Statistical Analysis and Security Evaluation of Chaotic RC5-CBC Symmetric Key Block Cipher Algorithm

Abdessalem Abidi[1], Anissa Sghaier[2], Mohsen Machhout[5]
Electronics and Microelectronics Lab.
Faculty of Sciences of Monastir
University of Monastir
Tunisia

Mohammed Bakiri[3]
Centre de Développement des Technologies
Avancées ASM/DMN Department
Cité 20 août 1956 Baba Hassen, B. P 17, 16303
Alger, Algeria

Christophe Guyeux[4]
FEMTO-ST Institute, UMR 6174 CNRS,
University of Franche-Comté, France

***Abstract*—In some previous research works, it has been theoretically proven that RC5-CBC encryption algorithm behaves as a Devaney topological chaos dynamical system. This unpredictable behavior has been experimentally illustrated through such sensitivity tests analyses encompassing the avalanche effect phenomenon evaluation. In this paper, which is an extension of our previous work, we aim to prove that RC5 algorithm can guarantee a much better level of security and randomness while behaving chaotically, namely when embedded with CBC mode of encryption. To do this, we have began by evaluating the quality of such images encrypted under chaotic RC5-CBC symmetric key encryption algorithm. Then, we have presented the synthesis results of an hardware architecture that implements this chaotic algorithm in FPGA circuits.**

Keywords*—*Cipher Block Chaining (CBC); Rivest Cipher 5 (RC5); chaotic dynamical system; sensibility; security; randomness

I. Introduction

The main types of symmetric cryptosystems used nowadays fall into two broad categories: block cipher algorithms which consists of processing a data blocks of fixed size and the stream cipher algorithms operating on a continuous stream of data [19], [5]. In this article, we focus on the study of one of the most famous symmetric key block cipher algorithms, namely the Rivest Cipher 5 (RC5) [16]. This encryption algorithm has been designed by Ronald Rivest and it first appeared in December 1994 [7]. Unlike DES [15] for instance, where the block size and the key size must be respectively 64 and 56 bits, in RC5, the block size, the number of rounds and the length of the secret key all can be of variable length. This provides the opportunity for great flexibility in both performance characteristics and the level of security.

As any block cipher algorithm, it is not sufficient to put anyhow the RC5 block cipher algorithm in a program. Hence, various modes of operation have been standardized in order to allow those ciphers to work with large data streams, without the risk of compromising the provided security. In our previous research work, the RC5 algorithm has been used inside the CBC mode of operation in order to form the so-called RC5-CBC. Indeed, the chaotic behavior of this algorithm has been theoretically proven according to the reputed definition of Devaney [9] and then experimentally evaluated through sensitivity tests involving the avalanche effect phenomenon [2].

The mathematical theory of chaos is fully legitimate for iterations over discrete infinite sets. The chaos theory that has been considered in our previous articles is the Devaney's topological one [9]. This theory does not only provide one of the best mathematical definition of chaos, but it also offers a framework with qualitative and quantitative tools to evaluate how unpredictable a recurrent system is [13].

The main purpose of this paper is to evaluate the influence of the chaotic behavior of an encryption system on its security level. Precisely, we have demonstrated that Rivest Cipher 5 algorithm can offer a much better level of security and randomness when behaving chaotically, that is to say, when embedded with CBC mode of operation. To this end, we have began by making a comparison between the quality of such selected images encrypted by chaotic RC5-CBC and the same images encrypted with the standalone RC5. In addition, we have interpreted the synthesis results of an hardware architecture that implements the chaotic RC5-CBC in FPGA circuits.

The remainder of this paper is organized as follows. In Section 2, we will recall some basic definitions concerning cipher block chaining mode of operation and RC5 encryption algorithm. Section 3 is devoted to sum up our various obtained results that have been detailed in [2]. Sections 4 and 5 are devoted to experimental evaluations that put in evidence RC5 presents a much better level of security and randomness when behaving chaotically namely while working with CBC mode of operation. In Section 6, we will discuss our contribution. This research work ends by conclusion section, in which contributions are recalled and summarized.

II. Literature Review

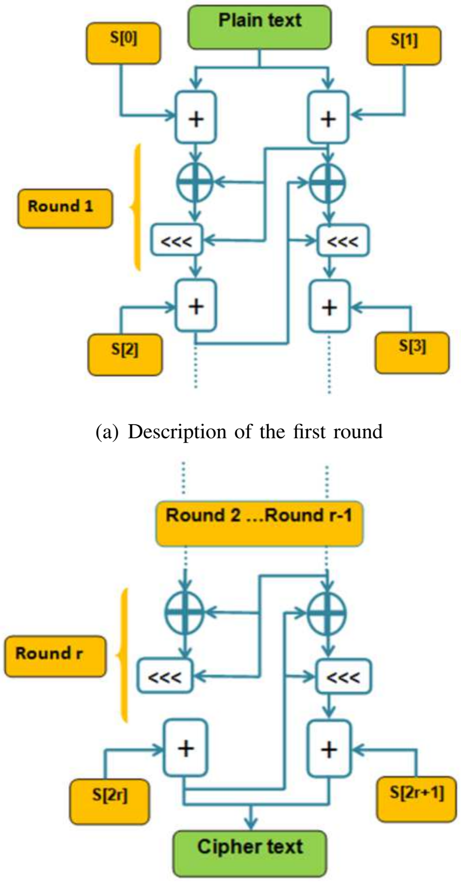
A. Rivest Cipher 5 Symmetric Key Encryption Algorithm

The RC5 encryption algorithm is a symmetric key block cipher algorithm designed by Ronald Rivest of Massachusetts Institute of technology (MIT) and it first appeared in December 1994 [12], [1]. Unlike DES [8] for instance, where the block size and the key size must be respectively 64 and 56 bits, in RC5, the block size, the number of rounds and the length of the secret key all can be of variable length. This provides the opportunity for great flexibility in both performance characteristics and the level of security.

As mentioned in Algorithm 1 and Fig. 1, the encryption using RC5 is based on only three operations: addition, exclusive-OR, and rotation. This makes RC5 both easy to implement for software and hardware applications, and more amenable to analysis than many other block ciphers. The connection between simplicity of design and simplicity of analysis was indeed one of Rivest main goals [3].

Algorithm 1 Encryption using RC5 Algorithm

```
Require: The input block to RC5 consists of two w-bits words given in two registers A and B.
Ensure: The output is also placed in the registers A and B.
  First, divide the original plain text into two blocks of equal sizes called A and B
  for $i = 1$ to r do do
    $A \leftarrow ((A \oplus B) <<< B) + S[2i]$
    $B \leftarrow ((B \oplus A) <<< B) + S[2i+1]$
  end for
```



(a) Description of the first round

(b) Description of the final round

Fig. 1. Encryption phase using RC5 block cipher algorithm

B. Description of RC5 Block Cipher Operating with CBC Mode

Fig. 2 depicts how RC5 algorithm is embedded with CBC mode of encryption in order to form the so-called RC5-CBC. In this algorithm, the input data is firstly divided into 16 bits blocks $(m_0, m_1, ..., m_n)$. The XOR function is applied between each m_i block and its corresponding previously encrypted C_{i-1} block to give CBC_Result_i block as output which, in turn, will be Xored with m_{i+1} block forming the input of the RC5 algorithm which provides as a result the C_i encrypted block and so on. For the first block, the initialization vector acts as the previous encrypted one. Finally, all blocks that have been encrypted separately are then gathered in a particular way, to obtain the complete encrypted message. For decryption, the path remains the same but this time starting from the encrypted block to obtain the original one using the decryption algorithm instead of the encryption function.

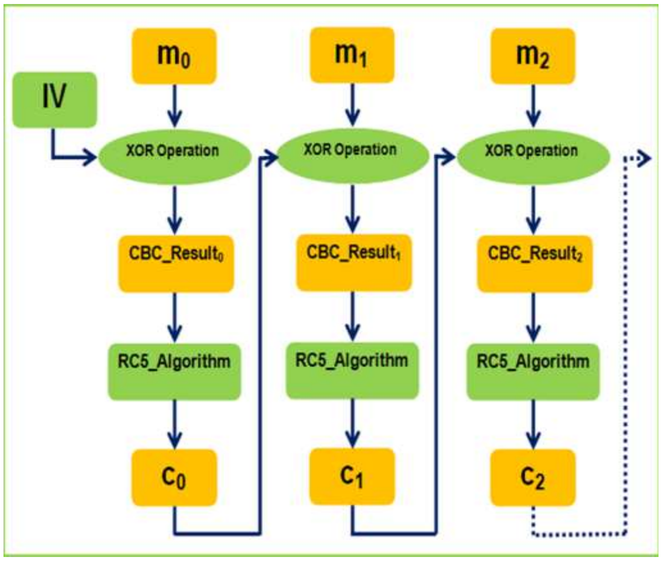


Fig. 2. CBC mode of encryption embedded with RC5 block cipher Algorithm

III. Previously Obtained Results

In this section we will summarize our previous results that have been detailed in [2].

A. Proving of Chaotic Behavior of RC5-CBC Block Cipher

In favor of evaluating the chaotic behavior of RC5-CBC block cipher according to the reputed definition of Devaney, it is indispensable to investigate the connectivity of its corresponding directed graph. Let us recall that:

Definition 1: Devaney's formulation of chaos [9]: The function f is chaotic on a metric space $(\mathcal{X}, d)$ if f is regular, topologically transitive, and has sensitive dependence on initial conditions. Banks et al. have proven that when f is regular and transitive on a metric space $(\mathcal{X}, d)$, then f has the property of sensitive dependence on initial conditions. This is why chaos can be formulated too in a topological space $(\mathcal{X}, \tau)$: in that situation, chaos is obtained when f is regular and topologically transitive [11]. Note that the transitivity property is often obtained as a consequence of the strong transitivity one, which is defined below.

Definition 2: f is strongly transitive on $(\mathcal{X}, d)$ if, for all point $x, y \in \mathcal{X}$ and for all neighborhood $\mathcal{V}$ of x, it exists $n \in \mathbb{N}$ and $x' \in \mathcal{V}$ such that $f^n(x') = y$. Therefore, the sole condition to put in evidence that RC5-CBC block cipher is chaotic according to Devaney consists of proving the strong connectivity of its corresponding directed graph $\mathcal{G}_g$.

In fact, there are different methods to check the connectivity of a given directed graph. In our previous research work, we have chosen to use the optimized method referred as Kosaraju's Depth First Traversal (DFS) algorithm [6], [10]. For the sake of completeness, its steps are recalled hereafter:

- All vertices are initialized as not been visited.
- Do a Depth First Search (DFS) traversal of graph starting from any arbitrary vertex v. Return False if DFS traversal does not visit all vertices.
- Reverse all edges (or find transpose or reverse of graph).
- Mark all vertices as not visited in reversed graph.
- Again do a DFS traversal of reversed graph starting from same vertex v (same as Step 2). If DFS traversal does not visit all vertices, then return False. Otherwise, return True.

Thanks to this technique, we have succeeded to prove the strong connectivity of the directed graph G_g. So, we have concluded that:

Theorem 1: The CBC mode of operation is chaotic according to Devaney when the embedded block cipher is the symmetric key encryption algorithm RC5.

To put a nutshell, our work that has been detailed in [2] consists primarily in constructing an ad hoc directed graph related to the RC5-CBC and then confirming its strong connectivity using the optimized method referred as Kosaraju's Depth First Traversal (DFS) algorithm [10], [14].

B. Sensitivity Tests

There are several attacks on symmetric ciphers based on the study of the relation between two encrypted blocks obtained by a small change either on their original blocks, or in the secret key used. To evaluate the risks against such attacks, some sensitivity tests have been introduced. Passing such a test shows on how much a slight change in the original block or in the key will affect the resulted encrypted block: higher is the change in the resulted block, better is the sensitivity of the encryption algorithm.

TABLE I. COMPARISON BETWEEN RC5 AND CHAOTIC RC5-CBC CORRELATION COEFFICIENT VALUES

Image	Correlation Coefficient for RC5	Correlation Coefficient for RC5-CBC
Lena	-0.02894	0.00509
Mandrill	-0.06669	-0.00052
Airplane	-0.00789	-0.00161
Boat	-0.0709	-0.0006

To measure the "avalanche effect in a block", the arithmetic average of Hamming distances has been used [20], and the following method has been applied. Two different original messages M_1 and M_2 which have only one bit of difference (namely, their Least Significant Bit LSB) are encrypted under RC5-CBC using the key K, to produce respectively two encrypted messages C_1 and C_2. Then, the Hamming distance (in bits) between these two encrypted messages is calculated using the following equation:

$$\begin{aligned}\text{Avalanche Effect}(\%) &= \frac{\text{changed bits in cipher text}}{\text{Total number of bits in cipher text}} \cdot 100\% \\ &= \frac{\text{RC5}_k(M_1) \oplus \text{RC5}_k(M_2)}{N} \cdot 100\% \\ &= \frac{C_{1,k} \oplus C_{2,k}}{N} \cdot 100\%,\end{aligned} \tag{1}$$

where N is the block size.

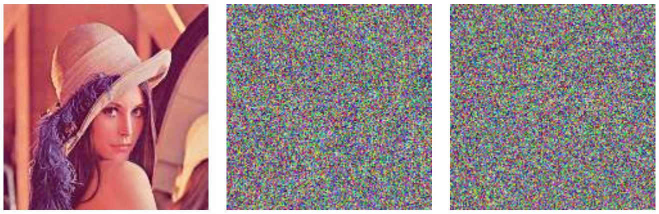
After having proved that RC5-CBC algorithm can exhibit a Devaney's chaotic behavior, this unpredictability is then illustrated and evaluated through hardware simulations, encompassing the analyzes of uniformity, sensitivity and degree of randomness. Through sensitivity tests, we have verified that, at each time, the cipher block chaining exhibits the sensitivity to the initial conditions, an aspect of chaos. Consequently, and due to the theoretical proofs, we can guarantee that any error on the IV (starting state) or on the message to encrypt (edges to browse) may potentially lead to a completely different list of visited states, that is, of a completely different cipher text. To sum up, thorough sensitivity test results, developed in [2], we have succeeded to confirm that RC5-CBC algorithm exhibits a high degree of randomness, key and plain sensitivity, in addition to satisfying the so-called avalanche effect. These experimental results confirm its theoretical chaotic behavior, which has been already proven through computations.

IV. SECURITY EVALUATION OF IMAGES ENCRYPTED UNDER CHAOTIC RC5-CBC ALGORITHM

The sensitivity of encryption methods applied to images can be measured using the linear correlation coefficient [17]. This coefficient can compute the degree of similarity between two adjacent pixels. Due to the meaning and content, this correlation is usually high (close to 1) in the case of a natural image. However, this correlation must be broken (close to 0) when encrypting the image [4], [18].

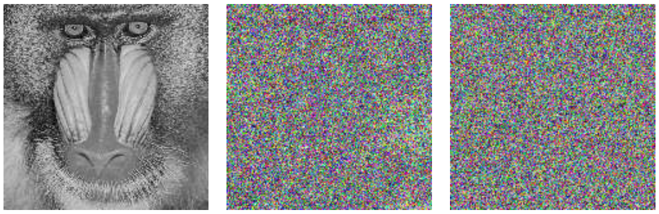
By examining Fig. 3, 4, and 5, in which the RC5 has been configured with a low number of bits, we can clearly remark that chaotic CBC mode improves the confusion of RC5 alone, enlarging the differences between the original and the encrypted images. We obtain indeed a real visual degradation, in which no useful information seems to be revealed by the ciphered image about the contents of the original one.

To measure this degradation, the correlation coefficient has been computed between original and RC5-encrypted images on the one hand, and between original and RC5-CBC encrypted images on the other hand. Obtained results, provided in Table I, allowed us to consider that a better confusion is achieved by RC5-CBC. This is due to the addition of chaotic CBC mode to be embedded with RC5 during the encryption operation.



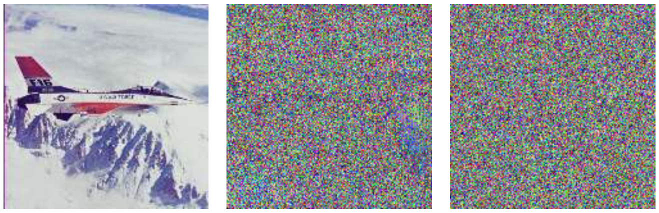
(a) Original Lena (b) Lena encrypted with RC5 standalone (c) Lena encrypted with Chaotic RC5-CBC

Fig. 3. Original and encrypted Lena



(a) Original Mandrill (b) Mandrill encrypted with RC5 standalone (c) Mandrill encrypted with Chaotic RC5-CBC

Fig. 4. Original and encrypted Mandrill



(a) Original airplane (b) airplane encrypted with RC5 standalone (c) airplane encrypted with Chaotic RC5-CBC

Fig. 5. Original and encrypted airplane

V. Hardware Implementation of Chaotic RC5-CBC

A. Proposed Architecture Design

In this section, we describe the hardware architecture of the proposed block cipher based on the RC5 standalone on the one hand, and on RC5 with CBC (chaotic) mode on the other hand. Hardware implementation encompasses the block ciphers in encryption and decryption modes, its embedding in Xilinx ISE 13.1, and its simulation with ModelSim, while experiments are validated using the Virtex6 FPGA device from Xilinx (xc6vlx75t-1ff484).

Fig. 6 illustrates the RC5 architecture data-path, which is mainly based on two parts. The first part performs the key expansion algorithm as defined in Section 2.2.1, which is based on three components named Simple Algorithmic Parts (SAP1, SAP2, SAP3); the second one is the encryption block as described in Section 2.2.2.

Let us firstly present the different blocks of key-expansion SAP1, SAP2, and SAP3. In the first part of the key expansion algorithm, RC5-CBC uses an expanded key table of w-bit words $S\,[0 \ldots t-1]$, such that $t = 2(r+1)$. The S table is initialized by a secret key K given by the user, which is represented by the SAP1 block. SPA1 converts K from bytes to words by directly copying the u $(w/8)$ consecutive key bytes into the c ($c = \lceil b/u \rceil$) positions of the L memory. SAP2 initializes S memory to a particular fixed pseudo-random bit pattern determined by the “magic constants” P_8 and Q_8. The associated hexadecimal values of P_8 and Q_8 are respectively 0xB7 and 0x9E. SPA2 block contains a bit-wise $\oplus$ primitive operation to add P_8 and Q_8. SAP3, for its part, is based on a scheduling loop in order to mix in the secret key K using S and L. This block contains three bit-wise $+$ primitive operations and two left-rotations of words denoted by $\lll$ (for example, $x \lll dec$ is a rotation left of word x by dec bits).

The encryption RC5-CBC block inputs are the two words A and B composing the block of plain text (m_0 XOR IV) and the resulting S table of the key-expansion parts. It is based on one XOR (A$\oplus$B), two left-rotation of words ($\lll A$ or $\lll B$) and four bit-wise $+$ primitive operations (to add shifted result to S[2*i] or S[2*i+1]). In each RC5 round, both registers A and B are updated to be used in the next round. The decryption algorithm can be easily derived from the encryption algorithm: it is based on two XORs (A$\oplus$B), two right-rotation of words (by $\ggg A$ or $\ggg B$), and four bit-wise $-$ primitive operations (to subtract S[2*i] from A and S[2*i+1] from B).

B. Synthesis Results

In this section, we present the hardware implementation results of both the RC5 and the RC5-CBC algorithms in encryption and decryption mode. Table II presents the implementation results of the RC5 and the RC5-CBC architectures in terms of area and execution time.

TABLE II. Synthesis Results.

	RC5	(Chaotic) RC5-CBC
Nbr of Slice Registers	617	731
Nbr of Slice LUTs	461	534
Frequency(MHz)	134.691	130.570
Execution Time (μs)	0,59	0,68
Throughput ($\frac{Mbit}{s}$)	27,28	23,47
Efficiency ($\frac{Mbit/s}{slices}$)	0,059	0,044

As a first conclusion, from this table, we can conclude the performance of chaotic RC5-CBC in terms of slices LUTs and execution time. Hence, RC5 can be both easy to implement for software and hardware applications, and more amenable to analysis than many other block ciphers. Being compared to RC5 design, the area occupancy and the execution time of the chaotic RC5-CBC are slightly bigger by about 26.65 % and 13.23 %, respectively. This can be justified by the fact that we have added the XOR block in the RC5-CBC architecture when compared with the RC5 only.

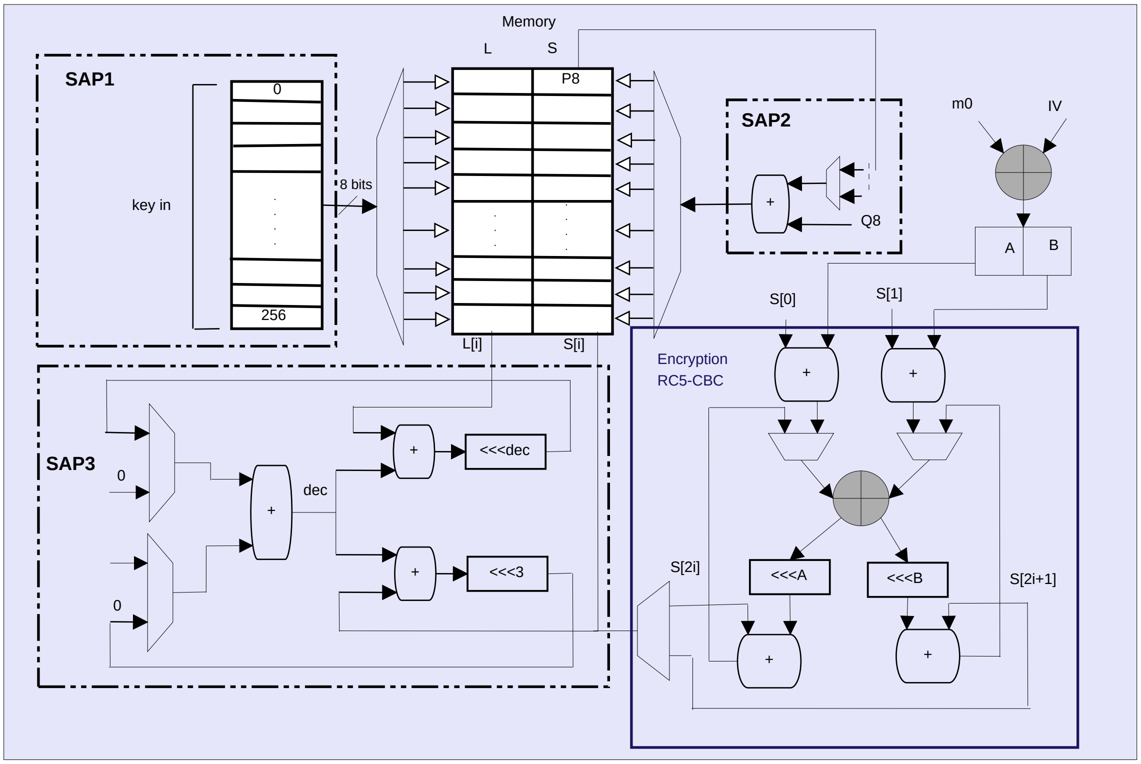


Fig. 6. RC5-CBC architecture design based on key expansion algorithm divided by three Simple Algorithmic Parts (SAP1, SAP2, SAP3) and a chaotic encryption block

In order to compare the efficiency of the RC5 and the chaotic RC5-CBC designs, we calculated the throughput and the efficiency of each approach as follows:

$$\text{Throughput} = \frac{\text{Frequency} \times \text{Number of Bits}}{\text{Cycles Number}} \quad \frac{Mbit}{s} \qquad (2)$$

$$\text{Efficiency} = \frac{\text{Throughput}}{\text{Area}} \quad \frac{Mbit/s}{slices} \qquad (3)$$

From Table II, we note that RC5 achieves a 16.23% higher throughput than RC5-CBC and it is 25% more efficient. It is obvious from the previous results that RC5 without CBC is slightly faster and occupied less memory space than CBC embedding RC5 algorithm. On the other hand, this later encryption technique presents a much better level of security and randomness while behaving chaotically, which has been verified in [2]. This better aimed level is caused by the adding of CBC block, which makes the loss of memory and speed strongly negligible in front of this performance presented by the chaotic RC5-CBC architecture.

VI. Discussion

The originality of our work is that we consider discrete infinite sets: we consider machine numbers (discrete aspect) and media of unbounded size (infinite set). While it is true that the machine's memory is infinite, the set of media that can be provided to the machine or that it can produce is infinite (discrete). And so, if we consider an algorithm iterating on a media stream, for example the RC5-CBC iterating on a video stream, then we are dealing with an algorithm iterating on the discrete infinite space of the Cartesian product between the finite memory of the machine and the infinite set of finite unbounded size binary sequences, corresponding to the input-output media of the machine. The main objective of our series of articles, regarding the chaotic topological behavior of the CBC mode of operation, is to understand in which extent this mode depends on its inputs. More precisely, is it possible to understand this dependence, in such a way that the effects of a modification of the IV and/or the message can be predicted. If so, this kind of weakness could be considered in the design of specific attacks, while if the converse is proven, that is to say, if the mid-to-long term effects of a slight modification of the input cannot be predicted, that chaotic dependence will make such attacks inefficient.

VII. Conclusions

In some previous research works, we have proven that RC5-CBC algorithm is chaotic according to Devaney. In this paper, we aimed to prove that this chaotic behavior can ensure a better level of randomness and security. This result has been illustrated through the analysis of the quality of such images encrypted under chaotic algorithm and the synthesis results of its hardware implementation in FPGA circuits.

References

[1] Abdullah, K.M., Houssein, E.H., Zayed, H.H.: Extended spins framework for security wireless sensor network. Int. J. Comput. Sci (2017), 14 (2017)

[2] Abidi, A., Guyeux, C., Machhout, M.: Evaluation of chaotic properties of CBC mode of encryption embedded with RC5 block cipher algorithm. Discontinuity, Nonlinearity, and Complexity (in press)

[3] Advani, N., Rathod, C., Gonsai, A.M.: Comparative study of various cryptographic algorithms used for text, image, and video. In: Emerging Trends in Expert Applications and Security, pp. 393–399. Springer (2019)

[4] AlZain, M.A., Faragallah, O.S.: Efficient chaotic tent map-based image cryptosystem. International Journal of Computer Applications **975**, 8887 (2017)

[5] Arora, M., Sharma, S., Engles, D.: Parametric comparison of emds algorithm with some symmetric cryptosystems. Egyptian informatics journal **18**(2), 141–149 (2017)

[6] Asadi, M.M., Mahboubi, H., Habibi, J., Aghdam, A.G., Blouin, S.: Connectivity assessment of random directed graphs with application to underwater sensor networks. IEEE Transactions on Control Systems Technology **25**(4), 1457–1464 (2017)

[7] Chandra, C.S., Lal, S.S., Saranya, A.: Evolution of cryptographic algorithms and performance parameters. Evolution **5**(01) (2016)

[8] Cygan, M., Fomin, F.V., Kowalik, Ł., Lokshtanov, D., Marx, D., Pilipczuk, M., Pilipczuk, M., Saurabh, S.: Parameterized algorithms, vol. 4. Springer (2015)

[9] Devaney, R.: An introduction to chaotic dynamical systems. CRC Press (2018)

[10] Dhingra, S., Dodwad, P.S., Madan, M.: Finding strongly connected components in a social network graph. International Journal of Computer Applications **136**(7), 1–5 (2016)

[11] Fadel, A., Dzul-Kifli, S.C.: Some chaos notions on dendrites. Symmetry **11**(10), 1309 (2019)

[12] Faragallah, O.S.: Digital image encryption based on the rc5 block cipher algorithm. Sensing and Imaging: An International Journal **12**(3-4), 73–94 (2011)

[13] Guyeux, C., Couturier, R., Héam, P.C., Bahi, J.M.: Efficient and cryptographically secure generation of chaotic pseudorandom numbers on gpu. The Journal of Supercomputing **71**(10), 3877–3903 (2015)

[14] Hsu, D.F., Lan, X., Miller, G., Baird, D.: A comparative study of algorithm for computing strongly connected components. In: 2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), pp. 431–437. IEEE (2017)

[15] Kouser, Z., Singhal, M., Joshi, A.M.: Fpga implementation of advanced encryption standard algorithm. In: 2016 International Conference on Recent Advances and Innovations in Engineering (ICRAIE), pp. 1–5. IEEE (2016)

[16] Kumar, S., Patidar, K., Kushwah, R., Chouhan, S.: Text data partitioning and image based rc5 encryption with block based key generation. International Journal of Advanced Technology and Engineering Exploration **4**(31), 101 (2017)

[17] Liu, W., Sun, K., Zhu, C.: A fast image encryption algorithm based on chaotic map. Optics and Lasers in Engineering **84**, 26–36 (2016)

[18] Noura, H., Sleem, L., Noura, M., Mansour, M.M., Chehab, A., Couturier, R.: A new efficient lightweight and secure image cipher scheme. Multimedia Tools and Applications **77**(12), 15457–15484 (2018)

[19] Santhi, H., Gayathri, P., Katiyar, S., Gopichand, G., Shreevastava, S.: Study of symmetric-key cryptosystems and implementing a secure cryptosystem with des. In: Information Systems Design and Intelligent Applications, pp. 299–313. Springer (2019)

[20] Vibar, J.C.N., Medina, R.P., Sison, A.M.: Erc5a–an enhanced rc5 algorithm on bit propagation in the encryption function. In: 2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS), pp. 479–482. IEEE (2019)