To appear In Proceedings of International Conference for Internet Technology and Secured Transactions (ICITST-2013)
December 9-12, 2013, London, UK

Lightweight Chaos-Based Cryptosystem for Secure Images

Z. Fawaz*, S. El Assad, M. Farajallah
Lebanese International University*
IETR/LUNAM University of Nantes
Nantes, France
Zeinab.fawaz90@hotmail.com
Safwan.elassad/mousa.farajallah@univ-nantes.fr

A. Khalil*, R. Lozi, O. Deforges
University of Nice
IETR/INSA of Rennes
ayman.khalil23@gmail.co
rlozi@unice.fr
olivier.deforges@insa-rennes.fr

Abstract— **In the last two decades, several chaos-based cryptosystems have been proposed. Some of them have architecture comprising a layer of permutation and a layer of diffusion and these layers are simultaneously executed in a simple scan of plain-image pixels. In this kind of cryptosystems, due to the channel effect, a bit error(s) in the cipher-image produces, at the decryption side, a random bit error in the estimated plain-image. In this paper, we propose a cipher-block encryption algorithm in CBC (Cipher Block Chaining) mode. It consists of a permutation process on the bits achieved by a 2D-cat map, followed by a bitwise XOR operation. Here, each permuted bit (confusion phase) is immediately diffused in a simple manner in the same phase. Therefore, the confusion and diffusion effects are stronger and the cryptanalyses for permutation-only ciphers become ineffective.**

Keywords- Chaos-based Cryptosystem; Chaotic generator; Cat map; Dependent Confusion-Diffusion processes; Security analysis

I. INTRODUCTION

The recent high demand of transmitting large amount of data over the network (satellites, mobile phones, and computers) is enforcing the researchers to find secure ways that satisfy the transmission and storage of these data confidentially. Researchers noted that existing cryptographic algorithms such as Data Encryption Standard (DES), and Advanced Encryption Standard (AES) are found unfit for multimedia data in the context of real-time applications [1]. From here comes the need for a chaos-based cryptosystem. The term "chaos" first appeared in cryptography field in [2] by Matthews in 1989, where he introduced chaos as a stream cipher based on 1D chaotic system. Indeed, chaotic systems have interesting features such as being ergodic and sensitive to the initial conditions and control parameters, making the system highly secured and robust against cryptographic attacks. For that, several chaos-based encryption algorithms [3-11] have been studied and implemented due to their ability to achieve diffusion confusion effects, needed in any cryptosystem. One of most popular structure adopted in some chaos-based cryptosystems is the Fridrich architecture [3], composing of permutation and diffusion layers. The permutation process is done by a 2-D chaotic map (Standard, Baker, Cat) and the diffusion process is usually achieved by a 1-D chaotic map. In such architecture, with fixed parameters, the two processes confusion-diffusion become independent and then the structure can be attacked. To overcome this problem, François & all [4] proposed a dependent confusion-diffusion structure based on a chaotic generator using linear congruence. The encryption process, achieved on the bits of the whole plain image, consists of a 1-D permutation process, coupled with a XOR operation. The cryptographic properties of the ciphered images are then increased. The only problem with this cryptosystem is the execution time which is high as compared to others chaos-based cryptosystems of the literature.

In this paper, we propose a dependent confusion-diffusion processes based on: a robust chaotic generator, a 2-D cat map and XOR operation. The encryption/decryption process, as in [4] is done on the bits, but block by block in CBC mode. Consequently, the proposed cryptosystem is more efficient, as compared with [4] in terms of: robustness against statistical attacks, error(s) propagation and especially in time of execution. The paper is organized as follow. In section II, we describe in detail the proposed chaos-based cryptosystem. Simulation results and performance analyses are presented in section III and a concluding section ends the paper.

II. PROPOSED CHAOS-BASED CRYPTOSYSTEM

A. Architecture

The architecture of the proposed cryptosystem is given in figure 1.

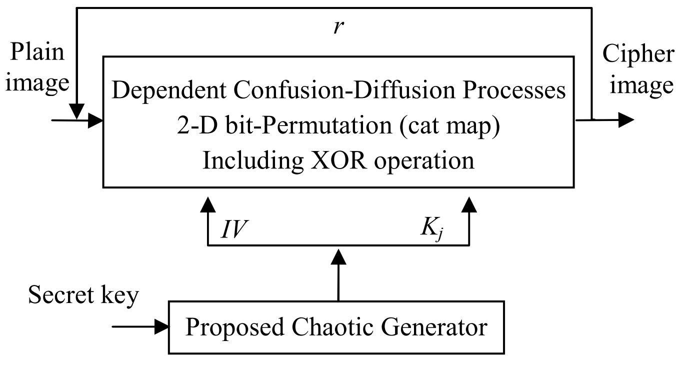


Fig. 1. Architecture of the proposed cryptosystem

Contrary to the traditional structures where both processes of confusion and of diffusion are independent, in the proposed structure, the two processes are dependent and they are applied only on one phase on every bit of the plain image.

The proposed cryptosystem is implemented in Cipher Block Chaining mode (CBC mode) on blocks of size equal to 256 bytes, then:

CBC Encryption on each block:

$$C_j = E_k(P_j \oplus C_{j-1}) \quad C_0 = E_k(P_0 \oplus IV) \tag{1}$$

CBC Decryption on each block:

$$P_j = D_k(C_j) \oplus C_{j-1} \quad P_0 = D_k(C_0) \oplus IV \tag{2}$$

The initial vector IV is generated from the chaotic generator in the encryption and decryption parts.

The experimental results show that, the proposed cryptosystem achieve the confusion-diffusion properties in one round, then, it has a high level of confidentiality and a shorter time encryption as compared to [4].

B. Dependent confusion-diffusion processes

The dependent confusion-diffusion processes are realized on each bit by a permutation process, achieved by a modified 2-D cat map, followed by a XOR operation. The modified 2-D cat map is given by the following equation.

$$\begin{bmatrix} i_n \\ j_n \end{bmatrix} = Mod\left(\begin{bmatrix} 1 & u \\ v & 1+u\times v \end{bmatrix} \begin{bmatrix} i \\ j \end{bmatrix} + \begin{bmatrix} r_i + r_j \\ r_j \end{bmatrix}, \begin{bmatrix} M \\ M \end{bmatrix} \right) \tag{3}$$

Where r_i and r_j are added to the standard model in order to overcome the problem of fixed point ($i = j = 0$).

In figure 2, we give the pseudo-code of dependent permutation-XOR operations for the encryption part of the cryptosystem.

```
for i= 0 to M-1
    for j = 0 to M-1
        i_n = (i + u * j + r_i + r_j) mod M
        j_n = ( v * i + (1 + v * u) * j + r_j) mod M
        Temp = data_bit(i, j)
        data_bit(i, j) = data_bit(i, j) XOR data_bit(i_n, j_n)
        data_bit(i_n, j_n) = Temp
    end j
end i
```

Fig. 2. Pseudo-code of dependent permutation-XOR operations for the encryption side.

In the decryption part of the cryptosystem, the pseudo-code of reverse dependent permutation-XOR operations is given by figure 3.

```
for i = M-1 to 0
    for j =M-1 to 0
        i_n = (i + u * j + r_i + r_j) mod M
        j_n = ( v * i + (1 + v * u) * j + r_j) mod M
        Temp = data_bit(i_n, j_n)
        data_bit(i_n, j_n) = data_bit(i_n, j_n) XOR data_bit(i, j)
        data_bit(i, j) = Temp
    end j
end i
```

Fig.3. Reverse dependent permutation-XOR operations for the decryption side.

C. Structure of the used chaotic generator

The proposed chaotic generator of a discrete chaotic sequences is a very simplified version of the one proposed by El Assad [11], see also El Assad and Noura patent [12]. It comprising two chaotic maps, namely the Skew tent map and the PWLCM map connected in parallel as shown in figure 4, and each one includes a technique of perturbation based on a linear feedback shift register (LFSR). The cryptographic properties of such generator are very high.

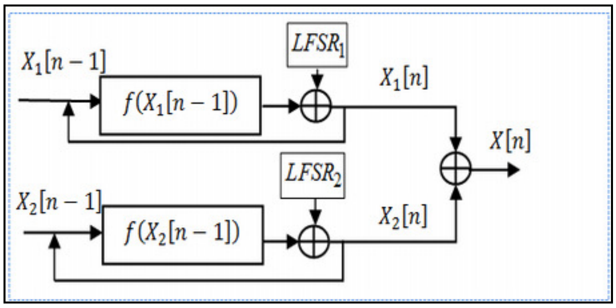


Fig.4. Structure of the used chaotic generator

The discrete Skew Tent Map and the discrete Piecewise Linear Chaotic Map (PWLCM) are defined as following.
Discrete Skew Tent Map:

$$X[n] = F\left[X[n-1]\right] = \begin{cases} \left\lfloor 2^N \times \dfrac{X[n-1]}{P} \right\rfloor & if\ 0 < X[n-1] < P \\ 2^N - 1 & if\ X[n-1] = P \\ \left\lfloor 2^N \times \dfrac{[2^N - X[n-1]]}{2^N - P} \right\rfloor & if\ P < X[n-1] < 2^N \end{cases} \tag{4}$$

Where P is the control parameter, ranging from 1 to 2^N-1, and N is the finite precision equal to 32 bits.

Discrete PWLCM map:

$$X[n] = F[X[n-1]] = \begin{cases} \left\lfloor 2^N \times \frac{X[n-1]}{P} \right\rfloor & \text{if } 0 < X[n-1] < P \\ \left\lfloor 2^N \times \frac{[X[n-1]-P]}{2^{N-1}-P} \right\rfloor & \text{if } P < X[n-1] < 2^{N-1} \\ \left\lfloor 2^N \times \frac{[2^N - P - X[n-1]]}{2^{N-1}-P} \right\rfloor & \text{if } 2^{N-1} \leq X[n-1] < 2^N - P \\ \left\lfloor 2^N \times \frac{[2^N - X[n-1]]}{P} \right\rfloor & \text{if } 2^N - P \leq X[n-1] < 2^N - 1 \\ 2^N - 1 & \text{Otherwise} \end{cases} \quad (5)$$

The control parameter P of the PWLCM is ranging from 1 to 2^{N-1}-1.

In all encryption algorithms, it is known that having a large key space always leads to a strong resistance against brute-force attacks, and this becomes evident even with today's super computers, where it may take several years to guess the plaintext, depending on how large is the key. In our new scheme, the key space resulting from the chaotic generator consists of four initial conditions, 2 are related to LFSR and 2 for the 2 maps, as well as having 2 other parameters P_1 for the Skew tent and P_2 for the PWLCM. So, the key space is

$$|K| = 2 \times N + |P_2| + |P_1| + |k_1| + |k_2| = 169 \text{ bits}$$

With $N = 32$, $|k_1| = 23$, $|k_2| = 19$, $|P_1| = 32$, $|P_2| = 31$

This large value of the key space ensures the resistance against brute force attack.

III. Simulation Results and Performance Analysis

A. *Correlation analysis*

The correlation analysis is measured as follow: we randomly selected 8000 pairs of adjacent pixels in vertical, horizontal, and diagonal directions from the plain and their ciphered images and then the correlation coefficient is calculated from equations (6) to (9) [13]:

$$\rho_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x) \times D(y)}} \quad (6)$$

Where:

$$\mathrm{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x)) \times (y_i - E(y)) \quad (7)$$

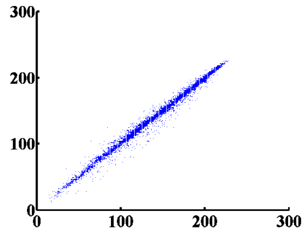
$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \quad (8)$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \quad (9)$$

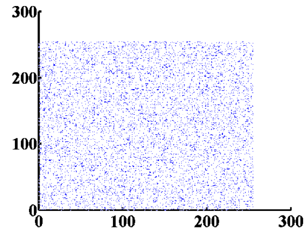
x_i and y_i are the gray values of two adjacent pixels in the plain images or in the ciphered images and N is the sample size (8000). The correlation values of the Pepeers image of size (512x512x3) and its ciphered one are listed in Table 1. We give also in figure 5, their correlation curves of adjacent pixels in horizontal, vertical and diagonal directions. We can observe from these results that, the high correlation coefficients in the plain image become almost zero-correlated in the cipher image, which means that, the cipher image is secure enough.

TABLE 1. Correlation coefficients of plain and ciphered images

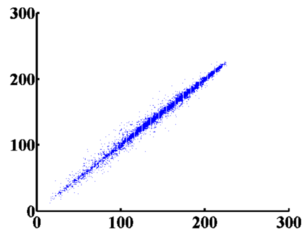
	Plain image	Cipher Image
Vertical	0.995577	0.010050
Horizontal	0.995154	0.008604
Diagonal	0.990814	0.006849



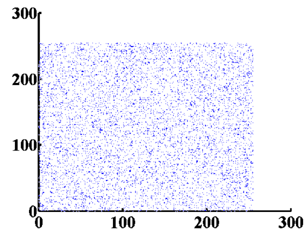
a-) Correlation of adjacent pixels in vertical direction of the plain image



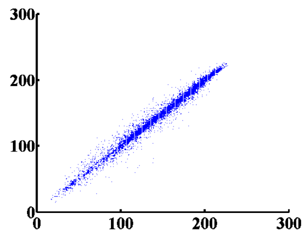
b-) Correlation of adjacent pixels in vertical direction of the cipher image



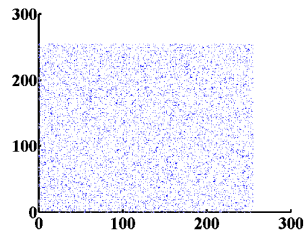
c-) Correlation of adjacent pixels in horizontal direction of the plain image



d-) Correlation of adjacent pixels in horizontal direction of the cipher image



e-) Correlation of adjacent pixels in diagonal direction of the Plain image



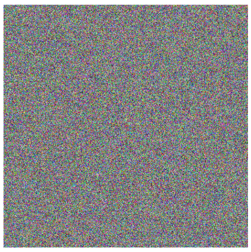
f-) Correlation of adjacent pixels in diagonal direction of the cipher image

Figure 5. Correlation analysis of the plain and ciphered images in vertical, horizontal, and diagonal directions

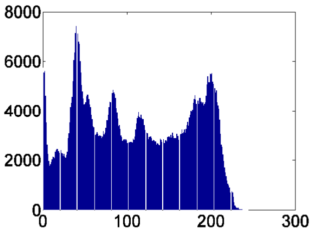
B. *Histogram analysis*

The encryption process of "peppers.bmp" makes the cipher image totally different from the original plain image. This property is clearly shown in figure 5 a), b), c) and d). We clearly remark that the histogram of the cipher image is uniformly distributed, compared to the plain one, hence it does not support any similarity to the plain image [14].

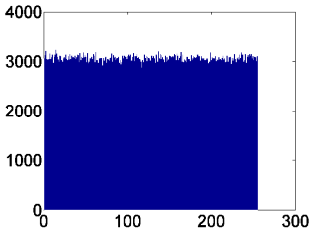
a). Plain Peppers Image



b). Cipher Peppers Image



c). Histogram of the Plain image



d). Histogram of the cipher image

Figure 1. Histograms of the plain and its ciphered images

To ensure the histogram uniformity of the ciphered image, we apply on it the chi-square test:

$$\chi^2_{exp} \sum_{i=0}^{Nv-1} \frac{(O_i - E_i)^2}{E_i} \quad (10)$$

The obtained experimental value 263.64 is less than the theoretical one which is 293 in case of alpha=0.05 and the number of intervals = 256.

C. *Plain text sensitivity analysis*

An encryption algorithm is said to be strong if it realizes the diffusion property, which means that a little bit change in the plain image will cause a completely different cipher image. This can be measured by: Hamming distance, Number of Pixel Change Rate (NPCR) when the pixels of the plain image change, and the Unified Average Changing Intensity (UACI) that represents the difference between the plain and cipher images. Hamming distance, NPCR and UACI are calculated as follows:

$$d_{Hamming}(C_1, C_2) = \sum_{K=1}^{L\times C\times P\times 8} C_1(K) \oplus C_2(K) \quad (11)$$

Another two security parameters, often used by the researchers to test the plain text sensitivity attacks based on bytes, are: Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI):

$$NPCR(C_1, C_2) = \frac{1}{L\times C\times P} \sum_{K=1}^{L\times C\times P} D(K) \times 100 \quad (12)$$

with

$$D(K) = \begin{cases} 1 & if\, C_1(K) \neq C_2(K) \\ 0 & f\, C_1(K) = C_2(K) \end{cases} \quad (13)$$

$$UACI(C_1, C_2) = \frac{1}{L\times C\times P\times 255} \sum_{K=1}^{L\times C\times P} |C_1(K) - C_2(K)| \times 100 \quad (14)$$

Where C_1 is the encrypted image from the original plain image, while C_2 is the encrypted image from a modified plain image by one bit change, the both encryption processes are done using the same secret key.

Table 2, presents the obtained results of the average of three parameters *HD*, *NPCR* and *UACT* of 1000 different secret keys, for the following parameters:

Table 2. *HD*, *NPCR*, and *UACI* values for the plain text sensitivity attack test

Test/Image size	***r***	$128\times128\times3$	$512\times512\times3$
HD	1	0.4965490	0.4998010
NPCR	1	99.262492	99.586479
UACI	1	33.281168	33.448491
HD	2	0.4985430	0.4999190
NPCR	2	99.456502	99.598569
UACI	2	33.357162	33.464932

It is clear from the results in Table that the proposed cryptosystem has high security level and almost optimal.

D. *Key sensitivity analysis*

One bit change in the secret key must produce a random image during the decryption process, or a completely different ciphered image during the encryption process. To measure this property, we change one bit in the secret key and encrypt the same plain image. Then, we calculate the three previous parameters *HD*, *NPCR* and *UACT,* between the two ciphered images. Obtained results given in table 3, show that, as we expected, the proposed cryptosystem is highly resistant to the key sensitivity attack.

Table 3. *HD*, *NPCR*, and *UACI* values for the key sensitivity attack test

Test/Image size	***r***	$128\times128\times3$	$512\times512\times3$
HD	1	0.5000740	0.4999830
NPCR	1	99.610026	99.606743
UACI	1	33.465514	33.464432
HD	2	0.4998200	0.4999780
NPCR	2	99.608195	99.608716
UACI	2	33.473052	33.459921

E. *Time analysis*

In any cryptosystem, speed is considered an important factor, especially in those intended for real time applications (images, videos) [8]. In table 4, we give the comparative average time results of the proposed cryptosystem, of that of ref [3] and of the AES algorithm. The simulation is done on the same C compiler using the following machine characteristics (for our cryptosystem and the used AES):
Sony VAIO; Intel® processor Core ™ Duo Processor CPU @ 1.83 GHz; 1 GB RAM; Windows XP.

The PC characteristics used by ref [3] are approximately similar to our PC. The test image is Peppers of different sizes.

Table 4. Average time in milli-second

	Proposed	Ref[4]	AES
128X128X1	5/5.6	140/150	11/14
256	20/23.3	900/960	46/58
512	80.6/97	7860/8020	178/222
1024	306/376.6	44500/45720	719/927

As we can see the proposed cryptosystem is twice shorter than the AES and at least 20 times faster than that proposed by ref [4].

Remark: we have used the AES algorithm given by the following website:

https://code.google.com/p/rikiglue/source/browse/src/frame/aes.cpp?spec=svn9239a0474d811daae909075568688a46134858c6&r=9239a0474d811daae909075568688a46134858c6.

IV. Conclusion and Perspectives

To improve the security and the speed of image transmission, we proposed in this paper, a dependent confusion-diffusion crypto-system achieving a permutation process on the bits using a modified 2D cat map, followed by XOR operation. Due, to this, the proposed cryptosystem can resist conventional known/chosen plaintext attacks. Also, it is strong against brute force, and statistical attacks. Moreover, it is faster than other known encryption/decryption algorithms.

Our future work concerns the enhancement of the proposed dependent confusion-diffusion structure and the implementation of Lozi [15] generator in finite precision N bits to produce integer values.

References

[1] Christina Fragouli, Jean-Yves le Boudec and Jörg Widmer, "Network Coding: An Instant Primer", *LCA-REPORT*-2005-010.

[2] R.Matthews, "On the Derivation of a 'Chaotic' Encryption Algorithm, *CRYPTOLOGIA*, vol.13, No.1, pp. 29-42, 1989.

[3] J. Fridrich, "Symmetric Ciphers Based no Two-Dimensional Chaotic Maps," International Journal of Bifurcation and Chaos, vol. 8, no. 6, pp. 1259-1284, 1998.

[4] M. François, T. Grosges, D. Barchiesi, R. Erra, « A new image encryption scheme based on a chaotic function », Elsevier, Signal Processing : Image Communication, vol.27, pp. 249-259, 2012.

[5] H. Yang, K.W Wong, X. Liao, W. Zhang, and P. Wei, "A fast image encryption and authentication scheme based on chaotic maps," *Communications in Nonlinear Science and Numerical Simulation*, vol. 15, no. 11, pp. 3507–3517, 2010.

[6] M. Chetto, S. El Assad, M. Farajallah, "A Lightweight Chaos-based Cryptosystem for Dynamic Security Management in Real-Time Overloaded Applications", Int. J. Internet Technology ans Secured Transactions, vol. x, No., 13 pages , 2013.

[7] R. Lozi, E. Cherrier, "Noise-resisting ciphering based on a chaotic multi-stream pseudo-random number generator", in 6th International Conference for Internet Technology and Secured Transactions, IEEE, Abu-Dhabi, UAE, Dec. 2011, pp. 91- 96.

[8] C.Y. Song, Y.L. Qiao, and X.Z. Zhang, "An image encryption scheme based on new spatiotemporal chaos," Optik, October 2012.

[9] N. Masuda, G. Jakimoski, K. Aihara, and L. Kocarev, "Chaotic block ciphers: from theory to practical algorithms," IEEE Transaction on Circuits and Systems, vol. 53, no. 6, pp. 1341-1352, 2006.

[10] S. Behnia, A. Akhshani, A.Akhshani, H. Mahmodi, A. Akhavan, "A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps", *Physics Letters A 366*, 2007, pp. 391-396.

[11] S. El Assad, "Chaos Based Information Hiding and Security," in 7th International Conference for Internet Technology and Secured Transactions, IEEE, London, United Kingdom, Dec. 2012, pp. 67- 72. Invited paper.

[12] S. El Assad (85%), H. Noura (15%), "Generator of chaotic Sequences and corresponding generating system" WO Patent WO/2011/121,218, 2011.

[13] M. Farajallah, Z. Fawaz, S. El Assad, O. Deforges, "A block cipher based on chaotic sequences suitable for wireless sensor networks", Securware-2013, Barecelona, Spain, August, 5 pages.

[14] A.Shtewi, B. Hasan, A. Hegazy, "An Efficient Modified Advanced Encryption Standard (MAES) Adapted for Image Cryptosystems", *IJCSNS International Journal of Computer Science and Network Security*, vol.10 No.2, February 2010

[15] A. Espinel, I. Taralova, R. Lozi "Dynamical and Statistical Analysis of a New Lozi Function for Random Numbers Generation", In *Proceeding of Physcon 2011*, León, Spain, 5-8 september, IPACS open Access Electronic Library.