A MULTIDIMENSIONAL MAP FOR A CHAOTIC CRYPTOSYSTEM

Rhouma Rhouma[1], *Belghith Safya*[2]
Syscom laboratory, Ecole Nationale d'Ingénieurs de Tunis. Tunisia
Phone : +(216) 98 96 74 23. Email : rhoouma@yahoo.fr [1], safya.belghith@enit.rnu.tn [2]

ABSTRACT

In this paper, we propose a new cryptosystem that is faster than that of Baptista and present a uniform distribution in his ciphertext. To increase the security, we use the logistic map and a 3-dimensional piecewise linear chaotic map in the generation of the associations tables. Simulation results show that performance and security of the proposed cryptographic scheme are better than the Baptista algorithm.

1. INTRODUCTION

In [1], Baptista proposed a chaotic cryptosystem based on partitioning the visiting interval of chaotic orbits of the logistic map. After its publication, several modified versions have been proposed [2–7]. On the other hand, some attacks have been reported as ways of breaking the original Baptista-type cryptosystem and some of its modified versions [8–11]. In this section, we give a brief survey on the chaotic cryptosystem of Baptista [1]. The author assumes that the message to be transmitted is a text composed by some alphabet. A portion of the attractor (ε-interval) is associated with every alphabetic unit and the encryption of a character is the number of iterations of the logistic map (equation 1) needed to make its trajectory, departing from some initial condition a_0, to reach the ε-interval associated with that character.

The secret key consists of three elements: the S associations between the S ε-intervals and the S units of an alphabet, the first initial condition a_0, and the control parameter g. The decryption of the ciphertext is performed by iterating the logistic map as much times as indicated by the ciphertext. The position of the final point, with respect to the S ε - intervals, informs the receiver about the original character.

As mentioned in [12], the original Baptista-type chaotic cryptosystem has the following four defects:

(1) The encryption speed is very low as compared with most conventional ciphers.
(2) The distribution of the ciphertext is non-uniform.
(3) It is insecure against some attacks proposed in [8, 9].
(4) The ciphertext size is larger than that of the plaintext.

In the next section, we propose a new version of the cryptosystem of Baptista. The distribution of the ciphertext is uniform and the encryption speed is higher than the one of the original versions of Baptista.

2. CRYPTOSYSTEM'S DESCRIPTION

We use two chaotic maps:

- The one dimensional logistic map governed by the following equation :

$$a_{n+1} = ga_n(1-a_n) \qquad \textbf{(1)}$$

- The three dimensional PLWCM map proposed by Mira [13] governed by the system T:

$$T\begin{cases} x_{k+1} = py_k + bz_k \\ \begin{cases} py_k + \lambda x_k - 6(a+\lambda) & \text{if } x_k > 6 \\ py_k - ax_k & \text{if } x_k < 6 \end{cases} \\ z_{k+1} = cz_k + dx_k \end{cases}$$

With a matrix notation the system will be:

$$X_{k+1} = A\ X_k + B\ e_k \qquad \textbf{(2)}$$

$$X_k = \begin{pmatrix} x_k & y_k & z_k \end{pmatrix}^T \ ; \ B\ = \begin{bmatrix} 0\,1\,0 \end{bmatrix}^T$$

$$\text{if } x_k < 6 \ : \ A = \begin{pmatrix} 0 & p & b \\ -a & p & 0 \\ d & 0 & c \end{pmatrix} \text{ and } e_k = -\ 6(a+\lambda)$$

$$\text{if } x_k > 6 : \ A = \begin{pmatrix} 0 & p & b \\ \lambda & p & 0 \\ d & 0 & c \end{pmatrix} \text{ and } e_k = 0$$

The set of parameters which make this system chaotic is: (a =1.2, b =0.5, c =0.9, d =-0.1, λ =3.5, p = 0.89). The phase space for these parameters is presented in the figure 1.

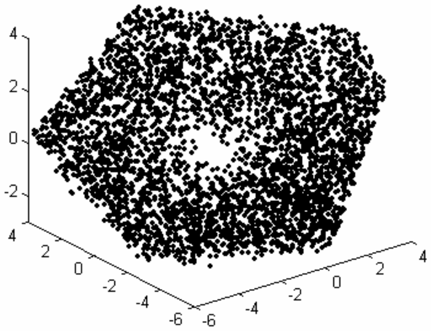

Figure 1: Phase space of the chaotic system proposed by Mira

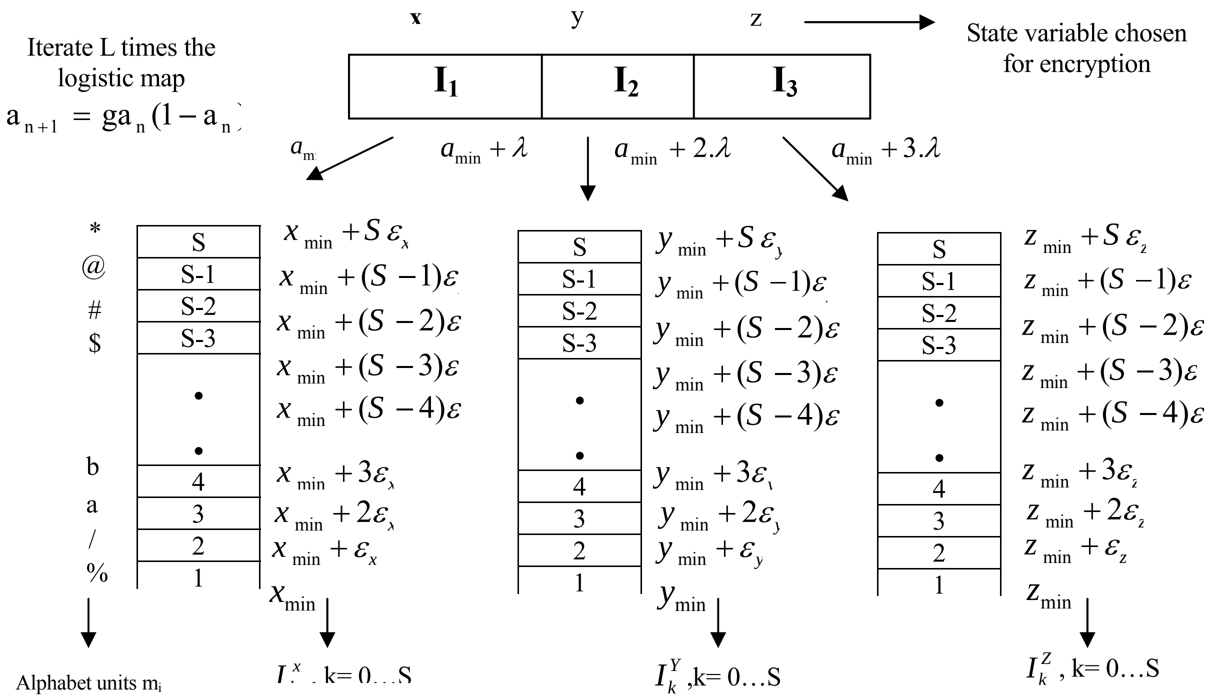
Iterate L times the logistic map
$a_{n+1} = ga_n(1-a_n)$
x
y
z
State variable chosen for encryption
I_1
I_2
I_3
a_{m}
$a_{\min}+\lambda$
$a_{\min}+2.\lambda$
$a_{\min}+3.\lambda$
* @ # $ b a / %
S
S-1
S-2
S-3
4
3
2
1
$x_{\min}+S\varepsilon_x$
$x_{\min}+(S-1)\varepsilon$
$x_{\min}+(S-2)\varepsilon$
$x_{\min}+(S-3)\varepsilon$
$x_{\min}+(S-4)\varepsilon$
$x_{\min}+3\varepsilon_x$
$x_{\min}+2\varepsilon_x$
$x_{\min}+\varepsilon_x$
$x_{\min}$
$y_{\min}+S\varepsilon_y$
$y_{\min}+(S-1)\varepsilon$
$y_{\min}+(S-2)\varepsilon$
$y_{\min}+(S-3)\varepsilon$
$y_{\min}+(S-4)\varepsilon$
$y_{\min}+3\varepsilon_y$
$y_{\min}+2\varepsilon_y$
$y_{\min}+\varepsilon_y$
$y_{\min}$
$z_{\min}+S\varepsilon_z$
$z_{\min}+(S-1)\varepsilon$
$z_{\min}+(S-2)\varepsilon$
$z_{\min}+(S-3)\varepsilon$
$z_{\min}+(S-4)\varepsilon$
$z_{\min}+3\varepsilon_z$
$z_{\min}+2\varepsilon_z$
$z_{\min}+\varepsilon_z$
$z_{\min}$
Alphabet units m_i
I_k^X , k= 0…S
I_k^Y ,k= 0…S
I_k^Z , k= 0…S

Figure 2: The 3*S associations between the alphabet units and the sub-intervals of the state variables

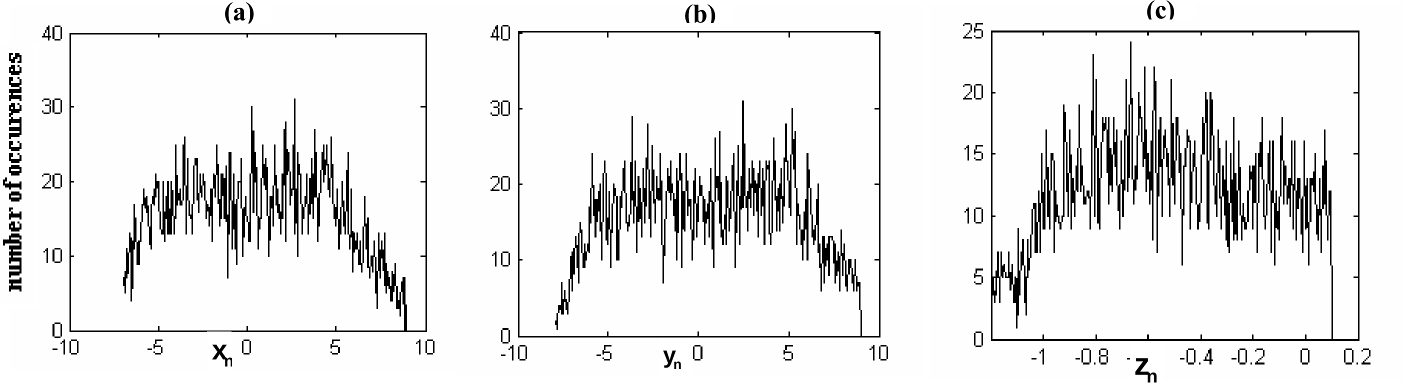

Figure 3: Natural invariant density of the state variable (a)x in the interval [-7, 9] (b)y in the interval [-8, 9] (c) z in the interval [-1.2, 0.1]

2.1 Creation of the associations tables

The first step of the creation of the association tables consists in dividing the interval of variation [0, 1] of the logistic map (equation.1) into three equal sub-intervals (I_1, I_2, I_3). Each one of them is associated with each one of the state variables (x, y, z) of the chaotic system T (equation.2). With this association, we can choose which state variable will be used for the next plaintext unit encryption. The plaintext is formed by S alphabets (S=256). Then, the variation interval of each state variable (x, y, z) is divided into S sub-intervals. At the last step, we make an association between the S alphabets of the plaintext and the S subintervals of each state variable. The figure 2 explains these associations. We note that the trajectories of the three state variables must visit frequently each sub-interval taken in the association tables. Consequently, there's no risk in associating a character to a sub-interval that the trajectory doesn't visit. Therefore, we compute the natural invariant density (see figure 3) of each state variable.

2.2 Notation

- I_k= $[a_{\min}+(k-1)\lambda, a_{\min}+k\lambda]$, $0\leq$ k ≤ 3 ;λ=($a_{\max}$-$a_{\min}$)/3 and $[a_{\min}, a_{\max}]$=$[0.2, 0.8]$ is the interval of the logistic map variation's (eq.1).
- I_k^x :$[x_{\min}+(k-1)\varepsilon_x, x_{\min}+k\varepsilon_x]$, $0\leq$k$\leq$S; $S=256$,$\varepsilon_x=(x_{\max}-x_{\min})/S$ and$[x_{\min}, x_{\max}]$=$[-7,9]$
- I_k^y : $[y_{\min}+(k-1)\varepsilon_y, y_{\min}+k\varepsilon_y]$, $0\leq$ k $\leq$S; $S=256$, $\varepsilon_y=(x_{\max}-x_{\min})/S$ and $[y_{\min}, y_{\max}]$=$[-8,9]$.
- I_k^z : $[y_{\min}+(k-1)\varepsilon_z, y_{\min}+k\varepsilon_z]$, $0\leq$ k$\leq$S; $S=256$, $\varepsilon_z=(x_{\max}-x_{\min})/S$ and $[z_{\min}, z_{\max}]$=$[-0.1,1.2]$.
- f(.) is the function of the associations between the S characters and the S sub-intervals.

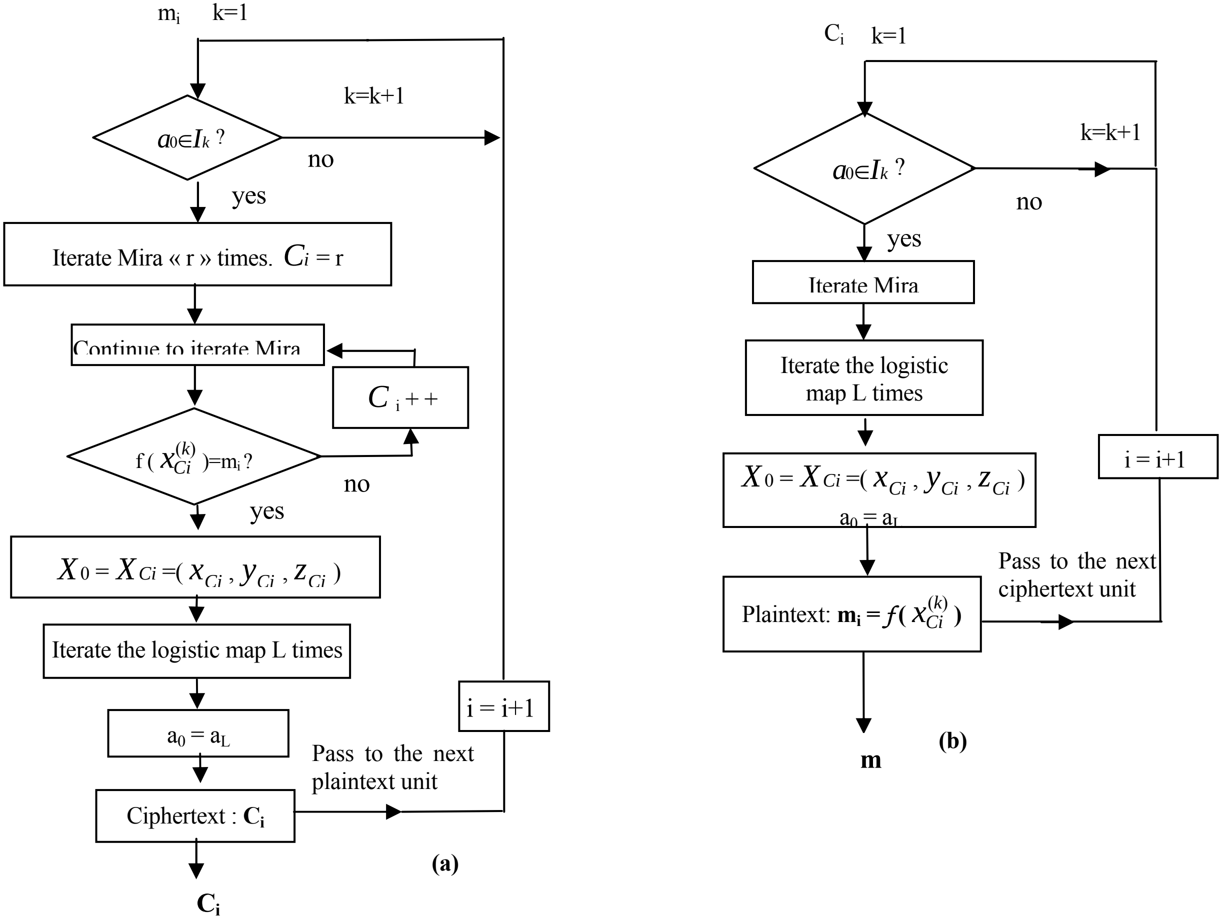
m_i k=1
k=k+1
$a_0 \in I_k$?
no
yes
Iterate Mira « r » times. C_i = r
Continue to iterate Mira
C_i++
f($x_{Ci}^{(k)}$)=m_i?
no
yes
$X_0 = X_{Ci} = (x_{Ci}, y_{Ci}, z_{Ci})$
Iterate the logistic map L times
$a_0 = a_L$
i = i+1
Pass to the next plaintext unit
Ciphertext : C_i
(a)
C_i
C_i k=1
k=k+1
$a_0 \in I_k$?
no
yes
Iterate Mira
Iterate the logistic map L times
$X_0 = X_{Ci} = (x_{Ci}, y_{Ci}, z_{Ci})$
$a_0 = a_L$
i = i+1
Pass to the next ciphertext unit
Plaintext: $m_i = f(x_{Ci}^{(k)})$
m
(b)

Figure 4: (a) Encryption scheme (b) Decryption scheme

2.3 Cryptosystem keys

The secret keys of the proposed cryptosystem are:

- The parameters of the chaotic system T: a, b, c, d, λ, p and the initial condition $X_0 = (x_0 \quad y_0 \quad z_0)$.
- The parameter of the logistic map: g , and the initial condition of the logistic map : a_0 .
- The $3 \times S$ associations of the three state variables: each association is between the relative S alphabets and its S-subintervals.
- The parameter L can be taken as a secret key. It can have also different values for different messages, so that the security can be enhanced. This is possible because L is not a critical parameter for initialising the decryption. The figure 5 shows an illustration of this procedure.

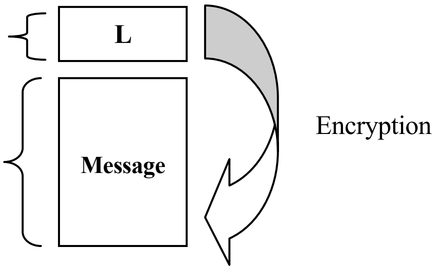

Figure 5: Encryption of the parameter L then encryption of the message

2.4 Encryption

For the encryption of each message block m_i, we shall first know which state variable to use. Thus, the first condition a_0 of the logistic map belongs to one of the 3 sub-intervals (I_1, I_2, I_3). That does allow the selection of the appropriate variable which will be used to encrypt the first character in the plaintext m_1. The next step is to randomly choose a number r between 0 and a pre-defined maximum $r_{\max}$ (this approach was first proposed by Wong [2]). Then, let the chaotic system T iterate for "r" times. After that, the iteration continues until the trajectory falls into the desired region. The ciphertext is the total number of iterations of the chaotic system T. We achieve the encryption of m_1 by iterating the logistic map L times. For the next character in the plaintext m_2, we use a_L to know which state variable we shall use (x or y or z). If for example we find that the trajectory falls in the third sub-interval, we shall use the table of association of the third state variable z. and so on. (see figure 4-a).

2.5 Decryption

To decrypt the ciphertext C_i, we shall first know which state variable to use. Thus, the first condition a_0 of the logistic map belongs to one of the 3 sub-intervals (I_1, I_2, I_3). That allows to select the appropriate variable which will be used to decrypt the first unit in the ciphertext. By iterating the chaotic system "T" (eq. 2) C_i times and the trajectory of the state variable (x or y or z) will fall in a sub-interval which is associated with the plaintext character. After that, we iterate the logistic map L times. For the next ciphertext unit we repeat the same procedure and so on. (see figure 4-b).

	Parameters	**Encryption time (s) / Total number of iterations**		
		Text file 0.21 Ko	**Text file 1.03 Ko**	**Image bmp 1.67 Ko**
Baptista method	**η = 0.7**	1.156 / 127760	5.7960 / 678150	15.38 / 1035019
	η = 0.9	3 / 283779	14.1250 / 1654365	46.09 / 3093528
Proposed method (L=100)	**r_{max}=500**	0.313 / 93391	1.359 / 455466	1.35 / 312439
	r_{max}=1000	1.562 / 150964	1.984 / 715259	1.703 / 476768
	r_{max}=5000	2.25 / 527861	7.516 / 2889543	4.61 / 1681521

Table 1: The encryption time on files of different sizes and types at different parameter values using the proposed and Baptista method's

3. RESULTS

In order to compare the performance of the proposed method with the original chaotic cryptographic scheme [1], we have chosen to use three files: 2 text files of sizes 0.21 and 1.03 Ko and an image bitmap file of 1.67 Ko. These three files are used for encryption. Two algorithms are implemented using Matlab programming languages running on a personal computer with a Pentium IV-2.53 GHz processor and 256 MB RAM.

- Algorithm 1: Baptista's original method with the different values of η.
- Algorithm 2: The proposed method with different values of r_{max} and for L =100.

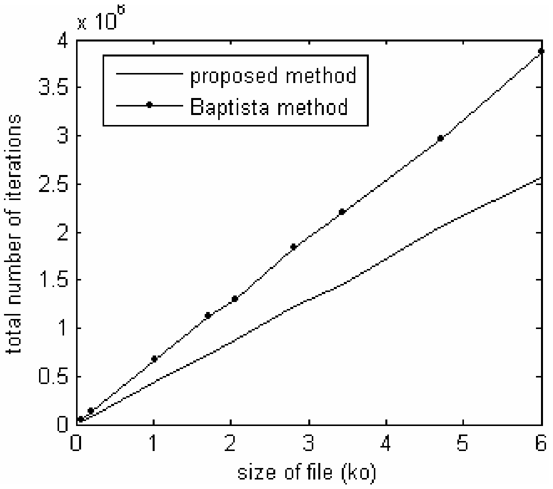

Figure 6 : Speed of the Baptista cryptosystem and the proposed system measured for different files of different sizes

The encryption speed and the total number of iterations are listed in Table 1. The proposed cryptosystem can be faster than the one proposed by Baptista if we choose appropriate values of r_{max} and L. It is clear that the total number of iterations for the encryption operation in the Baptista's method is always superior to the proposed one. That means that the encryption speed of the proposed method is higher than Baptista's method. (see figure 6).

Figure 7 shows the distributions of the ciphertexts obtained by encrypting 8 KB image bitmap file with the Baptista method (a) and the new proposed method (b). Two observations can be made about the distribution of the ciphertext of the proposed method: the first one is that it is very flat in the region between 0 and $r_{\max}$. The second is that it is more uniform than the distribution of the ciphertext of the Baptista method.

4. CONCLUSION

We have proposed modifications on the Baptista cryptosystem which can enhance the security of the cryptosystem by enlarging the key space through introducing other parameters. The distribution of the produced ciphertext is uniform. Results show that the proposed cryptosystem is faster than Baptista's.

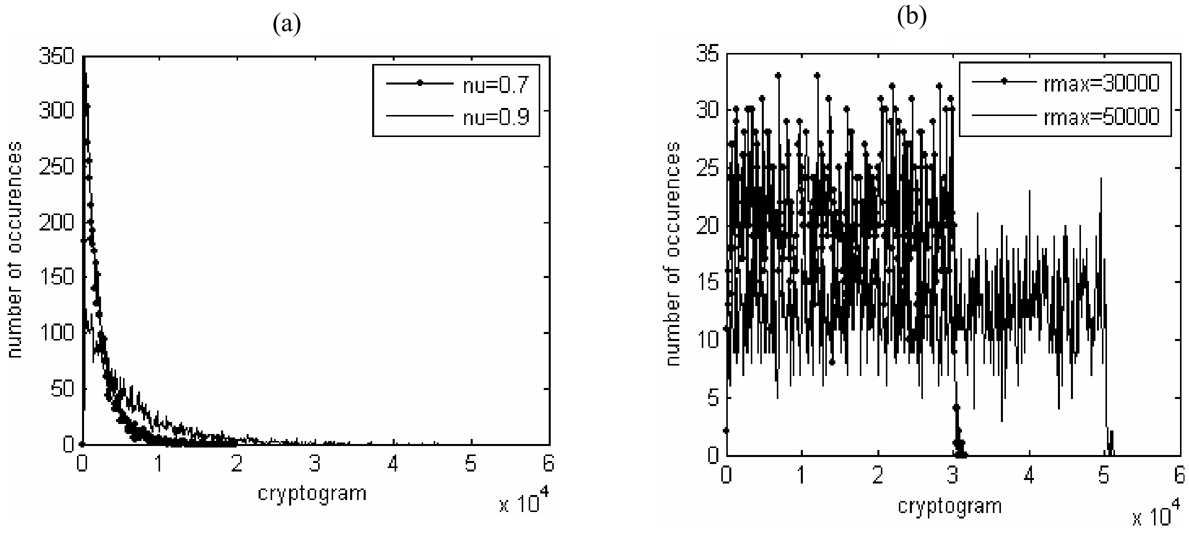

Figure 7 : Distribution of the ciphertext by (a) the Baptista original method (b) the proposed method

REFERENCES

[1] M.S. Baptista, Cryptography with chaos . Phys. Lett. A 240 (1–2) (1998) 50.

[2] W.-K. Wong, L.-P. Lee, K.-W. Wong, Comput. Phys. Communication. 138 (3) (2001) 234.

[3] K.-W. Wong, Phys. Lett. A 298 (4) (2002) 238.

[4] K.-W. Wong, Phys. Lett. A 307 (5–6) (2003) 292.

[5] K.-W. Wong, S.-W. Ho, C.-K. Yung, Phys. Lett. A 310 (1) (2003) 67.

[6] A. Palacios, H. Juarez, Phys. Lett. A 303 (5–6) (2002) 345.

[7] S. Li, X. Mou, Z. Ji, J. Zhang, Y. Cai, Phys. Lett. A 307 (1) (2003) 22.

[8] G. Jakimoski, L. Kocarev, Phys. Lett. A 291 (6) (2001) 381.

[9] G. Alvarez, F. Montoya, M. Romera, G. Pastor, Phys. Lett. A 311 (2–3) (2003) 172.

[10] G. Alvarez, F. Montoya, M. Romera, G. Pastor, Comput. Phys. Commun. 156 (2) (2003) 205.

[11] G. Alvarez, F. Montoya, M. Romera, G. Pastor, Phys. Lett. A 326 (3–4) (2004) 211.

[12] Shujun Li, Guanrong Chen , Kwok-Wo Wong , Xuanqin Mou , Yuanlong Cai. Baptista-type chaotic cryptosystems: problems and countermeasures Physics Letters A 332 (2004) 368–375.

[13]: Noninvertible piecewise linear maps applied to chaos synchronization and secure communications. G Millerioux and C. Mira. International Journal of bifurcation and chaos. Vol. 7, No. 7 (1997) 1617-1634.