# Integrated Confusion-Diffusion Mechanisms for Chaos Based Image Encryption

Sai Charan Koduru* and V. Chandrasekaran**
Department of Mathematics & Computer Science,
Sri Sathya Sai University, Prashanthi Nilayam, India
*sreecharan.k@gmail.com **drvchase@yahoo.com.au

## Abstract

*Most block-cipher image encryption schemes based on Chaos theory have independent modules for confusion and diffusion processes. None of the schemes thus far use chaos theory in the diffusion modules - thus not utilizing the capabilities of chaos to the fullest extent. We can do better: we integrate these mechanisms into a single step, thus making the encryption process efficient. This paper presents three novelties: (a) we extend 2D images to 3D by using grayscale image intensities in 8-bit binary form (b) we embed the diffusion mechanism into confusion by applying the 3D Baker map based confusion algorithm. Thus, the diffusion process is accomplished by a permutation of binary bits in the third dimension, eliminating the need for a separate diffusion process and (c) we extend the proposed method to color images by using the 24-bit color information. Color image encryption is usually performed by encrypting each channel independently and then combining these to get the encrypted image. We demonstrate that with this simplistic approach, decrypting even a single channel would reveal reasonable information contained in the image. In our approach, this drawback is eliminated because of the inherent dependence between the data contained in all the channels, thus highlighting the inherent superiority of the proposed algorithm for color image security.*

## 1 Introduction

In this information technology driven society, information security is an integral part of the technology. Every commercial medical information system needs to store large amounts of medical images of patients scans, x-rays etc. in their databases. There are very stringent legal requirements leading to strict security measures for such systems in order to protect the privacy of the patients. Cryptography is one security mechanism to keep away prying eyes (or ears). Further, it is not enough to have encryption schemes for just gray-level images, since large number of medical applications require full color processing. Image encryption also plays an equally important role in the secure transmission of images over the internet. Encryption and cryptography thus play a vital role is such image-storage, retrieval and transmission systems.

### 1.1 Generalized Image Encryption Framework using Chaos Theory

Cryptography has certain unique mathematical requirements: diffusion, confusion and dependence on keys. These properties are readily satisfied by chaotic functions by their sensitive dependence on initial conditions (function parameters), topological transitivity and ergodicity (randomness) [1, 3, 6]. This makes chaos theory a good, attractive option for cryptography. Therefore, chaos theory has been successfully applied to cryptography for about a decade now. Josef Scharinger[7] introduced chaos theory to encryption. Thereafter, Fridrich[4] proposed a general framework for using discrete chaotic maps for image encryption. This framework has been used time and again for image encryption, for example the works by Mao *et al.*[6, 2]. In this framework, the analog chaotic map is first discretized. Next, it is generalized by the introduction of some parameters. This map is then extended to three dimensions. The parameters of the map serve the purpose of the 'key' for the encryption system. This discrete generalized parametrized map is used in the encryption algorithm. As an example, we present the work on Cat map proposed by Mao *et al.*[2].

## 2 Cat Map Example

Eqn.1 gives the analog formula of the discrete Cat map on the unit square where $x_n$ and $y_n$ are the coordinates of the point under consideration.

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

This is generalized by the introduction of $a$ and $b$ as the

parameters.

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} mod\, 1 \quad (2)$$

This parametrized map is then extended to 3D as follows:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{bmatrix} = A_z \begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix} mod\, 1 \quad (3)$$

where,

$$A_z = \begin{bmatrix} 1 & a_z & 0 \\ b_z & a_z b_z + 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad (4)$$

As is evident from the formula, the number 1 at the right bottom of the matrix $A_z$ indicates that we leave $z_n$ unchanged, essentially performing 2D cat map in the x-y plane, leaving the $z$-coordinate unchanged. Similar expressions are provided for matrices $A_y$ and $A_x$, where the $y$- and $x$- coordinates are left unchanged respectively[2]. These formulae are then combined to give a general 3D Cat map of the form:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix} mod\, 1 \quad (5)$$

where A is a matrix function of the parameters $a_z, b_z$ etc.

We point out that Mao *et al.*[6] do not explicitly provide a method of combining $A_x, A_y$ and $A_z$ to arrive at the formula for matrix A. However, we have verified that a product of the these three matrices will give the matrix A. Hence we propose taking a product of the matrices $A_x, A_y$ and $A_z$ as a good method to obtain generalized maps, provided that the maps have a matrix notation and we are able to provide matrix formulae equivalent to $A_x, A_y$ and $A_z$.

## 3 Motivation

Traditional crypto-systems are often viewed as substitution-permutation (SP) networks[8], modelled by eqn.6 in terms of confusion($C$) and diffusion($D$) functions[5].

$$Y = [D(C(X, K_1), K_2)]^n \quad (6)$$

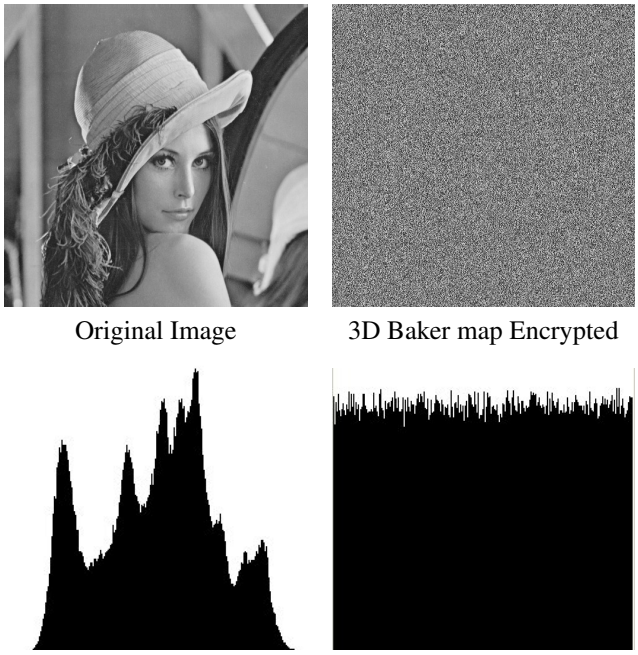
where $X$ is the message to be encrypted, $K_1, K_2$ are the keys for confusion and diffusion. In our case, confusion is achieved by the use of the Baker Map, which is essentially a permutation map while diffusion is achieved by the substitution in eqn.7. We first examine the process of diffusion in more detail. Mao at al.[2, 6] use the following function for diffusion:

$$C(k) = \phi(k) \oplus \{[I(k) + \phi(k)]\ mod\ N\} \oplus C(k-1) \quad (7)$$

The pixel intensity $I(k)$ is replaced by a new pixel value $C(k)$, the ciphered, or more precisely, the diffused value. In essence, eqn.7 simply changes the intensity values in the image. We note that this diffusion mechanism does *not* use chaos theory.

In our analysis, we view substitution of intensity values as a permutation of the bits that make up the intensity value. For example, 145 in binary is 10010001 and 146 in binary is 10010010, a mere permutation. Thus a substitution of 146 for 145 is a mere permutation of the bits in its binary representation. This simple observation gives us a novel approach to extend the image to three dimensions in which we integrate confusion and diffusion at the decimal representation by using only permutations on the binary representations. We emphasize that this permutation at the binary representation level is equivalent to integrating confusion and diffusion at the decimal level. Thus, by integrating confusion and diffusion using only permutations based on chaotic functions, we attempt to bring the properties of chaoticity into the diffusion mechanism as well.

## 4 3D Baker Map Based Image Encryption



Original Image | 3D Baker map Encrypted

Histogram of Original Image | Histogram of encrypted image

**Figure 1. Encryption using Baker maps with traditional piling algorithms (key used is 1234567890123456)**

As is evident from the framework described in sect.1.1, the image should be re-arranged into three dimensions in

order to use the 3D maps for encryption. We first present results based on traditional methods to 'pile up images to higher dimensions'. One of the standard methods to rearrange the map is to first find three integers $L', W', H'$ such that $L' \times W' \times H' = M \times N$, where $M$ and $N$ are the dimensions of the image. Then, the pixels of the image are distributed into the three dimensions such that the above equality is satisfied. Let us call the product $M \times N$ as $P$. The product $P$ is factorized into its prime factors $p_1, p_2, p_3, ..., p_n$ for some $n$. This list of prime factors is then divided into three parts which are then multiplied independently to get $L', W'$ and $H'$. The process of dividing into three parts uses the key provided by the user (see [6]). Fig.1 shows the result of encrypting an image using 1234567890123456 as the key.

## 5 Novel Extension to Three Dimensions

We propose the following simple treatment of an image: The image is viewed as a cube that is composed of bits arranged in three dimensional space. At each pixel location of this cube, the $z$-axis consists of the bits of the 8-bit binary representation of the intensities of the pixels at that location. For example, if the pixel value at location (10,10) of the image is 145, then its binary equivalent is 10010001. Thus, we consider the image to be a cube composed of binary strings where the LSB (least-significant-bit) is at the top of the cube while the MSB (most-significant-bit) is at the base of the cube (see fig.2). We now see that *every image is inherently three dimensional in nature*. Fig.3 shows the result of using this novel approach to encrypt an image. We see that the image is scrambles and a reasonable destruction of the histogram structure is achieved.

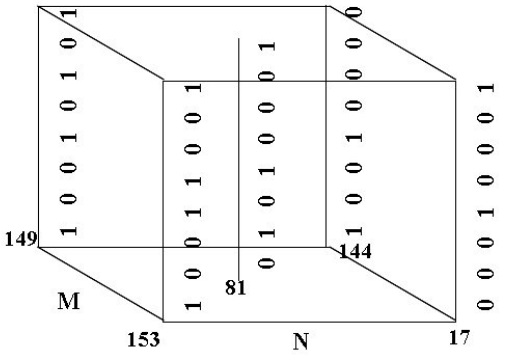
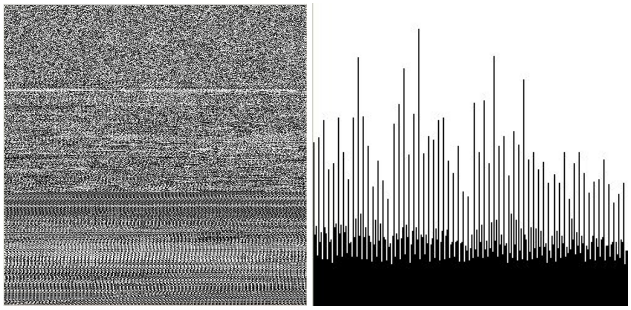



**Figure 2. The cube formed by the binary representation of the pixel intensities provides an alternative view of the image in 3 dimensions.**



3D Baker map encrypted Histogram of encrypted Image

**Figure 3. Encryption using Baker maps with binary-string piling algorithm**

## 6 Color Image Encryption

A naive approach to color image encryption is to independently encrypt the three channels (preferably using different keys). We observe that it is enough to decrypt just one channel of the color image thus encrypted to be able to see the 'necessary content'. Fig.4 (a) shows that encryption of a single channel is not enough - to the human eye, the image is almost indistinguishable from the original. (b) shows that decrypting just one channel reveals enough information to a human attacker of the system.

(a)Only R channel encrypted(b)Only B channel decrypted

**Figure 4. Partial decryption using Baker maps with traditional piling algorithm (key used is 1234567890123456)**

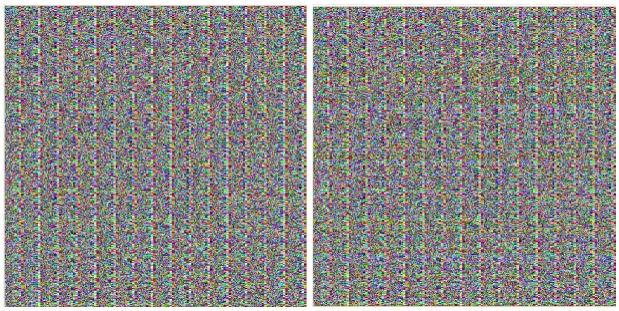
Alternatively, we could expand the intensity in each channel to 8-bits and use our new approach to encrypt each channel independently. But, this also has the same drawback, ie. decryption of just *one* channel is enough to give away the necessary visual information (see fig.5).

We now use the binary-string approach for color image encryption. We consider each pixel location to be consisting of a triplet $(i_1, i_2, i_3)$, comprising of the intensities for each of the three channels. We expand the intensity values

(a)Only R channel encrypted(b)Only B channel decrypted

**Figure 5. Partial decryption using binary-string piling algorithm, where each channel has been expanded to its binary representation and each channel is independently encrypted**

into their binary representation and concatenate the binary strings to form a 24-bit string at each pixel location. The cube formed by these strings is then subjected to the Baker map encryption algorithm. For partial-decryption, we wish to decrypt just one channel. That is, we treat the 24-bit binary-string based encrypted image as if it were composed of three channels of 8-bits each and use the 8-bit binary-string based decryption. The result of subjecting this cube of 24-bit binary strings is given in fig.6. We see that decrypting just one channel does *not* reveal any visual information.



Encrypted Partially Decrypted

**Figure 6. Encryption using Baker maps with binary-string piling algorithm with the binary representations of each channels concatenated.**

## 7 Conclusion and Discussion

In this paper we propose an alternative treatment of an image which helps us to achieve simultaneous confusion and diffusion. This integration allows us to incorporate chaoticity into the diffusion mechanism as well - a feature lacking in the diffusion formulae proposed in the literature. Our results show that a reasonable flattening of the histogram is achieved, as is evident in fig.3. However, we wish to point out that this algorithm is inherently slower than the traditional encryption. In traditional encryption schemes, the number of permutations is at least equal to the number of pixels in the image, while in our approach, the number of permutations per round is at least equal to 8 times the number of pixels (and hence 24 times for 3 channel color images) because the binary representation of the intensity has 8 bits. This process can be speeded up by the use of look-up tables. The look-up table can be generated once and then reused for multiple rounds of the map. Further, in the traditional Baker map based encryption schemes, the piling up algorithm uses part of the key. In this approach, there is no occasion to use the key for piling.

However, the superior performance of our algorithm is eveident in the case of color image encryption, where we treat the image as a cube of height 24 (bits), where 8 bits are contributed to by each channel of the color image. In this case, the superiority is in terms of robustness to partial decryption (decryption of a single channel), while retaining the encryption strengths of the algorithm proposed in [6].

## 8 Acknowlegements

We dedicate this work to our Chancellor, **Sri Sathya Sai Baba**. We would like to thank Mr. Srikanth Khanna, Research Scholar, SSSU, for his time, critical review and invaluable comments.

## References

[1] G. Alvarez and S. Li. Some basic cryptographic requirements for chaos-based cryptosystems. *Int. Jnl. of Bifur. and Chaos*, 16(8):2129–2151, 2006.

[2] G. Chen, Y. Mao, and C. K. Chui. A symmetric image encryption scheme based on 3d chaotic cat maps. *Chaos, Solitons & Fractals*, 21:749–761, 2004.

[3] B. Corrochano, editor. *Chaos Based Image Encryption,* in Handbook of Geometric Computing. Springer-Verlag, NY.

[4] J. Fridrich. Secure image ciphering based on chaos: Final report for afrl, 1997.

[5] S. Lian, J. Sun, and Z. Wang. Security analysis of a chaos-based image encryption algorithm. *Phisica A*, 2005.

[6] Y. Mao, S. Lian, and G. Chen. A novel fast image encryption scheme based on 3d chaotic baker maps. *International Journal of Bifurcation and Chaos*, 14(10):3616–3624, 2004.

[7] J. Scharinger. Fast encryption of image data using chaotic kolmogorov flows. *Journal of Electronic Imaging*, 7(2):318–325, 1998.

[8] J. Scharinger. Analysis and application of chaotic permutation systems. *Cybernetics Systems*, 1:57–62, 2002.