A MODIFIED CHAOTIC CRYPTOGRAPHIC METHOD

Wai-kit Wong, Lap-piu Lee and Kwok-wo Wong
Department of Electronic Engineering,
City University of Hong Kong,
83 Tat Chee Avenue, Kowloon Tong, HONG KONG

Abstract We propose a modified version of the chaotic cryptographic method based on iterating a logistic map. Simulation results show that the distribution of the ciphertext is flatter and the encryption time is shorter. Moreover, the trade-off between the spread of the distribution of ciphertext and the encryption time can be controlled by a single parameter.

Keyword: Chaotic Cryptography

1. Introduction

The use of chaotic systems for secure or private communications has been an active area of research in the past few years. It is based on the facts that chaotic signals are usually noise-like and chaotic systems are very sensitive to initial condition. Besides the analogue secure communications that are relied on the synchronization of chaotic systems [1-3], digital chaotic cryptographic approaches have also been proposed [4, 5].

Recently, Baptista proposed a chaotic cryptographic method that encrypts the message text as the number of iterations applied in the chaotic map in order to reach the region corresponds to that text [4]. He demonstrated his approach using a simple one-dimensional logistic map governed by the following equation:

$$X_{n+1} = bX_n(1 - X_n), \qquad (1)$$

where b is the gain and $X_n \in [0, 1]$.

Since the ciphertexts are small integers, they are suitable to be transmitted through today's public digital networks. In order to avoid statistical and differential cryptanalysis, a random number is generated each time the chaotic trajectory has reached the desired region. If it is greater than a

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35413-2_36

R. Steinmetz et al. (eds.), *Communications and Multimedia Security Issues of the New Century*

threshold η, the current number of iterations will be transmitted as ciphertext. Otherwise, the iteration will continue.

2. Drawbacks of Baptista's Method

There are two major drawbacks with Baptista's approach. First, the resultant ciphertext is usually concentrated at the smaller number of iterations, as observed from Fig. 1 that shows the distribution of the ciphertext obtained by encrypting a typical 495KB text file downloaded arbitrarily from the internet. In the figure, the solid line corresponds to the case that the threshold η is chosen as 0.7 while the dashed line shows the distribution when η is set at 0.9. Note that the statistics are gathered at intervals of 100 iterations. As the distribution of ciphertext is not flat enough, this property is not desirable in cryptography. The other drawback is that a sequence of random numbers may have to be generated for a single block of message text. The encryption time is thus longer and the random numbers generated may repeat at an early time. To deal with these drawbacks, we propose a modified method that will give a flatter distribution of ciphertext, with a single random number generation for each block of message text. Moreover, the trade-off between the spread of the distribution of ciphertext and the encryption time can be controlled by a single parameter.

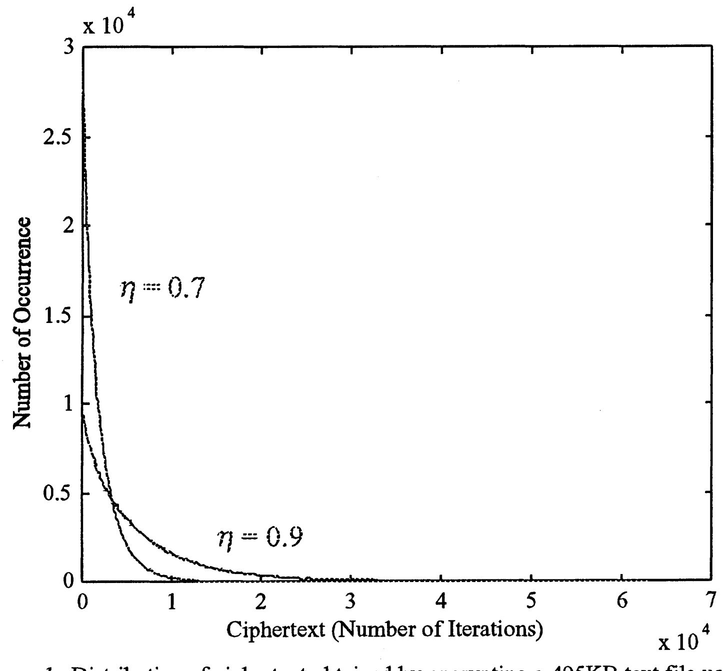

Figure 1. Distribution of ciphertext obtained by encrypting a 495KB text file using Baptista's method with $\eta = 0.7$ and 0.9. The statistics are gathered at intervals of 100 iterations.

3. The Modified Chaotic Cryptographic Method

Follow Baptista's method [4], we also use the logistic map in our modified version. We first define a mapping of ASCII code of the message text to different regions in the interval 0.2 to 0.8 of the phase space of the logistic map with gain b=3.9999995. For the encryption of each message block, we first generate a random number r between 0 and a pre-defined maximum $r_{\max}$. Then we let the logistic map iterate for r times. After that, the iteration continues until the trajectory first falls into the desired region. The total number of iterations is sent immediately as the ciphertext. We also use 16-bit integers for the ciphertext, therefore the maximum allowable number of iterations is limited to 65,535. Figure 2 shows the distribution of the ciphertext obtained by encrypting the same 495KB text file as used to obtain Fig. 1. The solid line corresponds to the case that $r_{\max}$ is chosen as 15,000 while the dashed line shows the result of setting $r_{\max}$ to 32,767. Again, the statistics are gathered at intervals of 100 iterations. It can be observed from the figure that the distribution is very flat in the region between 0 and $r_{\max}$.

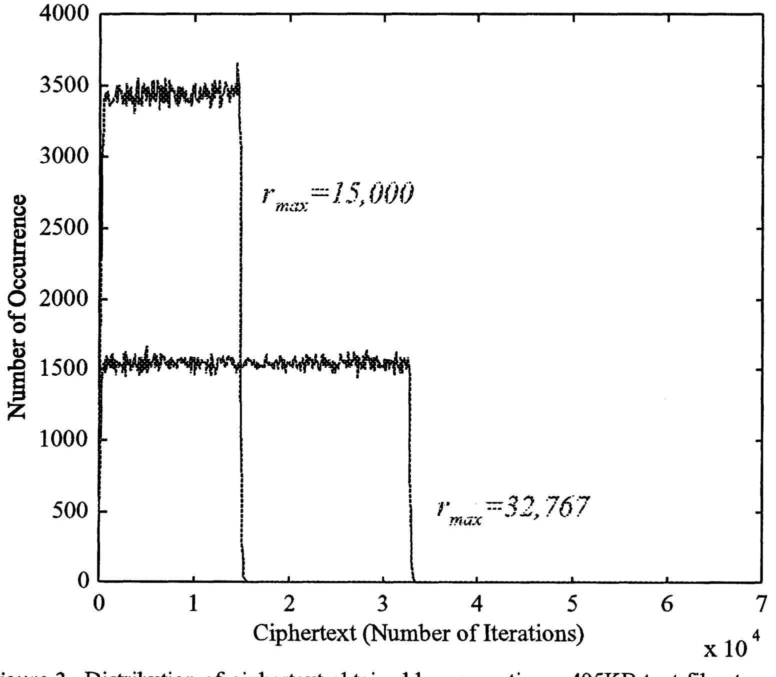

Figure 2. Distribution of ciphertext obtained by encrypting a 495KB text file at $r_{\max}$=15,000 and 32,767.

In our modified method, the trade-off between the spread of the distribution and the encryption time can be controlled by the parameter $r_{\max}$.

With a larger value of this parameter, the distribution of ciphertext spreads wider, but the encrypting time is longer. A small $r_{\max}$ accelerates the encryption process but results in a narrower distribution of ciphertext. The encryption times for text files of different sizes using different values of $r_{\max}$ are listed in Table 1. The results using Baptista's method at $\eta = 0.7$ and 0.9 are also given. The data show that our method is faster at most of the parameter values. Moreover, the encryption time increases linearly with the file size.

Although the time required to encrypt a 495KB text file is quite long, it takes less than 4 seconds for encrypting a file of 4KB size which is the typical size of an email without attachment. Therefore, the modified method is practical in secure e-mail communication. The secret keys are the gain of the logistic map and the initial condition. They can be sent to the receiver using public key cryptographic methods such as RSA [6]. Once these session keys are obtained, the proposed private key cryptographic approach can be used for the subsequent secure e-mail communications.

Table 1. The encryption time on text files of different sizes at different parameter values using the proposed and Baptista's methods.

Method	$r_{\max}$	Encryption time for a 4KB file / sec	Encryption time for a 40KB file / sec	Encryption time for a 495KB file / sec
Proposed Method	5000	1	17	240
	10,000	2	23	241
	15,000	2	29	308
	20,000	2	36	377
	25,000	3	42	448
	32,767	4	54	557
Baptista's Method	η=0.7	3	39	410
	η=0.9	8	110	1229

We have modified Baptista's chaotic cryptographic method based on iterating a logistic map. Simulation results show that the distribution of the ciphertext is flatter and the encryption time is shorter. Moreover, the trade-off between the spread of the distribution of the ciphertext and the encryption time can be controlled by a single parameter.

References

[1] G. Grassi, S. Mascolo, Electron. Lett. 34 (1998) 1844.

[2] Y.H. Chu and S. Chang, Electron Lett. 35 (1999) 271-273.

[3] T. Yang Tao, C.W. Wu, L.O. Chua, IEEE Trans. CASI 44 (1997) 469.

[4] M.S. Baptista, Phys. Lett. A 240 (1998) 50.

[5] E. Alvarez, A. Fernandez, P. Garcia, J. Jimenez, A. Marcano, Phys. Lett. A 263 (1999) 373.

[6] A.J. Menezes, P.C. Oorschot, and S.A. Vanstone, Handbook of Appl. Cryptography (CRC Press, New York, 1996).