International Journal of Information & Computation Technology.
ISSN 0974-2239 Volume 4, Number 11 (2014), pp. 1029-1034
© International Research Publications House
http://www. irphouse.com

# Low Complexity Efficient Image Encryption Technique Based on Chaotic Map

**Lalita Gupta**[1], **Rahul Gupta**[2]
**and Manoj Sharma**[3]

[1]*Electronics & Communication Engineering Department, MANIT Bhopal*
[2] *AISECT University Bhopal*
[3]*Airport Authority of India Bhopal,*

## Abstract

The chaotic cryptography is gaining more attention than others because of its lower mathematical complexity & better Security. It also avoids the data spreading hence reduces the transmission cost & delay. The digital image cryptography which is based on chaotic systems utilizes the discrete non-linear system dynamics generally called chaotic maps. Depending upon the type of system many types of chaotic maps are available. By combining them a large number of cryptographic techniques could be designed. In this paper presents a “Fast Efficient Low Complexity Image Encryption Technique” in the proposed technique; confusion and diffusion applied hence the encryption can be achieved quickly. Also the diffusion template is created by random number generator based on Gaussian distribution. The technique uses Bakers map and capable of providing the key length of 64 bits although it’s length can be extended further.

**Keywords-** cryptography, chaotic Maps, image shuffling, baker’s map, information entropy.

## 1. Introduction

With the proliferation of the Internet and maturation of the digital signal processing technology, applications of digital imaging are prevalent and are still continuously and rapidly increasing today. Yet the main obstacle in the widespread deployment of digital image services has been enforcing security and ensuring authorized access to sensitive data. In real-time communications, because of their low encryption and decryption speeds, they may introduce significant latency. Compared with text encryption, which most existing encryption standards aim at, image encryption (or more generally, multimedia encryption) has its own characteristics and special features with many unique specifications.

## 2. Chaos and Cryptography

Chaos is a phenomenon that occurs in nonlinear definable systems sensitive to initial conditions and has a pseudo-random behavior. Dynamic chaotic systems in case of Liapunov exponential equations meet will remain stable in chaos mode The distribution of a large number of keys is liable to cause horrendous management problems. So, one of the main advantages of chaotic system's realization is facilitated key management approach because this method only needs to protect and secure transmission of secret key (parameters and initial values of chaotic System), which has a little volume and therefore not only a little memory is needed to maintain it but also there is more confidence during its transfer. The unauthorized access to short length keys is significantly less possible than the effective length keys during data transmission through the insecure channel.

## 3. Proposed Algorithm

New image encryption scheme that consists of a pixel shuffler unit generalized 2d baker map and confused with noise image. So far, many researchers suggested using combination of Pixel scrambling and symmetric encryption [2]. Pixel scrambling has two important issues that are useful for image ciphering. It not only rearranges the pixel location (diffusion), but also changes the value of each pixel (confusion). Creating confusion in the image with bit xor with noise image nonlinear (liapunav exponential) function operation to satisfied condition of chaos. Pixel location displacement is appropriate before applying encryption, because unlike the text data has only two neighbors, each pixel in the image is in neighborhood with eight adjacent pixels. For this reason, each pixel has a lot of correlation with its adjacent neighbors. However, it is very important to disturb the high correlation among image pixels to increase the security level of the encrypted images. In order to dissipate the high correlation among pixels, we proposed shuffling operation. Pixel shuffler unit consists of a permutation map that is applied in two different directions: vertical and horizontal, to decrease adjacent pixels correlation.

### *3.1 Chaos of image using Baker map*

- *The two-dimensional Baker map*

The Baker map, B, is described with the following formulas

$B(x, y) = (2x, y/2)$ When $1/2 < x < 1$

$B(x, y) = (2x - 1, y/2 + 1/2)$ When $0 < x < 1/2$

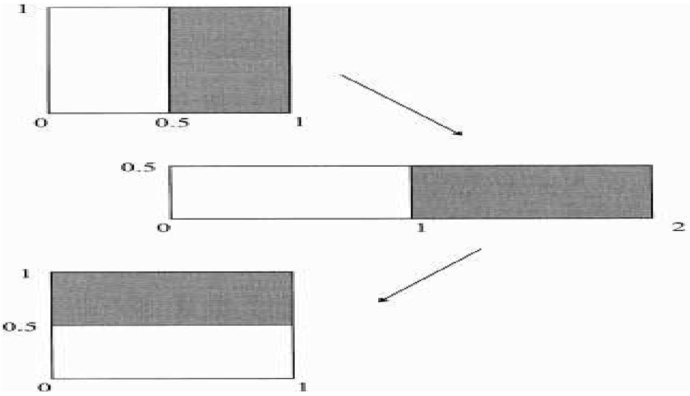

**Figure 1.** Baker map

when 1/2 < x < 1.The map acts on the unit square as depicted in Fig. 1 The left vertical column (0, 1/2) X (0, 1) is stretched horizontally and contracted vertically into the rectangle (0, 1) X (0, 1/2),and the right Vertical column (1/2, 1) X (0, 1) is similarly mapped onto (0, 1) X (1/2, 1). The Baker map is a chaotic bisection of the unit square I X I onto it.

- ***Generalized Baker map***

Instead of Dividing the square into two rectangles of the same size, the square is divided into k vertical rectangles (Fi−1; Fi) × [0; 1], i =1…….. K; Fi =p1+……..+pi; Fo =0 such that p1+……. +pk=1. The lower right corner of the ith rectangle is located at Fi =p1+………+pi. The generalized Baker map stretches each rectangle horizontally by the factor of 1/pi. At the same time, the rectangle is contracted vertically by the factor of pi. Finally, all rectangles are stacked on top of each other. Formally, It is convenient to denote the Baker map and its generalized version as B (1/2; 1/2) and B (pi………….. pk), respectively. The generalized map inherits all important properties of the Baker map such as sensitivity to initial conditions and parameters, mixing, and bijectiveness.

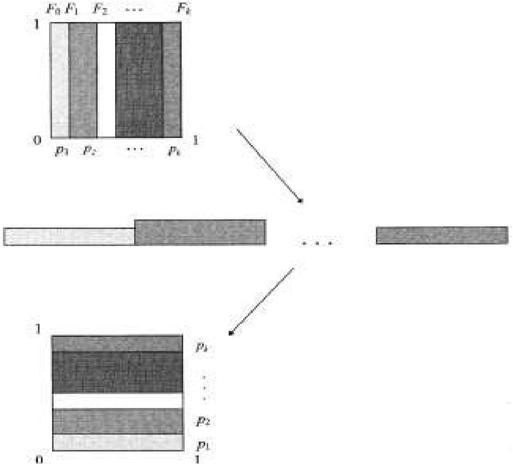
$F_0\,F_1\;\;F_2\;\cdots\;\;F_k$
1
0
$p_1\;\;p_2\;\;\cdots\;\;p_k$
1
. . .
1
$p_k$
$p_2$
$p_1$
0
1

**Figure 2.** *Generalized baker map*

$B(x, y) = (\frac{1}{p_i}(x - f_i), p_i\, y + f_i)$

For $(x, y) \{(f_i, f_i + p_i) \times (0, 1)$

## 4. Chaotic Image Encryption Scheme

The discrete 2D baker map designed is applied here to construct a fast and secure image encryption scheme. In this section of image encryption first to shuffled gray scale image on the basis of 2D generalize baker map for the confusion of image or changing pixel position of image and then diffused with the confused noise image. Non linear distribution (liapunov exponential function) of pixel and then shuffled pixel is bitxor with the diffusion noise image pixel for change the intensity of distribution of pixel.

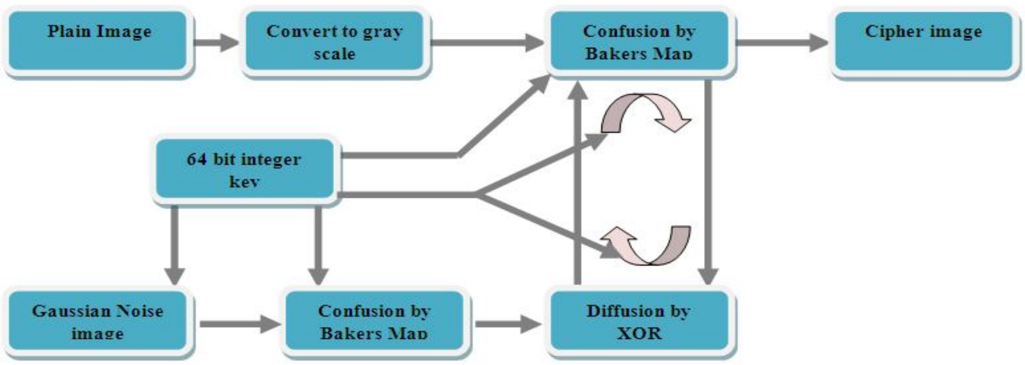

**Figure 3.** Block diagram of image encryption scheme

## 5. Result and Discussion

Assume that an 8-character ciphering key is used. This means that the key consists of 64 bits.

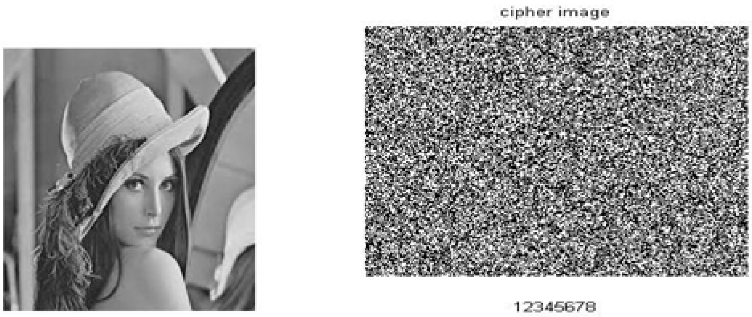

**Figure 4.** *Plain image and cipher image.*

Then, the least significant byte of the key is changed, so that the original key becomes “12345677” which is used to decrypt the cipher image.

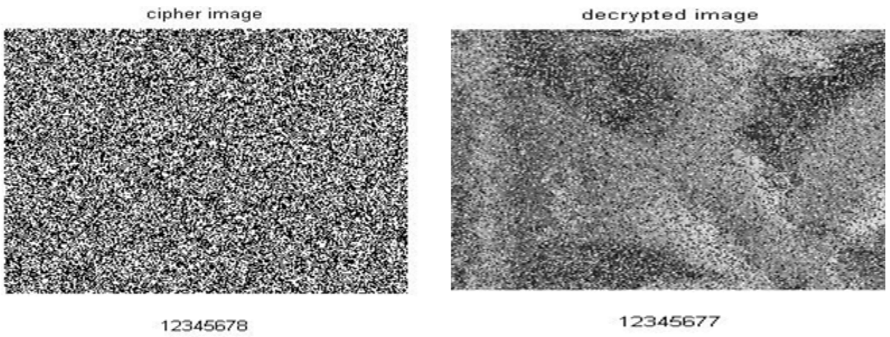

**Figure 5.** *One Bit Key Difference*

Compare difference with the selected encrypted key “12345678” and use decrypted key “12345677” change the LSB position of key. The result is: the image encrypted by the key “12345678" has 99% differences from the image decrypted by the key “12345677".

## 6. Conclusions

In this paper chaos-based cipher schemes for still images have been described. Both security analysis and experiments show that, taking into account the trade-off between attack expense and information value as well as other issues such as operational speed, computational cost, and implementation simplicity, these kind of chaos-based image encryption schemes is very practical. From an engineer’s perspective, chaos-based image encryption technology is very promising for real-time secure image and video communications in military, industrial, and commercial applications.

## References

[1] Yaobin Mao and Guanrong Chen “A Novel Fast Image Encryption Scheme Based on 3d Chaotic Baker Maps” International Journal Of Bifurcation and Chaos, Vol. 14, No. 10 (2004) 3613–3624.

[2] Alireza Jolfaei, Abdolrasoul Mirghadri “An Image Encryption Approach Using Chaos and Stream Cipher” Journal of Theoretical and Applied Information Technology 2010.

[3] Musheer Ahmad and M. Shamsher Alam “A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping” International Journal on Computer Science and Engineering, Vol.2 (1), 2009, 46-50.

[4] Xin Ma, Chong Fu, Wei-min Lei, Shuo Li “A Novel Chaos-based Image Encryption Scheme with an Improved Permutation Process” International Journal of Advancements in Computing Technology Volume 3, Number 5, June 2011.

[5] Zhang, G. J., Liu, Q. ”A Novel Image Encryption Method Based on Total Shuffling scheme” Optics Communications, 284, pp. 2775--2780 (2011).

[6] Bourbakis N, Alexopoulos C (1992) Picture data encryption using scan patterns. Pattern Recognition 25(6):567 – 581

[7] C.E. Shannon, “Communication Theory of Secrecy Systems,” Bell System Technology J, vol.28, 1949, pp .656–715.

[8] M. Henon, “A Two-Dimensional Mapping with a Strange Attractor,” Communication in Mathematical physics, vol. 50, 1976, pp. 69–77.