Article **ECORFAN Journal-Democratic Republic of Congo**
December 2019 Vol.5 No.9 10-16

Dynamic Partial Encryption System for Digital Image

Sistema de Cifrado Parcial Dinámico para Imágenes Digitales

RODRIGUEZ-CARDONA, Gustavo†, RAMIREZ-BELTRAN, Leonardo Humberto and RAMIREZ-TORRES, Marco Tulio*

Universidad Autónoma de San Luis Potosí / Coordinación Académica Región Altiplano Oeste

ID 1st. Author: *Gustavo, Rodríguez- Cardona* / **ORC ID**: 0000-0002-5844-6254

ID 1st.Coauthor: *Leonardo Humberto, Ramírez- Beltrán* / **ORC ID**: 0000-0002-1044-425X

ID 2nd Coauthor: *Marco Tulio, Ramírez- Torres* / **ORC ID**: 0000-0002-7457-7318

DOI: 10.35429/EJDRC.2019.9.5.10.16 Received July 28, 2019; Accepted December 20, 2019

Abstract

The present investigation is proposing a new partial encryption algorithm for digital image, using the synchronization of cellular automata based on the local rule 90. Unlike other partial encryption algorithm, which become vulnerable to attacks such as Replacement Attack or Reconstruction Attack, this system encodes different bit planes, in function of the secret key, that is, for each block of clear text, different bits are encrypted to prevent that with an elimination operation of the encrypted bits information can be revealed. The synchronization of cellular automata has proven to be a useful tool for data encryption because it is sensitivity to initial conditions and, in addition, rule 90 is considered a chaotic standard. Both characteristics ensure cryptographic and perceptive security. Based on the results of the security analysis, this research could be an attractive option for image encryption with less computer cost and without compromising information confidentiality.

Cellular automata, Rule 90, Chaotic

Resumen

En la presente investigación se propone un nuevo algoritmo de cifrado parcial para imágenes digitales, utilizando la sincronización de autómatas celulares basada en la regla local 90. A diferencia de otros algoritmos de cifrado parcial, los cuales llegan a ser vulnerables a ataques como Replacement Attack o Reconstruction Attack, este sistema cifra diferentes planos de bits, en función de la clave secreta, es decir, para cada bloque de texto en claro se cifran diferentes bits, para evitar que con una operación de eliminación de los bits cifrados se pueda revelar información. La sincronización de autómatas celulares ha demostrado ser una herramienta útil para el cifrado de datos, debido a su sensibilidad a condiciones iniciales y a que la regla 90 es considerada de patrón caótico, ambas características permiten cumplir con la seguridad criptográfica y perceptual. Con base en los resultados del análisis de seguridad, esta propuesta podría ser una opción atractiva para cifrado de imágenes con un menor costo computacional sin comprometer la confidencialidad de la información.

Autómatas celulares, Regla 90, Caótico

Citation: RODRIGUEZ-CARDONA, Gustavo, RAMIREZ-BELTRAN, Leonardo Humberto and RAMIREZ-TORRES, Marco Tulio. Dynamic Partial Encryption System for Digital Image. ECORFAN Journal-Democratic Republic of Congo. 2019, 5-9: 10-16

* Correspondence to Author (email: tulio.torres@uaslp.mx)
† Researcher contributing first author.

Introduction

Nowadays is more common that we perform more operations via internet, thus facilitating processes and optimizing time. However, this means that users require more security and protection in the transmission of personal data, since these files are exposed in transmission links. One of the techniques used to protect information is encryption systems. This technique consists on making the information unintelligible in such a way that it can only be retrieved using the correct algorithm key.

Currently, image encryption is a very active area of research due to the high demand of multiple tasks where it is required, for example: videoconferences, satellite communications, video surveillance, medical imaging systems, among others. Although there are already several conventional encryption algorithms, such as AES (Advanced Encryption Standard) and DES (Data Encryption Standard), they have often been impractical and insecure in some ways for image encryption due to their intrinsic properties, such as high data rate, strong adjacent correlation, etc (Lian s, 2008). That is the reason why security problems expands every day, since encryption algorithms must provide perceptual and cryptographic security.

To avoid high latency in the encryption system, one option is to use partial encryption algorithms. This type consists on the encryption of a specific number of bits of the clear text block, while the rest remain unchanged. All of the above results in the investigation and implementation of new image encryption schemes, such as dynamic systems based on non-linear systems. That is why this research proposes a partial encryption system based on the synchronization of cellular automata using rule 90, which is classified as a chaotic pattern. The evaluation allows us to conclude that it is a strong algorithm against cryptanalysis and statistical attacks (Espinoza, 2018).

Foundations

Cellular Automata

Cellular automata (CA) emerged in the 1940s by mathematician John Von Neumann (Von, 1966), who tried to model a machine that was capable of self-replication.

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 automatons form a two-dimensional grid where their cells evolve in discrete steps, according to a local update rule applied uniformly, over all cells. At the beginning, a state is assigned to the cells at time t = 0, where the new states will depend on their previous states and those of their neighborhood, as shown in Fig. 1.

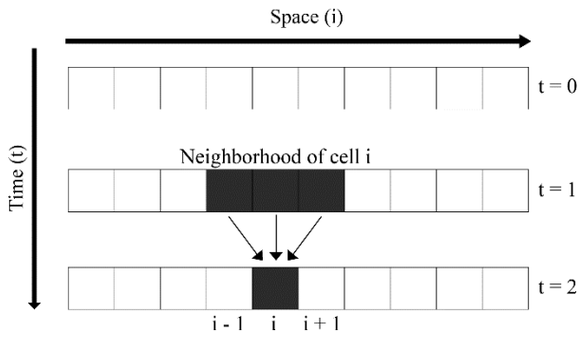


Figure 1 Space and Time Diagram of a cellular automaton
Source: Ramírez. (2015)

The assignment of values to all cells is known as configuration. The automaton receives an initial configuration and then progresses through other configurations in a sequence of discrete time steps. In each step all cells are updated simultaneously. A pre-specified rule determines the new value (Urias, 1998). This algorithm is used to calculate the next state of the cell.

Rule 90

Elemental Cellular Automata (ECA) differ from each other; just by choosing this local rule, they consider a neighborhood of radius 1, that is, a cell with its left and right neighbor. Each one can take only two values {0,1}, therefore there are only 8 combinations, resulting in 28 = 256 different local rules and ECA. Thus, local rule 90 is described by the expression of eq. (1):

$$X_i{}^{t+1} = (X^t{}_{i-1} + X^t{}_{i+1}) \; mod \; 2 \qquad (1)$$

In which X is the value in cell (0,1), $\boldsymbol{t}$ is the time and $\boldsymbol{i}$ is the index of its position. All cells obey the same rule, which can be given as a formula or as a table that specifies the new value for each possible combination of neighboring values. Rule 90 is one of the elementary rules of cellular automatons introduced by Stephen Wolfram in 1983 (Wolfram, 2018).

ISSN 2414-4924

The results of the rule are coded in the binary representation of the number 90 = 01011010.

Synchronization phenomenon

The synchronization phenomenon occurs after a period of time where the behaviors of two dynamic systems approach arbitrarily. The coupling of cellular automata occurs when a given set of coordinates (coupled coordinates) are copied from one of the systems, which is the cellular automaton known as the controller, in the system that will be called a replica. In this way, at each time step, both systems evolve with the same local rule and use the same coupled coordinates, thus synchronizing.

Next, in Fig. 2. we show a case considering n = 3, therefore the coupled coordinates are separated by $2^n - 1 = 7$ sites. In the same Fig. 2 we can see the evolution according to the rule 90 of cellular automatons of the controller and the replica with the same coupled coordinates. After $2^n - 1 = 7$ steps, the evolution of both cellular automata is the same (Urias, 1998).

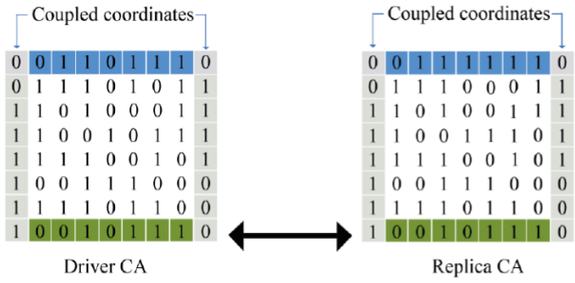


Figure 2 Synchronization phenomenon Left: CA controller. Right: CA replica
Source: Ramírez. (2015)

ESAC encryption system

The Synchronization System with Cellular Automata (SSCA) is a symmetric cipher that encrypts blocks of $\mathbf{2^k}$ -1 bit using for each block a subkey generated from an initial key. The SSCA system encrypts and decrypts a message divided into a sequence of 15-bit blocks, using a different key for each block. The same key must be used in the encryption and recovery of the original message.

The encryption mode requires a clear text block *p*, with size *L*, *p* will be the block to be encrypted. It also requires a random block *z*, with size *L + 1*, which will perform processing to *p*, and at the output it will have a processed data block $\hat{p}$. It also requires seeds that interact with each other to generate an encryption key *t* of size *N*. With this key, the data block is encrypted, obtaining the encrypted block *c*.

Based on the synchronization phenomena of the SSCA system, in ref. (Urias, 1998), the authors proposed a pseudorandom number generator (PRNG). Its main function is denoted as $h(\boldsymbol{p}, \boldsymbol{z})$and requires two vectors $\boldsymbol{p}$ and $\boldsymbol{z}$ of *n* bits and *n* + 1 bits, respectively. Where $\boldsymbol{p}$ is the pixel coefficient and $\boldsymbol{z}$ the random vector.

Pseudorandom Number Generator

Equations (2) for the generation of the key with N = 15 bits are shown below (Espinosa, 2018).

$$
\begin{aligned}
t1 &= x1 + y2 \\
t2 &= x2 + y1 + y3 \\
t3 &= x1 + x3 + y4 \\
t4 &= x4 + y1 + y3 + y5 \\
t5 &= x1 + x3 + x5 + y2 + y6 \\
t6 &= x2 + x6 + y1 + y5 + y6 \\
t7 &= x1 + x5 + x7 + y8 \\
t8 &= x8 + y1 + y5 + y7 + y9 \\
t9 &= x1 + x5 + x7 + x9 + y2 + y6 + y10 \\
t10 &= x2 + x6 + x10 + y1 + y3 + y5 + y9 + y11 \\
t11 &= x1 + x3 + x5 + x9 + x11 + y4 + y12 \\
t12 &= x4 + x12 + y1 + y3 + y9 + y11 + y13 \\
t13 &= x1 + x3 + x9 + x11 + x13 + y2 + y10 + y14 \\
t14 &= x2 + x10 + x14 + y1 + y9 + y13 + y15 \\
t15 &= x1 + x9 + x13 + x15 + y16
\end{aligned} \tag{2}
$$

Encryption function

In this paper, a partial encryption algorithm for 3 bits is proposed. It begins by encrypting the least significant bits, then the next group goes through its position and so on, until it covers all positions by performing such shift 8 times. In Ref. (Espinosa, 2018) the equations (3) were used for full 8-bit encryption.

$$
\begin{aligned}
c1 &= t1 \oplus t9 \oplus t13 \oplus t15 \oplus \widehat{p1} \\
c2 &= t2 \oplus t10 \oplus t14 \oplus \widehat{p2} \\
c3 &= t3 \oplus t11 \oplus t15 \oplus \widehat{p1} \oplus \widehat{p3} \\
c4 &= t4 \oplus t12 \oplus \widehat{p4} \\
c5 &= t5 \oplus t13 \oplus \widehat{p3} \oplus \widehat{p5} \\
c6 &= t6 \oplus t14 \oplus \widehat{p2} \oplus \widehat{p6} \\
c7 &= t7 \oplus t15 \oplus \widehat{p1} \oplus \widehat{p3} \oplus \widehat{p5} \oplus \widehat{p7} \\
c8 &= t8 \oplus \widehat{p8}
\end{aligned} \tag{3}
$$

Where $\boldsymbol{c}$ is encrypted text, $\boldsymbol{t}$ equals the secret key, and $\widehat{\boldsymbol{p}}$ is processed text.

Processing function

The processing function allows the calculation of a pseudorandom sequence through the backwards evolution in time of the cellular automaton. In Ref. (Urias, 1998) a pseudorandom number generator (PRNG) was used as a processing function, where the clear and random text blocks are taken as Boolean vectors. This processing and deprocessing function allows to change highly redundant values for others, with uniform distribution. The implementation of this generator is given by the following equations (4) and (5), based on ref. (Espinosa, 2018).

Processing

$$\begin{aligned}
\widehat{p1} &= p1 \oplus z2 \\
\widehat{p2} &= p2 \oplus z1 \oplus z3 \\
\widehat{p3} &= p1 \oplus p3 \oplus z4 \\
\widehat{p4} &= p4 \oplus z1 \oplus z3 \oplus z5 \\
\widehat{p5} &= p1 \oplus p3 \oplus p5 \oplus z2 \oplus z6 \\
\widehat{p6} &= p2 \oplus p6 \oplus z1 \oplus z5 \oplus z7 \\
\widehat{p7} &= p1 \oplus p5 \oplus p7 \oplus z8 \\
\widehat{p8} &= p8 \oplus z1 \oplus z5 \oplus z7 \oplus z9
\end{aligned} \tag{4}$$

Unprocessing

$$\begin{aligned}
p1 &= \widehat{p1} \oplus z2 \\
p2 &= \widehat{p2} \oplus z1 \oplus z3 \\
p3 &= \widehat{p1} \oplus \widehat{p3} \oplus z2 \oplus z4 \\
p4 &= \widehat{p4} \oplus z1 \oplus z3 \oplus z5 \\
p5 &= \widehat{p3} \oplus \widehat{p5} \oplus z2 \oplus z4 \oplus z6 \\
p6 &= \widehat{p2} \oplus \widehat{p6} \oplus z3 \oplus z5 \oplus z7 \\
p7 &= \widehat{p1} \oplus \widehat{p3} \oplus \widehat{p5} \oplus \widehat{p7} \oplus z4 \oplus z6 \oplus z8 \\
p8 &= \widehat{p8} \oplus z1 \oplus z5 \oplus z7 \oplus z9
\end{aligned} \tag{5}$$

Development

To perform the dynamic partial system, groups of 3 equations are made to encrypt the processed bits of $\widehat{\boldsymbol{p}}$. Table 1 shows the 8 encryption versions considered.

Version	Encrypted Bits
1	*c1 , c2, c3*
2	*c2 , c3, c4*
3	*c3 , c4, c5*
4	*c4 , c5, c6*
5	*c5 , c6, c7*
6	*c6 , c7, c8*
7	*c7 , c8, c1*
8	*c8 , c1, c2*

Table 1 Versions of partial encryption algorithms
Source: Prepared by the authors

Through this proposed algorithm, the user will be able to choose different versions of encryption mentioned in Table 1, in the order they want, due to its dynamic behavior. Therefore, the algorithm to encrypt an image consists of the following steps:

1. First, the image to be encrypted is selected.

Figure 3 Grayscale Lena image
Source: Prepared by the authors

2. The sequence of the encryption version taken from Table 1 of 8 combinations is chosen.

Figure 4 Key sequence for encryption
Source: Prepared by the authors

3. The pixel is entered as a block of clear text and we get *p*.
4. Then the pixel is processed with the vector *z* to obtain $\widehat{\boldsymbol{p}}$.
5. The *t* key is generated using the equations (2).
6. The 3 bits of the image are encrypted according to the encryption version in turn.
7. The encryption version is changed and repeated from step 2 to 6, until the entire image is encrypted.
8. The encrypted image is obtained.

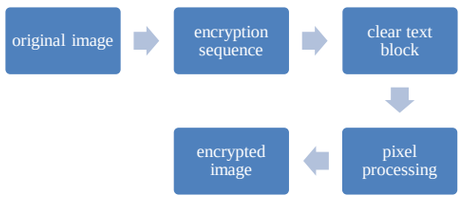
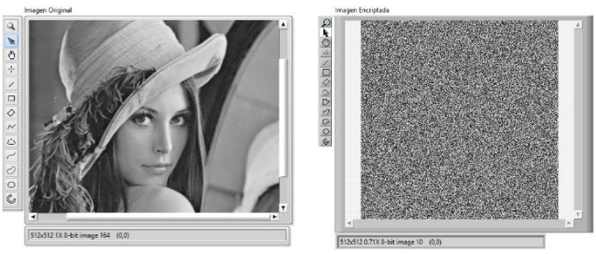


Figure 5 Steps for dynamic partial encryption
Source: Prepared by the authors

Results

To test the proposed encryption method, we considered the algorithm for several 512x512 grayscale images.



(a) (b)

Figure 6 (a) Original image of Lena. (b) Lena encrypted image using the proposed encryption
Source: Prepared by the authors

To measure the quality of the proposed encryption, several statistical tests were used, such as: histogram analysis and correlation coefficients (González, 2019), as well as cryptanalysis tests: Chosen-plaintext attack and bit replacement. The results are shown below:

Statistical Tests

Histograms

Histogram analysis shows how the pixels of an image are distributed, plotting the number of pixels according to the grayscale level. It consists of a test that measures the distribution of the pixels between the original and the encrypted image. In Fig. 7. the histogram of the original image is displayed, while in Fig. 8. the resulting histogram of the encrypted image is displayed. As we can see, the histograms of both images are different.

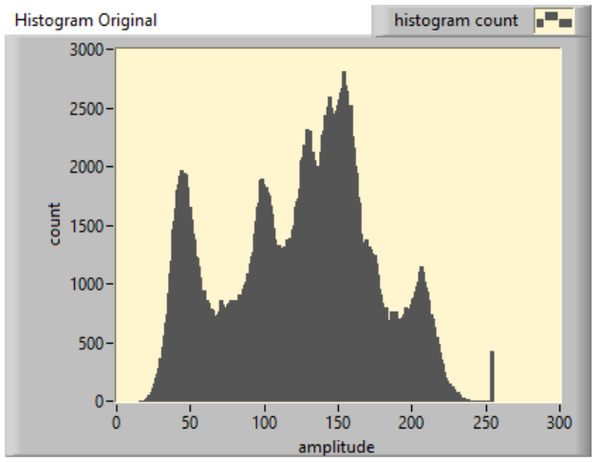


Figure 7 Histogram of the original image
Source: Prepared by the authors

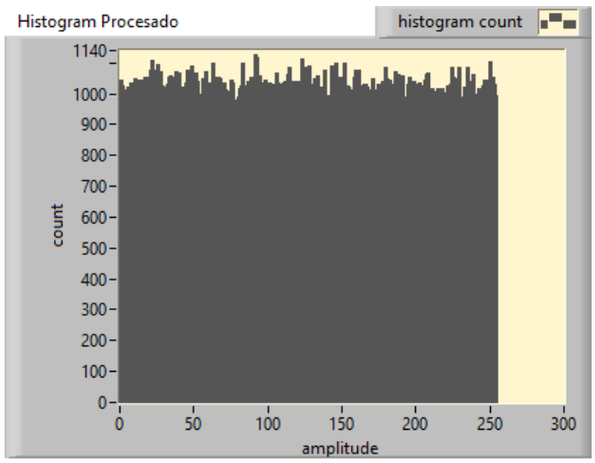


Figure 8 Histogram of the encrypted image
Source: Prepared by the authors

Correlation coefficients

In order to demonstrate that the encrypted image is different from the original image, we calculated the correlation coefficients between both images. If the calculated coefficient is close to 0 on both sides, it determines that there is no weak linear correlation, thus, the proposed system shows good performance. The results are shown in Table 2.

Image	Correlation
Lena	0.0001186

Table 2 Correlation coefficients of the encrypted image
Source: Prepared by the authors

Cryptanalysis Tests

Chosen plain-text attack

This test is intended for the attacker to reduce the security of the encryption system and reveal information.

RODRIGUEZ-CARDONA, Gustavo, RAMIREZ-BELTRAN, Leonardo Humberto and RAMIREZ-TORRES, Marco Tulio. Dynamic Partial Encryption System for Digital Image. ECORFAN Journal-Democratic Republic of Congo. 2019

Attackers can choose some images arbitrarily (images where all pixels have the same value), and obtain the corresponding encrypted images, all under the same conditions of the type of encryption used. The tests performed are shown in Fig. 9.

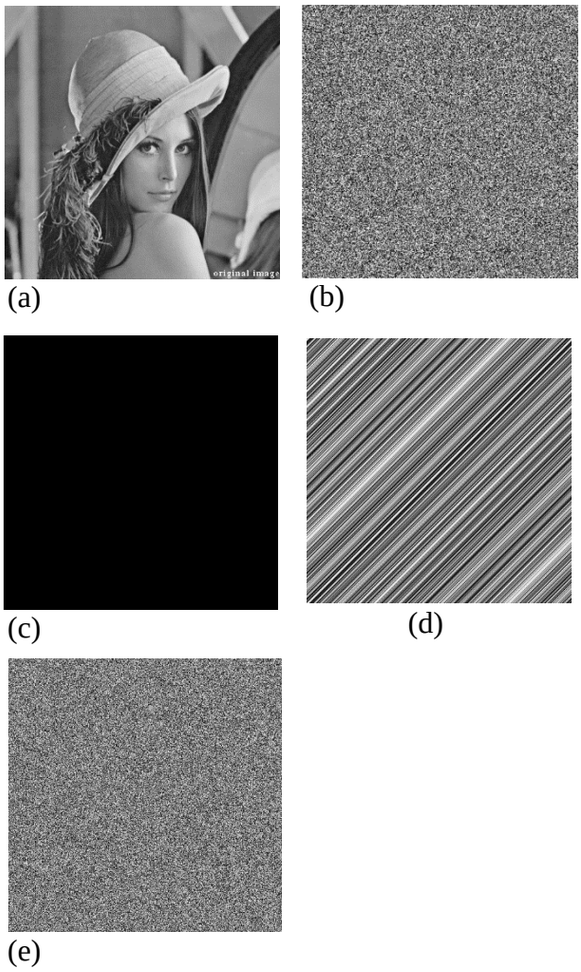


Figure 9 (a) Original image of Lena. (b) Encrypted image of (a). (c) Selected flat image. (d) Encrypted image of (c). (e) Image recovered
Source: Prepared by the authors

Replacement Attack

Assuming that the proposed encryption is secure, we carry out the attack known as a replacement attack, which consists on directly reconstructing the encrypted images. In this attack, the encrypted parts are replaced by artificial data that mimic the typical images [*IX*]. The encrypted bit plane is replaced by a constant 0, and the resulting decrease in the measured luminance is compensated by adding 64 to each pixel if only the most significant bit plane is encrypted. In Fig. 10. the resulting image can be seen, where no information is disclosed, denoting that the proposed system is safe.

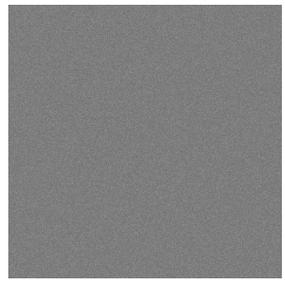


Figure 10 Image resulting from the replacement attack
Source: Prepared by the authors

Conclusions

In the present work, a dynamic partial encryption system for digital images was proposed, which was able to offer cryptographic security by using the synchronization of cellular automatons and rule 90 to better encrypt this information. Different statistical and cryptanalysis tests were carried out, with the success of the proposed algorithm. Therefore, this algorithm can be implemented in the encryption of important information.

References

Espinosa Olvera O. J. Análisis Estadístico de Cifrado Parcial, en imágenes digitales, UASLP, IICO, February 2018.

González Del Río Juan Daniel (2019). Diseño de trayectorias caóticas mediante el aumento de puntos de equilibrio en sistemas lineales por pedazos y su aplicación a la criptografía, (bachelor thesis). Universidad Autónoma de San Luis Potosí, CARAO, Salinas, SLP.

Lian, S. (2008). Multimedia content encryption: techniques and applications. Auerbach Publications.

Podesser, M., Schmidt, H. P., & Uhl, A. (2002, October). Selective bitplane encryption for secure transmission of image data in mobile environments. In CD-ROM Proceedings of the 5th IEEE Nordic Signal Processing Symposium (NORSIG 2002).

Ramirez Torres Marco Tulio, Application and implementation of an improved encryption system, (tesis de doctorado). Universidad Autónoma de San Luis Potosí, IICO, San Luis Potosí (2015).

Urias, J., Ugalde, E., Salazar, G.: Synchronization of cellular automaton pairs. Chaos: An Interdisciplinary Journal of Nonlinear Science, Vol. 8(4). AIP (1998) 814–818.

ISSN 2414-4924

Urias, J., Ugalde, E., Salazar, G.: A cryptosystem based on cellular automata. Chaos: An Interdisciplinary Journal of Nonlinear Science, Vol. 8(4). AIP (1998) 819–822.

Von Neuman, J.: Theory of Self-Reproducing Automata. Burks, A, W. University of Illinois Press (1966) 64-87.

Wolfram, S. Cellular automata and complexity: collected papres. CRC Press, (2018).:

ISSN 2414-4924