Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 4, April 2013, pg.422 – 428

RESEARCH ARTICLE

Adapted Encryption Algorithm with Multiple Skew Tent Map

Sarika Tyagi[1], Deepak chaudhary[2]
[1]Department of Information Technology, IET, Alwar, India
[2]Department of Information Technology, IET, Alwar, India

[1] *siddhityagi@gmail.com;* [2] *deepak.se17@gmail.com*

Abstract— In recent years, the chaos based cryptographic algorithms have some optional and efficient ways to develop secure encryption techniques. In this paper, we proposed a modified approach for encryption based on chaotic skew tent maps in order to meet the requirements of the secure transfer. In the projected encryption scheme, an external secret key of 128-bit and two chaotic skew tent maps are employed. The initial conditions for the both skew tent maps are derived using the external secret key. The results of several experimental, statistical analysis and key sensitivity tests show that the proposed encryption scheme provides an efficient and secure way for encryption and transmission.

I. 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]

Consequently, the traditional ciphers are not suitable for encryption as these ciphers require a large computational time and high computing power. For encryption only those ciphers are preferable which take lesser amount of time and at the same time without compromising security. Nowadays, information security is becoming more important in data storage and transmission.

A number of chaos based encryption scheme have been developed in recent years and In this respect, chaos based encryption techniques are considered good for practical use as chaos based algorithms provide a good combination of speed, high security, complexity, reasonable computational over- heads and computational power. Moreover, chaos-based and other dynamical systems based algorithms have many important properties such as the sensitive dependence on initial conditions and system parameters, pseudo random properties, ergodicity, non-periodicity. These properties meet some requirements such as sensitive to keys, diffusion and mixing in the sense of cryptography. Therefore, chaotic dynamics are expected to provide a fast and easy way for building superior performance cryptosystems. These characteristics of the chaotic maps have attracted the attention of cryptographers to develop new encryption algorithms which can be considered analogous to some cryptographic properties of ideal ciphers such as confusion, diffusion, balance and avalanche property etc. In this communication, a new encryption scheme is proposed based on chaotic skew tent maps in order to meet the requirements of the secure transfer. In recent years, a number of discrete chaotic cryptographic algorithms [4–13] have been proposed for realizing the private key cryptography with chaos. In most of the discrete chaotic cryptographic approaches [3–12] one chaotic map is used and either the system parameter or initial condition of the chaotic map or both is used as a secret key. Recently, Pareek et al. [13] have developed a cryptosystem using a one-dimensional chaotic map (logistic map) in which an external secret key has been used. Further in this algorithm neither system parameter nor initial condition of the chaotic map has been used as secret key however

these parameters have been generated with the help of external secret key. For improving the security of discrete chaotic cryptosystem utilizing the external secret key [13],In this paper, we use the concept of using more than one one-dimensional chaotic maps in cryptography. Inclusion of more than one chaotic map increases the confusion in the encryption process and it results in a more secure cryptosystem due to the fact that more confusion in encryption makes cryptosystem more secure. The proposed cryptosystem is a symmetric key block cipher algorithm in which multiple one-dimensional chaotic maps and an external secret key of 128-bit is used. The initial conditions for the both skew tent maps are derived using the external secret key by providing different weightage to its bits. In Section 3, we discuss the step by step procedure of encryption and in Section 4, the security analysis of the proposed encryption scheme such as key and plaintext sensitivity analysis, key space analysis to prove its security against the most common attacks. Finally, in Section 6, we conclude the paper.

II. ANALYSIS OF EXISTING CRYPTOSYSTEM

In [4-14],we investigate the essential weaknesses of existing cryptosystem and some redundancies that contribute little to its security.

First problem is is that the plaintext and the ciphertext are both divided into blocks of 8-bits, and the encryption and decryption are also based on this unit or restricted to it. A plaintext of 8-bit provides limited plaintext space and as well as the corresponding ciphertext space.

Secondly, there are some redundant processes that contribute little to the security of the cryptosystems but decelerate the encryption and decryption .The first redundancy is the variety of the system parameter (μ) of the skew tent map (x=$\mu x(1-x)$)in the existing algorithm. It is hoped that the time-varying (μ) calculated by an updating equation can enhance the security of the cryptosystem. However, the parameter and the initial value of the equation are totally determinative and public and an adversary can figure out the exact μ used in each iteration.

III. THE PROPOSED ENCRYPTION PROCEDURE

In this section, we discuss the step by step procedure of the proposed image encryption as well as decryption process using two chaotic skew tent maps.

1. The proposed encryption process utilizes an external secret key of 128-bit long. Further, the secret key is divided into blocks of 32-bit each, referred as session keys.

$$K = k_1 k_2 \ldots k_{32} \text{ (in hexadecimal)} \qquad (1)$$

here, k_i's are the alphanumeric characters (0–9 and A -F)

and each group of two alphanumeric characters represents a session key. Alternatively, the secret key can be represented in ASCII mode as

$$K = K_1 K_2 \ldots K_4 \text{ (in ASCII mode)} \qquad (2)$$

here, each K_i represents one 32-bit block of the secret key i.e. session key.

2. In the proposed algorithm, two chaotic skew tent maps are employed to achieve the goal of image encryption which are as follow:

$$f(x) = \begin{cases} \frac{x}{p1}, & x \in (0, p1) \\ \frac{1-x}{1-p1}, & x \in (p1, 1) \end{cases} \qquad (3)$$

$$f(y) = \begin{cases} \frac{y}{p2}, & x \in (0, p2) \\ \frac{1-y}{1-p2}, & x \in (p2, 1) \end{cases} \qquad (4)$$

Throughout the algorithm, keep the value of the system

parameter of the both skew tent maps set to 0.79 and 0.39 resp. for this system while the initial conditions (X_0 and Y_0) for these maps are calculated using some mathematical manipulations on session keys.

3. To calculate the initial condition X_0 for the first skew ten map, choose any two blocks of session keys i.e K_1 and K_3 and we compute a real number X_{01} using the XOR operation between them :

$$X_{01} = (0.K_1 \oplus K_{3)} \quad (5)$$

Further, we compute another real number X_{02} as follows

$$X_{02} = \sum_{i=1}^{8} (k_1)_{10}/128 \quad (6)$$

here k_i's are parts of secret key in hexadecimal mode as
explained in Eq. (1). Now we compute the initial condition X_0 the first skew tent map using X_{01} and X_{02} as:

$$X_0 = (X_{01}+X_{02}) \bmod 1 \quad (7)$$

4. To calculate the initial condition Y_0 for the second skew tent map, we choose two blocks of session keys i.e. $K_1K_2K_3$, and convert them into a binary string as:

$$Y_{01} = K_2 \oplus K_4 \quad (8)$$

Further, we compute another real number Y_{02} as follows:

$$Y_{02} = (\sum_{i=1}^{8} (k_i)_{10}/128) \oplus Y_{01} \quad (9)$$

Now we compute the initial condition Y_0 for the second logistic map using Y_{01} and Y_{02} as:

$$Y_0 = (Y_{01}+Y_{02}) \bmod 1 \quad (10)$$

5. Now we calculate the iteration number T_0 from the session key i.e iteration number is dependent on the key.

$$T_0 = K_{(60)} K_{(61)} K_{(62)} \ldots K_{(67)} \quad (11)$$

In this way, we convert a 128-bit key to the valid value range of initial condition of chaotic maps[0,1] with 2^{32} possible values. We also get a key dependent value for T_0 for the first time of chaotic iteration.

6. Update X_i , Y_i and T_i by the equations given below:

$$X_i = \begin{cases} X0, & i = 1 \\ Ci-1 \oplus Xi-1 & i > 1 \end{cases} \quad (12)$$

$$Y_i = \begin{cases} Y0, & i = 1 \\ Ci-1 \oplus Yi-1, & i > 1 \end{cases} \quad (13)$$

$$T_i = \begin{cases} T0, & i = 1 \\ Ti-1 & i > 1 \end{cases} \quad (14)$$

Where z(*) is a bit-wise XOR function between bytes.

7. Iterate the first skew tent map with the initial condition X_i by T times and update X_i to the latest status and similarly iterate the second skew tent map but one time for Y_i given as below:

$$X_i = t_1^T(X_i) \quad (15)$$

$$Y_i = t_2^1(Y_i) \quad (16)$$

Now the updated vales of X_i and Y_i are used to encrypt and decrypt the i^{th} plaintext and ciphertext block given as below:

$$C_i = p(P_i) \oplus C_{i-1} \oplus X_i \ominus Y_i$$

$$P_i = p^{-1} (C_i \oplus C_{i-1} \oplus X_i \oplus Y_i)$$

Where $C_0 = \sum_{i=16}^{23} (k_i)_{10}/128 \oplus K_2 \oplus K_3$

IV. SECURITY ANALYSIS

The proposed cipher is based on existing scheme given in [13,14], whereas all the existing weaknesses are eliminated by different approaches, together with the redundant operations that contribute little to the security. Firstly, we expand both the block size of plaintext/cipher text and the precision of chaotic variable to 32 bits. This gives a much larger space (2^{32}) for the plaintext/cipher text in a block as well as the initial condition of the chaotic map. Compared to the 8-bit block size and only 256 possible values for X_0 in the original schemes, this improvement gets rid of the brute-force attack that can serve as a foundation for further cryptanalysis. What's more, the initial conditions of the two skew tent maps X_0 and Y_0 are determined by key dependent transformations. Even when they are known, an adversary cannot recover the key. Besides the above expansion, we also introduce a permutation scheme into the plaintext block. Quite a lot of existing chaotic cryptosystems operate on a byte-wise plaintext block but do not possess any confusion or diffusion operation within the block. The permutation operation in our cipher is carried out by p(•), which is both plaintext and key dependent.

In [14] cryptosystems, the known-plaintext attack can easily derive the values which are critical to deduce the key. In our improved version, the two chaotic variables X_i and Y_i, whose initial values and updating procedures are related to the key and the ciphertext, respectively, are employed to mask the plaintext. In this manner, only the value of $X_i \oplus Y_i$ can be obtained, but none of X_i or Y_i alone is available to the attacker.

The problem that the sequence of X_i is independent of plaintext was solved by Wei et al. by associating the iteration number with the plaintext. In the proposed scheme, a similar method is employed in (11). Meanwhile, the updating of X_i is also associated with the status of X_{i-1}, the last ciphertext block (C_{i-1}). Besides, a simple and efficient method, i.e. the CBC mode, is also adopted in to enhance the diffusion effect of plaintext.

There are several redundant operations in various cryptosystems which contribute little to the security. In order to simplify the cryptosystem and accelerate the encryption/decryption speed, these redundant operations are eliminated in our scheme. From the simulation results and the analysis, these simplifications do not downgrade the security. Indeed, it improves the performance.

Although there are many advantages in the proposed cipher as stated above, one rule should be kept in mind for selecting the secret key in practical use: do not choose a secret key whose four parts K_1, K_2, K_3, and K_4 are exactly identical. Otherwise, the initial conditions of chaotic maps are zeros and no valid chaotic iterations exist under this condition.

V. KEY SPACE ANALYSIS

For a secure cipher, the key space should be large enough to make the brute force attack infeasible. The proposed image cipher has 2^{128} different combinations of the secret key. An cipher with such a long key space is sufficient for reliable practical use. However, one can have longer key for encryption/- decryption in the proposed cipher and it can be easily incorporated in the algorithm by making slight modification. A longer key would require more computational time for encryption/ decryption which may not be preferable for real time transmission. In the proposed cipher, two chaotic maps are employed for encryption/decryption which are sensitive on the initial condition. The initial conditions for these two skew tent maps are calculated from the secret key with different formulae and further, the initial conditions for these two chaotic skew tent maps are recalculated from the modified secret key.

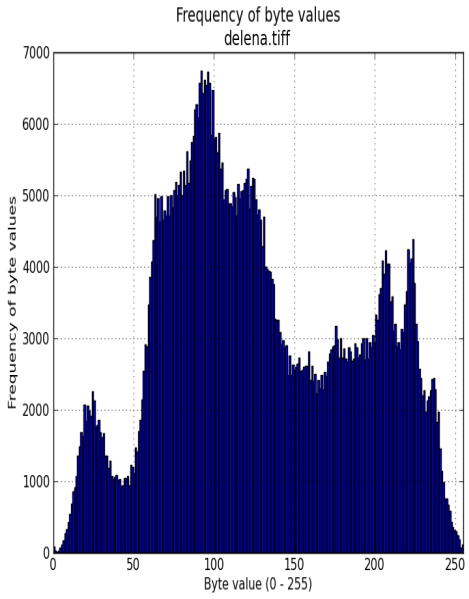
VI. SENSITIVITY ANALYSIS

An ideal encryption procedure should be sensitive with respect to the secret key i.e. the change of a single bit in the secret key should produce a completely different encrypted image. For testing the key sensitivity of the proposed encryption procedure, we have performed the following steps:

(a) An original image (Fig. 1a) is encrypted by using the secret key‘8D6CFB3A538F493DAEDCFD2CFA87A5E6’ (in hexadecimal) and the resultant image is referred as encrypted histogram A (Fig. 1b).

(b) The same original image is encrypted by making the slight modification in the secret key i.e. ‘AD6CFB3A538F493DAEDCFD2CFA87A5E6’ (the most significant bit is changed in the secret key) and the resultant histogram is referred as encrypted image B (Fig. 1c).

(c) Lastly, when we compare the two histograms there is difference between them because of the key changes.



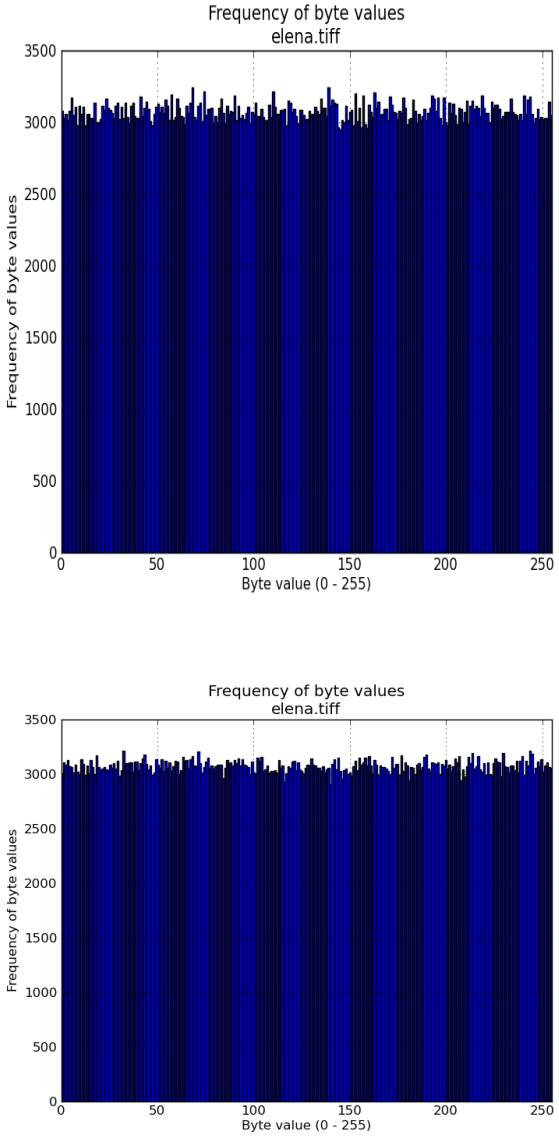


Fig.1 a) shows the original image b) histogram of the image(a). c) the distribution of ciphertext using key '8D6CFB3A538F493DAEDCFD2CFA87A5E6'.d) the distribution of the ciphertext using key 'AD6CFB3A538F493DAEDCFD2CFA87A5E6'.

VII. CONCLUSION

In this communication, a new way encryption scheme has been proposed which utilizes two chaotic skew tent maps and an external key of 128-bit. The initial conditions for both the skew tent maps are derived using the external secret key by providing weightage to its bits corresponding to their position in the key.. We have carried out key sensitivity analysis and key space analysis to demonstrate the security of the new encryption procedure.

Their inherent weaknesses as well as some redundancies that contribute little to the security are eliminated in the proposed method, based on these analyses, an improved cryptosystem is proposed. In the improved scheme, all the existing weaknesses of the existing cryptosystems are eliminated by different approaches. In order to obtain chaotic sequences with better cryptographic feature, two skew tent maps are utilized to instead of logistic map. Some new features such as permutation within ciphertext block, using two independent chaotic variables to mask the plaintext, etc., are also introduced into the system. Theoretic analyses both prove its superiority to the original cryptosystems.

REFERENCES

[1] G. Grassi, S. Mascolo, Electron. Lett. 34 (1998) 1844.
[2] Y.H. Chu, 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] Baptista MS. Cryptography with chaos. Phys Lett A 1998;240(1–2):50–4.
[5] Alvarez E, Fern_andez A, Garci_a PJim_enezJ, Marcano A. New approach to chaotic encryption. Phys Lett A 1999;263:373–5. Phys. Lett. A 263 (1999) 373.
[6] Matthews RAJ. On the derivation of a chaotic encryption algorithm. Cryptologia 1989;XII(1):29–42.
[7] Habutsu T, Nishio Y, Sasase I, Mori S. A secret key cryptosystem by iterating a chaotic map. In: Advances in cryptology-EUROCRYPT'91. Berlin: Springer; 1991. p. 127–40.
[8] Kotulski Z, Szczepanski J. Discrete chaotic cryptography. Ann Phys 1997;6(5):381–94.
[9] Kotulski Z, Szczepanski J, G_orski K, Paszkiewicz A, Zugaj A. Application of discrete chaotic dynamical systems in cryptography—DCC method. Int J Bifurcat Chaos 1999;9:1121–35.
[10] Wong WK, Lee LP, Wong KW. A modified chaotic cryptographic method. Comput Phys Commun 2000;138:234–6.
[11] Wong KW. A fast chaotic cryptography scheme with dynamic look-up table. Phys Lett A 2002;298:238–42.
[12] Wong KW, Ho SW, Yung CK. A chaotic cryptography scheme for generating short ciphertext. Phys Lett A 2003;310:67–73.
[13] Pareek NK, Patidar V, Sud KK. Discrete chaotic cryptography using external key. Phys Lett A 2003;309:75–82.
[14] N.K. Pareek a,b, Vinod Patidar a, K.K. Sud Image encryption using chaotic logisyic map phys Lett 2006:

