FPGA Hardware Co-simulation of New Chaos-Based Stream Cipher Based on Lozi Map

Lahcene Merah, Adda Ali-Pacha, Naima Hadj-Said, Belkacem Mecheri, and Mustafa Dellassi

***Abstract*—A novel stream cipher based on chaotic synchronization is presented in this paper, a simple and effective technique is used for this purpose; it consists of feeding back the ciphertext to the cryptosystem and incorporates it on the driver signal for synchronization. Simulation results showed that the proposed stream cipher (PSC) has good confusion/diffusion properties and provide a strong key. The performed statistical and security analysis on the PSC confirms its feasibility for security purposes. The hardware-in-the-loop co-simulation over Xilinx XC6SLX45 FPGA of the PSC is provided, where a clock frequency of 50.24 MHz is achieved corresponding to high throughput of 2.51 Gbps. The obtained results make the PSC suitable for nowadays needs of secure and robust crypto-systems.**

***Index Terms*—Chaos, encryptions, synchronization, NIST, diehard, *PRNG*, FPGA.**

I. Introduction

Nowadays, the generalization of internet over the world leads to more convenient access to digital content with increasing in demand of data exchange. Concurrently, private content became subject of illegal access, and hence protection from illegal users became one of the biggest challenges facing owners.

Usually, encryption is the convenient way to ensure high security, and to fulfill these needs, a variety of encryption systems have been proposed recently [1]. Unfortunately with today's computing power; most conventional ciphers such DES, AES, IDEA, PRNGs such LFSRs, etc. are not suitable for image/video encryption in real time because their speed is slow due to a large data volume and strong correlation among image pixels [2]. Recently, there has been significant interest in exploiting chaotic dynamics in cryptography and telecommunication fields. The use of chaos in cryptography has emerged as a prospective solution to many problems because chaotic systems are deterministic in nature and exhibit sensitive dependence on their initial conditions and parameter values [3].

In fact, applying chaos for cryptography did not take much attention until the discovery of chaotic synchronization, which made a turning-point in the application of chaos dynamics for information security. The first idea on this context was proposed by Pecora and Carroll in 1990 [4]. A huge number of schemes have been developed later, which allow combining the message signal with a chaotic waveform in order to secure it. Despite the diversity of these developed schemes, however, they can be classified into three main categories; chaotic masking, chaotic shift keying, and chaotic modulation.

The first chaotic masking schemes were addressed to analog communication systems, in which a low-power information-bearing signal is added to a chaotic waveform on the emitter side [5]-[8], then extract the information from the carrier on the receiver side. Chaotic shift keying (also known as chaotic switching) was designed to transmit digital information. In this case, the binary message is used to switch the transmitted signal between two statistically similar chaotic attractors with different configuration [9]-[11]. Chaotic modulation (also called chaotic parameter modulation) is another paradigm [12], in this case the message signal is used to applies a changes on one of the chaotic systems parameters. At the receiver end, an adaptive controller is used to adaptively tune the parameters of the chaotic system such that the synchronization error approaches zero. By doing this, the output of the adaptive controller can recover the message signal [9].

Roughly speaking, despite the suitable properties of chaos dynamics for cryptography; however, direct applying of chaos is poor in terms of security and has a number of shortcoming, the evidence for that, is the number of cryptanalysis and attacks that carried out on a number of proposed chaos based cryptosystems [13]-[18]. The poor in terms of security is due to the specific requirements of nowadays cryptography [19], the computing power available today and the diversity of cryptographic attacks.

To fulfill today's information security requirements; most efforts exerted by researchers recently focused on developing strong, fast and reliable encryption systems. The present paper addresses this issue; it provide a novel scheme of chaos based cryptosystem in which, security requirements of modern communications systems have been taken into account. Accordingly to Alvarez *et al* [19]; the aim of the current work is to develop a secure cryptosystem that respects the following points: resistant to the known cryptographic attacks, has a strong key, offers a high throughput to satisfy the needs of high multimedia data volume and provides low complexity of hardware implementation and power consumption.

This paper is organized as follow: In the second section, an overview on synchronization and relationship between cryptography and chaos is given. In the third section, the proposed stream cipher (PSC) is presented. The fourth section is devoted to the evaluation of the PSC in terms of security, in Section VI; the FPGA hardware co-simulation over Xilinx XC6SLX45 is given, finally a conclusion about the achieved results is given.

Manuscript received July 15, 2016; revised October15, 2016.

Lahcene Merah, Adda Ali-Pacha, and Naima Hadj-Said are with University of science and technology of Oran, Algeria (e-mail: merahlah@gmail.com.)

Belkacem Mecheri and Mustafa Dellassi are with University of Laghouat, Algeria.

DOI: 10.7763/IJET.2017.V9.1010

II. Synchronization and Relationship between Chaos and Cryptography

Since the early 1990's researchers have realized that chaotic systems can be synchronized. The recognized potential for communications systems has driven this phenomenon to become a distinct subfield of nonlinear dynamics [20]. This was based on the discovery of chaotic synchronization principles by Pecora and Carroll [4], which sparked an avalanche of works on application of chaos in cryptography [21]. It became possible to regenerate the chaotic sequence used for encryption in the emitter side at the receiver side, making the plain-text recoverable.

Roughly speaking, the synchronization has different aspects, what concerns us is the "*identical synchronization*", in which one chaotic system forces another one to follow its trajectories, the second system (named slave or response system) is a duplicate version of the first system (named master or driver system). The driver signal sent to the response system, is one of the states of the master system.

Chaos and cryptography have some common features, Shannon has mentioned to the tight relationship between chaos and cryptography in his paper [22], it is clear that he actually discussed a typical route to chaos via stretching and folding, which is well-known in today's chaos theory [19]. Many recent works have proven the existence of strong resemblance between cryptography and chaotic behavior [19], [21], [23], [24]. Broadly speaking, according to [19], commonalities between the two systems reside on four essential points:

- The confusion property of cryptographic systems has its counterpart for chaotic systems; the ergodicity property, which refer to the homogeneous distribution of the output for any input.
- Diffusion property of cryptographic systems is compared to the high sensitivity to initial conditions of the chaotic systems. A small deviation on the input, cause a large change on the output.
- A deterministic process can cause a random-like (pseudo-random) behavior; this is the case for both cryptographic PRNGs and the chaotic systems.

As mentioned above; chaos dynamics properties are strongly suitable for cryptographic purposes, and hence a huge number of chaos based schemes have been developed. As discussed later, depending on existing attacks, and nowadays security requirements; chaos based cryptosystems should be enhanced as possible as required to avoid any eventual vulnerability against any cryptanalysis.

Many designers have failed to highlight many points related to the security level. They didn't mention to how their schemes implemented, how the key is made, how its keys are strong, how are they strong against different known cryptanalysis, etc. Therefore, the aim of the current work is to take into account all these points, in order de design a strong cryptosystem exploiting the chaotic dynamics advantages.

III. The Proposed Stream Cipher (PSC)

The following section describes the principle functioning of the PSC. We have used the chaotic map of Rene Lozi (known as Lozi map) for our study; the Lozi map presents a simple a two-dimensional map similar to the Hénon map but with the term αx_k^2 replaced by $\alpha|x_k|$. It is given by the equations system:

$$\begin{cases} x_{k+1} = 1 + y_k - \alpha.|x_k| \\ y_{k+1} = \beta.x_k \end{cases} \quad (1)$$

Numerical evidence of chaotic behavior of Lozi map can be found with α =1.4 and β = 0.3 (Fig. 1).

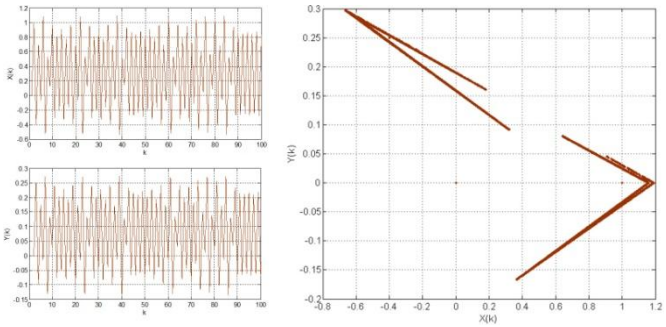

Fig.1. Lozi map outputs and 2D plot.

The computing precision adopted for the design is 64Q62 fixed point precision; 64 bits of length with 62 bits for the fractional part.

A. The Synchronization Mechanism for the PSC

Before explaining how the PSC works; we must explain how the synchronization occurs; the driver system is given by (1), whereas the response system is given by:

$$\begin{cases} x'_{k+1} = 1 + y'_k - \alpha.s(x_k) \\ y'_{k+1} = \beta.x'_k \end{cases} \quad (2)$$

The driver signal $s(x_k) = |x_k|$ is used to drive the response system. Note that $e_1 = x_{k+1} - x'_{k+1}$ and $e_2 = y_{k+1} - y'_{k+1}$ are the synchronization errors. By giving driver and the response systems different initial conditions, the evolution of e_1 and e_2 is given on the Fig.2. It is clear that after some iteration, the coupled systems synchronize and the difference between the outputs of the master and the slave system tends to zero.

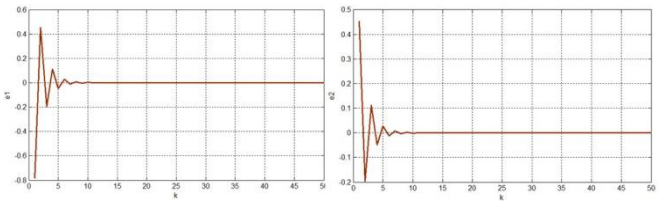

Fig. 2. Evolution of synchronization errors of Lozi coupled systems.

B. The Encryption Mechanism for the PSC

As many stream ciphers behaves, the Lozi map is used as Pseudo random number source, that generates chaotic sequence combined with plaintext. To avoid sending two signals over transmission channel (one for synchronization and other for bearing ciphertext); we propose an idea to incorporate the ciphertext on the driving signal $|x_k|$. The proposed idea is as follow: We take the driver signal $|x_k|$ which has 64 bits of length, then we divide it into two parts; the first containing the lower bits named *m* and the second

containing the upper bits named *d*, where $d + m = 64$ bits.

For the encryption purpose, the *m* lower bits of $|x_k|$ are XORed with those of the plain-text, the resulting cipher-text (which has m bits of length) is then concatenated with the d upper bits of $|x_k|$, and a new sample of $|x_k|$ is made which has 64 bits of length (d upper bits of the previous $|x_k|$ and m lower bits of the cipher-text). The new $|x_k|$ is the fed back to chaotic system, and sent in the same time to the receiver for synchronization and bearing cipher-text, Fig.3 presents the block diagram of the PSC.

On the receiver side, the response system synchronize with the driver one then the plain-text is recovered by XORing the *m* lower bits of the driver signal $|x_k|$ with m lower bits of the signal $|x'_k|$ that generated from the response chaotic system.

C. The PSC Key

The key is the first issue that encryption schemes designer should study carefully. The complexity and robustness of any cryptosystem doesn't mean anything if its key is easy to be found. Hence, the level of security of any cryptosystem must depend only on its key, how it made and how it is strong against different cryptographic attacks.

It is obvious that for chaos based cryptosystems, the key is made from the system control parameters, this is the case in our study; the control parameters *a* and *b* of the Lozi system are used for constructing the key.

It is well known that chaotic behavior of a given chaotic system cannot be maintained for any given control parameter, and consequently, parameters that not leads to a chaotic behavior, generates weak keys. The bifurcation diagrams can help us to define chaotic regions from those non-chaotic of a given system. Fig.4 presents the bifurcation diagrams of Lozi map.

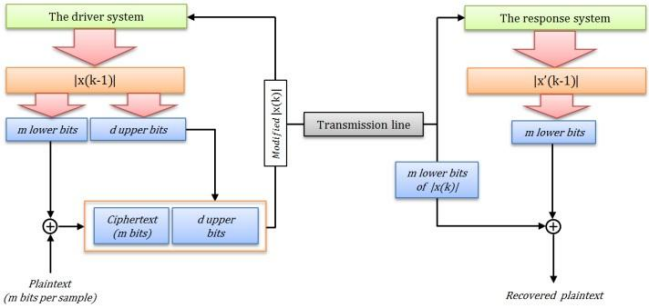

Fig. 3. Block diagram of the proposed stream cipher.

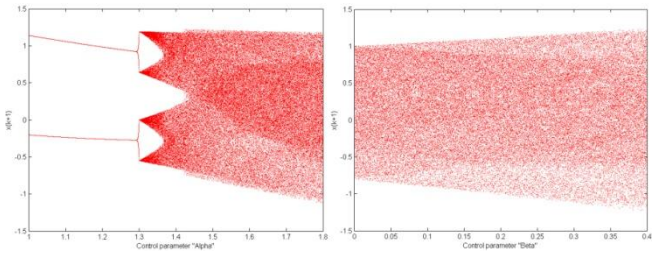

Fig. 4. Bifurcation diagrams of Lozi map for $1 \leq \alpha \leq 1.8$ and $0 \leq \beta \leq 0.4$.

Accordingly, each parameter used as key; should be out of non-chaotic regions. To avoid getting into this situation, we propose a simple method that consists of selecting restricted ranges for the keys around each parameter value. In accordance to the bifurcation diagrams of Lozi map; the chaotic behavior is maintained for $\alpha \in [1\ 1.8]$ and $\beta \in [0\ 0.4]$. So, the keys should be generated from these specified ranges.

The proposed way for generating the keys is as follow: We fix two constants $a = 1.5$ and $b = 0$; the constants *a* and *b* have 4 bits of length with two bits for the fractional part (4Q2). We specify also two integer numbers K_1 and K_2, each number has 60 bits of length. In fact, K_1 and K_2 represent the selected keys, they have both 0 to $2^{60} - 1$ possible value.

The new control parameters α' and β' are regenerated by concatenating a with K_1 and b with K_2, the results are reinterpreted as 64Q62, i.e. signed fixed point with 62 bits the fractional part, Fig.5 presents the block diagram of the way by which the PSC key is generated from the control parameters.

Thus, the defined ranges for α' and β' corresponding respectively to the minimum and the maximum of K_1 and K_2, in other words; for K_1 and $K_2 \in [0\ 2^{60} - 1]$, this corresponding to $\alpha \in [1.5\ 1.75]$ and $\beta \in [0\ 0.25]$. It is clear that α' and β' are found in ranges in which the chaotic behavior of the system is maintained.

Now, K_1 and K_2 are concatenated to produce the whole key (K), in fact, to generate a key that is equally strong; a very simple technique is used for this purpose, it consists of XORing and XNORing each lower bit of one key to the upper bit of the other key. For example; $K(0) = K_1(0)$ XOR $K_2(59)$, $K(1) = K_1(1)$ XOR $K_2(58)$,...., $K(119) = K_1(0)$ XNOR $K_2(59)$, and so on. With the proposed technique; the generated key will be equally strong.

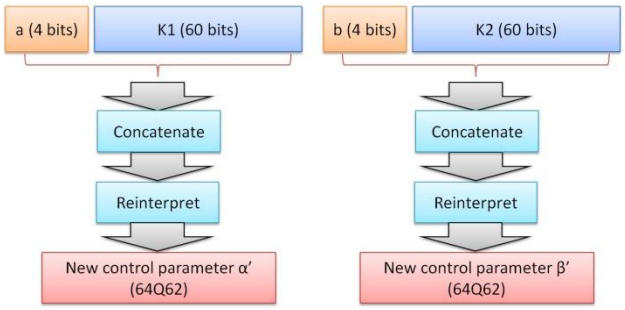

Fig. 5. The block diagram of the way by which the PSC key is generated from the control parameters.

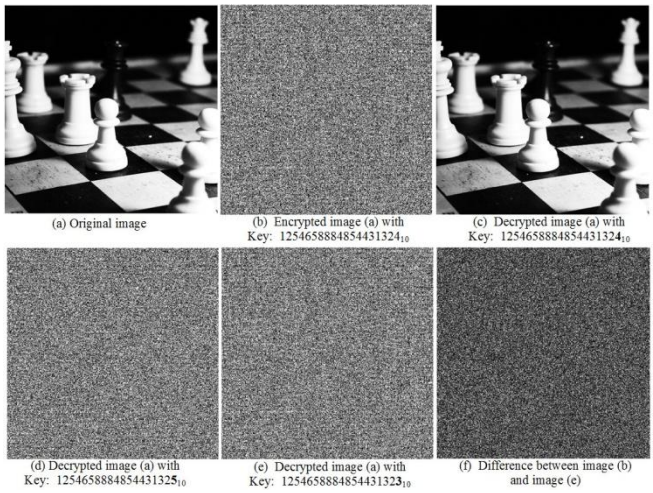

Fig. 6. Key sensitivity evaluation.

IV. Security Analysis of the PSC

The following section is intended to evaluate the PSC in terms of security, in which some security analysis are

performed.

A. Key Space and Sensitivity

The key space should be large enough to avoid brute force attacks; the authors in [19] suggest that in order to provide a sufficient security against brute-force attacks for stream ciphering; the key space size should be $K > 2^{100}$. In our case, the provided key space is 120 bits ($K = 2^{120}$), this is large enough for stream ciphering purposes.

The key sensitivity means that a slight change (flipping one bit) on the key leads to a large changes on the ciphertext. The keys should also equally strong, i.e. when an intruder uses a key that is very close to the real one (difference of one bit), no partial knowledge of the plaintext will be obtained. Fig. 6 presents the results of decryption process using different keys close to the real one.

By looking to the Fig. 6 (f); even the difference between the real key and the key used for decryption is one bit, the difference between the obtained encrypted images is 99.64%. This result confirms the strong of the key.

B. Statistical Analysis

It's well known that digital images have some special properties compared to other types of plaintexts, and these properties can be used by an attacker to get eventual relationship between ciphertext the plaintext.

- *Histogram analysis*: Gives us information about the distribution of the grey scale intensity value of pixels. Producing ciphertext with uniform histogram affirm the efficiency of the cryptosystem (confusion), Fig.7 presents the results of such analysis performed on the PSC. It is clear from these results that the PSC generate a cipher image with uniformly distributed histogram.

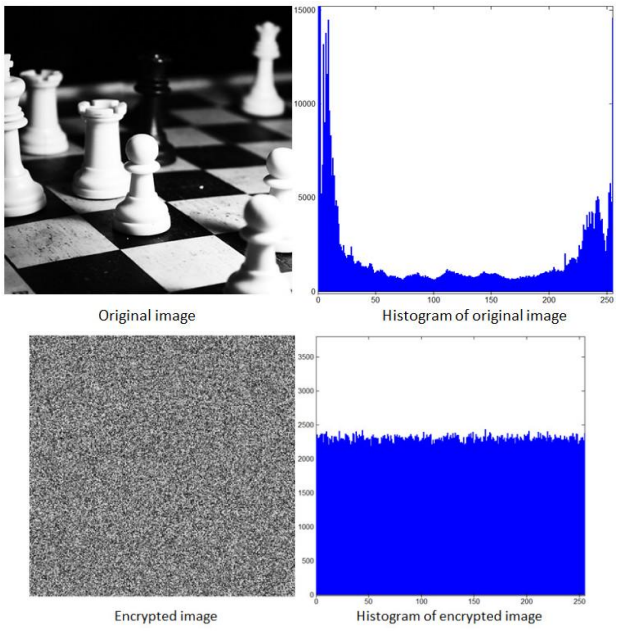

Fig.7. Histogram analysis.

- *Correlation of Adjacent Pixels*: For an ordinary image with meaningful visual perception, the correlation between adjacent pixels is always high as their pixel values are close to each other [25]. Thus, a good cryptosystem should produce cipher images with low correlation between adjacent pixels. Mathematical formulas used for computing the correlation between adjacent pixel over horizontal, vertical and diagonal direction can be found on [25]. It is clear from the obtained results (Table I and Fig. 8), that the adjacent pixels of the cipher image are completely decorrelated and thus far from the plain image.

TABLE I: CORRELATION COEFFICIENTS VALUES OF TWO ADJACENT PIXELS FOR THE ORIGINAL AND ENCRYPTED IMAGES

Direction	Plain image	Encrypted image
Diagonal	0.96391	0.03156
Horizontal	0.91252	0.01591
Vertical	0.97467	0.00770

C. Differential Cryptanalysis

Differential cryptanalysis is a chosen-plaintext attack where the attacker makes an infinitesimal change between two identical plaintexts (e.g., modifying only one pixel for two images), and observes the corresponding ciphertexts (denoted C_1 and C_2) to get a relationship leads to the cipher stream. Chen *et al* [25] have employed two measurements for this purpose (applied to image): number of pixels change rate (NPCR) and unified average changing intensity (UACI) where:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \quad (3)$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\% \quad (4)$$

$$\text{Where : } D(i,j) = \begin{cases} 0 \; if \; C_1(i,j) = C_2(i,j) \\ 1 \qquad otherwise \end{cases} \quad (5)$$

W and H represent respectively, the width and the height of the image. The differential cryptanalysis is performed to the PSC, and after 200 cipher rounds (encryption/decryption processes), the computed NPCR found confined in [99:51%; 99:70%], whereas the UACI in [33:05%; 33:79%], the obtained results show that the PSC resisted the differential cryptanalysis successfully.

D. Statistical Tests Application

In the most proposed chaos based cryptosystems, chaotic systems acts pseudo-random numbers generator. Generators suitable for use in cryptographic applications may need to meet stronger requirements than for other applications. In particular, their outputs must be unpredictable in the absence of knowledge of the inputs [26]. There are two famous batteries of statistical tests, the first proposed by the National Institute of Standards & Technology (NIST) and contain 15 tests [26], and the second is the Diehard tests; it was developed by George Marsaglia, published for the first time in 1995 on a CD-ROM and contain 18 statistical tests [27]. For both batteries; a p_value (level of significance) is computed and must greater or equal to 0.01 to say that test is passed successfully.

Experiment showed that the maximum value of m that the system can encrypt per clock cycle without altering the chaotic behavior is 48 bits. It should be noted also that, the Lozi map is perturbed continuously by the plain-text, so to be sure about the randomness of the chaotic sequence (*m* lower

bits of the driver signal), the statistical test will carried out on the chaotic sequence without any feedback, and on the chaotic sequence with load of a plain-text of zeros of values. The Fig.9 presents the distribution of p value for both tests NIST and DieHard. It is clear that all the tests are passed successfully with *p_value* > 0,01.

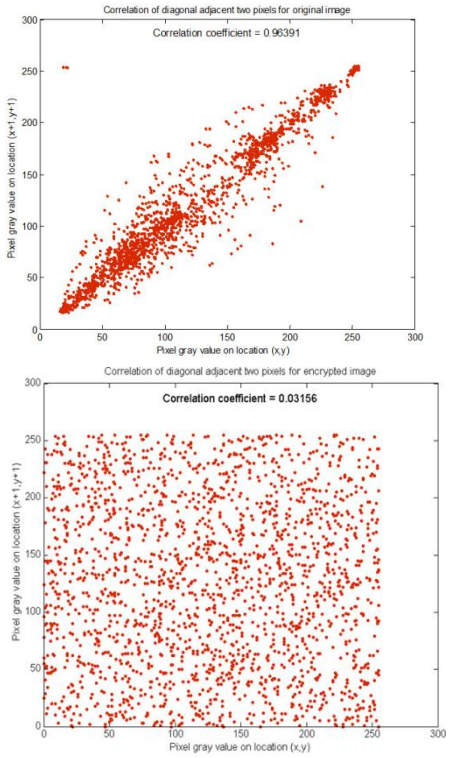

Fig. 8. Correlations of two vertically adjacent pixels of the original image and the encrypted one.

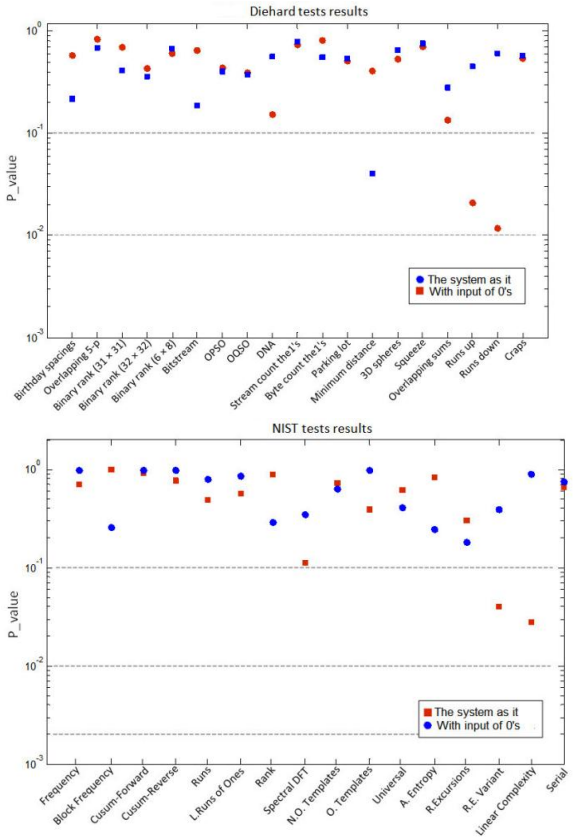

Fig. 9. Distribution of p value for both tests NIST and Diehard performed on the PSC.

V. FPGA Hardware Co-Simulation of the PSC

The PSC was designed using the direct VHDL coding, and then exported as black boxes to the MATLAB/SIMULINK environment, in order to perform the simulation and then the FPGA hardware co-simulation based on XSG (Xilinx System Generator tool). The hardware co-simulation is performed on Xilinx XC6SLX45 FPGA, the design was optimized by adding pipeline stages to obtain a maximum frequency. Table II summarizes the resources utilization and the achieved frequency.

TABLE II: Resource Utilization on Xilinx XC6SLX45 FPGA

	Utilization	Available
Slice Registers	386	54776
Slice LUTs	562	27288
DSP48A1s slices	32	58
Clock Freq (MHz)	50.24	

The maximum achievable frequency is 50.24 MHz, this means that the possible throughput is $m \times f = 50$ bits $\times$ 50,24 MHz = 2.51 Gbps.

The complete design is presented in Fig.10, when the plain-image signal is obtained from a webcam in real time, then passed through some Simulink blocks to convert the image frame into a serial pixel stream that enters the hardware. The serial data of the plain-image sent to the FPGA through the Ethernet point-to-point port (co-sim block). After the real time encryption process, the serial stream output from the hardware is taken and built back up a frame of data and viewed on the Simulink Video viewer.

The PSC real time FPGA hardware co-simulation works well and the obtained results were as expected.

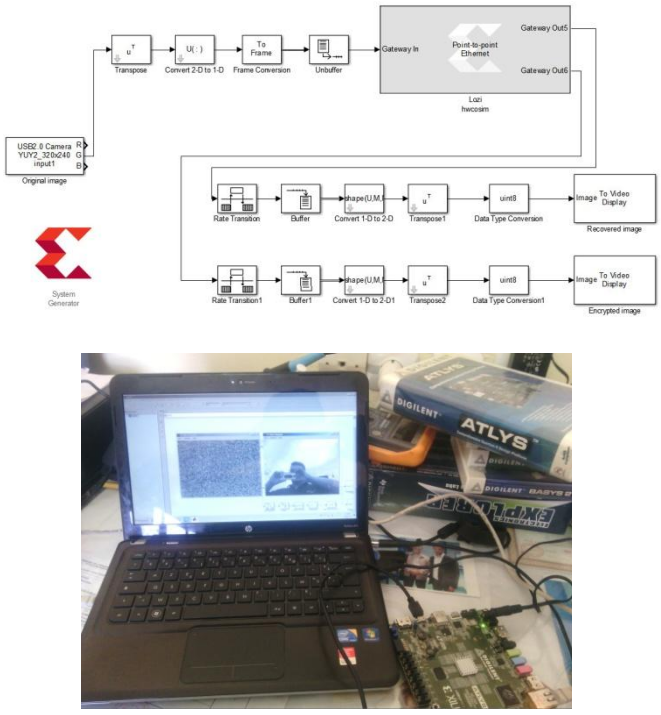

Fig. 10. Real-time hardware co-simulation of the PSC.

VI. Conclusion

To the best of authors' knowledge, this is the first stream cipher that provides good security properties with guaranteed of synchronization. By feeding back the cipher-text to the

chaotic system, ensuring synchronization and specifying an appropriate ranges from the control parameters for generating the keys; a reliable cryptosystem is obtained. Different security analysis performed on the PSC and the key space that provides, shows its efficiency for security purposes. The FPGA hardware co-simulation results showed that, the PSC can reaches a throughput of 2.51 Gbps which satisfies the nowadays high throughput demands.

REFERENCES

[1] C. Paar and J. Pelzl, "Understanding cryptography: A textbook for students and practitioners," Springer Science and Business Media, 2009.

[2] V. Das and N. Thankachan, "Computational intelligence and information technology: First international conference," Springer Science and Business Media, 2013.

[3] M. K. Khan, "Chaotic cryptography and its applications in telecommunication systems," 2013, pp. 513-514.

[4] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," *Physical Review Letters*, vol. 64, no. 8, p. 821.

[5] K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz, "Synchronization of Lorenz-based chaotic circuits with applications to communications," *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, vol. 40, no. 10, pp. 626-633, 1993.

[6] K. M. Cuomo, A. V. Oppenheim, and S. H. Isabelle, "Spread spectrum modulation and signal masking using synchronized chaotic systems," *Massachusetts Inst of Tech Cambridge Research Lab of Electronics*, 1992.

[7] L. Kocarev, K. S. Halle, K. Eckert, L. O. Chua, and U. Parlitz, "Experimental demonstration of secure communications via chaotic synchronization," *International Journal of Bifurcation and Chaos*, vol. 2, no. 03, pp. 709-713, 1992.

[8] Ö. Morgül and M. Feki, "A chaotic masking scheme by using synchronized chaotic systems," *Physics Letters A*, vol. 251, no. 3, pp. 169-176, 1999.

[9] T. Yang, "A survey of chaotic secure communication systems," *International Journal of Computational Cognition*, vol. 2, no. 2, pp. 81-130, 2004.

[10] H. Dedieu, M. P. Kennedy, and M. Hasler, "Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits," *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, vol. 40, no. 10, pp. 634-642, 1993.

[11] U. Parlitz, L. O. Chua, L. Kocarev, K. S. Halle, and A. Shang, "Transmission of digital signals by chaotic synchronization," *International Journal of Bifurcation and Chaos*, vol. 2, no. 04, pp. 973-977, 1992.

[12] A. G-Modulation, "Secure communication via chaotic parameter modulation," *IEEE Transactions on Circuits and Systems—I: Fundamental Theory and Applications*, vol. 43, no. 9, pp. 817, 1996.

[13] G. Pérez and H. A.Cerdeira, "Extracting messages masked by chaos," *Physical Review Letters*, vol. 74, no. 11, 1995.

[14] A. Jacobo, M. C. Soriano, P. Colet, and C. Mirasso, "Breaking chaotic encryption using PDE's," in *Proc. IEEE European Conference on Lasers and Electro-Optics 2009 and the European Quantum Electronics Conference. CLEO Europe-EQEC 2009*, pp. 1-1, 2009.

[15] G. Alvarez and S. Li, "Breaking network security based on synchronized chaos," *Computer Communications*, vol. 27, no. 16, pp. 1679-1681, 2004.

[16] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International Journal of Bifurcation and Chaos*, vol. 16, no. 8, pp. 2129-2151, 2006.

[17] M. Kalpana and P. Balasubramaniam, "Stochastic asymptotical synchronization of chaotic Markovian jumping fuzzy cellular neural networks with mixed delays and the Wiener process based on sampled-data control," *Chinese Physics B*, vol. 22, no. 7, p. 078401, 2013.

[18] E. Solak, C. Çokal, O. T. Yildiz, and T. Biyikoğlu, "Cryptanalysis of Fridrich's chaotic image encryption," *International Journal of Bifurcation and Chaos*, vol. 20, no. 5, pp. 1405-1413, 2010.

[19] G. Alvarez and S. Li, "Breaking an encryption scheme based on chaotic baker map," *Physics Letters A*, vol. 352, no. 1, pp. 78-82, 2006.

[20] Y. Zhang, and P. R. Nanchang, Breaking a RGB Image Encryption Algorithm Based on DNA Encoding and Chaos Map.

[21] A. Pande and J. Zambreno, "A chaotic encryption scheme for real-time embedded systems: design and implementation," *Telecommunication Systems*, vol. 52, no. 2, pp. 551-561, 2013.

[22] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656-715, 1949.

[23] L. Kocarev, "Chaos-based cryptography: A brief overview," *IEEE Circuits and Systems Magazine*, vol. 1, no. 3, pp. 6-21, 2001.

[24] P. L. Carmen and L. R. Ricardo, "Notions of chaotic cryptography: Sketch of a chaos based cryptosystem," *Applied Cryptography and Network Security*, p. 267, 2012.

[25] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons and Fractals*, vol. 21, no. 3, pp. 749-761, 2004.

[26] A. Rukhin *et al.*, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Booz-Allen and Hamilton Inc Mclean Va, 2001.

[27] M. George. Diehard Statistical Tests. [Online]. Available: http://stat.fsu.edu/geodiehard.html

Lahcene Merah is a graduate student working with Pr. Adda Ali-Pacha on his dissertation 'Securing mo-dern communication systems using chaotic signals'. He received his engineering dipl-oma on electronics in 2004 from Laghouat University in Algeria; he continued his study on communication systems in University of science and technology of Oran where he received his magister degree in 2010, he preparing his PhD from the same university where his research interests are in the application of chaotic signals to the information security and the embedded systems.

Adda ALI-Pacha was born in Algeria. He graduated in telecommunications engineering of Oran in January 1986. He got a university degrees in mathematics in June 1986 and a magister in signal processing in November 1993. Later he obtained a Ph.D. in safety data in December 2004.

He worked in the telecommunications administration (PTT Oran) in the position of the head of telephone traffic for two years (1986 -1988), since 1989 he is at the University of Sciences and Technology of Oran (U.S.T.O) Algeria, as a teacher/researcher in the Electronics Institute.

The Telecommunication domains are his favorite interest fields' research.

Hadj-Said Naima received the engineering degree in telecommunications from the Telecommunications Engin-eering of Oran (ITO) in 1986, and the magister degree also from ITO in (1992) and a PhD from the University of Sciences and Technology, Mohamed Boudiaf (USTO,MB) Oran (Algeria) in 2005. He is an associate professor at the computer sciences Department of University of Sciences and Technology, Mohamed Boudiaf (USTO,MB) Oran (Algeria). His research interests are in the area of Digital Communications, and cryptography.