A Novel Cryptosystem for Binary Images

A. Martín del Rey

Department of Applied Mathematics

E.P.S., University of Salamanca

C/ Santo Tomás s/n, 05003-Ávila

SPAIN

Abstract. In this work a novel cryptosystem for binary images is developed. It is based on the use of hybrid cellular automata as pseudorandom bit generators. Such automata have good statistical properties as pseudorandom bit generators for cryptographic purposes. Moreover, the proposed cryptosystem is secure against brute force attacks.

Keywords: Binary Images. Cellular Automata. Cryptography. Hybrid Cellular Automata.

A. Martín del Rey obtained the M.S. degree in Mathematics from the University of Salamanca in 1996 and Ph. D. in Mathematics from National University of Distance Learning (UNED) in 2000. From 1997 until 2001 he was an assistant professor in the Department of Applied Mathematics, University of Salamanca, and since 2002 he has been an associated professor in the same department. His current research interests include image processing, cellular automata, cryptography and ordinary differential equations.

1. Introduction

In the current age of global communications, the need for security and privacy in the transmission of electronic data has become a basic necessity. In this respect, public and private organizations depend on cryptographic methods to guarantee confidentiality, integrity and authenticity in data storage and transmission.

Nevertheless, Cryptography has been used for a long time. Basically, the predominant users of it were the governments in order to protect national secrets and strategies, but the proliferation of computers and the growth of digital information made Cryptography be used by private sector too.

Strictly, Cryptography (see [1,2]) is the study of mathematical techniques related to aspects of security information such as confidentiality, data integrity, entity authentication, and data origin authentication. Moreover, Cryptanalysis is the study of mathematical techniques for attempting to break cryptographic techniques. Cryptology is the study of cryptography and cryptanalysis.

There are two types of cryptosystems: symmetric and asymmetric cryptosystems. In symmetric cryptography (also called secret-key cryptography) the same key is used for both encryption and decryption, whereas in asymmetric cryptography (also called public-key cryptography) there are two keys: one for encryption -which is publicly known, and other for decryption, which must remain secret. The most common algorithms in asymmetric cryptography are block ciphers and stream ciphers. Specifically, a stream cipher is a secret-key algorithm which generates a cipher sequence of bits by means of the secret key. Encryption is accomplished by combining the cipher sequence with the plain text (the bit sequence of the text to be sent), usually with the bitwise XOR operation. There are several methods to generate the cipher sequence starting from the secret key (see [3]): LFSR generators, BBS generator, etc. All of them must be cryptographic secure in order to avoid cryptanalysis attacks.

There are several mathematical techniques that can be used for cryptographic purposes, and one of them is the use of discrete dynamical systems ([4]). In the present paper we focus our attention in a special type of such mathematical tools called cellular automata.

Cellular automata (CA for short) are finite state machines consisting of a finite number of interconnected cells arranged linearly in one dimension, each of which can be in one of a finite number of possible states. Here, we only consider Wolfram cellular automata, that is, cellular automata whose state set is $\mathbf{Z}_2 = \{0, 1\}$. Every cell essentially comprises of a memory element and a combinatorial logic that generates the next-state of the cell from the present states of its neighbouring cells. When all cells evolve according to the same logic function, the CA is called uniform, otherwise it is called hybrid.

The use of cellular automata to design cryptosystems goes back to middle eighties when S. Wolfram proposed the cellular automaton with rule number 30 as a pseudorandom bit generator ([5]) for cryptographic purposes. Since then, many CA-based cryptosystems have been proposed not only for text ([6]-[14]) but also for images ([15, 16]).

There are many others cryptographic protocols for images (see, for example, [17]-[27]), but no one of them can be considered as a stream cipher. Moreover, some of them present problems such as the lost of resolution of the recovered image.

In this work a novel cryptosystem for binary images is defined. Specifically, it consists of a stream cipher cryptosystem whose cryptographic secure pseudorandom bit generator is a hybrid boolean cellular automaton. It is secure against statistical and brute force attacks. Furthermore, no lost of resolution appears in the recovered image.

The rest of the paper is organized as follows: In Section 2, the basic theory about hybrid cellular automata is presented; in Section 3, their interpretation as pseudorandom bit generators is shown; the proposed cryptosystem is detailed in Section 4 and an example is shown in Section 5; the security analysis of the cryptosystem is presented in Section 6; and finally, the conclusions are presented in Section 7.

2. Hybrid Cellular Automata

Wolfram hybrid cellular automata (HCA for short) are discrete dynamical systems formed by a finite collection of identical objects called *cells*: $<i>$ with $1 \leq i \leq n$, which can be assumea a state: 0 or 1, that change in every

$$a_i^{(t)} = f_i\left(a_{i-1}^{(t)}, a_i^{(t)}, a_{i+1}^{(t)}\right), \quad 1 \leq i \leq n,$$

step of time according to some transition rules: $f_1, \ldots, f_n$, as follows:

where $a_i^{(t)}$ stands for the state of the cell $<i>$ at time t.

Note that the transition rule is different for each cell, *i.e.*, the cell $<i>$ evolves according to the rule defined by the boolean function f_i. Those cellular automata for which $f_1 = \ldots = f_n$, are called *uniform cellular automata*. As the number of cells is finite, boundary conditions must be considered in order to assure the well-defined dynamics of the CA. In this paper, *null boundary conditions* are taken, *i.e.*,

$$a_i^{(t)} = 0 \Leftrightarrow i < 1 \text{ or } i > n.$$

The vector $C^{(t)} = (a_1^{(t)}, \ldots, a_n^{(t)})$ is called *configuration* of the HCA at time t, and $C^{(0)}$ is the *initial configuration*. Moreover, **C** is the set of all possible configurations of the hybrid cellular automata, in such a way that for HCA with n cells and two states, one has $|\mathbf{C}| = 2^n$. Moreover, the vector

$$E_{\langle i \rangle}^{(0,k)} = \left(a_i^{(0)}, \ldots, a_i^{(k)}\right),$$

is called *temporal evolution* of the cell $<i>$ from $t = 0$ to $t = k$.

A particular and very important type of HCA are the linear HCA (LHCA for short). The transition rules of a LHCA are linear functions in such a way that the evolution of such automata is given as follows:

$$a_i^{(t)} = f_i\left(a_{i-1}^{(t)}, a_i^{(t)}, a_{i+1}^{(t)}\right) = \alpha_i a_{i-1}^{(t)} + \beta_i a_i^{(t)} + \gamma_i a_{i+1}^{(t)} \pmod 2,$$

where $1 \leq i \leq n$, and α, β, $\gamma \in \mathbf{Z}_2$ for every i. The importance of this type of automata is based on the

interpretation of its dynamics in terms of Linear Algebra: Its evolution is given by the following system of linear equations:

$$\begin{cases} a_1^{(t+1)} = \beta_1 a_1^{(t)} + \gamma_1 a_2^{(t)} \pmod 2 \\ a_2^{(t+1)} = \alpha_2 a_1^{(t)} + \beta_2 a_2^{(t)} + \gamma_2 a_3^{(t)} \pmod 2 \\ \qquad \ldots \\ a_{n-1}^{(t+1)} = \alpha_{n-1} a_{n-2}^{(t)} + \beta_{n-1} a_{n-1}^{(t)} + \gamma_{n-1} a_n^{(t)} \pmod 2 \\ a_n^{(t+1)} = \alpha_n a_{n-1}^{(t)} + \beta_n a_n^{(t)} \pmod 2 \end{cases}$$

that is:

$$C^{(t+1),\mathrm{T}} = M \cdot C^{(t),\mathrm{T}} \pmod 2,$$

where $C^{(t),T}$ stands for the transpose matrix of $C^{(t)}$, and M is the *transition matrix* of the LHCA:

$$M = \begin{pmatrix} \beta_1 & \gamma_1 & 0 & \cdots & 0 & 0 \\ \alpha_2 & \beta_2 & \gamma_2 & \cdots & 0 & 0 \\ 0 & \alpha_3 & \beta_3 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \beta_{n-1} & \gamma_{n-1} \\ 0 & 0 & 0 & \cdots & \alpha_n & \beta_n \end{pmatrix}$$

Furthermore, the *characteristic polynomial* of the LHCA, $p_c(x)$, is defined as the characteristic polynomial associated to its transition matrix.

All the information related to the evolution of the LHCA can be resumed in the *global transition function* Φ_f: **C** → **C**, which assigns to every one of the possible configurations of the LHCA its successor in time. Using the global function we can obtain a graphic representation of the evolution of the LHCA by means of the *state transition diagram*. It is an oriented graph whose vertices are the 2^n configurations of the automata so that there exists an edge between to vertices: C and C', if $\Phi_f(C) = C'$. It is said to be that a LHCA has *maximum length period* when there exists a cycle of length 2^n-1 in its state transition diagram. As a consequence in such automata, starting from an initial configuration, $C^{(0)}$, the evolution traverses the rest of configurations of the automata except for the null configuration: $N = (0,\ldots,0)$ -which is a loop of the state transition diagram as $\Phi_f(N) = N$-. It is also known that a LHCA with maximum length period have a primitive characteristic polynomial (see [28]); *i.e.*, the characteristic polynomial is irreducible of degree n such that the minimum value of m for which such polynomial divides x^m+1 is $m = 2^n$-1. It is a well-known fact that the LHCAs with maximum length period has good properties as pseudorandom bit generators (see [3]).

In this work, we focus our attention on LHCAs whose local transition functions are two. Specifically, we will consider the following two transition functions:

$$a_i^{(t+1)} = f\left(a_{i-1}^{(t)}, a_i^{(t)}, a_{i+1}^{(t)}\right) = a_{i-1}^{(t)} + a_{i+1}^{(t)} \pmod 2 \qquad (1)$$

$$a_i^{(t+1)} = g\left(a_{i-1}^{(t)}, a_i^{(t)}, a_{i+1}^{(t)}\right) = a_{i-1}^{(t)} + a_i^{(t)} + a_{i+1}^{(t)} \pmod 2 \qquad (2)$$

They stand for the cellular automata with Wolfram rule numbers 90 and 150 (see [29]), respectively.

Moreover, we assume that these LHCAs have n = 256 cells. Consequently, each LHCA is characterized by its *characteristic vector*:

$$V = \langle \beta_1, \beta_2, \ldots, \beta_{256} \rangle,\ \beta_i \in Z_2,$$

in such a way that for every i with $1 \le i \le n$, if $\beta_i = 0$ then the evolution of the cell $< i >$ is given by

the local transition function given by (1), while if $\beta_i = 1$, the evolution of the cell $< i >$ is given by (2). As a consequence, its transition matrix is of the following form:

$$M = \begin{pmatrix} \beta_1 & 1 & 0 & \cdots & 0 & 0 \\ 1 & \beta_2 & 1 & \cdots & 0 & 0 \\ 0 & 1 & \beta_3 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \beta_{n-1} & 1 \\ 0 & 0 & 0 & \cdots & 1 & \beta_n \end{pmatrix}$$

3. Hybrid Cellular Automata as Pseudorandom bit Generators

Cellular automata and, particularly LHCA, can be considered in a very simple way as pseudorandom bit generators. Starting from an initial configuration on length n,

$$C^{(0)} = \left(a_0^{(0)}, \ldots, a_{n-1}^{(0)}\right),$$

it is easy to construct a sequence of bits of length $k \cdot n >> n$ by simple linking together the first k configurations, $C^{(0)},\ldots, C^{(k-1)}$, of the evolution. Nevertheless, this is not a cryptographic secure procedure: If an adversary obtains a portion (of length greater than n) of such linked sequence, and knows the cellular automata used, it is very easy to generate the rest of configurations given by such automata during its evolution.

More secure bit sequences can be obtained by simply sampling the values that a fixed cell attains in the evolution of the CA; that is, the bit sequence generated by the CA is the temporal evolution of a particular cell $< i >$:

$$E_{\langle i\rangle}^{(0,l)} = \left(a_i^{(0)}, a_i^{(1)}, \ldots, a_i^{(l)}\right)$$

Note that this procedure is computationally more expensive than the previous one, but it is also much more hard for an adversary to generate the rest of the sequence knowing only one state of each past configuration.

To assure good pseudorandom properties of a bit sequence, the generator has to pass several statistical tests (see [30, 31]). The five basic statistical tests that are usually used for determining whether a sequence of bits possesses some specific features that a truly random sequence would be likely to exhibit are the *frequency test*, the *serial test*, the *poker test*, the *run test* and the *autocorrelation test* (see [3]). They have been developed *ad hoc* for cryptographic use and they are based on Golomb's randomness postulates (see [32])

The main importance of the LHCAs formed by the transition rules (1) and (2) comes from their good properties as pseudorandom bit generators. It is proven that such automata pass the statistical tests proposed above (see [33]). Furthermore, they are the unique LHCAs formed by two transition rules and null boundary conditions which can exhibit maximum length period (see [34]). Nevertheless, not all LHCAs with rule numbers (1) and (2) have maximum length period. Cattel y Muzio showed in [35] that this property depends on the characteristic vector of the LHCA. Furthermore, they proved that only two LHCA combining the Wolfram rule numbers 90 and 150 with n = 256 cells have maximum length period. Their characteristic vectors are the following (see [36, 37]):

$$\begin{aligned} V_1 = <\, & 1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,\\ & 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,\\ & 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,\\ & 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,\\ & 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,\\ & 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,\\ & 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,\\ & 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 >, \end{aligned} \tag{3}$$

$$\begin{aligned} V_2 = <\, & 0,0,0,1,1,1,0,0,1,1,1,0,0,1,0,0,1,0,1,0,0,1,1,0,0,0,1,1,0,0,1,1,\\ & 1,1,0,0,0,1,1,1,1,0,1,0,0,1,1,0,1,1,1,0,0,1,0,1,0,1,0,0,1,0,1,1,\\ & 1,1,1,0,0,1,0,1,0,0,0,1,0,0,0,1,1,0,1,1,0,0,0,0,1,1,1,0,0,0,0,0,\\ & 0,0,1,0,1,1,0,0,1,1,0,0,0,1,0,0,0,0,1,1,1,1,0,1,0,1,1,1,1,1,0,1,\\ & 1,1,0,1,1,1,1,0,1,0,1,1,1,1,0,0,0,0,1,0,0,0,1,1,0,0,1,1,0,1,0,0,\\ & 0,0,0,0,0,1,1,1,0,0,0,0,1,1,0,1,1,0,0,0,1,0,0,0,1,0,1,0,0,1,1,1,\\ & 1,1,0,1,0,0,1,0,1,0,1,0,0,1,1,1,0,1,1,0,0,1,0,1,1,1,1,0,0,0,1,1,\\ & 1,1,0,0,1,1,0,0,0,1,1,0,0,1,0,1,0,0,1,0,0,1,1,1,0,0,1,1,1,0,0,0>, \end{aligned} \tag{4}$$

Moreover, the characteristic polynomial of such LHCA is (see [36]):

$$p_c\,(x) = x^{256} + x^{16} + x^3 + 1.$$

4. The Proposed Cryptosystem

The cryptographic protocol proposed in this work is, basically, a stream cipher for binary (black and white) images. It consists of three phases: The setup phase, the encryption phase, and the decryption phase.

4.1 The setup phase

In this phase, the binary image is transformed into a boolean matrix in order to interpret it as a configuration of a LHCA. In this way, every binary digitalized image defined by $r \times s$ pixels can be modelized as a boolean matrix $I = (p_{ij})$ with $1 \le i \le r$, $1 \le j \le s$,

$$p_{ij} = \begin{cases} 1, \text{ if the color of } (i, j) \text{ - th pixel is black} \\ 0, \text{ if the color of } (i, j) \text{ - th pixel is white} \end{cases}$$

4.2 The encryption phase

In this second phase, the algorithm to encrypt the image is developed in the following steps:

1. The sender constructs a LHCA with transition rules (1)-(2), whose characteristic vector is randomly chosen between the two characteristic vectors given by (3) and (4). Furthermore, the sender also randomly chooses the initial configuration of such automata, $C^{(0)}$. Recall that it is formed by 256 cells and it constitutes the secret key of the cryptosystem; consequently, $C^{(0)}$ and the characteristic vector are shared with the receiver.

2. The sender calculates the temporal evolution of the cell < 128 > from $t = 128$, to $t = 128 + r \cdot s$-1:

   $$E_{\langle 128\rangle}^{(128,128+r\cdot s-1)} = \left(a_{128}^{(128)}, a_{128}^{(129)}, \ldots, a_{128}^{(128+r\cdot s-1)}\right),$$

   which is given by the evolution of the LHCA. It constitutes the cipher sequence.

3. The sender transforms the matrix I, which defines the image, as the bit sequence:

   $S = (p_{11}, p_{12}, \ldots, p_{1s}, \ldots, p_{i1}, p_{i2}, \ldots, p_{is}, \ldots, p_{r1}, p_{r2}, \ldots, p_{rs})$,

   by simply linking together the rows of such matrix.

4. The sender add bit to bit (XOR operation) the bit sequence S to the cipher sequence $E_{\langle 128\rangle}^{(128,128+r\cdot s-1)}$, and consequently, the cryptogram is obtained:

   $$C = \left(p_{11} \oplus a_{128}^{(128)}, \ldots, p_{rs} \oplus a_{128}^{(128+r\cdot s-1)}\right)$$

5. Finally, using C, the sender can construct the `graphic' cryptogram by simply taking $p_{ij} \oplus a_{128}^{(128+(i-1)\cdot s+s-1)}$ as the color of its (i,j)-th pixel. This image is sent to the receiver.

4.3 The decryption phase

To decrypt the `graphic' cryptogram, the receiver must transform it in a sequence of bits by simply linking together the rows of such matrix. Then, he constructs the cipher sequence starting from the secret key, $C^{(0)}$, and the LHCA used, and add it bit to bit to the bit sequence obtained from the `graphic' cryptogram. As this operation is evaluative, the bit sequence representing the image defined by I, is obtained.

5. An Example

Let us consider a black and white detail of the image ``Lena" with a size of 128×128 pixels as our test image (see Figure 1). If the sender uses the LHCA given by the characteristic vector (3) and a random initial configuration $C^{(0)}$ -the secret key-, the cipher sequence is obtained considering $E_{\langle 128\rangle}^{(128,16511)}$.

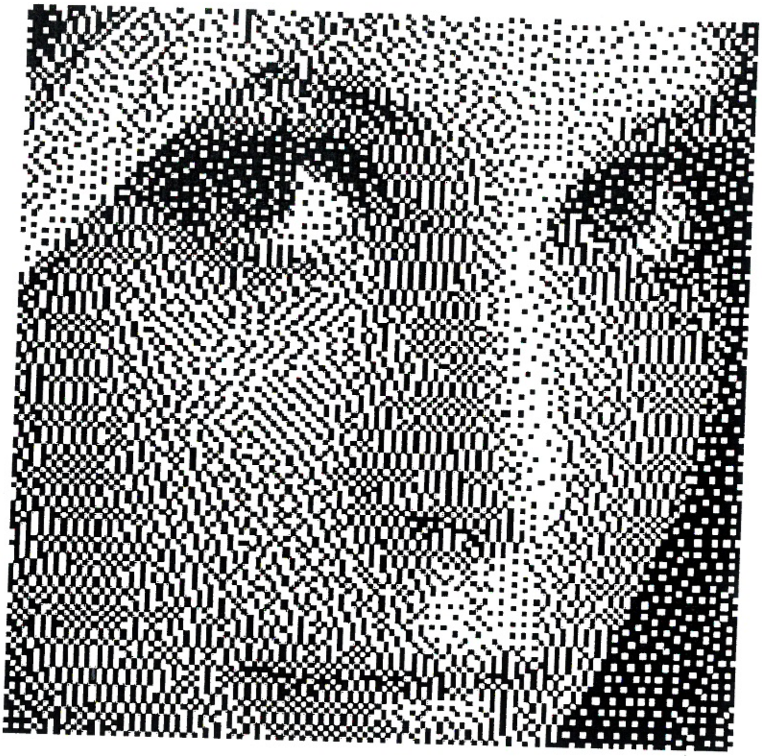

Figure 1: B&W Detail of `"Lena" of Size 128×128.

In Figure 2 the `graphic' representation of such bit sequence is shown.

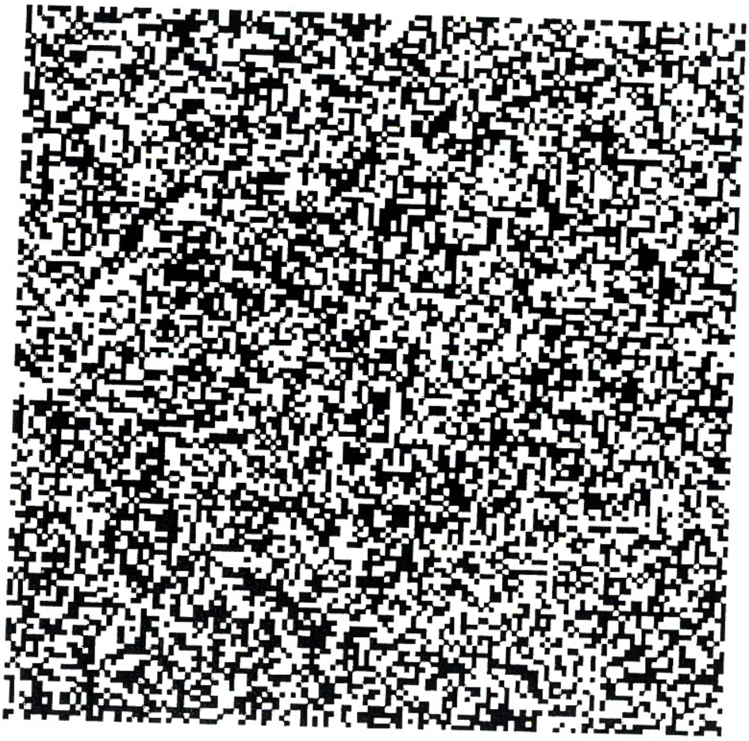

Figure 2: B&W Image Which Stands for the Cipher Sequence

Finally, if one adds bit to bit both sequences, the cryptogram is obtained. Its `graphic' representation is shown in Figure 3.

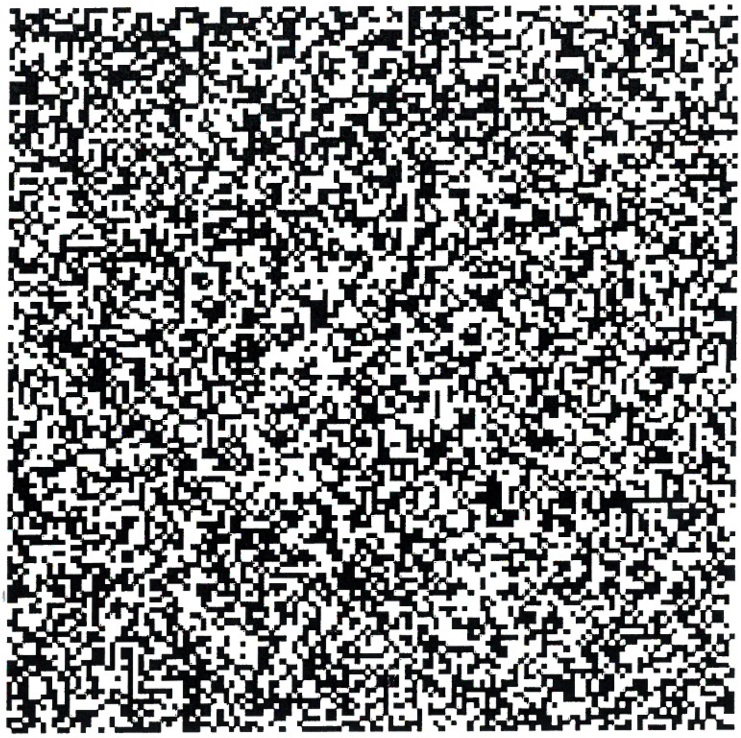

Figure 3: B&W Image Which Stands for the Cryptogram

6. Security Analysis

As we mentioned above, the LHCAs combining the Wolfram transition rules (1) and (2), and given by the characteristic vectors (3) or (4), have good pseudorandom properties with cryptographic purposes; consequently, statistical attacks are avoided. Moreover, as the length of the key used, $C^{(0)}$, is of 256 bits, then the security of the cryptosystem against brute force attacks is guaranteed (see [3]) because the total number of possible keys is roughly $1.15\cdot 10^{77}$.

Due to the structure of the transition functions, which implies that the state of a particular cell at time step $t+1$ depends on its own state and on the states of its nearest-right and nearest-left neighbour cells at time t, it is easy to check that if only one state of the initial configuration

(the secret key) is changed, then the propagation of such modification is done diagonally (see [38]). As a consequence, if we consider a LHCA with 256 cells and we take as cipher sequence the temporal evolution $E^{(0,t)}_{\langle 128\rangle}$, the change of the state of the cell < 129 > or of the cell < 127 >, with $i > 1$, in $C^{(0)}$ yields a new cipher sequence $\overline{E}^{(0,t)}_{\langle 128\rangle}$ whose first i-1 bits: $a^{(0)}_{128},\ldots,a^{(i-2)}_{128}$, are equal to the first i-1 bits of $E^{(0,t)}_{\langle 128\rangle}$. As a consequence, to guarantee the security of the proposed cryptosystem against changes of the secret key, $C^{(0)}$, we take $k = 128$ as the initial step of the cipher sequence.

As an example of the security of this protocol, if we take into account the results in Section 5, and we try to decrypt the image in Figure 3 using a cipher sequence obtained starting from a secret key which differs from the original one in only one bit: The state of cell < 128 >, then no information about the original image (Figure 1) is obtained, as it is shown in Figure 4.

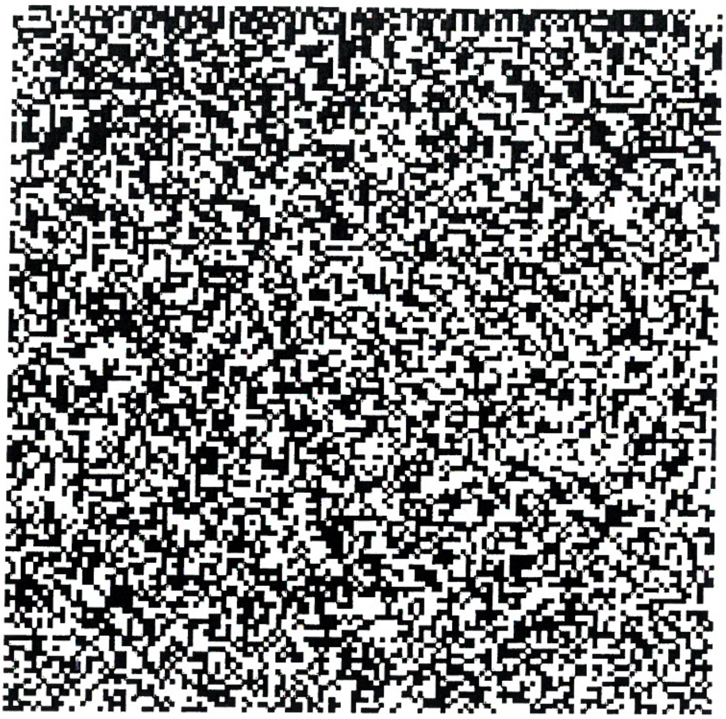

Figure 4: Decripted B&W Image Using a Modified Cipher Sequence

7. Conclusions

In this work a novel cryptosystem for binary images is developed. It is based on the use of hybrid cellular automata formed by two Wolfram transition rules as pseudorandom bit generators. Such automata have good statistical properties as pseudorandom bit generators for cryptographic purposes; consequently, statistical attacks are avoided. Moreover, the proposed cryptosystem is secure against brute force attacks.

Acknowledgements

This work has been supported by the Consejería de Educación y Cultura of Junta de Castilla y León (Spain), under the grant SA052/03.

REFERENCES

1. SCHNEIER, B., **Applied Cryptography, Second Edition**, John Wiley & Sons, 1996.
2. STINSON, D.R., **Cryptography. Theory and Practice, Second Edition**, Chapman & Hall / CRC Press, 2002.
3. MENEZES, A., VAN OORSCHOT, P. and VANSTONE, S., **Handbook of Applied Cryptography**, CRC Press, 1997.
4. SCHMITZ, R., **Use of Chaotic Dynamical Systems in Cryptography**, J. Franklin I. 338, pp. 429-441, 2001.
5. WOLFRAM, S., **Random Sequence Generation by Cellular Automata**, Adv. Appl. Math. 7, pp. 123-169, 1986.
6. BARDELL, P.H., **Analysis of Cellular Automata used as Pseudorandom Pattern Generators**, Proc. 1990 International Test Conference, pp. 762-768, 1990.
7. BAHR, A., **An Alternative Cellular Automata Cryptogram**, Studies in Informatics and Control 11, pp. 339-347, 2002.

8. DÍAZ, R., HERNÁNDEZ, A., HERNÁNDEZ, L., HOYA, S., MARTÍN, A., and RODRÍGUEZ, G., **Wolfram Cellular Automata and their Cryptographic use as Pseudorandom Bit Generators**, Internat. J. Pure Appl. Math. 4, pp. 97-103, 2003.

9. GUAN, P., **Cellular Automaton Public-Key Cryptosystem**, Complex Systems 1, pp. 51-57, 1987.

10. GUTOWITZ, H. A., **Cryptography with Dynamical Systems**, Proc. NATO Advanced Study Institute, pp. 237-274, 1993.

11. MEIER, W. and STAFFELBACH, O., **Analysis of Pseudorandom Sequences generated by Cellular Automata**, LNCS 547, pp. 186-189, 1992.

12. NANDI, S., KAR, B. K. and CHAUDHURI, P. P., **Theory and Applications of Cellular Automata in Cryptography**, IEEE Trans. Comput. 43, pp. 1346-1357, 1994.

13. TOMASSINI, M. and PERRENOUD, M., **Cryptography with Cellular Automata**, Appl. Soft. Comput. 1, pp. 151-160, 2001.

14. TOMASSINI, M., SIPPER, M., ZOLLA, M. and PERRENOUD, M., **Generating High-Quality Random Numbers in Parallel by Cellular Automata**, Future Generation Computer Systems 16, pp. 291-305, 1999.

15. HERNÁNDEZ, L., MARTÍN, A. and HERNÁNDEZ, A., **Encryption of Images with 2-Dimensional Cellular Automata**, Proc. 6th Multiconference on Systemics, Cybernetics and Informatics, Orlando, USA, pp. 471-476, 2002.

16. ALVAREZ MARAÑÓN, G., HERNÁNDEZ ENCINAS, A., HERNÁNDEZ ENCINAS, L., MARTÍN DEL REY, A. and RODRÍGUEZ SÁNCHEZ, G., **Graphics Cryptography with Pseudorandom Bit Generators and Cellular Automata**, LNAI 2773, pp. 1207-1214, 2003.

17. BOURBAKIS, N. G., **Image Data Encryption and Compression using G-SCAN**, IEEE Conference on Systems, Man and Cybernetics, pp. 1117-1120, 1997.

18. BOURBAKIS, N. G. and ALEXOPOULOS, C., **Picture Data Encryption using SCAN Patterns**, Pattern Recognition 25, pp. 567-581, 1992.

19. CHANG, CH., HWANG, M. and CHEN, T., **A New Encryption Algorithm for Images Cryptosystems**, J. Syst. Software 58, pp.83-91, 2001.

20. CHANG, H. K. and LIOU, J. L., **An Image Encryption Scheme Based on Quadtree Compression Scheme**, Proc. Int. Comput. Symp., Taiwan, pp.230-237, 1994.

21. CHANG, CH.-CH. and YU, T.-X., **Cryptanalysis of an Encryption Scheme for Binary Images**, Pattern Recognition Lett. 23, pp. 1847-1852, 2002.

22. CHUNG, K.L. and CHANG, L. C., **Large Encrypting Binary Images with Higher Security**, Pattern Recognition Lett. 19, pp. 461-468, 1998.

23. FRIDRICH, J., **Symmetric Ciphers Based on Two-Dimensional Chaotic Maps**, Internat. J. Bifur. Chaos 8, pp.1259-1284, 1998.

24. KUO, C.J., **Novel Image Encryption Technique and its Application in Progressive Transmission**, J. Electron. Imaging 2, pp. 345-351, 1993.

25. MANICAM, S.S. and BOURBAKIS, N. G., **Image and Video Encryption using SCAN Patterns**, Preprint.

26. NAOR, M. and SHAMIR, A., **Visual Cryptography**, LNCS 950, pp. 1-12, 1995.

27. TZENG, W. and HU, A., **A new approach for Visual Cryptography**, Des. Codes Cryptogr. 27, pp. 357-390, 2002.

28. CHAUDHURI, P., CHOWDHURY, D.R., NANDI, S. And CHATTOPADHYAY, S., **Additive Cellular Automata. Theory and Applications. Volume 1**, IEEE Computer Society Press, 1997.

29. MARTIN, O., ODLYZKO, A.M. and WOLFRAM, S., **Algebraic Properties of Cellular Automata**, Comm. Math. Phys. 93, pp. 219-258, 1984.

30. KNUTH, D.E, **The art of computer programming, Vol. 2. Seminumerical algorithms 3^a ed.**, Addison-Wesley, Reading, MA, 1998.

31. NIEDERREITER, N., **Random number generation and quasi-Monte Carlo methods**, SIAM, Philadelphia, 1992.

32. GOLOMB, S.W., **Shift register sequences**, Holden-Day, San Francisco, 1967.

33. FRAILE, C., **The Use of Linear Hybrid Cellular Automata as Pseudorandom Bit Generators in Cryptography**, Ph. D. Dissertation, University of Salamanca (Spain), 2003.

34. NANDI, S. and CHAUDHURI, P.P., **Analysis of Periodic and Intermediate Boundary 90/150 Cellular Automata**, IEEE T. Comput. 45, pp. 1-12, 1996.

35. CATTELL, C. and MUZIO, J. C., **Synthesis of One-Dimensional Linear Hybrid Cellular Automata**, IEEE T. Comput. Aid. Des. 15, pp. 325-335, 1996.

36. CATTELL, C. and MUZIO, J. C., **Minimal Cost One-Dimensional Linear Hybrid Cellular Automata of Degree through 500**, J. Electron. Test. 6, pp. 255-258, 1995.

37. CATTELL, C. and MUZIO, J. C., **Tables of Linear Cellular Automata for Minimal Weight Primitive Polynomials of Degrees up to 300**, Technical Report, Department of Computer Science, University of Victoria (Canada), 1997.

38. WOLFRAM, S., **Cellular Automata**, Los Alamos Science 9, pp. 2-21, 1983.