Graphic cryptosystem using memory cellular automata

L. Hernández Encinas[1], *A. Hernández Encinas*[2], *S. Hoya White*[2],

A. Martín del Rey[3], *G. Rodríguez Sánchez*[4]

[1]Instituto de Física Aplicada, CSIC, C/Serrano 144, 28006-Madrid, España, E-mail: luis@iec.csic.es

[2]Dpto. de Matemática Aplicada, E.T.S.I.I., Universidad de Salamanca

Avda. Fernández Ballesteros 2, 37700-Béjar, España, E-mails: {ascen, sarahw}@usal.es

[3]Dpto. de Matemática Aplicada, E.P.S., Universidad de Salamanca, C/Santo Tomás s/n 05003-Ávila, España, E-mail: delrey@usal.es

[4]Dpto de Matemática Aplicada, E.P.S., Universidad de Salamanca, Avda. Requejo 33, 49022-Zamora, España, E-mail: gerardo@usal.es

Abstract:

In this paper, a new graphic cryptosystem based on reversible memory cellular automata is introduced. Its main feature is that the original image and the cipher image are defined by the same palette of colors and that the recovered image is equal to the original one, that is, there is not loss of resolution. Moreover, it is proved that the proposed cryptosystem is secure against brute-force attacks, statistical attacks and chosen plaintext attacks.

Keywords: Cellular Automata. Graphic Cryptosystems. Image Processing.

1. Introduction

Dynamical systems have been widely used in cryptography (see [4]). Nevertheless, there are few protocols based on dynamical systems specifically designed to encrypt images (see, for example [2]). Usually, these protocols are difficult to implement due to the difference between the chaotic arithmetic defined by the dynamical system used and the discrete arithmetic of the computers. Moreover, the decrypted image usually presents a loss of resolution and definition and consequently, it is not exactly the original one.

Recently, the use of cellular automata to encrypt images has been proposed (see [1, 3]). Their main feature is that the recovered image has no loss of resolution.

In this paper, the use of memory reversible cellular automata is proposed in order to design a graphic cryptosystem. It allows one to cipher images defined by any number of colors.

The original image and the cipherimage are defined by the same palette of colors and the decrypted image is identical to the original one, that is, no loss of resolution nor definition takes place.

The rest of the paper is organized as follows: In Section 2, some basic concepts related to memory cellular automata are presented. In Section 3, the new cryptosystem for images is introduced and its security is proved. In Section 4 an example is shown, and finally, the conclusions and further work are presented in Section 5.

2. Memory cellular automata

A cellular automaton (CA) is a discrete dynamical system formed by a finite or infinite number of identical objects called cells, which are endowed with a state that changes in discrete time steps according to a deterministic rule. Specifically, a CA can be defined by means of a 4-uplet $A = (C, S, V, f)$, where C is the cellular space formed by n cells: $< i >$, $0 \leq i \leq n\text{-}1$. S is the state set, that is, the set of all posible values of the cells. In this work, S is a finite set with $|S| = k$; consequently $S = \mathbf{Z}_k$. The set of indices of C is the finite ordered subset $V \subset \mathbf{Z}$, $|V| = m$, such that for every cell $< i > \in C$, its neighborhood, V_i, is the ordered set of m cells given by $V_i = \{\langle i+\alpha_1\rangle,\ldots,\langle i+\alpha_m\rangle, \text{con } \alpha_i \in V\}$.

Moreover, the local transition function, $f : S^m \rightarrow S$, is the function that determines the evolution of the states of the cells taking into account the states of the neighbor cells. Then, if $a_i^{(t)} \in S$ stands for the state of the cell $< i >$ at time t, and $V_i^{(t)}$ is the set of states of the neighborhood of the cell $< i >$ at time t, the next state of the cell is: $a_i^{(t+1)} = f\left(V_i^{(t)}\right) = f\left(a_{i+\alpha_1}^{(t)},\ldots,a_{i+\alpha_m}^{(t)}\right)$.

As the cellular space is finite, boundary conditions must be given in order to assure that the evolution of the cellular automata is well-defined. In this work, periodic boundary conditions are considered: $i \equiv j \pmod{n}$ then $a_i^{(t)} = a_j^{(t)}$.

The set of states of all cells at time *t* is called the configuration at time *t* and it is represented by the vector $C^{(t)} = \left(a_0^{(t)}, \ldots, a_{n-1}^{(t)}\right) \in S^n$. In particular, $C^{(0)}$ is the initial configuration. If we denote by **C** the set of all possible configurations of a CA, the global function of the CA is a linear transformation $\Phi : \mathbf{C} \to \mathbf{C}, C^{(t)} \mapsto C^{(t+1)}$, that yields the configuration at the next time step during the evolution of the CA. If Φ is bijective then there exists another CA, called its inverse, whose global function is Φ^{-1}. When such inverse cellular automaton exists, the CA is called reversible and the evolution backwards is possible.

In general, the evolution of a CA considers that the state of every cell at time $t + 1$ depends on the state of its neighborhood at time *t*. Nevertheless, one can consider that this evolution also depends on the states of other cells at times $t - 1$, $t - 2$, etc. In this case, the transition function can be represented in the following way: $a_i^{(t+1)} = \sum_{h=0}^{k} f^{(t-h)}\left(V_i^{(t-h)}\right)$, where $f^{(t-h)}$ is a specific local transition function. These CA are called memory cellular automata.

3. The graphic cryptosystem

Let *I* be an image defined by $n = r \times s \geq 128$ pixels and by a palette of *c* colors. This image can be represented by a matrix, *M*, of order $n = r \times s$, with coefficients in $\mathbf{Z}_c$, where $c = 2^b$ and $b = 1, 8, 24$, for black and white images, grey level images and color images, respectively. The coefficient (i, j) of *M* stands for the color's numeric value of the pixel $(i,$

j) of the image *I*. As a consequence, if all rows of *M* are linking together, a linear array of *n* integers is obtained: $P = (p_0,...,p_{n-1})$. It is called the associate linear array to the image *I*.

The proposed cryptosystem consists of three phases. In the first phase (the setup phase), the two users agree the key to be shared and the CA to be used is defined. In the second phase (the encryption phase), the sender encrypts the secret image (plainimage) to be sent to the receiver. Finally, in the third phase (decryption phase), the receiver uses the inverse CA to the one considered in the setup phase and decrypts the received image (cipherimage).

Setup phase. Before encrypting an image, the sender and the receiver, agree to use a 1024-bit secret key for the cryptosystem, *K*. Using such key, a pseudorandom sequence of $2n + 2$ bits is generated by means of the generator BBS. As a consequence, two sequences of $n + 1$ bits are obtained: $K_0 = \left(b_0^{(0)},\ldots,b_n^{(0)}\right)$ and $K_1 = \left(b_0^{(1)},\ldots,b_n^{(1)}\right)$. Subsequently, the sender constructs the linear array, *P*, associated to the image *I* and, using a random number generator, obtains a sequence of *n* integer numbers in $\mathbf{Z}_c$, $Z = \{z_0,\ldots,z_{n-1}\}$. Finally, a memory CA, $A = (C, S, V, f)$, is defined to be used in the cryptosystem. Its main features are the following: the cellular space *C*, is a sequence of $n = r \times s$ cells; the state set is $S = \mathbf{Z}_c$; the neighborhoods are defined by $V = \{-n/2,...,n/2\}$; and the local transition function is:

$$a_i^{(t+1)} = \sum_{j=-n/2}^{n/2} b_{n/2+j}^{(t \,(\mathrm{mod}\, 2))} a_{i+j}^{(t)} + a_i^{(t-1)} \,(\mathrm{mod}\, c), \quad 0 \le i \le n-1. \tag{1}$$

Note that this CA is reversible and its inverse is given by the following local transition function:

$$a_i^{(t+1)} = -\sum_{j=-n/2}^{n/2} b_{n/2+j}^{(t \,(\mathrm{mod}\, 2))} a_{i+j}^{(t)} + a_i^{(t-1)} \,(\mathrm{mod}\, c), \quad 0 \le i \le n-1. \tag{2}$$

Note that it is suppose that $n = r \times s$ is even. If *n* is odd, then an aditional random pixel will be added to the original image in order to obtain an even number of pixels.

Encryption phase. In this phase, the sender defines the first configutations of the CA: $C^{(0)} = P$, $C^{(1)} = Z$, and using the CA given by (1), computes the configurations $C^{(2)}$ and $C^{(3)}$. The cipherimage, J, is given by linking together the images, J_1 and J_2, whose associated linear arrays are the configurations $C^{(2)}$ and $C^{(3)}$. The size of the image J is of $2n = (2r)\times s$ pixels. The maximum number of colors of the cipherimage is c, and consequently I and J are defined by the same palette of colors. Remark that the random configuration $C^{(1)}$ can be destroyed when the encryption phase is finished.

Decryption phase. To decrypt the cipherimage, J, the receiver computes the configurations $\overline{C}^{(0)} = C^{(3)}$ and $\overline{C}^{(1)} = C^{(2)}$, taking into account J. Subsequently, he applies the CA twice to obtain $\overline{C}^{(3)} = P$, which is the linear array associated to I. Note that the recovered image is exactly the original image due to the reversibility of the CA used.

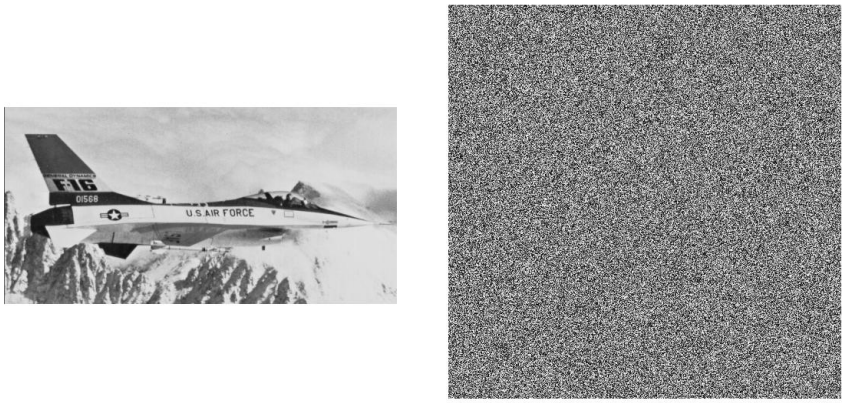
If the number of pixels of the original image is $n = r\times s$, where $16 \le n \le 127$, the above encryption and decryption protocols work correctly by virtue of the periodic boundary conditions.

The proposed cryptosystem is secure against brute-force attacks due to the lenght of the key: 1024 bits. Also, it is secure against statistical attacks since the generator BBS is used and the configuration $C^{(1)}$, is obtained by means of a random number generator. Moreover, the cryptosystem is secure against chosen plaintext attacks: if a possible attacker chooses an homogeneous image: $a_i^{(0)} = p \in \mathrm{Z}_c$, $0 \le i \le n-1$, then, to obtain the bit sequences used in the protocol: K_0 y K_1, he has to solve the system of $2n$ non-linear equations with $3n+2$ unknown variables: $b_j^{(0)}, b_j^{(1)}, a_k^{(1)} = z_k$, with $0 \le j \le n$, $0 \le k \le n-1$, given by the following equations:

$$a_i^{(2)} = \sum_{j=-n/2}^{n/2} b_{n/2+j}^{(0)} a_{i+j}^{(1)} + p \,(\mathrm{mod}\, c)\,,\ a_i^{(2)} = \sum_{j=-n/2}^{n/2} b_{n/2+j}^{(1)} a_{i+j}^{(2)} + a_i^{(1)} \,(\mathrm{mod}\, c)\,,\ \ 0 \le i \le n-1.$$

4. Example

The image (a) of the Figure 1 is a grey-level image with 216 colors and defined by 512×512 pixels. Its cipherimage is given by the image (b) of the same figure. It is also a grey-level image. It is defined by 256 grey levels and by 512×1024 pixels.



(a) (b)

Figure 1. (a) Original image (b) Cipherimage

5. Conclusions and further work

We have proposed a new graphic cryptosystem in order to encrypt an image defined by pixels and by any number of colors. This cryptosystem is based on a memory reversible cellular automaton and uses a cryptographically secure pseudorandom number generator in the encryption protocol. The session key of the cryptosystem has 1024 bits. Furthermore, the encrypted image is of the same type than the original one, that is, both images are defined by the same color palette. Moreover, the decrypted image is identical to the original one, that is, no loss of resolution nor definition takes place. In relation to the security of the proposed cryptosystem, we have stated that it is secure against brute-force attacks,

statistical attacks and chosen plaintext attacks. Further work aimed at designing an algorithm with a lesser cipherimage and with the same level of security.

Acknowledgements

The authors want to thank L. Hernández Encinas and G. Álvarez Marañon for their valuable suggestions. This work has been supported by Consejería de Educación y Cultura of Junta de Castilla y León (Spain), under grant number SA052/03.

References

[1] Álvarez Marañón, G., Hernández Encinas, L., Hernández Encinas, A., Martín del Rey, A., Rodríguez Sánchez, G., Graphic cryptography with pseudorandom bit generators and cellular automata. *Lect. Notes Artif. Intell.* **2773** (2003) 1207-1214.

[2] Fridrich, J., Symmetric ciphers based on two-dimensional chaotic maps. *Internat. J. Bifur. Chaos* **8** (1998) 1259-1284.

[3] Hernández Encinas, L., Martín del Rey, A., Hernández Encinas, A., Encryption of images with 2-dimensional cellular automata, in Proceedings of 6-th Multiconference on Systemics, Cybernetics and Informatics, Vol. I: Information Systems Development, Orlando, 2002, pp. 471-476.

[4] Schmitz, R., Use of chaotic dynamical systems in cryptography. *J. Franklin Inst.* **338** (2001) 429-441.

Luis Hernández Encinas obtained the Ph. D. in Mathematics from the University of Salamanca in 1992. He is scientific research in CSIC. His current research interests include image processing, cellular automata and cryptography.

Ascensión Hernández Encinas obtained the Ph. D. in Physics from the University of Salamanca in 1990. She is associated professor of the Department of Applied Mathematics in the University of Salamanca. Her current research interests include dynamic climate, image processing, cellular automata and cryptography.

Sara Hoya White obtained the Ms. D. in Engineering from the University of Salamanca in 1999. She is assistant professor of the Department of Applied Mathematics in the University of Salamanca and actually she is working in her Ph. D. Thesis. Her current research interests include image processing, cellular automata and cryptography.

Angel Martín del Rey obtained the Ph. D. in Mathematics from UNED in 2000. He is associated professor of the Department of Applied Mathematics in the University of Salamanca. His current research interests include differential equations, image processing, cellular automata and cryptography.

Gerardo Rodríguez Sánchez obtained the Ph. D. in Mathematics from the University of Salamanca in 1996. He is full professor of the Department of Applied Mathematics in the University of Salamanca. His current research interests include image processing, cellular automata and cryptography.