1-22

Improvement of Cryptosystem Using Two Chaotic Maps

Yuji Okazaki Yoko Uwate Yoshifumi Nishio
(Tokushima University)

1. Introduction

The characteristic of chaos is suitable for the cryptography [1]. In the past study, we have proposed a cryptosystem using two chaotic maps [2]. In this study, we propose an improved version of the cryptosystem using two chaotic maps by changing one of parameters of the maps according to chaotic sequences.

2. Encryption and decryption functions

The encryption function and the decryption functions in the proposed systems are described as follows,

F :

$$\begin{cases} X_{k+1} = Y_k(1-\sqrt{1-X_k}) \\ \qquad\qquad (0 \le Y_k \le b) \\ Y_{k+1} = Y_k/b \\ \\ X_{k+1} = Y_k + \sqrt{1-X_k}(1-Y_k) \\ \qquad\qquad (b < Y_k \le 1) \\ Y_{k+1} = (Y_k-1)/(b-1) \end{cases}$$

F^{-n} :

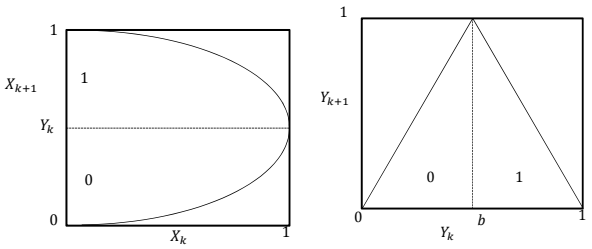
$$\begin{cases} X_k = \dfrac{2}{Y_{k+1}} X_{k+1}\left(1-\dfrac{X_{k+1}}{2Y_{k+1}}\right) \\ \qquad\qquad (Y_{k+1} < X_{k+1} \le 1) \\ Y_k = bY_{k+1} \\ \\ X_k = \left(\dfrac{X_{k+1}+1-2Y_{k+1}}{1-Y_{k+1}}\right)\left(2-\dfrac{X_{k+1}+1-2Y_{k+1}}{1-Y_{k+1}}\right) \\ \qquad\qquad (0 \le X_{k+1} \le Y_{k+1}) \\ Y_k = (b-1)Y_{k+1}+1 \end{cases}$$

where F is an encryption map and F^{-1} is a decryption map. The value of b is a private key in this cryptosystem. These maps are shown in Figs. 1 and 2. The threshold value dividing branches and selected branch of the function giving X_{k+1} are decided by the value of Y_k. Namely, the chaotic maps change their shapes depending on the value of the sequences.

3. Cryptosystem

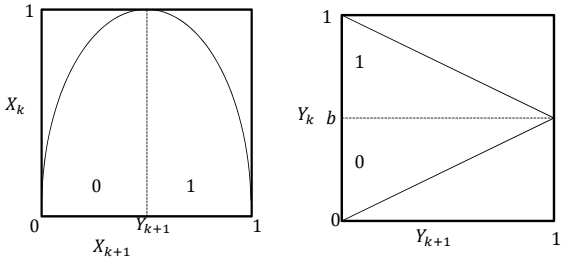
3.1 Encryption

Initial point Y_0 as a plaintext and X_0 as a subtext are set to F, where, $Y_0, X_0 \in (0,1)$, and X_0 is an arbitrary value. Calculate $(X_n, Y_n) = F_n(X_0, Y_0)$, namely n-times iterations of F. The ciphertext Y_n is transferred with X_n, which is necessary to decryption as a one-time key. Whenever the map is repeated, a different shape of the chaotic map is used because the threshold value X_k changes. When the branch of Y_k is 0, the branch of X_k is selected as 0, while when the branch of Y_k is 1, the branch of X_k is selected as 1.



(a) (b)

Figure 1: Encryption map F. (a) Inverse logistic map. (b) Tent map.



(a) (b)

Figure 2: Decryption map F^{-1}. (a) Logistic map. (b) Inverse tent map.

3.2 Decryption

Calculate $(X_0, Y_0) = F^{-n}(X_n, Y_n)$, namely n-times iterations of F^{-n}, and the decrypt the plaintext Y_0.

4. Conclusions

In this study, we have proposed an improved cryptosystem using two chaotic maps Because one of the parameters of the maps changed at every calculations in the proposed system, we expect that more complicated chaotic sequence can be generated and hence the proposed system is stronger against attacks than the existing chaotic cryptosystems.

Performance comparison with the existing cryptosystems is an important future work.

References

[1] T. Habutsu, Y. Nishio, I. Sasase, and S. Mori, "A Secret Key Chaotic Map," Trans. of IEICE, vol.E73, no.7, pp.1041-1044, 1990

[2] S. Aono, M. Wada, and Y. Nishio, "Improvement of a Cryptosystem Using Two Chaotic Maps," Proc. of NCSP'06, pp.349-352, Mar. 2006.