On the Speed of "Image Encryption with Chaotically Coupled Chaotic Maps"

A. Akhavan [1], A. Samsudin [1] and A. Akhshani [2,3]

[1] School of Computer Sciences, Universiti Sains Malaysia, 11800 USM, Penang, Malaysia

[2] Department of Physics, IAU, Orumieh Branch, Orumieh, Iran

[3] School of Physics, Universiti Sains Malaysia, 11800 USM, Penang, Malaysia

Abstract

Pisarchik et al. presented an image encryption algorithm based on chaotically coupled chaotic maps. But G. Arroyo et al. found some flaws and security weaknesses in the proposed cryptosystem. In this letter, the speed of this chaotic cryptosystem is analyzed and the encryption speed claimed by the authors is argued. The maximum possible speed for the proposed algorithm is calculated analytically. Although it was claimed that, the chaotic cryptosystem is high-speed, our analysis shows that such a claim is not true.

***Keywords*:** *Chaotic cryptography, Security analysis, Encryption speed, Logistic map.*

1. Introduction

Naturally chaotic systems are well-known for their ergodic behavior and sensitivity to initial conditions and control parameters and complexity. The existence of these characteristics has made these systems as good candidate for cryptographic proposes and the use of these systems for designing an efficient cryptographic system is a very important issue.
In recent years, many different chaotic cryptosystems in digital domain have been proposed [1, 2, 3]. Meanwhile, security analysis of various proposed chaotic cryptosystems also attracts increasing attention, and some chaotic cryptosystems have been found insecure [4, 5, 6, 7]. Eventually in most of the cases, the application and the design of the algorithm is as crucial as the type and strength of the dynamical system. Apart from the security consideration and simple implementation, running speed of the algorithm is also an important aspect for a good chaotic cipher [8, 3].

Normally, floating-point arithmetic [9] leads to slower encryption speed and adds to the realization complexity and computation cost. Therefore, fixed-point arithmetic is usually suggested for encryption algorithms. In the other hand, the floating point decimals are not distributed uniformly in the discrete space, which makes the analysis digital dynamical properties much harder [8, 3]. This paper studies the speed of the cryptosystem designed by Pisarchik et al. [9]. In recent years, Pisarchik et al. have proposed a number of cryptosystems based on chaos [10, 9], some of which have been cryptanalyzed successfully [11, 12, 13]. But the schemes have never been analyzed from the speed view point, so that in this paper, we have tried to analysis encryption speed of the proposed algorithm claimed by the authors in [9]. In [9] the encryption speed is claimed to be 140 MB/s which is almost twelve times faster than Advanced Encryption Standard (AES) [14]. The results of our analysis indicate that such a claim cannot be true.
The rest of the paper is organized as follows. In the next Section the structure of the cryptosystem is described. After that, in Section 3 a practical run time for the described cryptosystem is measured and recorded. In Section 4 a theoretical run time speed based on CPU's ideal multiplication power is described and the ideal runtime speed is compared with the claimed speed. Finally, conclusions are drawn in Section 5.

2. The Chaotic Cryptosystem

In this section, we try to practically find out number of operations needed for the algorithm to encrypt an image, and simulate it practically on a machine with the same specifications mentioned in the paper [9].
The basic idea of the proposed cryptosystem is on converting plaintext into an array of flouting point numbers, which considering that it would be done

pixel by pixel, this array would need 3 times numbers pixels division and multiplication operations to make the suggested array, according to the equations (1) and (2) where P is plaintext and X_0 is used as initial condition for the chaotic map.

$$P = \{p_1 = p_1^R, p_2 = p_1^G, p_3 = p_1^B, p_4 = p_2^R, \ldots, p_i, \ldots, p_h = p_{MN}^B\}. \quad (1)$$

$$X_0 = P/[255(x^{max} - x^{min})], \quad (2)$$

Then in order to make the system more secure the authors have tried creating new control parameter a_i for each pixel, which considering that a logistic map is used for this propose, at least another set of 3 multiplication operation per pixel is carried out (see equations (3) and (4)).

$$z_{i+1} = cz_i(1 - z_i) \quad (3)$$

For $c = 4$, $z_i \in [0,1]$ and the parameter value for map is :

$$a_i = 0.43z_i + 3.57, \quad (4)$$

Later in the coupling step, the maps are coupled unidirectionally according to [10] and another chaotic map is iterated equal to the number of pixels, in this case logistic map, with Eq. (2) multiplicative operations. And also the control parameter b is again regenerated for iteration separately, so that another 3 multiplicative operation should be performed for each pixel. So by now we have over 14 multiplications carried out for each pixel in order to encrypt it. In this paper, we assume that there are no more multiplications needed in this algorithm, to complete the encryption process, although still the main step has not started.

3. Practical Run Time

In order to practically test the speed of an algorithm, with at least 14 multiplicative operations in its structure, we try a simple exercise. Equation (5) shows a simple equation with 14 multiplicative operations in its structure. So that, Eq. (5) is iterated several times and the operation time is recorded (see Table 1 for more detail).

$$x_{n+1} = x_n \times x_n \ldots \times x_n, \quad (5)$$

Table 1

Number of Multiplications	CPU	Operating System	Size in MB/s
14	Intel 3.1 GHz	MS Windows XP	36.3
10	Intel 3.1 GHz	MS Windows XP	65.5
14	Intel Core i5	MS Windows 7	36.7
14	Intel Core i5	Linux Fedora	37.1

According to the results mentioned in the Table 1, the speed of the similar operation with the mentioned processors and the environments, could hardly increase by $36\ MB/s$, which way smaller than the claimed encryption speed.

4. Theoretical Run Time

In order to investigate the issue more precisely, let us consider there are no other threads running on the processor, meaning that the processor is solely engaged to do the encryption operations. In this scenario, we can simulate a hypothetically ideal 3.1 GHz CPU. Naturally every Intel 3.1 GHz CPU has the tendency of demanding 3 cycles for accomplishing an 8, 16, 32 or 64 bit multiplication [15] which according to this a procedure of 14 multiplication would be carried out with 14 multiply 3 cycle (42 cycles). Now imagine we have 42 cycles for each byte to be encrypted, so that our hypothetically ideal CPU would process $1\ MB$ in $(1024 \times 1024 \times 42)$ cycles. Again considering that the CPU is ideal, an Intel 3.1 GHz CPU, can carry out a maximum of 3.1 GHz of cycles per second. The number of multiplications that can be performed by such a CPU, would only be enough to encrypt about $70\ MB/s$.

5. Conclusion

In this letter we have analyzed the speed of the cryptosystem proposed in [9]. In [9], the authors claim that, the encryption speed of the proposed algorithm is $140\ MB/s$. Both the theoretical and experimental results indicate that, such a claim cannot be true. Consequently, the cryptosystem introduced by [9] should be discarded as a high-speed chaotic cryptosystem for a real-time encryption.

Acknowledgment

This work was supported by USM (No:1001/PICOMP/817059).

References

[1] M.S. Baptista, Cryptography with chaos. Physics Letters A 240 (1998)50-4.

[2] J. Fridrich, Symmetric ciphers based on two-dimensional chaotic maps, Internat. J. Bifur. Chaos 8(6)(1998) 1259-84.

[3] G. Alvarez, S. Li, Some basic cryptographic requirements for chaos-based cryptosystems, Internat. J. Bifur. Chaos 16 (2006) 2129-2151.

[4] D. Arroyo, C. Li, S. Li, G. Alvarez, Cryptanalysis of a computer cryptography scheme based on a filter bank, Chaos, Solitons & Fractals 41 (2009) 410-413.

[5] D. Arroyo, C. Li, S. Li, G. Alvarez, W.A. Halang, Cryptanalysis of an image encryption scheme based on a new total shuffling algorithm, haos, Solitons & Fractals 41 (2009) 2613-2616.

[6] R. Rhouma, S. Belghith, Cryptanalysis of a new image encryption algorithm based on hyper-chaos, Phys. Lett. A 372 (2008) 5973-5978.

[7] E. Solak, R. Rhouma, S. Belghith, Cryptanalysis of a multi-chaotic systems based image cryptosystem, Optics Communications 238 (2010) 232-236.

[8] S. Li, X. Mou, B.L. Yang, Z. Ji, J. Zhang, Problems with a Probabilistic Encryption Scheme based on Chaotic Systems, Internat. J. Bifur. Chaos 13 (2003) 3063-3077.

[9] A.N. Pisarchik, M. Zanin, Image encryption with chaotically coupled chaotic maps, Physica D 237 (2008) 2638-2648.

[10] A.N. Pisarchik, N.J. Flores-Carmona, M. Carpio-Valadez, Encryption and decryption of images with chaotic map lattices, Chaos 16 (3) (2006) Art. No. 033118.

[11] E. Solak, C. Çokal, Comment on ``Encryption and decryption of images with chaotic map lattices" [Chaos 16, 033118 (2006)], Chaos 18 (3) (2008) Art. No. 038101.

[12] D. Arroyo, R. Rhouma, G. Alvarez, S. Li, V. Fernandez, On the security of a new image encryption scheme based on chaotic map lattices, Chaos 18 (2008) Art.No. 033112.

[13] D. Arroyo, S. Li, J.M. Amigóc, G. Alvarez, R. Rhoumad, Comment on ``Image encryption with chaotically coupled chaotic maps", Physica D 239 (2010) 1002-1006.

[14] Crypto++ Library, http://www.cryptopp.com.

[15] Intel, Intel 64 and IA-32 Architectures Optimization Reference Manual (2007).