A Fast Encryption Scheme Based on Chaotic Maps

Su Su Maung, and Myitnt Myint Sein

Abstract— *In this paper, a fast encryption scheme based on chaotic maps is proposed. Firstly the dynamical 8×8 S-box is produced by using logistic map and 2D standard map. Secondly a sequence of pseudo-random bytes is generated by using 2D chaotic cat map to index the entries of the S-box. The output bytes from the S-box are XOR-ed with the plaintext to produce the ciphertext. The results of simulations show that this encryption scheme is secure and fast enough to be used in real-time image encryption applications.*

Keywords— **Chaos, Image Encryption.**

1. INTRODUCTION

In recent years, with the rapid development of the Internet and the multimedia technology, the security of digital information including image, audio, and other multimedia has attracted more and more intention. Cryptography has been used to send secure message over unsecured channel. For secure communication, cryptographically secure pseudo-random bits which are used as a key stream for a stream cipher are needed. The idea of using chaos for data encryption is certainly not new and can be traced to the classical Shannon's paper [3]. Secure communication method based on chaotic maps has been utilized [4-9]. One or more one dimensional maps are used as pseudo-random number generators producing a key stream which is then XOR-ed with the plaintext to produce the ciphertext. According to its own properties of sensitive dependence on initial condition and system parameter of the chaotic system, it is easy and convenient to obtain cryptographically secure pseudo-random bits with changing the initial condition or system parameter slightly.

In this paper, a method using dynamical 8×8 S-box based on chaotic maps is proposed. The substitution boxes (S-boxes) have been widely used in almost all traditional cryptographic system, such as DES, AES. RC4 which is a variable-key-size stream cipher also uses a 8×8 S-box [2]. The entries are a permutation of the numbers 0 through 255, and the permutation is a function of the variable-length key. To obtain dynamical 8×8 S-box, using chaotic maps is the best approach [1]. A different initial value and control parameter will result in a different S-box. For more randomness, the values of S-box are randomly chosen by another chaotic map.

The paper is organized as follows. In Section 2 the descriptions of chaotic maps are introduced. Section 3 designs the dynamical 8×8 S-box and Section 4 describes a new image encryption scheme using that S-box while security analysis is made in Section 5. Finally, conclusion is drawn in Section 6.

2. DESCRIPTION OF CHAOTIC MAPS

Chaos is a dynamical system that is extremely sensitive to its initial conditions. It is a deterministic nonlinear system that has random-like behaviors. Chaos theory has become a new branch of scientific studies today. Discrete chaotic dynamic systems (i.e., maps) are used in cryptography. There are many chaotic systems such as logistic, lorenz, chen, and chua system etc. In this paper, we use logistic map, cat map, and standard map.

2.1 Logistic Map

Logistic map is one of the simplest form of one dimensional chaotic maps and mathematically its equation can be written as:

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

Where x_n is a real value in (0,1), and μ is control parameter satisfying $0 \leq \mu \leq 4$. The logistic map is chaotic on the condition $0.35699 \leq \mu \leq 4$.

2.2 Cat Map

The cat map is two dimensional invertible chaotic map introduced by Arnold and Avez. The mathematical formula is:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod 1 \tag{2}$$
$$= \left(x_n + y_n \bmod 1, x_n + 2y_n \bmod 1 \right)$$

where x (mod 1) means the fractional parts of a real number x by subtracting or adding an appropriate integer. The map is known to be chaotic. The unit square is first stretched by the linear transform and then folded by the modulo operation.

Su Su Maung was with Mandalay Technological University, Mandalay, Myanmar. She is now with the department of Information Technology, e-mail: susuela@gmail.com)

Myint Myint Sein was with University of Computer Studies, Yangon, Myanmar. email chuchu0228@gmail.com)

2.3 Standard Map

The standard map is described with the following formulas:

$$a_{i+1} = (a_i + b_i) \bmod 2\pi,$$

$$b_{i+1} = (b_i + k\sin(a_i + b_i)) \bmod 2\pi \qquad (3)$$

where k is control parameter satisfying $k>0$, and a_n and b_n are real values in $[0,2\pi)$ for all n. The standard map is discretized from $[0,2\pi) \times [0,2\pi)$ to $N \times N$ by substituting $x=aN/2\pi$, $y=bN/2\pi$, $K=kN/2\pi$. After discretizarion, the map becomes

$$x_{i+1} = (x_i + y_i) \bmod N,$$

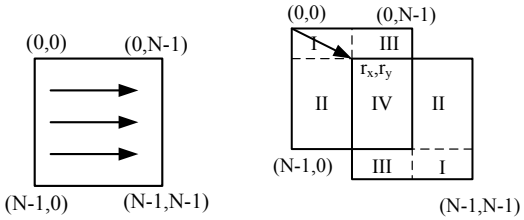
$$y_{i+1} = (y_i + K\sin\frac{x_{i+1}N}{2\pi}) \bmod N \qquad (4)$$

where K is a positive integer.

The pixel values at the origin of the standard map, the cap map and the baker map remains unchanged after any number of iterations. That is if $(x_0,y_0)=(0,0)$, then $(x_0^n, y_0^n)=(0,0)$ after n times of iterations. To avoid this, the standard map is changed from the normal scan order into a random one. Generate random couple (r_x,r_y), where r_x and r_y are in $(0,N\text{-}1)$. Then the whole image shifts in horizontal and vertical directions by r_x and r_y, respectively. That is, left top pixel shifts from (0,0) to (r_x,r_y). The three outside parts (I,II, and III) are returned to the corresponding parts as shown in Fig.1 and then the modified standard map becomes

$$x_{i+1} = (x_i + r_x + y_i + r_y) \bmod N,$$

$$y_{i+1} = (y_i + r_y + K\sin\frac{x_{i+1}N}{2\pi}) \bmod N \qquad (5)$$

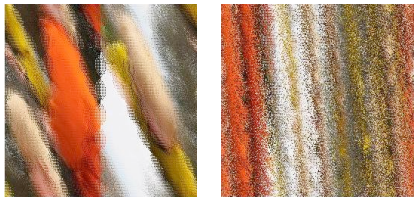


(a) (b)

Fig.1. Scan Order: (a) Normal Scan Mode, (b) Random Scan Mode

The results of applying the modified standard map to the test image after one, two and nine iterations are shown in Fig.2.

(a) (b)



(c) (d)

Fig.2. The Encrypted Images using Standard Map: (a) Twin, (b) After One Iteration, (b) Two Iterations and (c) Nine Iterations

3. DESIGNING DYNAMICAL S-BOX BASED ON CHAOTIC MAPS

Firstly, choose two numbers: one is an initial value x_0 which is a float number in (0,1), another is a control parameter μ where $0.35699 \le \mu \le 4$. Then use these values to compute the logistic map. The values obtained from the logistic map are digitized by a threshold function T and placed in a byte array. The function T is defined as follows:

$$T(x) = \begin{cases} 00\ldots00 & 0 \le x < \frac{1}{2^k} \\ 00\ldots01 & \frac{1}{2^k} \le x < \frac{2}{2^k} \\ \ldots\ldots\ldots\ldots\ldots\ldots & \\ 11\ldots10 & \frac{2^k-2}{2^k} \le x < \frac{2^k-1}{2^k} \\ 11\ldots11 & \frac{2^k-1}{2^k} \le x < 1 \end{cases} \qquad (6)$$

Generally, we suppose $1 \le k \le 10$. In our scheme, we use k=8. In this way, an integer table on the range of $0\text{-}2^n$ can be obtained. Secondly, a key-dependent permuting is used to shuffle the table nonlinearly by applying the same transformation of the standard map several times. To take advantage of the diffusion, the standard map is first discretized to a finite square lattice of points and then changed from the normal scan order into a random one. After applying the modified standard map to the integer table for further permutation, the required dynamical 8×8 S-box is obtained.

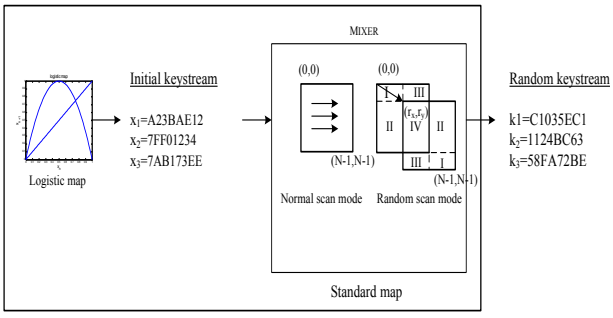


Fig. 3. S-box Generation

4. ENCRYPTION USING DYNAMICALS-BOX

Encryption is byte by byte operation operating on each byte. The entry of S-box is randomly indexed by pseudo-random bytes generated from two dimensional cat map.

Table 1. An example 8×8 S-box

763	4	17	231	244	25	195	5	95	6	94	176	255	183	45	67
47	189	76	197	127	75	221	243	20	208	1	32	211	27	189	23
255	204	185	87	253	120	119	215	247	10	74	190	44	4	5	253
91	244	115	15	54	161	254	183	255	26	218	246	222	249	99	86
25	67	249	34	31	147	189	127	147	211	247	17	208	227	174	235
151	232	226	88	12	95	6	1	198	214	196	0	239	193	253	178
242	255	252	252	63	176	241	213	84	12	126	53	16	235	179	3
183	5	151	132	64	123	127	14	237	237	92	170	254	83	200	8
34	103	119	248	0	155	151	37	239	66	24	148	1	5	243	46
243	75	18	80	155	231	164	67	148	74	56	47	56	240	166	153
13	196	199	234	156	72	230	11	26	196	107	235	219	89	214	46
254	207	38	1	20	80	139	249	109	181	8	252	20	36	46	90
155	220	187	0	50	254	158	250	52	249	143	247	207	118	26	136
245	22	88	210	139	19	34	4	218	212	4	40	3	125	4	140
176	141	0	194	142	42	24	1	255	228	255	62	136	66	253	98

According to the property of high sensitive dependence on the initial condition and system parameter of the chaotic map, a different initial value and control parameter will result in a different value. These values could not be easily predicted by an adversary without knowing the initial condition. In this way, we get cryptographically secure pseudo-random bits.

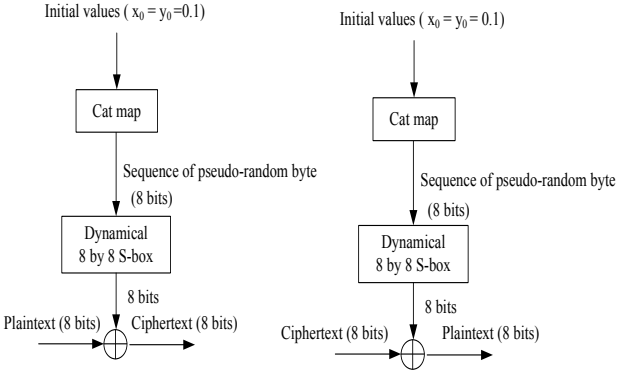
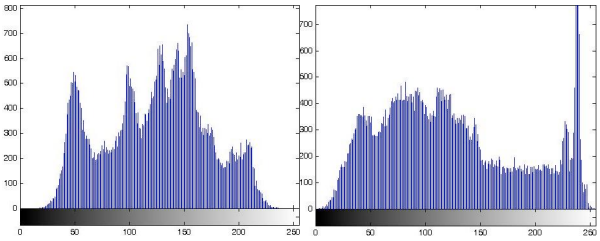


Fig.4. Encryption Scheme

The resultant 8 bits value of S-box is simply XOR-ed with the plaintext to produce the ciphertext and XOR-ed with the ciphertext to produce the plaintext. Fig. 4 shows the encryption scheme and Fig.5-8 show the plane images, the encrypted images, and the histograms of the plane images and the encrypted images. From the Fig., one can see that the encrypted images are hardly recognizable.

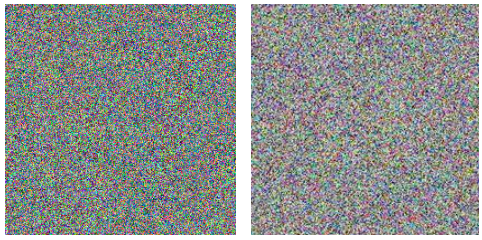
(a) (b)

Fig.5. Plane Images: (a) Lena, (b) Twin



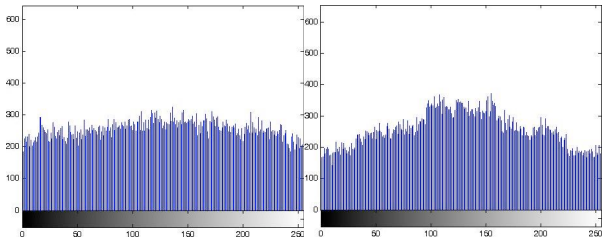
(a) (b)

Fig.6. Histograms of Plane Images: (a) Lena, (b) Twin



(a) (b)

Fig.7. Encrypted Images: (a) Lena, (b) Twin



(a) (b)

Fig.8. Histograms of Encrypted Images: (a) Lena, (e) Twin

5. SECURITY ANALYSIS AND TEST RESULTS

Statistical analysis has be performed on the proposed encryption scheme. It is showed that the new encryption scheme has very good confusion and diffusion properties. This is showed by a test on the histogram of the encrypted image and on the correlations of the adjacent pixels in the encrypted image.

The histogram of the encrypted image shown in Fig.8 is uniform and significantly different from the original one.

To test the correlations of two horizontally adjacent pixels, two vertically adjacent pixels, and two diagonally adjacent pixels, we can use the following two formulas:

$$\mathrm{cov}(x, y) = E(x - E(x))(y - E(y)) \quad (7)$$

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (8)$$

Where x and y are gray values of the adjacent pixels. In sample computation, the following discrete formulas are used:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \quad (9)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2 \quad (10)$$

$$\mathrm{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)) \quad (11)$$

Randomly select 1000 pairs of the adjacent pixels form the plain image and the encrypted image to calculate the correlation coefficients. The pixel distribution of the horizontal correlations of the plain image and the encrypted image is shown in Fig.9. Similarly, the correlation coefficients for diagonal and vertical are shown in Table 2.

Table 2. The correlation coefficients of the adjacent pixels

Position	Plain Image	Ciphered Image
Horizontal	0.9792	0.0308
Vertical	0.9839	0.0230
Diagonal	0.9547	0.0050

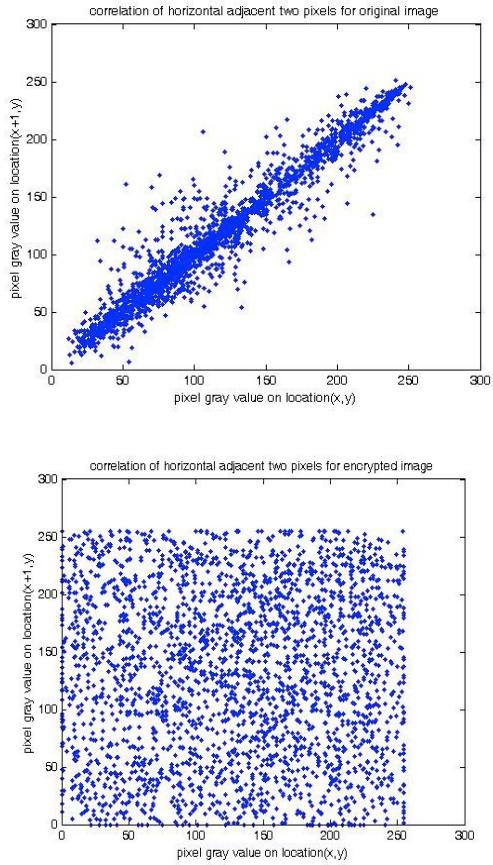
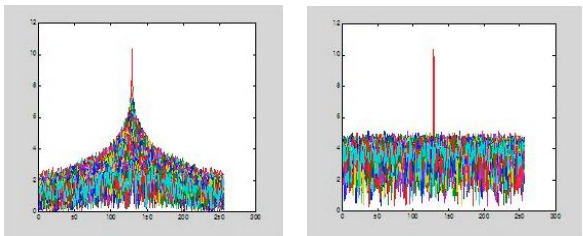


Fig.9. The Horizontal Correlations of the Lena Plain Image and the encrypted image

Two-dimensional discrete Fourier transform and shift zero-frequency component of discrete Fourier transform to center of spectrum by plotting 2 D diagram (see Fig. 10) represents average distribution of spectrum energy. The result indicates the nice diffusion characteristics.



(a) (b)

Fig.10. The 2D Spectrum: (a) the Plane Image, (b) the Encrypted Image

The correlation coefficient between source image and cipher image is 0.00041818. The value is nearly equal to zero and it expresses that source image and cipher image is almost independent. The correlation coefficient among different cipher images obtained by different user keys is 0.00374. The value closes zero, i.e., different cipher images are independent.

Using PC which is Pentium IV 2.80GHz CPU with 704MB of RAM and the Lena color image, the encryption speed is as shown in Fig. 11. Compared with traditional ciphers, the proposed chaos-based cryptosystem has high encryption speed. This advantage

makes it suitable for large-volume data encryption such as image. In addition, the encryption process and decryption process are symmetric, and easy to be realized, which makes it suitable for multimedia encryption. The graph shown in Fig.11 shows the relationship between the encryption speed and the plaintext size. From the Fig., it can be seen that the increase of the plaintext size, the time difference becomes larger and larger, that is, the encryption speed increases with the plaintext size. Therefore, for large-volume data, the chaotic cryptosystem proposed here is better overall.

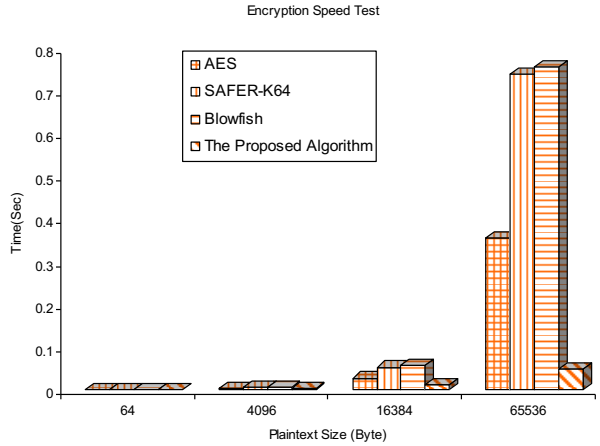


Fig.11. Encryption Speed Test

6. CONCLUSION

In this paper, new encryption scheme using dynamical S-box and chaotic maps has been proposed. Security analysis and other tests of this scheme are performed. Comparing with existing traditional ciphers, the new scheme has higher security and faster enciphering and deciphering speeds that is suitable for multimedia applications. So the proposed scheme is very suitable for the real-time digital image encryption.

REFERENCES

[1] Tang, G., Lieu, X. and Chen, Y. 2004. A novel method for designing S-boxes based on chaotic maps. In *Chaos, Solitons and Fractals*. 23(4), 413-419.

[2] Schneier, B. 1994. Applied Cryptography, Protocols, Algorithms, and Source Code in C. John Wiley & Sons.

[3] Shanoon, C. E. 1949. Communication theory of secret systems. In *J. of Bell Syst. Tech*. 28(4).

[4] Tang, G. and Liao, X. A method for designing dynamical S-boxes based on discretized chaotic map. In *Chaos, Solitons and Fractals*. 23(7), 1901-1909.

[5] Chen, G., Mao, Y. and Charles K. Chui. 2003. A symmetric image encryption scheme based on 3D chaotic cat maps. In *Chaos, Solitons and Fractals*. 23(12), 749-761.

[6] Jakimoski, G., and Kocarev, L. 2001. Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps. In *IEEE Trans. Circuit&Syst. I*. 48(2), 163-169.

[7] Masuda, N. and Aihara, K. 2002. Cryptosystems with Discretized Chaotic Maps. In *IEEE Trans. Circuit&Syst. I*. 49(1), 28-40.

[8] Kocarev, L. and Jakimoski, G. 2001. Logistic map as a block encryption algorithm. In *Physic Letters*. A 289(9), 199-206.

[9] Shiguo, L., Jinsheng, S. and Zhiquan, W. 2004. A block cipher based on a suitable use of the chaotic standard map. In *Chaos, Solitons and Fractals*. 26(11), 117-129.