Military Technical College
Kobry El-kobbah,
Cairo, Egypt

5th International Conference
on Electrical Engineering
ICEENG 2006

Cryptosystem Based On 2-D Chaotic Maps

Alaa Fahmy[1]

ABSTRACT

Chaos is one of the recent sciences that have great applications in the field of cryptography. Baker map is one of the most popular two dimension (2-D) chaotic map that been used to construct a cryptosystem. Moreover, a proposed hybrid cryptosystem has been introduced with examples of two test images. This proposed cryptosystem provides large key space, produces the same results of other chaotic maps with less number of iterations, reduces the encryption time, and produces complex permutation mechanism.

KEYWORDS: Chaos, and cryptography

1. INTRODUCTION

Chaos theory is one of the most recent developments in mathematics, having effectively been founded by the meteorologist Edward Lorenz in the 1960 [1, 2, 3]. A chaotic system can be defined as the system that does not repeat its past behavior. Consider a system started twice, but from slightly different initial conditions. For non-chaotic systems this leads to an error in prediction that grows linearly with time. For chaotic systems, this error grows exponentially with time. Therefore, the state of the system is essentially unknown after a very short time. This phenomenon is known as sensitivity to initial conditions [4]. The discrete maps, which generating chaotic solutions have the sensitivity of parameters feature [5].

This paper describes the steps of encryption based on invertible two-dimensional chaotic maps such as: Baker map, and a proposed Hybrid map. Section 2 presents chaos based encryption, meanwhile section 3 deals with how to construct cipher by using Baker map. Section 4 introduces the proposed hybrid map. Finally section 5 concludes the paper.

2. Chaos Based Encryption

The idea of using chaos for data encryption is certainly not new and can be traced to the classical Shannon's paper [6]. The word chaos doesn't appear in Shannon's paper. Shannon proposes mixing, and transformations. It has been mentioned that stretching and folding mechanism of chaos often formed by repeated

[1] Assoc. Prof. Dept. of Electrical Engineering, Military Technical College, Cairo, Egypt.

products of two simple non-commuting operations. In 1991 Toshiki [5] suggests a cryptosystem in which, the inverse of tent map was applied "N" times to an initial condition, which represents a plaintext. The decryption is achieved by applying the tent map "N" times.

The proposed cryptosystem is a symmetric block encryption technique based on two-dimensional chaotic maps, which are used to create complex, and key-dependent permutation. The process of developing a chaos-based cipher can be summarized as presented in [7]. The process proceeds as follows: choosing a chaotic map to be generalized by introducing parameters into this map. Then, the map is modified so that its domain and range are both have the same square lattices of points. The map is then extended to three dimensions so that the values of the pixels (the colors levels) can be changed. Finally, a diffusion step is introduced by composing the generalized discretized map with a simple diffusion mechanism.

3. Cipher Construction By Using Baker Map

Three two-dimension chaotic maps such as: Baker, Cat, and Standard can be used [8]. Baker map is choosing, which can be generalized, descretized, and applied to two RGB test images. Each of 256 x 256 pixels with color-depth 24 bits (true color) and have a highly non-uniformly histogram.

3.1 Baker map.

The Baker map, B, is described with the following formulas [7]:

$$B(x, y) = (2x, y/2) \quad \text{when } 0 \le x < 1/2, \tag{1}$$

$$B(x, y) = (2x-1, y/2+1/2) \quad \text{when } 1/2 \le x \le 1. \tag{2}$$

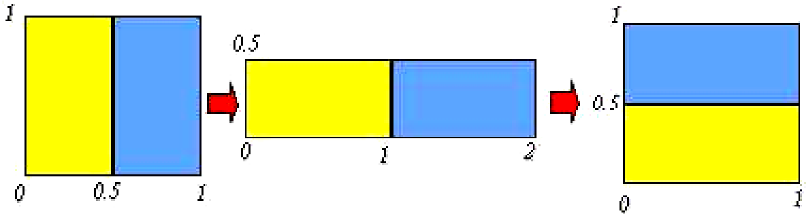


Fig. 1 Baker Map

The map acts on the unit square as depicted in Fig.1. The left vertical column [0,½) × [0, 1) is stretched horizontally and contracted vertically into a rectangle [0, 1) × [0, ½), and the right vertical column [½, 1) × [0, 1) is similarly mapped onto [0, 1) × [½, 1).

Baker Map's Generalized

The map can be generalized in the following way: 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, $F_i=P_1+\ldots+P_i$, $F_0=0$, such that $P_1+\ldots P_k=1$ as shown in Fig.2.

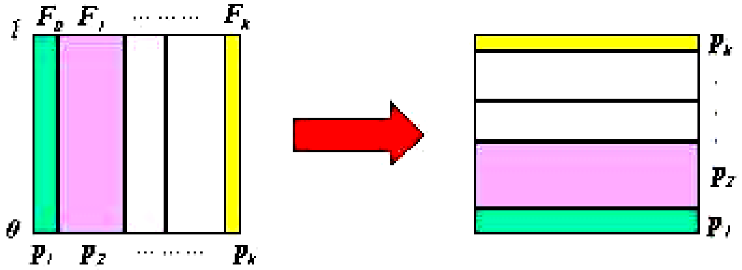


Fig.2 Generalized Baker Map

The lower right corner of the ith rectangle is located at $F_i=P_1+\ldots+P_i$. 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 as in Fig.2. Formally,

$$B(x,y)=\left(\frac{1}{p_i}(x-F_i), p_i y+F_i\right) \text{ For } (x,y)\in[F_i, F_i+p_i)\times[0,1), \qquad (3)$$

It is convenient to denote Baker map and its generalized version as $B_{(1/2,1/2)}$ and $B_{(P1,\ldots,Pk)}$, respectively. The generalized map inherits all-important properties of the Baker map such as sensitivity to initial conditions, and mixing.

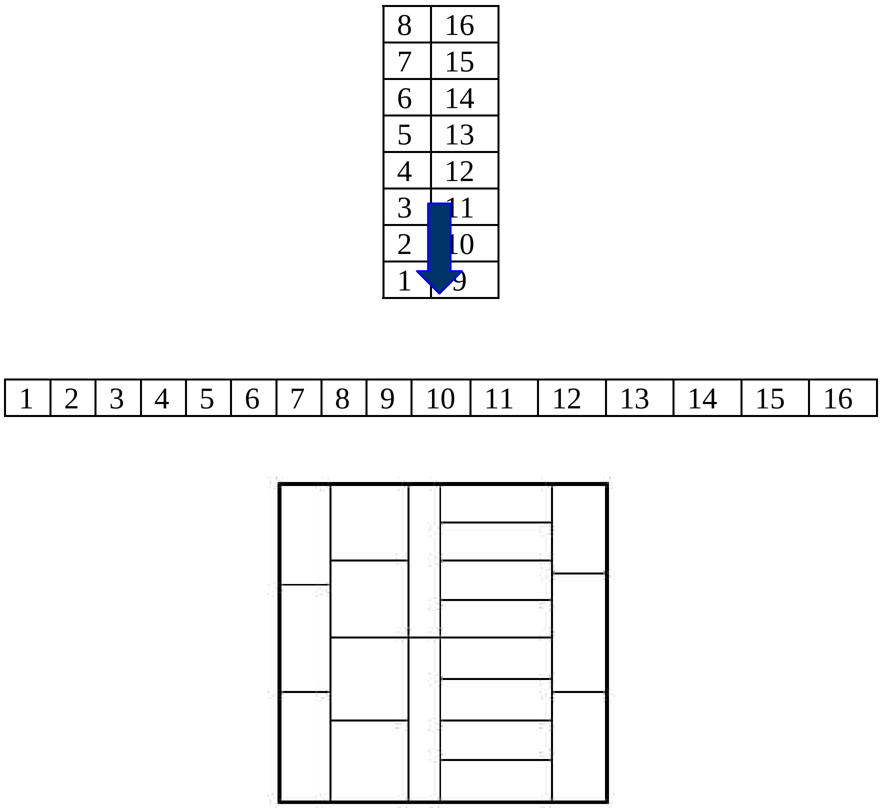
Baker Map's Discretized

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. The discretized generalized Baker map will be denoted by $B_{(n1,\ldots nk)}$, where the sequence of k integers, $n_1,\ldots n_k$ is chosen such that each integer n_i divides N, and $n_1,\ldots n_k=N$. Denoting $N_i=n_1+\ldots+n_i$ the pixel (r, s), with $N_i\leq r<N_i+n_i$ and $0\leq S<N$ is mapped to [7]:

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

This formula is based on the following geometrical considerations. An N × N square is divided into vertical rectangles of height N and width n_i. Following the action of the generalized Baker map, these vertical rectangles should be stretched in the horizontal direction and contracted in the vertical direction to obtain a horizontal $n_i\times$ N rectangle. To achieve this for the discretized map, each vertical rectangle N × n_i is divided into n_i boxes N/ n_i x n_i containing exactly N points (Fig.3). Each of these boxes is mapped to a row of pixels. Since there are n_i boxes, a horizontal rectangle n_i × N is obtained, as required.

Now, how the pixels in each box are mapped to a row of pixels need to be specified. Since the original Baker map is continuous on each box, the only possible discretization is to map the box column by column. An example for N = 16, n_i = 2 is shown below. The rectangle N/ n_i x n_i = 16/2 × 2 = 8 × 2 is mapped to a row of 16 pixels as follows:

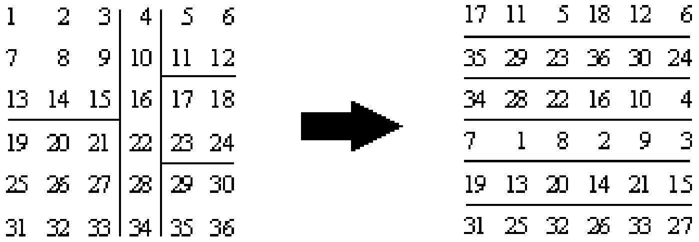


8	16
7	15
6	14
5	13
4	12
3	11
2	10
1	9

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Fig.3 Discretized Baker Map

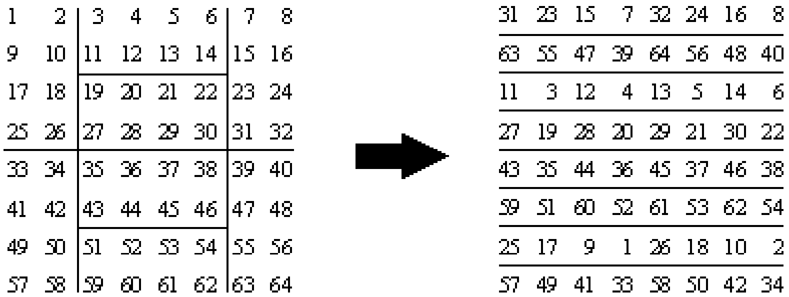
Examples of permutations for a complete 6-pixel image and 8-pixel image are worked out in details as shown in Fig.4, and Fig.5. For the 6-pixel image, a 3-1-2 division is used, while in the 8-pixel case the division is 2-4-2.



1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21	22	23	24
25	26	27	28	29	30
31	32	33	34	35	36

17	11	5	18	12	6
35	29	23	36	30	24
34	28	22	16	10	4
7	1	8	2	9	3
19	13	20	14	21	15
31	25	32	26	33	27

Fig. 4 Permutation Induced By Discretized Baker
Map For 6-Pixel Image (division 3, 1, 2)



1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

31	23	15	7	32	24	16	8
63	55	47	39	64	56	48	40
11	3	12	4	13	5	14	6
27	19	28	20	29	21	30	22
43	35	44	36	45	37	46	38
59	51	60	52	61	53	62	54
25	17	9	1	26	18	10	2
57	49	41	33	58	50	42	34

Fig. 5 Permutation Induced By Discretized Baker
Map For 8-Pixel Image (division 2, 4, 2)

Baker Map's key

The chaotic map key is formed by the parameters of the map, and the number of applications of the map. For Baker map, the key K_B is: $K_B=\{C,n_1,\dots,n_k\}$,where C is the number of iterations of Baker map, $n_1,\dots n_k$ are a sequence of k integers, which are chosen such that each integer n_i divides N, and $n_1+\dots+n_k=N$ for N × N square. The Baker map is applied to an RGB test images of 256 x 256 pixels with color-depth 24 bits-per-pixel. The image was selected such that it has a non-uniform histogram as dedicated in Fig.6.

The cipher key is a sequence of k integers of the following divisors of 256: 1, 2, 4, 8, 16, 32, 64, 128, 256, such that, the sum of the sequence equal 256. The cipher key is generated and consists of the following sequence of 18 divisors of 256:

$$(8\ 4\ 8\ 16\ 1\ 4\ 64\ 4\ 64\ 8\ 16\ 8\ 2\ 4\ 32\ 8\ 4\ 1) \qquad (5)$$

The computer results of applying the generalized discretized Baker map from one to ten iterations produces encrypted images as demonstrated in Fig.7. The fact that spatially localized information in the original image becomes non-local and uncorrelated in the encrypted image. This can be illustrated with the following example. The original image consists of a 22 × 22 color square on a white background of a 256 × 256 pixels (Fig.8-a). A cipher key (eq.5) was used to iterate the discretized generalized Baker map from one to six iterations. The result is shown in Fig.8-b. The color pixels are scattered all over the image in an apparently random manner.

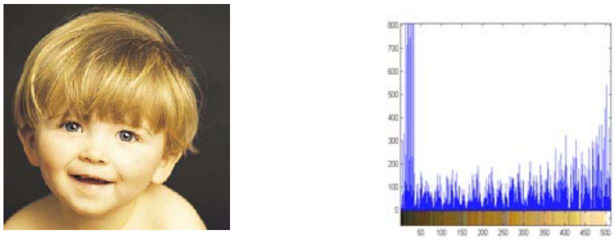


Fig. 6 RGB Test Image 256 x 256 Pixels with Color-Depth 24 Bits & its Histogram

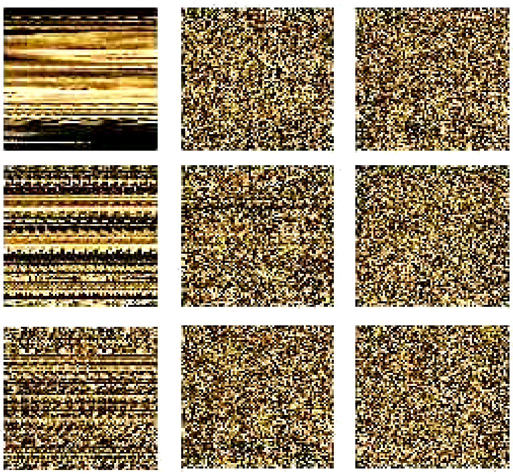
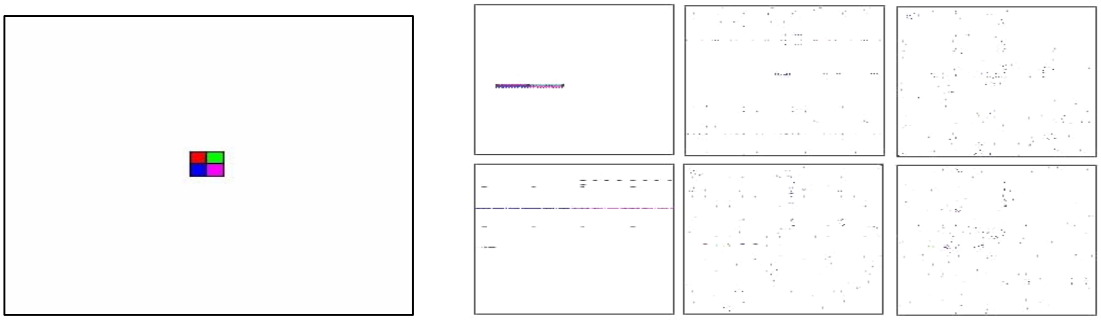


Fig.7 Test Image After Applying Generalized Discretized Baker Map from 1 to 9 Iterations with Ciphering Key (8 4 8 16 1 4 64 4 64 8 16 8 2 4 32 8 4 1)



(a) (b)

Fig.8 (a) An image Consisting of a 22 x 22 Pixels Color Square on a White Background, (b) Encrypted Image After Applying The Generalized Discretized Baker Map From One to Six Iterations

4. Proposed Hybrid Map

A proposed hybrid map was suggested as shown in Fig.9. The main idea of the proposed map is to perform more complex permutation mechanism by using additional three maps. First, linear map (Baker map), second the nonlinear map (Standard map), and finally linear map (Cat map). The proposed hybrid map is applied to the two test images of Fig.6 and Fig.8-a. The enciphered images are shown in Fig.10, and Fig.11. Using the two-dimensional chaotic maps keys parameters, which are: Baker map key: (8 4 8 16 1 4 64 4 64 8 16 8 2 4 32 8 4 1), Standard map key: K = 140, and Cat map key: $A_{(1,1,1,2)}$.

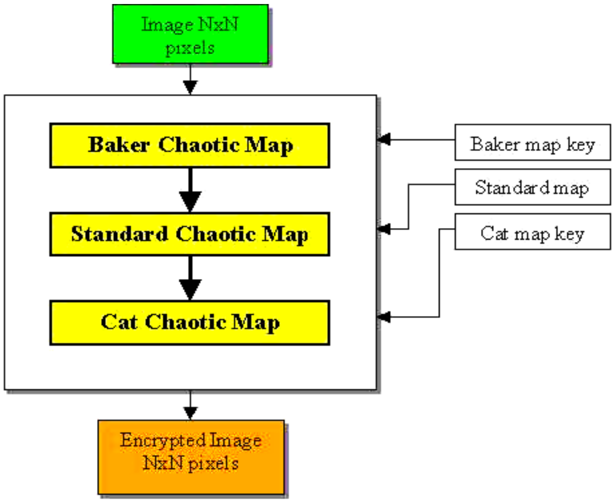


Fig.9 Proposed Hybrid Map

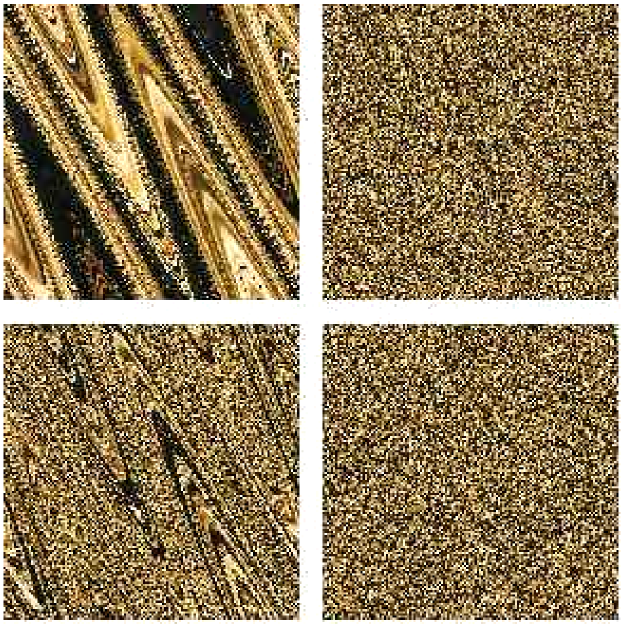


Fig. 10 First Test Image after Applying Proposed Hybrid Map from One to Four Iterations

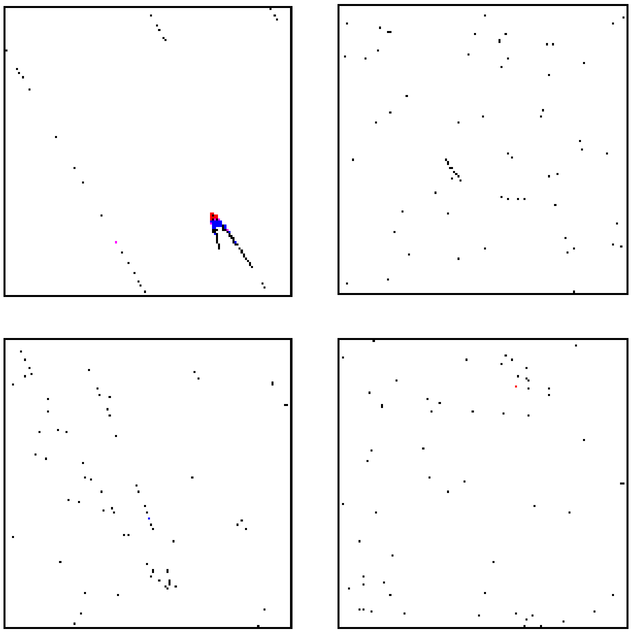


Fig. 11 Second Test Image 1-4 Iterations

It is clear that, the encrypted image by using the proposed hybrid map has the following features compared to a single chaotic map:

- Large key space.
- It produces the same results of other chaotic maps but with less number of iterations, which reduces the encryption time.
- Produces a complex permutation mechanism.

Until now, the encrypted image histogram is similar to the original image histogram (Fig.6), because the encryption is based on complex permutation of the image pixel value and does not change the pixels values.

5. Conclusion

Chaos has been used in the field of cryptography. One of the most popular two-dimension chaotic maps, namely, Baker map has been used to construct a cryptosystem. Moreover, a proposed hybrid cryptosystem, which uses Baker, Cat, and Standard maps have been introduced with an example of two test images. This proposed cryptosystem provides large key space, produces the same results of other chaotic maps with less number of iterations, reduces the encryption time, and produces complex permutation mechanism.

REFERENCES

[1] http://users.ox.ac.uk/~quee0818/chaos/chaos.html.
[2] http://www.duke.edu/~mjd/chaos/chos.html.
[3] http://www.imho.com/grae/chaos/chaos.html.
[4] G. L. Baker and J. P. Gollub, “Chaotic Dynamics: an I introduction”, Cambridge University Press, 1990.
[5] T. Habutsu, Y. Nishio, I. Sasase, and S. Mori, “A Secret Key Cryptosystem by

Iterating a Chaotic Map," Advances in Cryptology - EUROCRYPT' 91, LNCS 547, Springer-Verlag, 1991.

[6] C. Shannon, "Communication Theory of Secrecy Systems." Bell System Technical Journal, 28, pp. 656-715, 1949.

[7] J. Fridrich, "Symmetric Ciphers Based on Two-Dimensional Chaotic maps", International Journal of Bifurcation and Chaos, Vol. 8, No. 6, June 1998.

[8] B. Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C ", John Wily & Sons, Inc., New York, 1996.