Fast and Secure Encryption System Based on a Chaotic Map

M. Garcia-Bosque, C. Sánchez-Azqueta, S. Celma

Grupo de Diseño Electrónico (GDE)
Instituto de Investigación en Ingeniería de Aragón (I3A)
Universidad de Zaragoza, Mariano Esquillor s/n, 50018, Zaragoza, Spain.
Tel. +34-976762707, e-mail: mgbosque@unizar.es

Abstract

In this paper we propose a new fast and secure stream cipher based on a Modified Logistic Map and a Linear Feedback Shift Register.

Introduction

In the last years, it has become necessary to encrypt high amounts of data in real time. Unfortunately, most of the ciphers that are used nowdays are unable to encrypt data at high speed or are not secure enough.

In this context, chaos-based cryptosystems and, specially, chaotic maps, have emerged as a promising alternative to classical encryption since they are expected to achieve a good balance between speed and security [1].

In this paper, we propose and analyze a secure communication system based on a combination of a Modified Logistic Map (MLM) and a Linear Feedback Shift Register (LFSR).

Modified Logistic Map

The classic logistic map is expressed by the following equation:

$$f(x_i) = x_{i+1} = \gamma x_i(1-x_i), \qquad \in [0,1] \qquad (1)$$

This map presents chaos for most values of $3.57 < \gamma \leq 4$ while, for $\gamma > 4$, most initial values leave the interval [0,1] and diverge.

However, this map has some issues thast prevent it from being implemented directly in cryptosystems. First, there is an open and dense set of parameters γ for which the map is regular (i.e. there exist periodic windows). It is necessary to avoid using these parameters in order to generate truly chaotic sequences. Furthermore, the images are not uniformly distributed in the interval [0,1]. Instead, it can be easily proved that the images are distributed in the interval $[0, \gamma/4\,]$. Therefore, by measuring the length of the attractor, the value of γ can be determined. This can be a problem if the value of γ is being used as part of the key.

In our work, we have used a Modified Logistic Map proposed in [2] that is capable of solving these issues.

The MLM, is expressed mathematically as:

$$x_{i+1} = \begin{cases} \gamma x_i(1-x_i)\ (\mathrm{mod}\ 1), & x \in I_{ext} \\ \dfrac{\gamma x_i(1-x_i)\ (\mathrm{mod}\ 1)}{\frac{\gamma}{4}\ (\mathrm{mod}\ 1)}, & x \in I_{int} \end{cases} \qquad (2)$$

with $I_{ext} \in (0,1)\backslash I_{int}$, $I_{int} = [\eta_1, \eta_2], \eta_1 = (1/2) - \sqrt{\frac{1}{4} - \left[\frac{\gamma}{4}\right]}/\gamma$ and $\eta_2 = (1/2) + \sqrt{\frac{1}{4} - \left[\frac{\gamma}{4}\right]}/\gamma$ where $[\gamma/4]$ is the greatest integer minor or equal to $\gamma/4$.

Proposed algorithm

When the MLM is digitized, the sequence generated becomes periodic since the maximum number of possible different values of x_i is 2^n, where n is the number of bits. However, the period lengths of the sequences generated by the MLM are usually much shorter than this value, which results in poor randomness [3].

Our algorithm solves this problem by perturbing the orbits generated by the MLM with a Linear Feedback Shift Register (LFSR). For this purpose, the Least Significant Bit (LSB) of each x_i is XORed with a bit generated by a LFSR. The resulting sequence of bits is combined with the plaintext using an XOR gate. On the other hand, the perturbed $\tilde{x}_i$ is used to generate the next number x_{i+1} using (2). It can be proved that, if the period P_z of the LFSR is a prime number, the period of the generated sequences P_w will be $P_w \geq P_z$ [4]. The block diagram of the MLM is shown in Fig. 1 while the block diagram of the whole encryption system is

This work has been partially supported by MINECO-FEDER (TEC2014-52840-R) and FPU fellowship (FPU14/03523).

shown in Fig. 2.

Results

The proposed MLM-LFSR algorithm has been able to encrypt images efficiently as shown in Fig. 3. Furthermore, in order to analyze the security of this algorithm, the generated sequences have been subjected to the National Institute of Standards and Technology (NIST) SP 800-22 battery of test.

The sequences have passed all the tests proving that our system is secure (Fig. 4).

Conclusions

A new encryption algorithm based on a MLM and an LFSR has been proposed. The sequences generated by this algorithm have passed the NIST randomness test, proving that this system is secure.

Currently, this system is being implemented in a Zedboard development board that includes a Zynq-7020 SoC. The implementation results will be presented in a future paper.

REFERENCES

[1]. SHAH, J., and SAXENA, V. Video Encryption: A Survey. *International Journal of Computer Science Issues*. 2011, 8(2), 525-534.

[2]. CHEN, S.L., CHANG, S.M., LIN, W.W., and HWANG, T. Digital secure communication using robust hyper-chaotic systems. *International Journal of Bifurcation and Chaos*. 2008, 18 (11), 3325-3339.

[3]. GARCIA-BOSQUE, M., SÁNCHEZ-AZQUETA, C., and CELMA, S. Secure communication system based on a logistic map and a linear feedback shift register. *2016 IEEE International Symposium on Circuits and Systems (ISCAS)*. May 2016.

[4]. GARCIA-BOSQUE, M., SÁNCHEZ-AZQUETA, C., and CELMA, S. Lightweight Ciphers Based on Chaotic Map-LFSR Architectures. *12th IEEE Conference on PhD Research in Microelectronics and Electronics (PRIME 2016)*. June 2016.

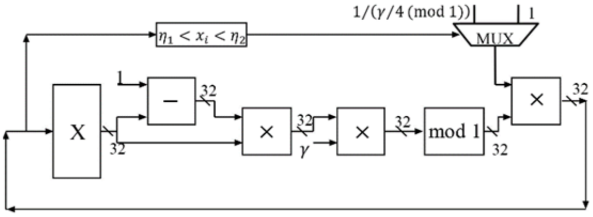


Fig. 1. Block diagram of a 32 bits Modified Logistic Map generator.

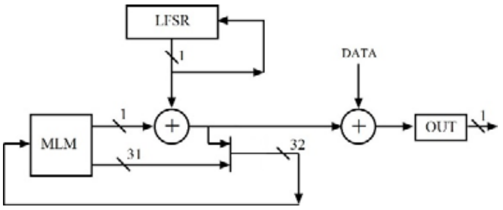
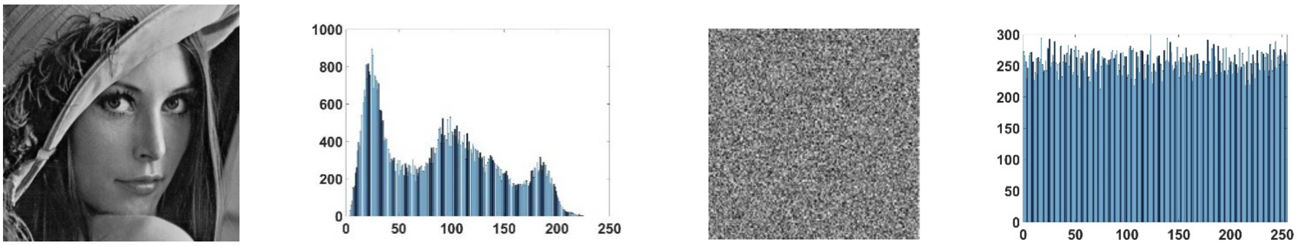
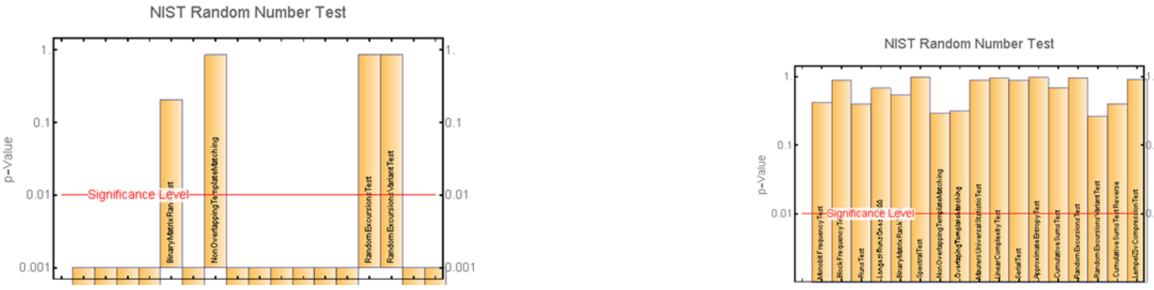


Fig. 2. Block diagram of the encryption system.



(a)

(b)Fig. 3. (a) Test image and (b) encrypted image using our algorithm with their respective histograms.



(a)

(b)

Fig. 4. NIST results for a sequence generated using (a) only the MLM and (b) the MLM-LFSR proposed algorithm.