Multimedia Encryption using Tools in System Engineering

Su Su Maung[1], Kitdakorn Klomkarn[1], Noriyuki Komine[2], and Pitikhate Sooraksa[1]
[1]Department of Information Engineering
Faculty of Engineering, King Mongkut Institute of Technology Ladkrabang
Chalongkrung Rd., Bangkok, Thailand 10520
s7061143@kmitl.ac.th, kkkitdak@kmitl.ac.th, kspitikh@kmitl.ac.th
[2]Department of Applied Computer Engineering
School of Information and Electronics, Tokai University
1117 Kitakaname, Hiratsuka-Shi, Kanagawa-ken, Japan
komine@keyaki.cc.u-tokai.ac.jp

Abstract. *This paper proposes an image encryption scheme based on chaotic maps. In this method, the dynamical S-box obtained by iterating chaotic maps is used. A sequence of pseudo-random bytes generated from two dimensional cat map is used to index the entry of the S-box. The output 8 bits* (*0-255*) *of the S-box are XOR-ed with the plaintext to produce the ciphertext and XOR-ed with the ciphertext to produce the plaintext. Standard statistical tests of this scheme are performed.*
Keywords: encryption, multimedia, chaos, system engineering

1 Introduction

In recent years, cryptography has been used to send secure message over an 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. 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.
This paper is organized as follows. In Section 2, the descriptions of chaotic maps are introduced. The design of dynamical 8×8 S-box and the encryption scheme is described in Section 3 and 4, respectively while statistical tests and analysis are made in Section 5. Finally, conclusion is drawn in Section 6.

2 Descriptions of chaotic maps

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

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

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.

The baker map: The baker map**,** B, is described with the following formulas:

$$B(x,y) = (2x, y/2) \qquad 0 \le x \le 1/2 \qquad (2)$$
$$B(x,y) = (2x-1, y/2 + 1/2) \qquad 1/2 \le x \le 1$$

The map acts on the unit square. The left vertical column [0, 1/2) × [0, 1**)** is stretched horizontally and contracted vertically into the rectangle [0, 1) × [0, 1/2), and the right vertical column [1/2, 1) × [0,1**)** is similarly mapped onto [0, 1) × [1/2, 1). The baker map is a chaotic bijection of the unit square $I \times I$ onto itself. The map can be generalized**.** Instead of dividing the square into two rectangles of the same size, the square is divided into k vertical rectangles $[F_{i-1}, F_i) \times [0, 1)$, $i = 1, ..., k$, $F_i = p_1 + ... + p_i$, $F_0 = 0$ such that $p_1 + \ldots + p_k = 1$. The lower right corner of the i-th rectangle is located at F_i. The generalized baker map stretches each rectangle horizontally by the factor of $1/p_i$. At the same time, the rectangle is contracted vertically by the factor of p_i. Finally, all rectangles are stacked on top of each other. Formally,

$$B(x,y) = (1/p_i(x-F_i), p_i y + F_i) \qquad (3)$$

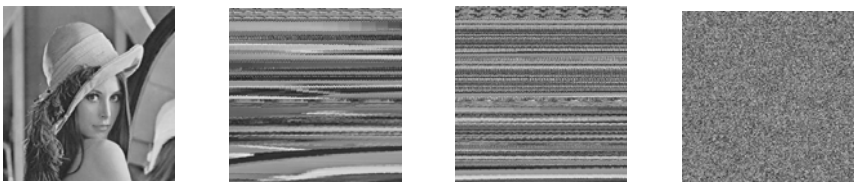
for

$$(x, y) \in [F_i, F_i + p_i) \times [0,1),$$

Since an image is defined on a lattice of finitely many points (pixels), a correspondingly discretized form of the generalized baker map needs to be derived. In particular, the discretized map is required to assign a pixel to another pixel in a bijective manner. Since the discretized map is desired to inherit the properties of the continuous basic map, the discretized map should become increasingly close to the basic map as the number of pixels tends to infinity. We define a sequence of k integers, $n_1, \ldots, n_k$ such that each integer n**,** divides N**,** and $n_1 + ... + n_k = N$. Denoting $N_i = n_1 + ... + n_i$, $N_0 = 0$, the pixel (r, s)**,** with $N_i \le r < N_i + n_i$ and $0 \le s < N$ is mapped to

$$B(n_1,\ldots,n_k)(r,s) = \left(\frac{N}{n_i}(r - N_i) + s \bmod \frac{N}{n_i}, \frac{n_i}{N}(s - s \bmod \frac{N}{n_i}) + N_i \right) \qquad (4)$$

The results of applying the discretized baker map to the test image after 1, 2, and 9 iterations are shown in Fig.1.



(a) (b) (c) (d)

Fig.1: Original image (a), after applying the baker map one times (b), two times (c), nine times (d)

The logistic map: One of the simplest forms of one dimensional chaotic maps and mathematically its equation can be written as:

$$x_{n+1} = \mu x_n (1 - x_n) \tag{5}$$

3 Dynamical S-box based on chaotic maps

First, choose two numbers: one is an initial value *x* which is a float number in (0,1), another is a control parameter μ where $0 \le \mu \le 4$. Then use these values to compute the logistic map. The value obtained from the logistic map is digitized by multiplying with proper scale and then the 8 least significant bits are extracted to easily place them in a byte array. In this way, an integer table on the range of 0-2^n can be obtained. Secondly, a key-dependent permuting is used to shuffle the table nonlinearly by applying the same transformation of the baker map several times. To take advantage of the diffusion, the baker map is first generalized by introducing parameters and then discretized to a finite square lattice of points. After applying the discretized baker map to the integer table for further permutation, the required dynamical 8×8 S-box is obtained.

Table 1: An example 8×8 S-box

92	34	10	145	74	248	167	72	235	47	81	139	210	245	248	69
250	149	37	7	65	7	30	33	19	152	149	254	194	231	231	34
74	154	126	253	149	253	106	158	210	213	248	61	248	253	87	244
70	138	117	160	185	7	99	58	202	88	45	9	202	9	230	188
149	27	0	202	28	210	1	101	8	253	5	255	99	206	20	198
41	139	28	196	90	92	101	1	243	235	244	224	86	115	42	195
47	239	101	244	230	255	244	119	100	0	41	253	38	96	138	2
167	2	91	94	29	240	235	2	233	17	75	184	230	10	212	132
243	185	74	237	117	203	95	250	45	165	19	125	89	233	47	180
28	209	26	119	167	152	253	186	28	246	9	73	139	36	251	216
253	2	149	168	221	9	7	61	255	36	27	20	231	124	1	216
244	38	100	255	248	129	238	12	253	255	253	202	228	0	63	26
42	82	28	211	243	16	66	154	250	35	240	146	9	172	178	244
133	222	55	168	144	255	44	92	28	1	57	229	73	4	177	236
128	115	229	250	154	0	5	44	248	3	189	20	240	14	4	145
92	34	10	145	74	248	167	72	235	47	81	139	210	245	248	69

4 Encryption scheme using dynamical S-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. 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. 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. 3 (b) shows the enciphered image using this encryption scheme and the image is hardly recognizable.

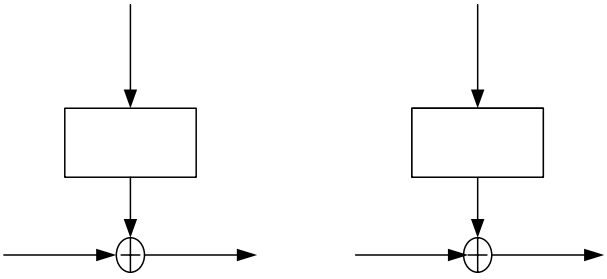


Fig. 2: Encryption scheme

(a) (b)

Fig. 3: Plain image (a), cipher image (b)

5 Standard statistical tests and analysis

In order to test the method, we have performed certain statistical tests. The tests we use in this paper are the standard criteria specified in FIPS PUB 140-2 tests [4], and consist of four tests, totaling a number of 16 items. In these statistical tests of random numbers one considers a single bit stream of 20,000 consecutive bits output from the generator. The bits are then subjected to each of the tests below.

Any failure to pass the specified criteria means that the sequence must be rejected. The four tests are described below.

Monobit Test: The number of ones in the 20,000 bit stream, here we denote X, is counted and the test is passed if $9{,}725 < X < 10{,}275$.

Poker Test: The 20,000 bit stream is divided into 5,000 contiguous 4-bit segments. Count the number of occurrences of each of the 16 possible 4-bit values and denote the number of occurrences as $f(i)$ where $0 \le i \le 15$. Evaluate the following:

$$X = \frac{16}{5000}\left(\sum_{i=0}^{15}[f(i)]^2\right) - 5000 \qquad (6)$$

The test is passed if $2.16 < X < 46.17$.

Table 2: The required interval for runs test

Length of Run	Required Interval
1	2315-2685
2	1114-1386
3	527-723
4	240-384
5	103-209
6+	103-209

Runs Test: A run is defined as the maximal sequence of consecutive bits of either all ones or all zeros. The runs (for both consecutive zeros and consecutive ones) of all lengths (≥ 1) in the sample stream are counted. The test is passed if the number of runs is within the corresponding interval specified in Table 2. The runs of greater than 6 are considered to be of length 6.

Long Run Test: A long run test is passed if there are no long runs of length 26 or more (of either zeros or ones). To test the quality of the random bits generated, we will have to test a total of sixteen items (one for the monobit test, one for the poker test, twelve for the runs test, and two for the long run test).

In this paper, we employ the logistic map to generate the chaotic integer table, which initial value x_0=0.1 is chosen and the value of μ in Eq.(5) is selected as 3.9996. By applying the baker map with a sequence of 6 divisors of 16 (2 2 4 4 2 2) nine times, we can obtain the dynamical 8×8 S-box. We generate a sequence of pseudo-random numbers by using the cat map with parameters x_0=0.1 and y_0=0.1. The generated random bytes are used to index the entries of S-box. For the 16 total number of testing items, the test result is about 75%.

6 Conclusion

In this paper, new encryption scheme using dynamical S-box and chaotic maps has been proposed. Standard statistical tests of this scheme are performed. We show

that this new scheme can generate a high percentage of usable pseudo-random numbers, while maintaining a large enough key space.

Acknowledgment

This paper is supported by JICA project for AUN-SeedNet under CR Program 2005, and is supported in part by The Thailand Research Funds under grant RSA4680007.

References

1. G. Tang, X. Lieu and Y. Chen, "A novel method for designing S-boxes based on chaotic maps," *Chaos, Solitons and Fractals* 23, pp. 413-419, April 2004.
2. B. Schneier, "Applied Cryptography, Protocols, Algorithms, and Source Code in C," John Wiley & Sons, 1994.
3. C. E. Shanoon, "Communication theory of secret systems," Bell Syst. Tech. J., vol. 28, no. 4, pp. 656-715, 1949.
4. National Institute of Standard and Technology and Communication Security Establishment, *Derived Test Requirement* (*DTR*) *for FIPS PUB 140-2, Security Requirements for Cryptographic Modules*.
5. G. Tang and X. Liao, "A method for designing dynamical S-boxes based on discretized chaotic map," *Chaos, Solitons and Fractals* 23, pp. 1901-1909, July 2004.
6. G. Chen, Y. Mao and Charles K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons and Fractals* 23, pp. 749-761, Dec. 2003.
7. G. Jakimoski and L. Kocarev, "Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps," *IEEE Trans. Circuit&Syst. I*, vol. 48, pp. 163-169, Feb. 2001.
8. N. Masuda and K. Aihara, "Cryptosystems With Discretized Chaotic Maps," *IEEE Trans. Circuit&Syst. I*, vol. 49, pp. 28-40,Jan. 2002.
9. L. Kocarev and G. Jakimoski, "Logistic map as a block encryption algorithm," *Physic Letters* A 289, pp. 199-206, Sep. 2001.