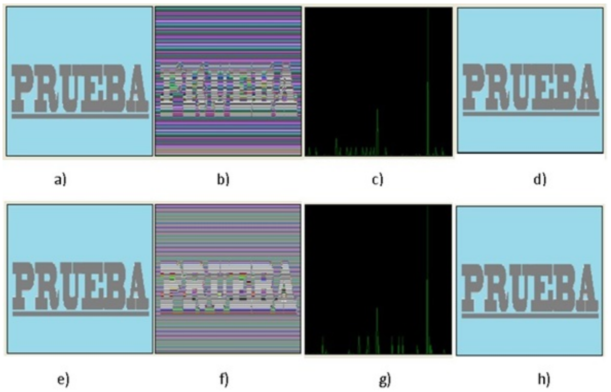

Figure 1: Implementation of AES and DES algorithm to the image that shows the word TEST. In a), b), c) and d) results of applying AES, and e), f), g) and h) result of applying DES.

Figure 2 shows the result of encrypting and decrypting using cellular automata. The system developed allows you to enter the desired user password to encrypt the image in this case has been made using a password of 8 bits with the word password, and developments that are obtained by the cellular automaton. Recall that as mentioned above for each character in the word password an evolution is generated, starting from the image that is generated by the XOR function within the algorithm; in this case 8 evolutions was generated more the image XOR.

**Test 2.** For this test an image of a robot is used with a white background as shown in Figure 3. The procedure followed is the same as test 1. Figure 3 shows the results after applying the AES and DES algorithms, in each observed that the result of the encrypted image even contour thereof shown, and in the histogram is observed peaks information indicating information predominates.

In figure 4 shows the application of the encryption algorithm and decryption shown by cellular automata, and using the *password* key word again.

As shown in the above figures, the images with the AES and DES encrypt algorithms, still contain encrypted image features of the original image, such as its contour, and It shows that the histogram shows peaks information in representative regions of information predominate, on the other hand, using the algorithm proposed using cellular automata is noted that in the image coded not perceived none of the original image, this is confirmed by observing the histogram which is obtained more linear compared to the histograms generated by the AES and DES.

## 4. Conclusions

It has proposed an algorithm encryption and decryption of information, specifically applied to images using cellular automata. Compared with AES and DES algorithms, these can be seen that the information is not encrypted at all, showing the outline of the image, information that can be corroborated with the histogram, where information peaks are observed corresponding to the information image that predominate, on the other hand, by applying the encryption algorithm using cellular automata, it is observed as the image is completely lost, the corresponding histogram is displayed so that no protruding peaks hiding information. Upon decode the information, each algorithm returns the original image without any loss of information.

**Acknowledgements.** The authors would like to thank the Instituto Politécnico Nacional (Secretaría Académica, EDI, EDD, COFAA, SIP, ESCOM and CIDETEC), the CONACyT and SNI for their economical support to develop this work.

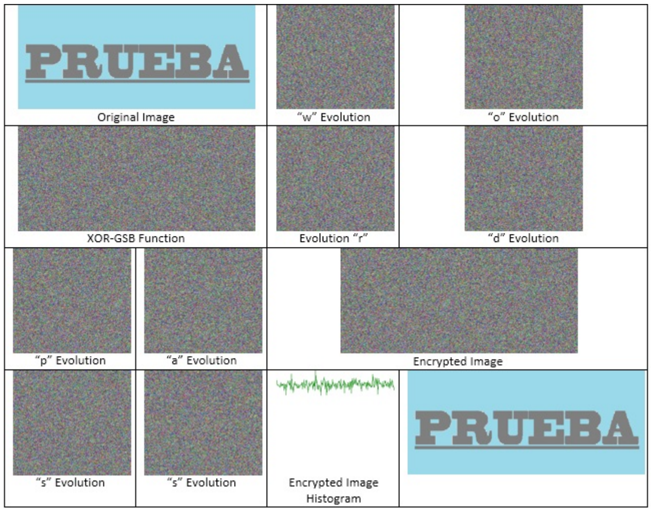

Figure 2: Encryption and decryption by cellular automata.

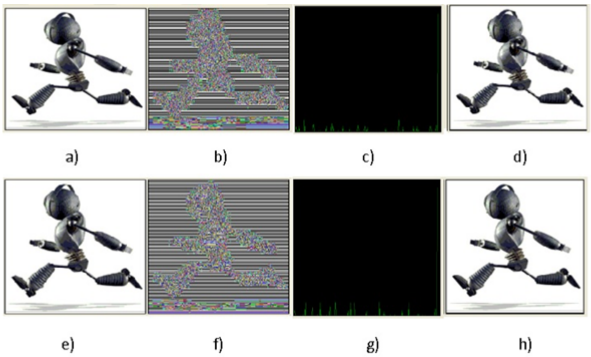

Figure 3: Implementation the algorithm AES and DES to the image of a robot. In a), b), c) and d) results of applying AES, and e), f), g) and h) result of applying DES.

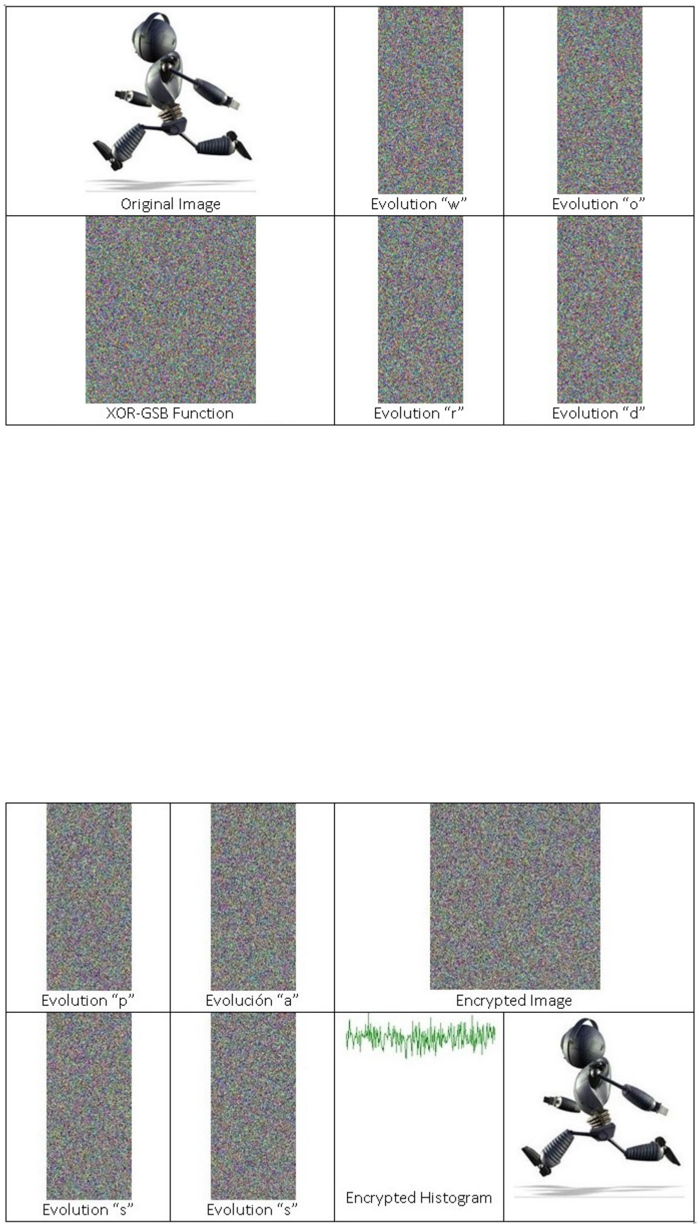

Figure 4: Encryption and decryption by cellular automata.

# References

[1] Dinghui Zhang, Fengdeng Zhang, Chaotic encryption and decryption of JPEG image, *Optik - International Journal for Light and Electron Optics*, **125** (2014), no. 2, 717-720. http://dx.doi.org/10.1016/j.ijleo.2013.07.069

[2] Kousik Mukherjee, A method of implementation of frequency encoded all optical encryption decryption using four wave mixing, *Optik - International Journal for Light and Electron Optics*, **122** (2011), no. 16, 1407-1411. http://dx.doi.org/10.1016/j.ijleo.2010.09.017

[3] Madhusudan Joshi, Chandrashakher, Kehar Singh, Color image encryption and decryption for twin images in fractional Fourier domain, *Optics Communications*, **281** (2008), no. 23, 5713-5720. http://dx.doi.org/10.1016/j.optcom.2008.08.024

[4] Yu-Guang Yang, Ju Tian, Si-Jia Sun, Peng Xu, Quantum-assisted encryption for digital audio signals, *Optik - International Journal for Light and Electron Optics*, **126** (2015), no. 21, 3221-3226. http://dx.doi.org/10.1016/j.ijleo.2015.07.082

[5] Aihan Yin, Shengkai Wang, A novel encryption scheme based on timestamp in gigabit Ethernet passive optical network using AES-128, *Optik - International Journal for Light and Electron Optics*, **125** (2014), no. 3, 1361-1365. http://dx.doi.org/10.1016/j.ijleo.2013.08.030

[6] Salim M. Wadi, Nasharuddin Zainal, Rapid Encryption Method based on AES Algorithm for Grey Scale HD Image Encryption, *Procedia Technology*, **11** (2013), 51-56. http://dx.doi.org/10.1016/j.protcy.2013.12.161

[7] Cai-hong Liu, Jin-shui Ji, Zi-long Liu, Implementation of DES Encryption Arithmetic based on FPGA, *AASRI Procedia*, **5** (2013), 209-213. http://dx.doi.org/10.1016/j.aasri.2013.10.080

[8] Ping Ping, Feng Xu, Zhi-Jian Wang, Image encryption based on non-affine and balanced cellular automata, *Signal Processing*, **105** (2014), 419-429. http://dx.doi.org/10.1016/j.sigpro.2014.06.020

[9] Jun Jin, An image encryption based on elementary cellular automata, *Optics and Lasers in Engineering*, **50** (2012), no. 12, 1836-1843. http://dx.doi.org/10.1016/j.optlaseng.2012.06.002

**Received: October 23, 2015; Published: December 12, 2015**