ISSN 1870-4069

Image Encryption System Based on Cellular Automata and S-Box

Juan Contreras[1], Marco Ramírez[1], Jesús Aboytes[2]

[1] Coordinación Académica Región Altiplano Oeste-UASLP, Salinas, Mexico
[2] Instituto de Investigación en Comunicación Óptica, UASLP, San Luis Potosí, Mexico
juanjosetorres96@outlook.com, tulio.torres@uaslp.mx,
agustin.aboytes@upslp.edu.mx

Abstract. This investigation presents an image encryption system and its security analysis, it is based on cellular automata and a substitution box. The joint of these two techniques, allow to encrypt digital images with a high adjacent redundancy and pass different statistical and differential tests and cryptanalytic attacks. The synchronization phenomenon of cellular automata, is sensitive to initial conditions, therefore has been used in Pseudo Random Number Generators (PRNG) and cryptosystems. In this system, the synchronization phenomenon is used to change the coefficients of the pixels, but the process is not equal for each bit, thus the s-box is used to make the system robust and for compliance with the bit independence criterion among others.

Keywords: image encryption, cellular automata, S-box.

1 Introduction

Nowadays, we can perform many operations for internet, thus facilitating processes and optimizing times. But, this requires providing security to users, given that their data are exposed on the transmissions or at the storage location. One of the techniques used to protect information are cryptographic algorithms. This technique consists of making the information unintelligible, in such a way that it can only be recovered using the correct key.

Currently, image encryption is a very active field of research, due to the multiple areas where it is required, for example: in the pay-television service, medical imaging systems, videoconferences, military communications, video surveillance, among others. Although there are several conventional encryption algorithms, such as AES (Advanced Encryption Standard), DES (Data Encryption Standard) and IDEA (International Data Encryption Algorithm), they have often been impractical for image encryption, due to the intrinsic properties of these, such as large volumes, a strong adjacent correlation, a high redundancy, among others [1]. Therefore, the security problem extends because the algorithms for image encryption must provide perceptual security and cryptographic security.

This has encouraged the search and implementation of new schemes for image encryption, such as the large number of encryption systems with a chaotic approach [2, 3, 4]. That is why in this research the synchronization of cellular automata is combined

based on rule 90, which is of discrete chaotic dynamics and the substitution boxes (S-box) to provide a strong algorithm against cryptanalytic and statistical attacks and pass the visual inspection.

2 Background

2.1 Cellular Automata

The concept of cellular automata (CA) was introduced in the decade of the 40's by the mathematician John von Neumann and Stanislaw Ulam [5]. The CAs are used to model complex behaviors where local interactions are involved. In fact, CAs represent a class of dynamic systems capable of describing the evolution of systems using simple rules, without the need to use differential equations.

The cellular automata consist of an ordered set of cells, in the form of a grid, where each cell has a finite number of states. The cellular automata form a grid of two dimensions, where their cells evolve in discrete steps according to a local rule of update applied uniformly, on all cells. At the beginning, a state is assigned to the cells at time $t = 0$, where the new cell states will depend on their previous states and those of their neighborhood, see Fig 1.

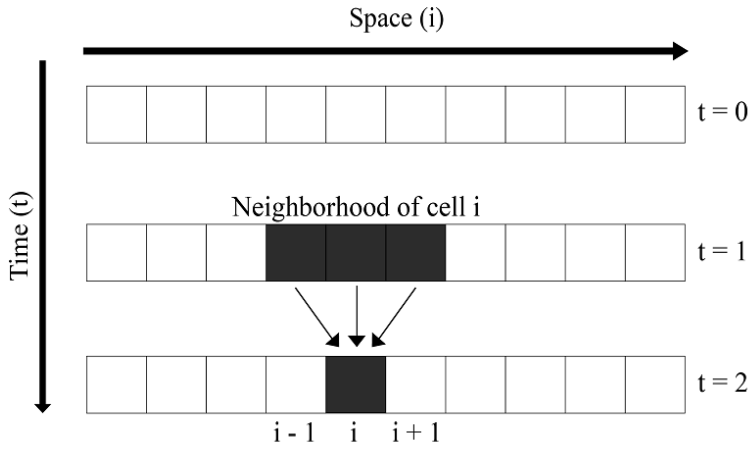

Fig. 1. Space-time diagram of a one-dimensional cellular automaton.

The elementary cellular automata (ECA) are CA of one dimension, with two states and neighborhood of radius 1. A local rule of cellular automata is the algorithm used to calculate the next state of the cell. The ECAs differ among themselves, only by choosing the local rule, they contain only three variables (cells) and each one can take only two values (1,0), therefore there are only 8 combinations, resulting in $2^8 = 256$ local rules and ECA different. For example, the local rule 90 is described by the following expression:

$$x_i^{t+1} = A\left(x_{i-1}^t + x_{i+1}^t\right). \quad (1)$$

The phenomenon of synchronization occurs when, after a period of time, the behavior of two dynamic systems approaches arbitrarily. In the case of CA, after a number of steps in time *t*, the difference between the vectors **x** and **y** corresponding to the controller and replicating cellular automaton respectively, will eventually result in the zero vector **0** = (0,0 ... ,0). For this it is necessary that in each step, both vectors evolve using the same local rule.

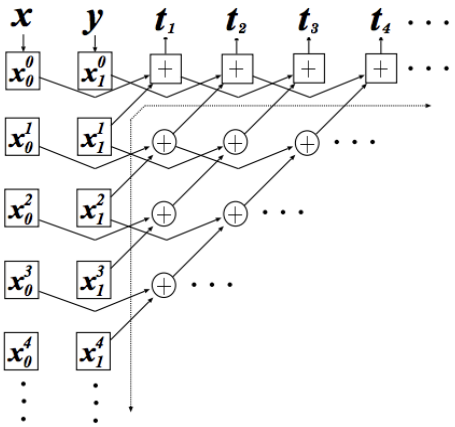

Fig. 2. Generator of pseudo-random sequences.

In Ref. [6] it was shown that a pair of ECAs that evolve using the local rule 90, synchronize if the coupled coordinates are separated by a block of $N = 2^n-1$ decoupled sites, where *n* is a positive integer. Based on the phenomenon of synchronization, in Ref. [7] the authors proposed a Pseudo-Random Number Generator (PRNG). The main function is called *h*, and it requires two vectors **x** and **y** of n bits and *n + 1* bits respectively. To calculate a pseudo-random sequence, the function requires that the cellular automaton evolve backwards. Such a situation is described in Fig. 2.

Where the XOR gates are represented with the circles that in the middle have a cross, the connectivity of these represent the local rule 90, and the resulting vector is called vector *t*.

In Ref. [8] a preprocessing function was created to exchange the values of the plaintext, based on the pseudo-random number generator, making a modification in its feedback, see Fig. 3. The process applied to images consists in receive each pixel coefficient as if it were the vector **x**, the vector **y** will be replaced after each iteration by the resulting vector $\hat{m}$, concatenating the least significant bit of the vector **y** precedent as the most significant bit of the new vector. This function allows to break the high adjacent correlation of the images, allowing a dynamic substitution of the information.

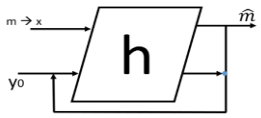

Fig. 3. Preprocessing function based om the *h* function.

2.2 S-box

On the other hand, in cryptography, substitution boxes are a basic component in symmetric algorithms. The boxes are used in cipher blocks to exchange the plaintext and in this way hide the relationship between the encryption key and the encrypted text [9].

The design and selection of a replacement box is a careful process, because it requires to be resistant to attacks of cryptanalysis. See Fig. 4 shows the S-box used in the AES encryption system, it has been tested and pass all the design principles.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	IE	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Fig. 4. S-box of the AES system in hexadecimal notation

3 Encryption Algorithm

3.1 New *h* Function

For the development of this image encryption algorithm, it is feasible to join both tools, synchronization phenomenon of CA and substitution boxes. The preprocessing operation is able to break the high correlation of the images and the substitution boxes provide security against attacks of differential cryptanalysis and bit independence criterion.

To increase the initial condition, a new version of the preprocessing operation was performed, where three *h* operations are used. So that there is no correlation between the original image and its processed version, see Fig. 5.

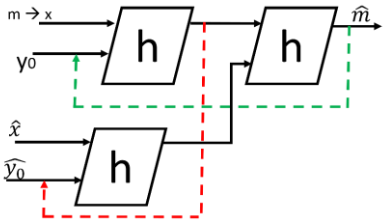

Fig. 5. Improved preprocessing function with three *h* functions.

3.2 Description of the Algorithm

The algorithm to encrypt an image works in the following way:

1º Select a block of plaintext 24-bits long (3 pixels in gray scale).

2º The new preprocessing function is applied to the plaintext blocks of the image.

3º The preprocessed block is divided in blocks of 8-bits, the value of each block is replaced using the S-box.

4º Subsequently, the columns and the rows of the resulting image are inverted in such a way that the pixel (n, n) now occupies the place (0,0), calculating the complement of each coordinate.

5º Finally, the preprocessing function with the transformed image is used again.

The secret key of this algorithm is at least 148 bits since two extended preprocessing functions are used, therefore, given the current processing is not susceptible to breaking using brute force attacks [10].

4 Results

The results of the security analysis applied to the encrypted images are shown in this section. Various statistical tests, cryptanalytics attacks and the calculation of NPCR (Number of Changing Pixel Rate) and UACI (Unified Averaged Changed Intensity) indices were applied to validate the quality of the encryption. For the tests, we use images widely used in the image processing with different characteristics: mandrill, Lena and peppers. All in gray scale to 8 bits and dimensions 512 x 512 pixels.

4.1 Histograms

The first test consists of calculating histograms of both the plainimage and its encrypted version, see Fig. 6. It shows the case of the Lena image, where we can see that the histogram of its encrypted version is uniform, thus hiding the redundancy of data from the original image.

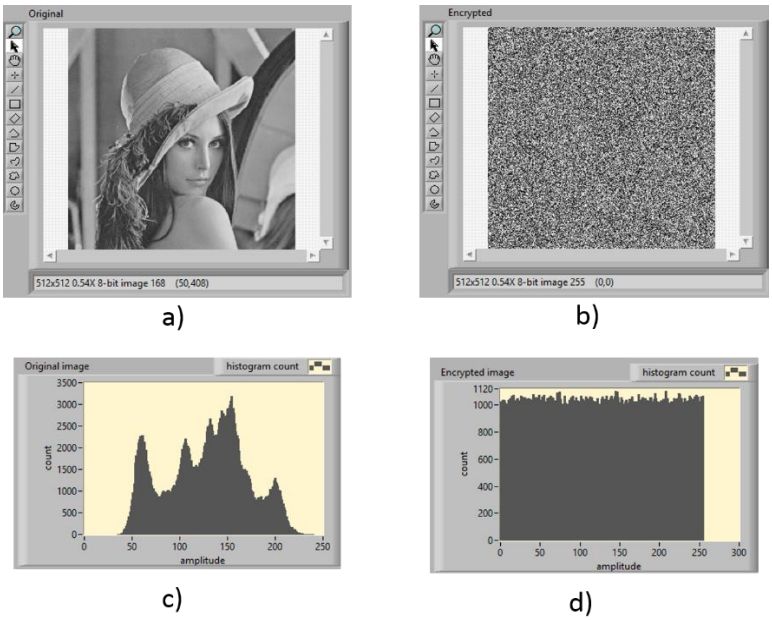

Fig. 6. Analysis of histograms a) Image of Lena, b) Image of Lena encrypted, c) Histogram of the original image of Lena and d) Histogram of the encrypted version of Lena.

4.2 Correlation

The second test that was performed was the calculation of the correlation coefficient between the original image and its encrypted version. This test tries to demonstrate the independence that exists between the encrypted image and the original image. According to the interpretation of this coefficient, there is no correlation between the images if the result is close to 0. Table 1 shows the results of this test applied to the three test images.

Table 1. Correlation coefficients between plainimages and their corresponding encrypted version.

Image	Coeficient
Peppers	-0.0025700
Lena	0.0011410
Mandrill	0.0005676

4.3 NPCR and UACI

In the encryption of images, it is common to analyze the resistance of the algorithms to differential attacks using two measurements: NPCR and UACI. Both measurements are based on small changes in two images and encrypt them under the same key. To illustrate this, let us assume that we have two encrypted images C^1 and C^2, whose corresponding plainimages have only one pixel different from each other, and both have been encrypted with the same secret key. The coefficients in the grayscale of both

images in row i and column j are marked as C^1 (i, j) and C^2 (i, j) respectively. The NPCR and UACI indices are defined in equations (2) and (3).

$$NPCR: N(C^1, C^2) = \sum_{i,j} \frac{D(i,j)}{T} \times 100\% \tag{2}$$

$$UACI: U(C^1, C^2) = \sum_{i,j} \frac{|C^1(i,j) - C^2(i,j)|}{F \cdot T} \times 100\% \tag{3}$$

where D (i, j) is determined in the following way: if C^1 (i, j) = C^2 (i, j), then D (i, j) = 0, otherwise D (i, j) = 1, T is the total of pixels of the images and F denotes the maximum value valid in the format of the image. For gray scale images at 256 levels, the theoretical values are UACI = 33.464% and NPCR = 99.609%, [11]. It is important highlight that to demonstrate the operation, a pixel will be modified to the image. The results obtained for our algorithm are shown in Table 2, where the least significant bit of the pixel **m**(255,255) was modified.

Table 2. Numercial results for NPCR and UACI.

Image	NPCR	UACI
Peppers	99.6235%	33.434992%
Lena	99.6021%	33.425587%
Mandrill	99.6128%	33.361058%

As is shown in the Table 2, the results in the most cases are upper than the theoretical values, just in one case is lower for 0.0069%.

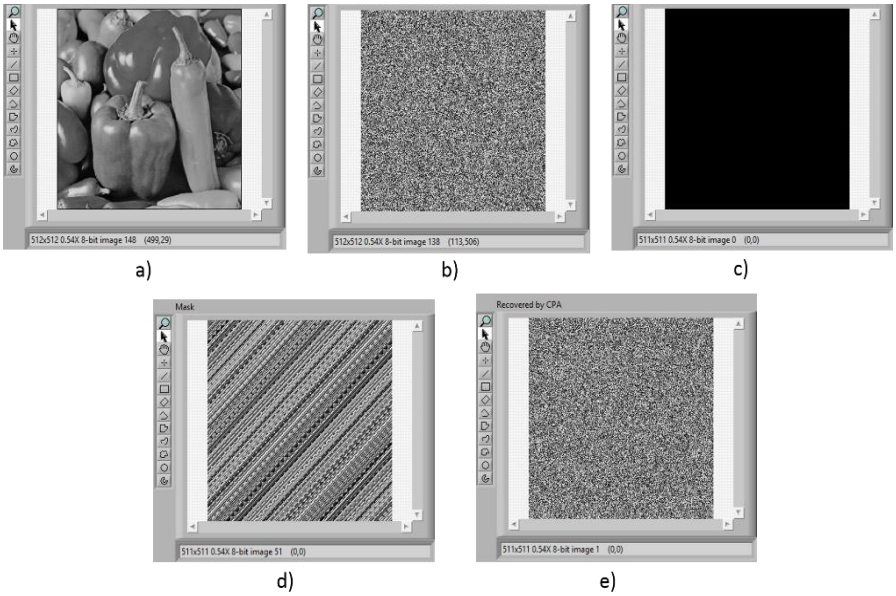

Fig. 7. Chosen-plainimage attack applied to the test image of the peppers. a) Original image, b) encrypted image of the peppers, c) solid image chosen, d) image mask and e) the recovered image.

4.4 Chosen-plainimage Attack (CPIA)

Finally, we performed the Chosen-plainimage attack (CPIA). In Ref. [12] they point out that if a cryptosystem is secure against CPIA attack, it is also safe against other cryptanalysis attacks such as cipherimage-only attack or known-plainimage attack.

This attack implies that the adversary is able to choose the plainimages and obtain their respective encrypted version, but he does not know the secret key. The attack begins by selecting the images to be encrypted, as can be seen in Fig. 7, the image of the peppers is used, Fig. 7a) and a solid black image, Fig. 7c). Both images are encrypted under the same secret key, the results are Fig. 7b) and 7d). Finally, an XOR operation is performed pixel by pixel between both encrypted images, the result will be what is called the recovered image, Fig. 7e). As we can see in our case the resulting image does not reveal information of the original image.

5 Conclusions

In the present work, a new algorithm for image encryption was proposed, the quality of encryption was measured with different tests and kinds of images, offering cryptographic and perceptual security, in all the cases. Both tools, the synchronization of cellular automata and the substitution boxes are complemented to securely encrypt this information. This encryption system could be a feasible option to encrypt high redundancy image, without revel any pattern. Therefore, it presents a better performance than AES system in ECB (Electronic Code Book) mode.

References

1. Lian, S.: Multimedia content encryption: techniques and applications. Auerbach Publications (2008)
2. Niyat, A.Y., Moattar, M.H., Torshiz, M.N.: Color image encryption based on hybrid hyper-chaotic system and cellular automata. Optics and Lasers in Engineering, 90, 225–237 (2017)
3. Belazi, A., El-Latif, A.A.A., Belghith, S.: A novel image encryption scheme based on substitution-permutation network and chaos. Signal Processing, 128, 155–170 (2016)
4. Belazi, A., El-Latif, A.A.A., Diaconu, A.V., Rhouma, R., Belghith, S.: Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms. Optics and Lasers in Engineering, 88, 37–50 (2017)
5. Von Neumann, J., Burks, A.W.: Theory of self-reproducing automata. IEEE Transactions on Neural Networks, *5*(1), 3–14 (1966)
6. Urıas, J., Salazar, G., Ugalde, E.: Synchronization of cellular automaton pairs. Chaos: An Interdisciplinary Journal of Nonlinear Science 8(4), 814–818 (1998)
7. Urias, J., Ugalde, E., Salazar, G.: A cryptosystem based on cellular automata. Chaos, 8(4), 819–822 (1998)
8. Ramirez-Torres, M.T., Murguia, J.S., Carlos, M.M.: Image encryption with an improved cryptosystem based on a matrix approach. International Journal of Modern Physics C, *25*(10), 1450054 (2014)
9. Chandrasekaran, J., Subramanyan, B., Selvanayagam, R.: A chaos based approach for improving non linearity in S box design of symmetric key cryptosystems. In: International Conference on Computer Science and Information Technology, pp. 516–522. Springer, Berlin, Heidelberg (2011)

10. Paar, C., Pelzl, J.: Understanding: a textbook for students and practitioners. Springer Science & Business Media (2009)
11. Wu, Y., Noonan, J.P., Agaian, S.: NPCR and UACI randomness tests for image encryption. Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT) 1(2), 31–38 (2011)
12. del Rey, A.M., Sánchez, G.R., De La Villa Cuenca, A.: Encrypting digital images using cellular automata. In: International Conference on Hybrid Artificial Intelligence Systems, pp. 78–88. Springer, Berlin, Heidelberg (2012)