J. Automation & Systems Engineering 3-4 (2009): 226-235

Regular paper

JASE
Journal of Automation
& Systems Engineering

A New Image Encryption System Using Self Programmable Cellular Automata Stream Cipher

Zied Guitouni, Mohsen Machhout and Rached Tourki

With the ever growing in digital image processing and network communication, the cryptography protocols have become an essential requirement for the protection of the information's in communication and in storage of digital image. In this paper, we present a novel image security system based on 1-D Self Programmable Cellular Automata (SPCA). The reconfigurable architecture design and the hardware implementation on a reconfigurable platform Virtex II XC2V1000-6fg456 FPGA device of the proposed cryptosystem are described. In our scheme we used the 1-D SPCA to generate a high quality of key stream. The experimental results show the high quality of the encrypted image.

Keywords: 1-D Cellular Automata, Programmable cellular automata, Encryption image and statistical analysis.

1. INTRODUCTION

With the rapid developments in digital image processing and Internet multimedia applications, protection of image is serious issue in communication privacy and in storage and transmission of digital image. Therefore, security of digital image is necessary in many applications, such as Internet communication, multimedia systems, medical imaging, pay-TV and military communication. Since 1990, many specific methods for image encryption have been proposed, such as SCAN–based methods [1], chaos-based method [2], true structure-based method [3], and other methods. Cellular automata (CA) has been applied successfully to several physical systems, processes and scientific problems that involve local interactions, as image processing, data encryption and byte error correcting codes [10].

In this paper, we present a new image encryption method based on 1-D Self Programmable Cellular Automata (1-D SPCA). This method consists in replacing the pixel values of digital image by Xoring them with a key generated by the SPCA stream cipher. The architecture design and the hardware implementation of the cryptosystem based on 1-D SPCA in reconfigurable structure are described. In our scheme the encryption and the decryption devices share the identical modules, which give appropriate solutions for implementation of the cryptographic modules in high speed applications.

The reasons for using 1-D SPCA for image encryption/decryption are the local interactions of the CA, the very large of the number of CA evolution rules, the dynamical variation of the logical combination (CL) in function of the neighborhood of cell and the simple recursive CA substitution only requires integer arithmetic and/or logic operations. These characteristics make them easier to implement in hardware than other methods. The proposed cryptosystem is featured by its large key space, the high statistical quality of key

Electronic and Micro-Electronic Laboratory, Faculty of Sciences of Monastir, Monastir, Tunisia. ziedguitouni@yahoo.fr.

stream generated by the SPCA and the high speed to CA parallel information processing property.

This paper is organized as follows. In section 2, we introduce the theory of CA and stream generation. In section 3 we described the proposed image encrypted system using the SPCA Stream Cipher. The hardware implementation results are presented in section 4. Finally, we offer some concluding remarks in section 5.

2. 1-D CELLULAR AUTOMATA AND STREAM GENERATION

2.1. 1-D Cellular automata

A 1-D binary CA is an array of cells (registers) $[q_0(t),q_1(t),\ldots,q_n(t)]$ where each cell's state q_i Є {0,1} and i Є [0, n-1] is any of its permissible state [4]. At each discrete time step (clock cycle), each cell of the CA updates its state using a transition rule based on a Boolean function applied to the current states of each cell's state transition neighborhood $q_i(t+1) = f_i(q_1(t),q_2(t),\ldots)$. The conventional nearest three-cell state transition neighborhood, having a radius r = 1, consists of itself q_i and its left/right most neighbors q_{i-1}/q_{i+1} Cellular automata can be uniform, with the same set of state transition neighborhood/rules are used for each cell, or hybrid, where each cell can use a different set [11].

Wolfram [8] first proposed CA as Pseudo-random Number Generator (PNG). He has used uniform, 1-D CAs with r = 1, and rule 30, Hortensius et al. [5] and Nandi et al. [6] used nonuniform CAs with two rules 90 and 150, and it was found that the quality of generated Pseudo Number Sequences (PNSs) was better than the quality of the Wolfram system. Recently Tomassini and Perrenoud [7] proposed to use non uniform, 1D with r = 1 and four rules 90, 105, 150 and 165, which provide high quality pseudo number sequences and huge space of possible secret keys which is difficult for cryptanalysis.

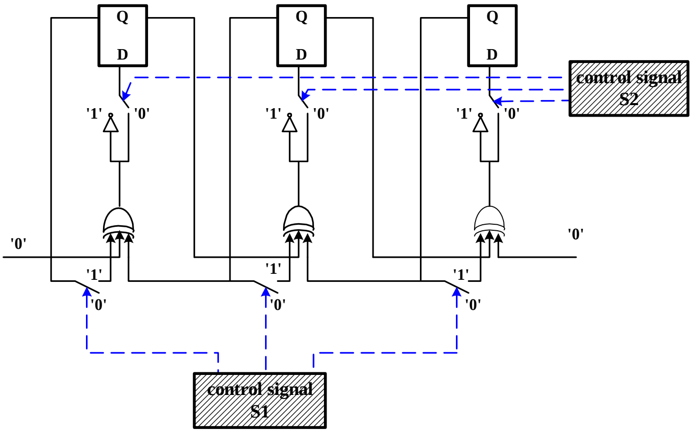


Fig. 1. Programmable cellular automata with rule 90/105/150/165.

2.2 Programmable cellular automata

The Programmable cellular automata (PCA) [8, 14], is a CA whose the state transition rule is not fixed for each cell, but controlled by a number of control signal that different functions can be generated.

Figure.1 shows the PCA shown with four programmed state transition rule, denoted as PCA 90/105/150/165. When the control signal S1 is open and the control signal S2 is open, rule 90 is applied to the cell. The cell configured with rule 150 when the control signal S1 is open and control signal S2 is closed.

In table 1, we present the different states of the control signal S1 and control signal S2 and the corresponding rule.

Table.1. The state transition rule for PCA 90/150/165/105

control signal S1	**control signal S2**	**Rule name**
0	0	90
0	1	150
1	0	165
1	1	105

2.3 Proposed self programmable cellular automata

The basic idea for the proposed self programmable cellular automata, consist to connected the control signal S1 and S2 with the output of the ith cell and the (i+1)th cell, where i Є [0,n-2] and n the total number of cells. The increased complexity of the proposed SPCA lies in the dynamical variation of the logical combination (CL) in function of the neighborhood of cell (center and right) for each discrete time step (clock cycle). In figure.2, we presented the proposed SPCA with rules 90/150/165/105.

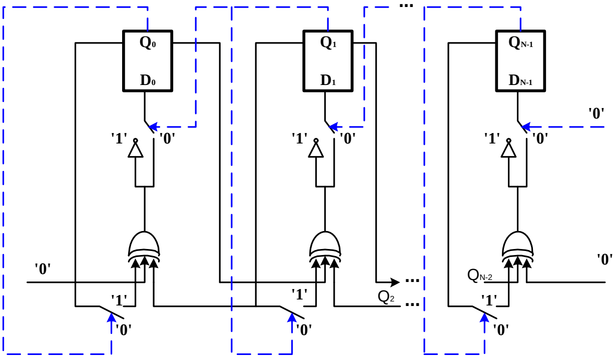


Fig.2. Proposed SPCA with rule 90/105/150/165.

In table 2, we presented the variation CL in function of the state of ith cell and the (i+1)th cell at the time t, and the corresponding rule.

Table 3. The state transition rule for SPCA 90/150/165/105

$Q_i(t)$	**$Q_{i+1}(t)$**	**CL**	**Rule name**
0	0	$Q_{i-1}(t) \oplus Q_{i+1}(t)$.	90
0	1	$Q_{i-1}(t) \oplus Q_i(t) \oplus Q_{i+1}(t)$.	150
1	0	$Q_{i-1}(t) \overline{\oplus} Q_{i+1}(t)$	165
1	1	$Q_i(t) \overline{\oplus} [Q_{i-1}(t) \oplus Q_{i+1}(t)]$	105

After this briefly description of the theory of the CA. In the next section we selected the SPCA of length 256 in design of image encryption system.

3. IMAGE ENCRYPTED SYSTEM USING THE SPCA STREAM CIPHER

3.1 Image encryption/decryption method

The basic idea of the digital image encryption system with the proposed SPCA is to substitute the pixel values by XORing the plain data with a SPCA stream generated. For the image encryption; at the same time, the input is also a sequence of 8-bit (one Pixel) data and the output is a sequence of 8-bit encrypted data. The encryption method is defined as:

$$E(x) = CAT(S(x), K(x)), 1 \le x \le N$$

Where, the $CAT(S(x), K(x))$ means that $S(x)$ and $K(x)$ execute CA transform. The CA transform is logic operation. It can be expressed as:

CAT1: $E(x) = S(x) \text{ xor } K(x)$, when the input signal select = 1, (sel = 1).

CAT2: $E(x) = S(x) \text{ xnor } K(x)$, when the input signal select = 0, (sel = 0).

In the next subsection, we presented the proposed architecture of the SPCA cryptosystem.

3.2 Proposed architecture

The proposed architecture of the SPCA cryptosystem is shown in figure 3. It is consist by three blocs:

- The input interface: is consisted by the Serial /Parallel interfaces take care of reading input data, and the control unit used to generate control signals for all other units. Among other actions, the control unit determines when to reset the cipher hardware, to accept input data and to register output results.
- The self programmable CA stream cipher: is used to generate a high quality of stream cipher.

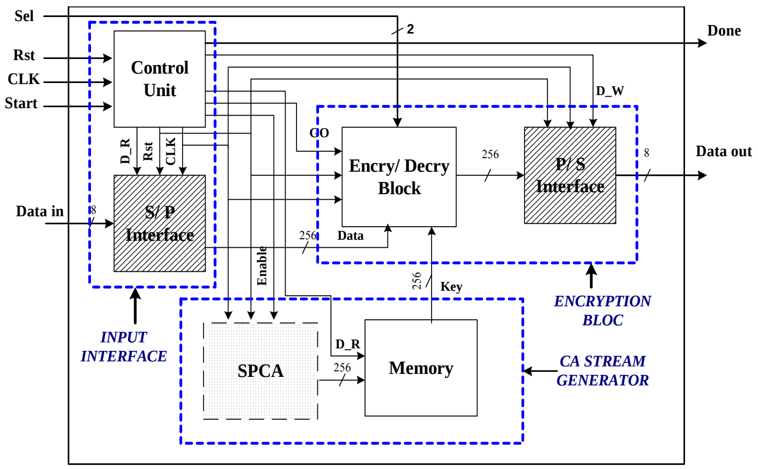


Fig.3. Proposed architecture of the SPCA crypto system

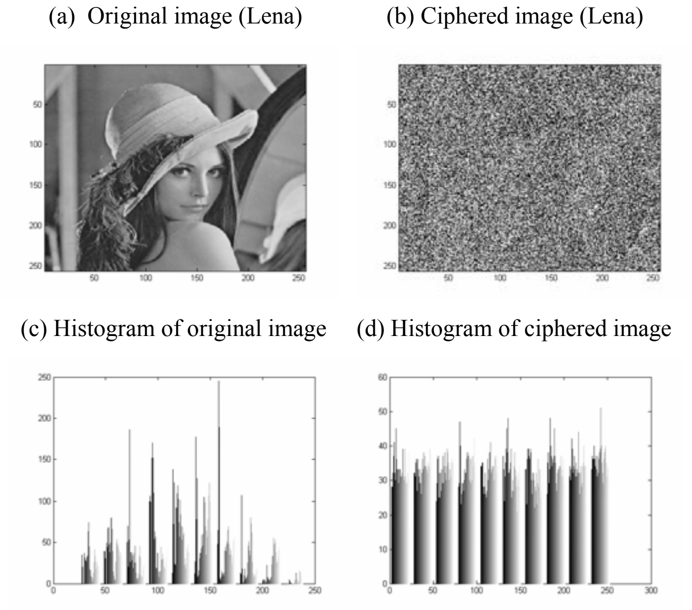
The encryption bloc: is consisted by the encryption/decryption unit is used to encrypt input data, and the Parallel/ Serial interfaces take care of writing encrypted output.

3.3 Security analysis

A good encryption scheme should resist all kinds of known attack, such as known-plaintext attack, statistical attack, differential attack, and various brute-force attacks. In this section we tested the sensitivity of the proposed SPCA crypto system by statistical approach. These tests are based on the histograms of the ciphered image, on the variation of Entropy values, and on the variation of the correlation of two vertical and horizontal adjacent pixels of the ciphered image.

3.3.1 Histogram variation

In this subsection, we have chosen the standard image Lena (256 x 256), we calculate their histograms. The simulation results are shown in figure 4.



(a) Original image (Lena)

(b) Ciphered image (Lena)

(c) Histogram of original image

(d) Histogram of ciphered image

Fig.4. Histograms of the original and ciphered image (Lena).

According to figure 4, we noticed that the histogram of the ciphered image (Lena) is fairly uniform and is significantly different from that of the original image. Therefore, it does not provide any indication to employ any statistical attack on the image under consideration.

3.3.2 Correlation and Entropy variation

In this subsection, we study the variation of the correlation and the entropy of the ciphered image.

- The correlations between two vertically adjacent pixels and two horizontally adjacent pixels respectively, in a ciphered image are given by;

$$Cov(x,y) \ = E((x - E(x)(y - E(y)) \, .$$

Where *x* and *y* are grey-scale values of two adjacent pixels in the ciphered image.

Firstly, we randomly selected n pairs of two adjacent pixels from an image. Then, we calculate the correlation coefficient of each pair. In figure 5, we present the vertically correlation of the original image and the ciphered image Lena. According to figure 5, we noticed that the uniform distribution of the ciphered image.

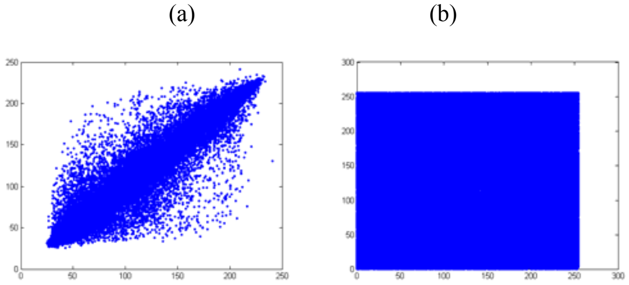


Fig.5 Vertically correlation of original image (a) and ciphered image (b)Lena (256 x 256)

- The entropy is calculated using this following equation [12]:

$$H_e = -\sum_{k=0}^{G-1} P(K)\log_2(P(K))$$

Where: H_e: entropy, G: gray value of input image (0.. 255) and $P(K)$: is the probability of the occurrence of symbol K.

3.3.3 Variation in function of init state (init key)

In order to study the sensitivity of the proposed SPCA cryptosystem in function of the initial values, we have realized many experiments for different init values. For each experiment we determined the correlation coefficients and the entropy value. The results are shown in table.3. We noticed that vertical and horizontal correlations are almost constant; these values are in the range of 0.04 to 0.06. The entropy value is about 8.

Table 3. Sensitivity of SPCA crypto system for different init value

Key	**Lena (256×256)**			**Lisaw (200×320)**		
	C_V	C_H	Entropy	C_V	C_H	Entropy
K1	0.049	0.045	7.997	0.054	0.044	7.997
K2	0.053	0.046	7.997	0.055	0.043	7.997
K3	0.050	0.050	7.997	0.058	0.041	7.997
K4	0.047	0.048	7.997	0.056	0.044	7.997
K5	0.047	0.048	7.997	0.055	0.044	7.997
K6	0.052	0.047	7.996	0.056	0.044	7.997
K7	0.047	0.051	7.997	0.057	0.043	7.997
K8	0.045	0.051	7.997	0.058	0.043	7.997
K9	0.044	0.048	7.997	0.053	0.041	7.997
K10	0.045	0.053	7.997	0.057	0.044	7.997

3.3.4 Variation in function of original image

In this subsection, we study the sensitivity of the proposed SPCA cryptosystem in function of the original image. Table 4 shows the correlation coefficients and the entropy value for different standard images such as “Lena”, “Lisaw,” “Mouse,” “Cheetah” and “Clown”. According to table.4, we noticed the high quality of the ciphered image.

Table.4. Sensitivity of hybrid CA crypto system for different standard images

Image	*Cv*	*Ch*	Entropy
Lena (256 x 256)	0.049	0.045	7.997
Cheetah (200 x 320)	0.056	0.044	7.997
Clown (200 x 320)	0.055	0.045	7.997
Lisaw (200 x 320)	0.054	0.044	7.997
Mouse (200 x 320)	0.054	0.044	7.997

4. EXPERIMENTAL RESULTS

4.1 Synthesis results

We have implemented our proposed architecture of the SPCA cryptosystem in VHDL language on a FPGA device, and synthesized using Xilinx ISE^{TM} tools. The results of performance (in terms of throughput), Frequency (Mhz), consumed area (in terms of FPGA CLB slices and LUT) and Power consumption (mw) for the implemented Processor, are presented in Table.5

Table.5. Synthesis results

Performance metrics	SPCA	SPCA
	stream cipher	crypto system
Freq (Mhz)	251.66	172.88
Total number of Slices	455 (8%)	1037 (20%)
Total number of LUTs	289 (2%)	1348 (13%)
Throughput (Mbps)	64000	44260.02
Dynamic power (mW)	131.79	414.27
Total power (mW)	483.09	765.57

According to table.5, we noticed a low area occupation of our proposed architecture of cryptosystem about 1037 Slices and a high throughput 44.260 Gbps for the reconfigurable hardware platform Virtex II (XC2V1000-6fg456) FPGA device. As illustrated in table 5, our design is economic in power consumption about 414.27 mw for the dynamic power because the encryption/decryption scheme uses integer logic operations (XOR or XNOR). These characteristics make this cryptosystem able to be implemented in an embedded system.

For the SPCA stream cipher, our design is economic in consuming computational resource is about 455 slices, the throughput is very important, it is about 64 Gbps. Low power consumption for this proposed stream cipher, it is about 131.79 mw for the dynamic power and 483.09 for the total power.

4.2 Performance comparison

The encryption/decryption method is tested and evaluated based on VHDL language. The results are obtained from a Xilinx ISE^{TM} Virtex II FPGA device. Different standard images have been used, “Lena” , “Lisaw”, “Man”, “Cow”, “San Diego”, “Conference” and “ Bread” (greyscale format) in the simulations. Table.6 shows the average time required by the SPCA cryptosystem for each image.

Table 6. Average time required by CA processor for different images

Image	Image Size	Encryption time
Lena	256×256	0.379 (ms)
Lisaw	200×320	0.370 (ms)
Man	640×480	1.776 (ms)
Cow	512×512	1.516 (ms)
San Diego	512×512	1.516 (ms)
Conference	640×480	1.776 (ms)
Bread	768×512	2.274 (ms)

Table.7 examines quantitatively the encryption time of the MIE, the VC, the N/KC and the AES [9] compared to the SPCA encryption method. In this table we have chosen the ciphered image Lena (256 x 256) We can note clearly that our proposed method is much faster than its counterpart.

Table 7. Encryption time using different algorithms with Lena as testes

Algorithm	Encryption time
MIE	270 (ms)
VC	1980 (ms)
N/KC	150 (ms)
AES	31.75 (ms)
1-D SPCA	0.379 (ms)

5. CONCLUSION

Cellular Automata have been applied successfully to several physical systems, processes and scientific problems that involve local interactions, such as image processing, data encryption and byte error correcting codes. In this paper, we present a novel image security system based on 1-D SPCA. The reconfigurable architecture design and the hardware implementation of the cryptosystem based on1-D SPCA are described. The security analysis of our proposed cryptosystem by statistical approach shows that the high quality of the SPCA for encryption image. The comparative results shown, that the timing performance of the proposed system is superior to ones other algorithms such as MIE, the VC and the AES. The proposed cryptosystem is economic in computational resource because the encryption/decryption scheme uses logic operations. The high quality of the ciphered image depends only on the dynamic transition function (rules) and on the key stream generated by the 1-D SPCA.

REFERENCES

[1] N. Bourbakis, C. Alexopoulos, Picture data encryption using SCAN patterns, Pattern Recognition, vol. 25 (6), pp567-581, 1992

[2] J. Scharinger, Fast encryption of image data using chaotic Kolmogorov flows, Electronic Imagining, Vol. 17 (2), pp 318-325, 1998.

[3] L. Chang, Large encrypting of binary images with higher security, Pattern Recognition Letter, Vol. 19 (5), pp 461-468, 1998.

[4] S-U Guan and S. K. Tan, Pseudorandom Number Generation With Self-Programmable Cellular Automata, IEEE Transactions on computers,- Aided design of integrated circuits and systems, vol 23, pp 1095-1101,July 2004.

[5] P.D. Hortensius, R.D. McLeod, and H.C. Card, Parallel Random Numbers VLSI Systems using Cellular Automata, IEE Transactions on Cmputers, vol. 38, no. 10, pp.1,466-1,473 October 1989.

[6] S.Nandi, B.K. Kar, and P.P. Chaudhuri, Theory and application of Cellular automata in cryptography, IEEE transactions on computers, vol.43, pp.1,346-1,357,1994.

[7] M. Tomassini and M. Perrenoud, “Cryptography with Cellular Automata”, Elsevier, Applied Soft Computing, vol.1, pp 151-160. (2001)

[8] S. Wolfram, Cryptography with Cellular automata, in advances in cryptography— crypto’25 (Springer-Verlag Lecture Notes in computer Sciences 218), pp. 429-432, 1986.

[9] M. Zeghid, M. Machout, R. T, A Modified AES Based Algorithm for Image Encryption, International Journal of Computer Sciences and Engineering, Vol.1 (1), pp. 70-75, 2007.

[10] R. J. Chen and J. L. Lai, Image security system using recursive cellular automata substitution, Pattern Recognition Vol. 40, 2006, pp. 1621-1631.

[11] Z. Guitouni, M. Machhout , M. Zeghid et R. Tourki, A Comparison of Architecture Design and FPGA Implementation of Programmable Cellular Automata Generator and Stream Generators, IJCSES International Journal of Computer Sciences and Engineering Systems, Vol.2, No.3,pp 185-192, 2008.

[12] M. A. Bani Younes and A. Jantan, Image Encryption Using Block-Based Transformation Algorithm, IAENG International Journal of Computer Science, Advance online publication: 19 February 2008.