NOTICE: This is the author's version of a work that was published in *Physica D*, vol. 239, no. 12, pp. 1002-1006, 2010, DOI: 10.1016/j.physd.2010.02.010. Changes resulting from the publishing process, such as peer review, editing, corrections, structural formatting, and other quality control mechanisms may not be reflected in this document. Changes may have been made to this work since it was submitted for publication.

Comments on "Image encryption with chaotically coupled chaotic maps"

David Arroyo*[,a], Shujun Li[b], José María Amigó[c], Gonzalo Alvarez[a], Rhouma Rhouma[d]

[a] *Instituto de Física Aplicada, Consejo Superior de Investigaciones Científicas, Serrano 144, 28006 Madrid, Spain*
[b] *Fachbereich Informatik und Informationswissenschaft, Universität Konstanz, Fach M697, Universitätsstraße 10, 78457 Konstanz, Germany*
[c] *Centro de Investigación Operativa, Universidad Miguel Hernández, Avda. de la Universidad s/n, 03202 Elche, Spain*
[d] *Syscom Laboratory, Ecole Nationale d'Ingénieurs de Tunis, 37, Le Belvédère 1002 Tunis, Tunisia*

Abstract

This paper studies the security of a recently proposed chaos-based cryptosystem. It is shown that the encryption architecture of this cryptosystem possesses some important problems related to its implementation and its robustness against noise. Some security problems are also highlighted.

Key words: Chaos, cryptography, logistic map, cryptanalysis, timing attack.

1. Introduction

Chaotic systems show an ergodic behavior and a high sensitivity with respect to the initial conditions and the control parameters. These main characteristics of chaos have been exploited in the design of new strategies to encrypt information. Nevertheless, the efficient design of new chaos-based encryption systems cannot be done just by selecting a dynamical system that shows a chaotic behavior. Indeed, it is necessary to select the adequate dynamical system for the chosen encryption architecture. To have a good performance, the selected chaotic system is expected to be robust, which means it remains chaotic in a continuous range of the parameter space [1]. Furthermore, the association between the selected dynamical system and the encryption architecture must result in an invertible and efficient encryption procedure.

In recent years, Pisarchik et al. have proposed a number of cryptosystems based on chaos [2, 3, 4, 5, 6], some of which [2, 4, 5] have been cryptanalyzed successfully [7, 8, 9, 10]. In [6] a new cryptosystem is proposed as an improvement of the one described in [4]. In the present paper we show that this new proposal is also flawed by some old problems of the original one and also by some new problems.

The rest of the paper is organized as follows. In the next section the cryptosystem under study is described. After that, in Sec. 3 some problems related to the practical implementation of the cryptosystem are analyzed. Finally, Sec. 4.2 shows some attacks to the cryptosystem under consideration, and the last section summarizes the results of the previous sections and concludes the paper.

2. Description of the encryption scheme

The encryption scheme described in [6] is based on the logistic map given by

$$x_{n+1} = \mu x_n (1 - x_n), \tag{1}$$

*Corresponding author: David Arroyo (david.arroyo@iec.csic.es).

where $x_n \in [0,1]$ and $\mu \in [3.57, 4]$. The maximum value returned by Eq. (1) is reached for $x_n = 0.5$, and it is given by

$$x_{\max} = \mu/4. \tag{2}$$

After a number of transient iterations, all the values derived from any initial condition x_0 will lie inside the interval $[x_{\min}, x_{\max}]$, where $x_{\min}$ is the output of Eq. (1) for $x_n = x_{\max}$, i.e.,

$$x_{\min} = \frac{\mu^2}{4}\left(1 - \frac{\mu}{4}\right). \tag{3}$$

In [6] the authors point out that the logistic map might be replaced by other chaotic systems because the periodic windows of the logistic map, being dense in the parametric interval considered, represent a problem. One recommended option is a robust chaotic system like the piecewise smooth system proposed in [1]. Since the cryptanalysis we are going to explain is independent of the choice of the chaotic system, we direct attention to the implementation with the logistic map, as proposed in [6].

Given an $M \times N$ color image with R, G, B color components, an initialization process is performed to convert the integer values of each pixel to real numbers that can be encrypted using the above chaotic logistic map. First, the 2-D image is scanned in the raster order (i.e., left to right, top to bottom) to form three 1-D integer sequences $\{P_i^c\}_{i=1}^{MN}$ (c = R, G and B), where $P_i^c \in \{0, \cdots, 255\}$ denotes the color component c of the i-th pixel. Then, these three integer sequences are mixed to get a new sequence of integers P as

$$P = \{P_i\}_{i=1}^{h} = \left\{P_1^R, P_1^G, P_1^B, P_2^R, P_2^G, P_2^B, \ldots, P_{MN}^R, P_{MN}^G, P_{MN}^B\right\}, \tag{4}$$

where $h = 3MN$. Finally, P is transformed into an array of floating-point numbers $X = \left\{x_0^{(i)}\right\}_{i=1}^{h}$, where[1]

$$x_0^{(i)} = x_{\min} + (x_{\max} - x_{\min})P_i/255. \tag{5}$$

The previous equation maps the set of integers $\{0, 1, \ldots, 255\}$ into the phase space of the logistic map. This map, which is part of the encryption procedure of [6], is therein incorrectly defined as $x_0^{(i)} = P_i/[255(x_{\max} - x_{\min})]$ (see Eq. (7) in [6]). It is obvious that this equation cannot ensure $x_{\min} \leq x_0 \leq x_{\max}$. We correct this error in this present paper.

After the above initialization, the encryption proceeds by performing the following steps:

- *Step 1*: Taking y_0 and $\mu_b \in [3.57, 4]$ as the initial condition and the control parameter, respectively, iterate the logistic map h times to get a chaotic sequence $\{y_i\}_{i=1}^{h}$. Let us denote the minimal and maximal values of the chaotic orbit of the logistic map with control parameter μ_b by $y_{\min}$ and $y_{\max}$, which are the values obtained by replacing μ with μ_b in Eqs. (3) and (2), respectively.

- *Step 2*: A *chaotic key sequence* $K = \{k_i\}_{i=1}^{h}$ is derived from the above chaotic sequence $\{y_i\}_{i=1}^{h}$ via the following equation:

$$k_i = \text{round}((h-1)(y_i - y_{\min})/(y_{\max} - y_{\min})) + 1 \in \{1, \ldots, h\}. \tag{6}$$

  If $k_i = i$ happens, set $k_i = (k_i - 1) \bmod h$.

- *Step 3*: For $i = 1, \ldots, h$, take $x_0^{(i)}$ and $\mu_a \in [3.57, 4)$ as the initial condition and control parameter, respectively, and iterate the logistic map n times to get $x_n^{(i)}$, which is then used to update the value of the k_i-th element of $X = \left\{x^{(i)}\right\}_{i=1}^{h}$ as follows:

$$x^{(k_i)} = \left(x_n^{(i)} + x^{(k_i)}\right) \bmod 1. \tag{7}$$

  This last step is repeated R rounds to finish the encryption procedure.

[1] In [6], the authors used a wrong equation: $x_0^{(i)} = P_i/[255(x_{\max} - x_{\min})]$. It is obvious that this equation cannot ensure $x_{\min} \leq x_0 \leq x_{\max}$. We correct this error in this present paper.

After performing the above encryption procedure, the ciphertext C is given by[2]

$$\begin{aligned} C = \{c_i\}_{i=1}^{h} &= \left\{\text{round}(255 \cdot x^{(i)})\right\}_{i=1}^{h} \\ &= \left\{c_1^R, c_1^G, c_1^B, \ldots, c_{MN}^R, c_{MN}^G, c_{MN}^B\right\}. \end{aligned} \tag{8}$$

It is stated in [6] that the secret key consists of the following four sub-keys:

1. The control parameter of the logistic map used in Step 1 (for the generation of the chaotic key sequence K), i.e., μ_b.
2. The initial condition of the logistic map used in Step 1, i.e., y_0.
3. The control parameter of the logistic map used in Step 3 (for updating the elements of X), i.e., μ_a.
4. The number of chaotic iterations in Step 3, i.e., n.
5. The number of encryption rounds, i.e., R.

Decryption proceeds similarly to encryption but in reverse order. For more details about the encryption/decryption procedures, the reader is referred to [6].

The authors of [6] also mention that the control parameter μ_a can be dynamically generated by iterating another logistic map with the control parameter μ_c from a given initial condition z_0. In this case, μ_c and z_0 replace the role of μ_a in the secret key. Furthermore, they add the possibility of using different initial conditions y_0 and z_0 for each encryption round. To avoid complicating unnecessarily the description of our cryptanalysis, we will focus on the basic implementation of the cryptosystem.

3. Implementation problems

3.1. Use of non-invertible functions

An efficient cryptosystem must allow the perfect recovery of the plaintext from the ciphertext when the key is known. Yet the algorithm in [6] includes some transformations that cannot be inverted, thus implying an error in the decryption. First of all, if the cryptosystem described in [6] is implemented using floating-point arithmetic, then the cryptosystem is impaired by the round-off operations of that arithmetic. This problem was also present in the previous proposal of the authors [4], as it has been pointed out in [9] and in [8, Sec. III.B]. Indeed, Eq. (7) in the Step 3 of the encryption procedure is a non-invertible function when floating-point arithmetic is used. On the other hand, it is emphasized in [6] that the ciphertext is a discretized version of the vector X in the last encryption round (see Eq. (8)). This discretization procedure is based on the round function, which is a non-bijective function that impedes the reconstruction of X from C. This problem can be easily overcome by selecting X as ciphertext.

In order to confirm the above assertions, some experiments were done. First, we study the problem derived from the implementation using floating-point operations and, consequently, we consider that the ciphertext is given by X. The plain image in Fig. 1 was encrypted and later decrypted, with secret key $\mu_a = 3.9898$, $\mu_b = 4$, $y_0 = 0.8989$, $n = 100$, and $R = 4$. Figure 2 depicts (a) the cipher-image, (b) the result of the decryption process, and (c) the difference between the original image and the recovered image. In order to quantify the underlying decryption error, the Mean Square Error (MSE) was computed. For P and P' being a plain image and the decrypted image respectively, the MSE for the color component c is defined as

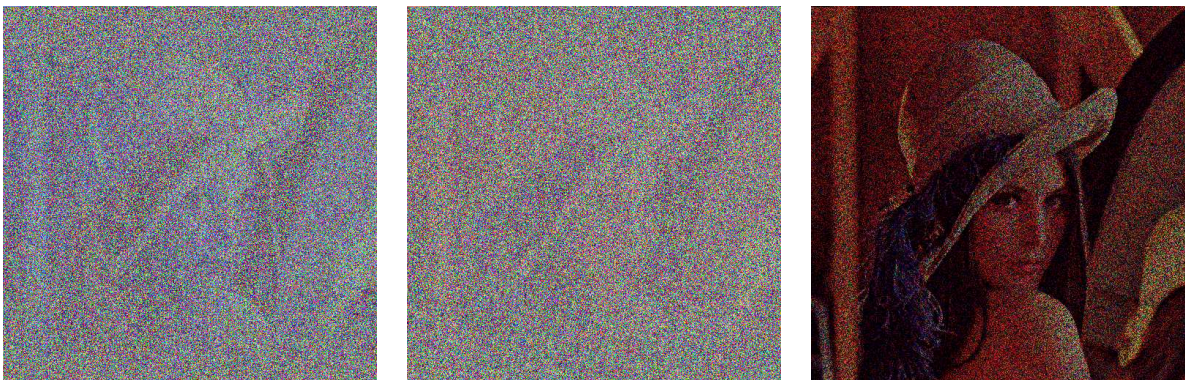
$$MSE_c = \sum_{i=1}^{m} (P_c^i - {P'}_c^i)^2 / m, \tag{9}$$

where $c \in \{R, G, B\}$, $m = M \times N$ is the number of pixels of the images considered, and the sequences $\left\{P_c^i\right\}_{i=1}^{m}$ and $\{P_c'\}_{i=1}^{m}$ are the result of scanning P and P' in the raster order. For the key settings above,

[2] In Step 3 of Sec. 2.4 in [6], the authors highlight that X is recovered from C doing $X = C/[255(x^{\max} - x^{\min})]$. It seems to be an error, since it is possible to have either $x^{(i)} < x_{\min}$ or $x^{(i)} > x_{\max}$.

Figure 1: The plain image "Lena".

the results were $MSE_R = 8189.8541$, $MSE_G = 7028.8354$, and $MSE_B = 5527.4588$. This underlying error can be easily avoided by truncating the values returned by Eq. (7). Hereafter we work with double precision floating-point arithmetic, but we store only the first 14 decimal digits of the values obtained through Eq. (7). Next we analyze the problem derived from using the round function to generate the ciphertext. In this case we consider the original cryptosystem, where the ciphertext is given by C, but the problem with the floating-point arithmetic was solved according to our previous recommendation. The plain image given by Fig. 1 was encrypted using the same key as above. The encrypted image was later decrypted using the same key, and the MSEs for the red, green and blue components were 9878.2642, 8497.4556, 6701.2127, respectively. Consequently, the ciphertext of the scheme described in [6] cannot be the one given by Eq. (8). In the sequel we overcome this problem by selecting X as ciphertext. Finally, we tested the improved image encryption scheme with the two suggested enhancements, and the MSEs dropped to zeros.



(a) (b) (c)

Figure 2: Analysis of the underlying decryption error due to the round-off operations of floating-point arithmetic. (a) Ciphertext of the plain image "Lena". (b) Recovered image of "Lena" using the same key. (c) The error image between the original and the recovered "Lena".

3.2. Robustness against noise

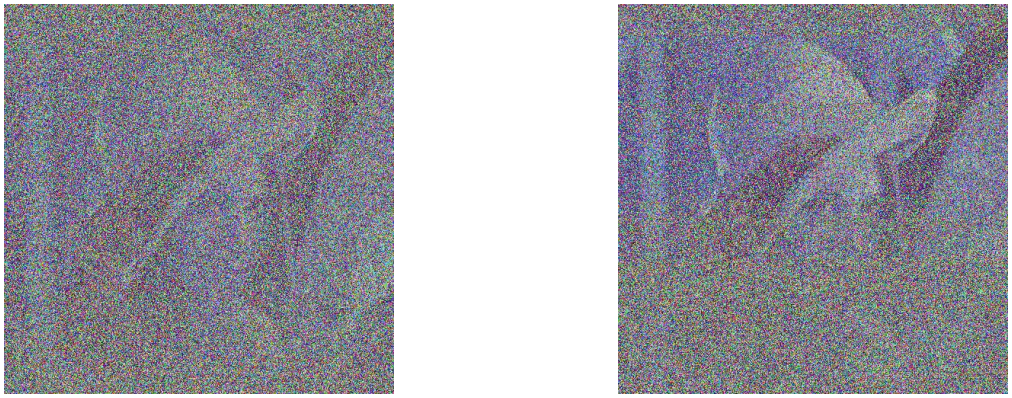
A well designed encryption system must guarantee the diffusion property, i.e., a small change in either the key or the plaintext must lead to a totally different ciphertext. Therefore if the ciphertext is slightly modified, then the decryption process should return a plaintext totally different from the original one. The authors of [6] claim that their cryptosystem implements a good diffusion procedure. At the same time, they also claim that the cryptosystem is robust against noise, which contradicts the previous assertion about

diffusion. In order to clarify this point, we performed some simulations where the ciphertext was modified by randomly selecting 8 bytes of the ciphertext, which were later modified with deviation equal to 10^{-14}. For $\mu_a = 3.9898$, $\mu_b = 4$, $y_0 = 0.8989$, $n = 100$, and $R = 1$, the image shown in Fig. 1 was encrypted, then modified through the 8 selected pixels, and finally decrypted. The MSEs between the original image and the one obtained after decryption were (7377.6144, 6266.0972, 4859.0834). Fig. 3(a) shows the result of decryption. If we increase the number of rounds from 1 to 4, the MSEs were (10447.1534, 8987.2725, 7062.4080), and the decrypted image is shown in Fig. 3(b). As a result, we conclude that the cryptosystem is not robust against noise.

(a) (b)

Figure 3: Decrypted images when 8 values of the ciphertext are modified by introducing a deviation equal to 10^{-14}. The parameters used in the experiments are: $\mu_a = 3.9898$, $\mu_b = 4$, $y_0 = 0.8989$, $n = 100$, and the number of rounds is (a) $R = 1$; (b) $R = 4$.

4. Security Problems



(a) (b)

Figure 4: Leaking of perceptual information when "Lena" is encrypted with $\mu_a = 3.9898$, $y_0 = 0.8989$, $n = 100$, $R = 3$, and (a) $\mu_b = 4$; (b) $\mu_b = 3.6898$.

4.1. Unencrypted pixels

Assuming the chaotic key sequence $\{k_i\}_{i=1}^{h}$ is an i.d.d. sequence, we have $\text{Prob}(k_i = j) = p_0 = 1/(h-1)$, where $j \neq i$. Then, the probability that one pixel will not be encrypted by any other $h-1$ pixels is $p_1 = (1-p_0)^{h-1}$. When h is relatively large, $p_1 = e^{-1} \approx 0.3679$. For R rounds of encryption, the final probability that each pixel is not encrypted becomes $p_R = p_1^R = e^{-R} \approx 0.3679^R$. In [6], the recommended range of R is $\{3, \ldots, 11\}$. Taking $R = 3$, we have $p_R \approx 0.0498$, which means that around 5% of all pixels are not encrypted at all. This is apparently not a good feature for an image encryption scheme. The implications of the previous theoretical analysis have been examined by means of experimental simulations. Figure 4 shows the leaking of perceptual information from the encrypted image corresponding to Fig. 1 for two different keys with $R = 3$. A more exhaustive analysis of the rate of unencrypted pixels is performed in Fig. 5. It informs about a deviation from the theoretical expected behavior, which is a consequence of the non-uniform probability distribution function associated to the orbits of the logistic map. This is the reason why for $\mu_b = 4$ the percentage of unencrypted pixels is around 10% for $R = 3$, instead of being around 5%. Furthermore, different values of μ_b lead to probability distribution functions with different shapes, which implies different rates of unencrypted pixels as shown in Fig. 5. Therefore, the efficiency of the cryptosystem defined in [6] requires to replace the logistic map by other chaotic map with uniform probability distribution function for all the values of the control parameter. Indeed, the ergodicity of a chaotic map must be analyzed thoroughly when it is selected as the core of a chaos-based cryptosystem [11, Sec. 2.3].

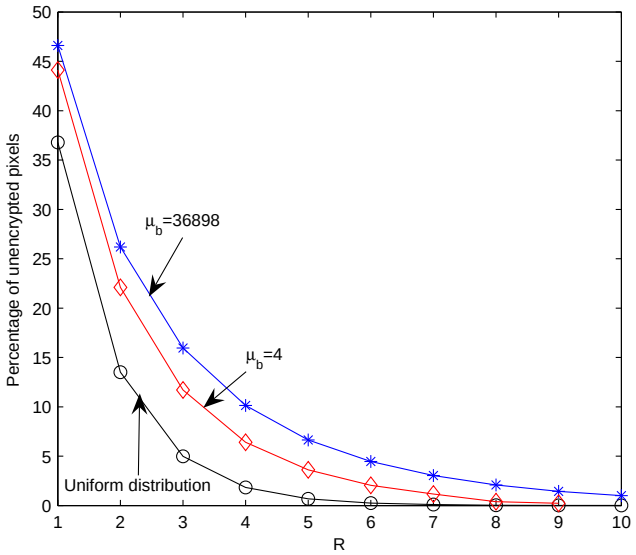


Figure 5: Percentage of unencrypted pixels with respect to the number of encryption rounds. The parameters used in the experiments are: $\mu_a = 3.9898$, $y_0 = 0.8989$, $n = 100$. Three different situations have been considered: selection of pixels to encrypt according to the logistic map with $\mu_b = 3.6898$ and $\mu_b = 4$, and selection of pixels based on a random sequence with uniform probability distribution function.

4.2. Timing attack

The encryption/decryption time (EDT) should not be dependent on the value of the key. In [6] it is stated that the number of encryption rounds R and the number of iterations n are part of the secret key of the cryptosystem, which calls for a timing attack as it was done in the case of [4] in [8, Sec. IV.B]. As a matter of fact, one can expect that the EDT increases as n does for most values of R, μ_a and μ_b. Similarly, because the encryption/decryption proceeds through R repeated cycles, the EDT will also become larger if

the value of R increases. To be more precise, for a given plain image we can expect the following bilinear relationship between the EDT and the values of n and R:

$$\mathrm{EDT}(n, R) \approx (c \times n + d) \times R + e, \tag{10}$$

where c corresponds to the common operations consumed on each map iteration, d to the operations performed in each cycle excluding those involved in the map iterations, and e to those operations performed on the initialization process and the postprocessing after all the R cycles are completed. In addition, because

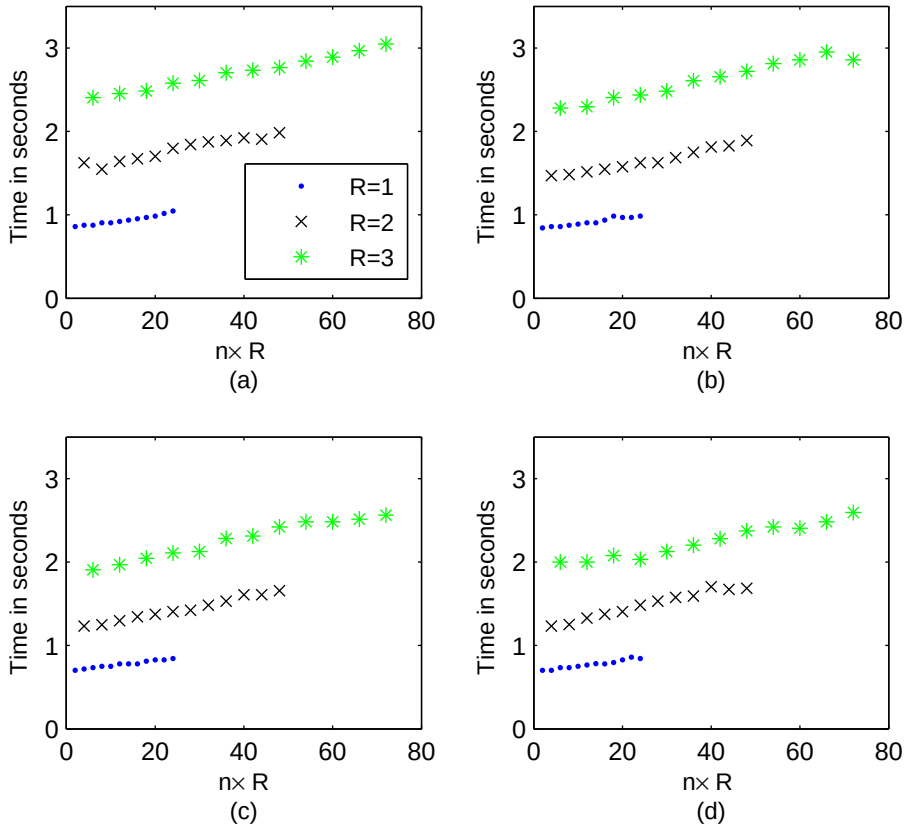


Figure 6: The encryption time for a 512×512 image with the following parameters of the image encryption scheme: (a) $\mu_a = 3.9898$, $\mu_b = 3.8458$, $y_0 = 0.2391$; (b) $\mu_a = 3.8956$, $\mu_b = 3.8612$, $y_0 = 0.9501$; (c) $\mu_a = 3.8542$, $\mu_b = 3.8998$, $y_0 = 0.2311$; (d) $\mu_a = 3.9898$, $\mu_b = 4$, $y_0 = 0.8989$.

μ_a, μ_b and y_0 are just the control parameters and the initial condition of the chaotic map, it is expected that EDT will be independent of their values. With the aim of verifying this hypothesis, some numerical experiments have been made under the following scenario: an 512×512 image with random pixel values was encrypted for different values of μ_a, μ_b, y_0, n and R. The encryption time corresponding to each key is shown in Fig. 6, from which one can see that Eq. (10) is verified.

For the sake of clarity, let us examine the effect of the timing attack on the key space of the cryptosystem described in [6]. The secret key of the basic implementation of that cryptosystem is given by μ_a, μ_b, y_0, n, R. According to Pisarchik et al., there exist around 10^6 possible values for μ_a, around 10^6 possible values for μ_b, around 10^{10} possible values for y_0, around 10^3 possible values for n, and 10 possible values for R. In this case, the key space is $\#K \approx 10^{26}$. Regarding the timing attack, once the encryption time is known, a brute force attack on either n or R enables the recovering of either R or n. Since the number of possible values

for R is smaller than the one concerning n, we should perform a brute force attack on R. As a result, the new key space is given by $\#K \approx 10^6 \cdot 10^6 \cdot 10^{10} \cdot 10 = 10^{23}$. Although the reduction of the key space is not drastic, it exists and should be taken into account during the design and description of the cryptosystem.

The above timing-attack informs that partial knowledge of the key leads to the recovering of other parts of the key. This is not admissible in the context of well-designed cryptosystems [12, Rule 7]. Consequently, we must conclude that the cryptosystem defined in [6] is not well designed.

5. Conclusions

Although in [6] it is claimed that the therein introduced cryptosystem is an improvement of [4], we have shown that both cryptosystems are marred by the same shortcomings that were pointed out in [8, 9]. In addition, some additional flaws of the cryptosystem in [6] have been reported, too. Indeed, the encryption procedure described in [6] is based on a non-invertible function, and some parts of the key can be estimated from the observation of the encryption/decryption times. Moreover, we have shown that the cryptosystem is not robust against noise, which was presented as a virtue of the cryptosystem by its authors. As a result, the use for secure communications of the cryptosystem proposed in [6] should be discarded.

Acknowledgments

The work described in this paper was supported by *CDTI, Ministerio de Industria, Turismo y Comercio of Spain* in collaboration with Telefónica I+D, Project SEGUR@ with reference CENIT-2007 2004, *CDTI, Ministerio de Industria, Turismo y Comercio of Spain* in collaboration with SAC, project HESPERIA (CENIT 2006-2009), and *Ministerio de Ciencia e Innovación of Spain* in collaboration, project CUCO (MTM2008-02194). Shujun Li was supported by a fellowship from the Zukunftskolleg of the Universität Konstanz, Germany, which is part of the "Excellence Initiative" Program of the DFG (German Research Foundation).

References

[1] S. Banerjee, J. A. Yorke, C. Grebogi, Robust chaos, Physical Review Letters 80 (14) (1998) 3049–3052.
[2] N. K. Pareek, V. Patidar, K. K. Sud, Discrete chaotic cryptography using external key, Physics Letters A 309 (1-2) (2003) 75–82.
[3] N. K. Pareek, V. Patidar, K. K. Sud, Cryptography using multiple one-dimensional chaotic maps, Communications in Nonlinear Science and Numerical Simulation 10 (715-723) (2005) 7.
[4] 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.
[5] N. Pareek, V. Patidar, K. Sud, Image encryption using chaotic logistic map, Image and Vision Computing 24 (9) (2006) 926–934.
[6] A. N. Pisarchik, M. Zanin, Image encryption with chaotically coupled chaotic maps, Physica D 237 (2008) 2638–2648.
[7] G. Alvarez, F. Montoya, M. Romera, G. Pastor, Cryptanalysis of a discrete chaotic cryptosystem using external key, Physics Letters A 319 (3-4) (2003) 334–339.
[8] 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.
[9] 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.
[10] C. Li, S. Li, M. Asim, J. Nunez, G. Alvarez, G. Chen, On the security defects of an image encryption scheme, Image and Vision Computing 27 (9) (2009) 1371–1381.
[11] D. Arroyo, Framework for the analysis and design of encryption strategies based on discrete-time chaotic dynamical systems, Ph.D. thesis, ETSIA of the Polytechnic University of Madrid, Madrid, Spain, avalaible online at `http://digital.csic.es/handle/10261/15668` (July 2009).
[12] G. Alvarez and S. Li, Some basic cryptographic requirements for chaos-based cryptosystems, Int. J. Bifurc. Chaos **16**, 2129–2151 (2006).