

# Comparative Analysis of Color Image Encryption Using 2D Chaotic Maps

Shubhendu Kumar, Bhavna Sinha and Chittaranjan Pradhan

**Abstract** Digital image encryption can be done either by using the cryptography techniques or chaotic maps. Here, we have given focus to the chaotic maps due to the simplicity as compared to the cryptography techniques. In this paper, we have presented the color image encryption using different 2D chaotic maps, such as 2D Logistic map, Henon map, Baker map, Arnold cat map and Cross chaos map. The efficiency of these image encryption techniques is verified by the differential attack. NPCR (number of pixels change rate) and UACI (unified average changing intensity) have been chosen as the evaluation parameters.

**Keywords** 2D logistic map · Henon map · Baker map · Arnold cat map · Cross chaos map · Encryption · Chaotic maps

## 1 Introduction

With the rise and emergence of the Internet, the transmission of huge scale of image data over communication media such as cell phones, facsimile, television, computer networks, satellites etc. has increased [1]. These digital data are easily accessible to others creating opportunities for pernicious parties to defile the confidential information and making commercial copies of the copyrighted content without permission of the original owner.

Image encryption has emerged out to be a potential solution to this problem of protecting intellectual property and ensuring righteousness to the digital data. Image

---

S. Kumar (✉) · B. Sinha · C. Pradhan  
KIIT University, Bhubaneswar, India  
e-mail: shubhendukumar4332@gmail.com

B. Sinha  
e-mail: bhavna25sinha@gmail.com

C. Pradhan  
e-mail: chitaprakash@gmail.com

Encryption works by locking an image file with a ‘key’ and providing that key only to its authorized user. This provides a high degree of security enhancing its robustness [2]. Once the encrypted file is opened, it becomes vulnerable to any form of dissemination without any further form of control.

In the color image encryption we have three planes RGB (Red, Green, Blue). Each of these three planes is quantized separately. The pixels of the original image are scrambled and mingled through random sequence which is chaotic in nature. The original image can be recovered after several iterations depending on initial conditions. The scrambling takes place by arranging pixels and taking each bit of image and XORed with random sequence that is generated [3]. The features like non-deterministic, randomness, periodicity of chaotic maps make the digital image data more secure.

## 2 Image Encryption Using 2D Chaotic Map

The several disadvantages of 1D logistic map led to the introduction of various 2D chaotic maps which makes the digital image data more secure. Figure 1 shows the 2D chaotic maps that we analyzed upon.

### 2.1 2D Logistic Map

The 2D logistic map came into picture to encounter the disadvantages of 1D logistic map. The increased number of control parameters and key spaces makes it a bit tough to predict the secret content for the pernicious parties [4]. The color image is first broken down into 3 planes (Red, Blue, Green). For each plane we generate 2 chaotic sequences with chaotic behavior defined as:

$$Z(X, Y) = \begin{cases} X_{i+1} = \mu_1 * X_i(1 - X_i) + \beta_1(Y_i)^2 \\ Y_{i+1} = \mu_2 * Y_i(1 - Y_i) + \beta_2((X_i)^2 + X_i * Y_i) \end{cases} \quad (1)$$

where,  $i = 0, 1, 2, \dots$ .  $\mu_1, \beta_1, \mu_2, \beta_2$  are the system control parameters.  $X_0$  and  $Y_0$  are the initial conditions. The range of the control parameters are:  $2.75 < \mu_1 \leq 3.4$ ,  $0.15 < \beta_1 \leq 0.21$ ,  $2.70 < \mu_2 \leq 3.45$ ,  $0.13 < \beta_2 \leq 0.15$ ,  $0 < X_i, Y_i \leq 1$ .

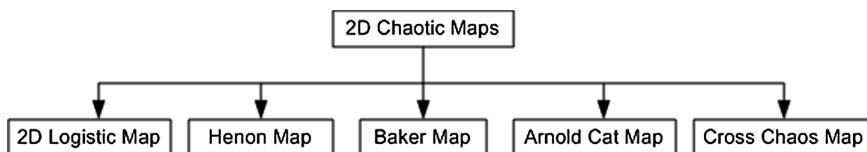


Fig. 1 2D chaotic map classification

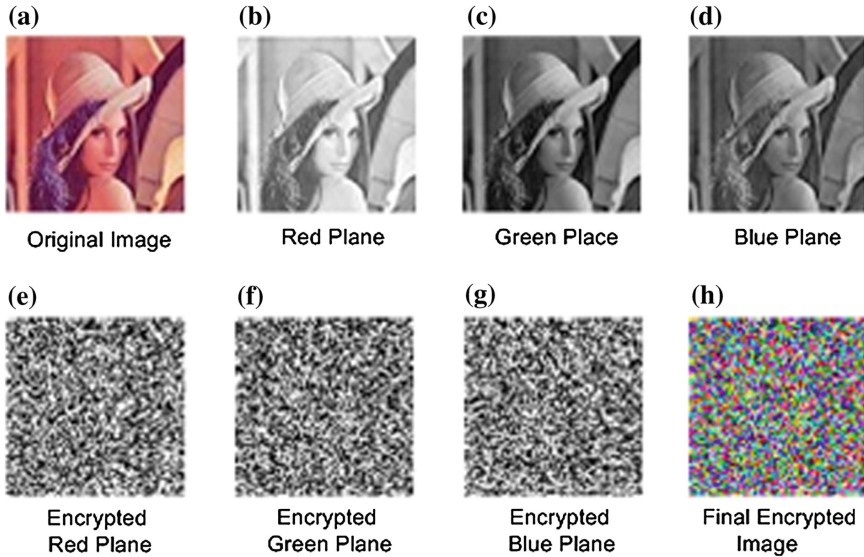


Fig. 2 Results for image encryption using 2D logistic map

Let us take one  $M \times M$  color image which is broken down into 3 planes (Red, Green and Blue). For each of the three planes, we generate the random sequence by using the above equation. The 1D matrix,  $Y$  is transposed and multiplied with  $X$  to generate a 2D matrix of size  $M \times M$ , called  $K$ . The elements of the matrix  $K$  are quantized to binary format using the following equation:

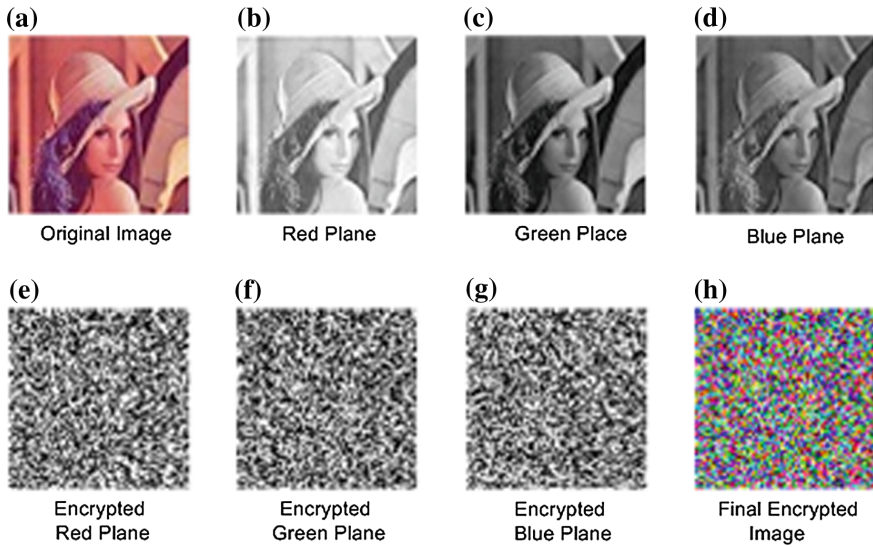
$$P(x) = \begin{cases} 0, & \text{if } 0 < K(i,j) \leq 0.5 \\ 1, & \text{if } K(i,j) > 0.5 \end{cases} \quad (2)$$

Each element of the quantized matrix is then XORed with the respective bit of every pixel of the  $M \times M$  color image. This is done with the bits of all the three planes individually. The three planes are then concatenated to form a single plane and thus an encrypted image is produced.

The original image can be recovered by providing the appropriate key along with the correct value of the initial condition. For ‘lena64’ image, the encrypted image using 2D logistic map is shown in Fig. 2. Here, we have taken  $\mu_1 = 2.93$ ,  $\beta_1 = 0.17$ ,  $\mu_2 = 3.26$ ,  $\beta_2 = 0.14$ ,  $X_0 = 0.895$  and  $Y_0 = 0.923$ . The decryption will be done by taking the same arguments.

## 2.2 Henon Map

Henon map was proposed by Michel Henon in 1976 which is a discrete time dynamical and 2D invertible map represented with an attractor. This map generates



**Fig. 3** Results for image encryption using Henon map

a random sequence which is used to encrypt the shuffled pixels of the  $M \times M$  original image. The sequence is generated by the formula defined as [5, 6].

$$Z(X, Y) = \begin{cases} X_{i+1} = 1 - a * (X_i)^2 + Y_i \\ Y_{i+1} = b * Y_i \end{cases} \quad (3)$$

where,  $i = 0, 1, 2, \dots$   $a$  and  $b$  are control parameters. We take one  $M \times M$  color image and is broken down into 3 planes (RGB).

For each plane, 2 chaotic sequences are generated using the above equation and taking  $a = 1.4$  and  $b = 0.3$  as the control parameters. The 1D matrices  $X$  and  $Y$  are reconstructed as row and column matrices respectively. These matrices are multiplied together to generate a matrix  $K$  of size  $M \times M$ . This matrix is quantized to a binary format using Eq. (2).

Each element of the quantized matrix  $P(x)$  is XORed with each bit of every pixel of  $M \times M$  color image to produce an encrypted image for each plane. All the 3 encrypted images are concatenated to a single plane. The original image can be recovered by providing appropriate system keys and initial conditions. Figure 3 shows the result of image encryption using Henon map.

### 2.3 Baker Map

Baker Map is a 2D chaotic map from unit square  $M \times M$  into itself which is again a discrete time dynamical system. It is an extension of 1D Tent map exhibiting

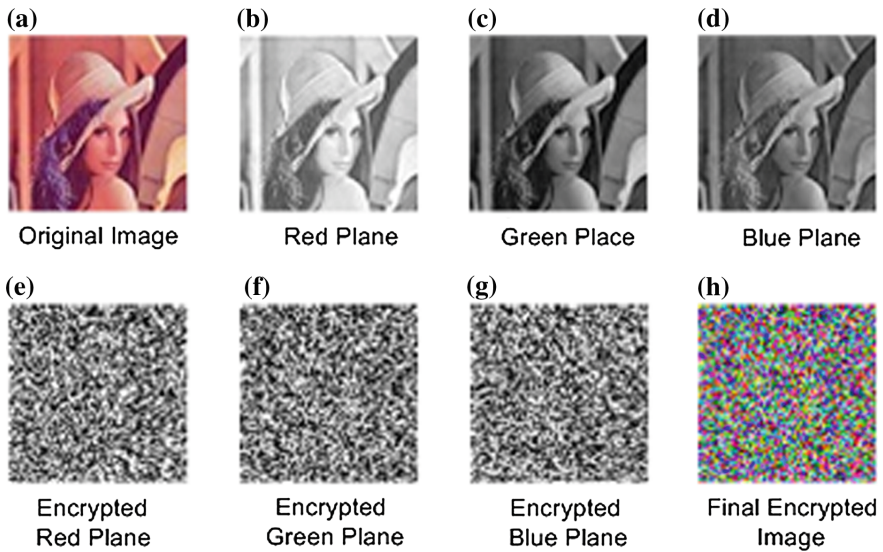


Fig. 4 Results for image encryption using Baker map

deterministic chaos feature. The parameters are the encryption key for the encryption of the chaotic function. There are two alternative definitions of the Baker map. One definition folds over or rotates one of the sliced halves before joining and the other definition doesn't. The folded baker map [7] is generated as:

$$Z(X, Y) = \begin{cases} [X_{i+1}, Y_{i+1}] = [2X_i, \frac{Y_i}{2}], & \text{if } 0 \leq X_i < 0.5 \\ [X_{i+1}, Y_{i+1}] = [2(1 - X_i), 1 - \frac{Y_i}{2}], & \text{if } 0.5 \leq X_i < 1 \end{cases} \quad (4)$$

where,  $X_0$  and  $Y_0$  are the initial conditions. Here,  $X_i$  is expanded twice horizontally and  $Y_i$  is contracted to half vertically. This matrix is quantized to a binary format using Eq. (2). The quantized sequence is XORed with each bit of every pixel of  $M \times M$  color image. Thus, producing an encrypted image for all the 3 planes separately. The encrypted results of all the 3 planes are concatenated to form a single plane, producing an encrypted image of the original image. The original image can be recovered by providing the appropriate initial values of  $X_0$  and  $Y_0$ . Image encryption using Baker map is shown in Fig. 4.

### 2.4 Arnold Cat Map

Arnold cat map is a chaotic map from the torus into itself, named after Vladimir Arnold, who demonstrated its effect using cat's image in 1960s [8]. This chaotic map transforms the image by shuffling the pixels through several iterations. The

image returns to its original state after a number of iterations of transformations, known as Arnold's period. A  $M \times M$  color image is taken and broken down into 3 planes (RGB). Equation for 2D Arnold cat map is given as [9]:

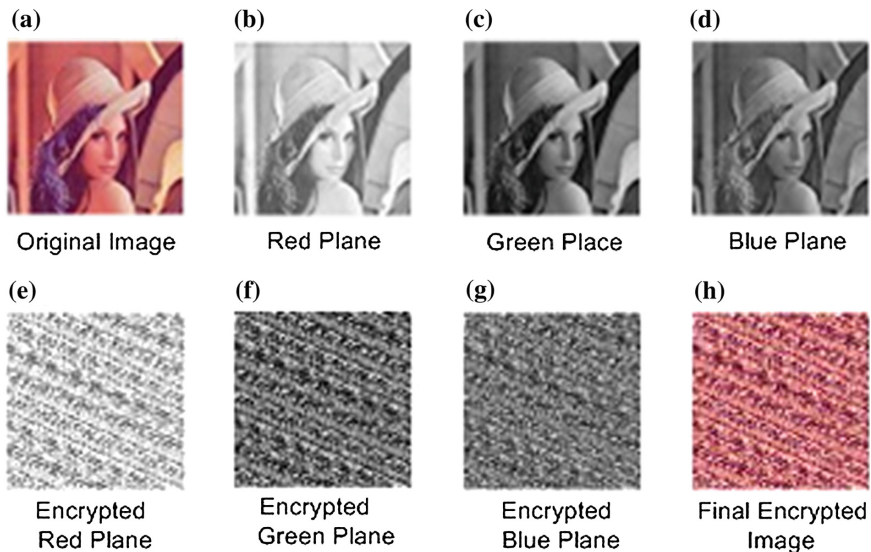
$$Z(X, Y) = \begin{cases} X_{i+1} = (X_i + aY_j) \bmod N \\ Y_{j+1} = (bX_i + (ab + 1)Y_j) \bmod N \end{cases} \quad (5)$$

where,  $a$  and  $b$  are the control parameters of the system. The above equation is applied on the original pixel co-ordinates  $(X_i, Y_j)$  to form a new pixel co-ordinates  $(X_{i+1}, Y_{j+1})$ . The iteration continues by replacing the old pixel positions. The results of the 3 planes are concatenated together to a single plane. The original image can be recovered by iterating the pixels till Arnold's period. The 2D Arnold cat map holds chaotic behavior along with diffusion, randomness and enhanced security; thus making it more robust and dynamic than 1D chaotic map.

Figure 5 shows the result of color image encryption using Arnold cat map. Here, we have taken the parameters as:  $a = 2$ ,  $b = 3$  and *Arnold's period* = 17.

## 2.5 Cross Chaos Map

Cross chaos map is a chaotic map which is used for randomization purpose. The two chaotic sequences are generated as [10, 11]:



**Fig. 5** Results for image encryption using Arnold cat map

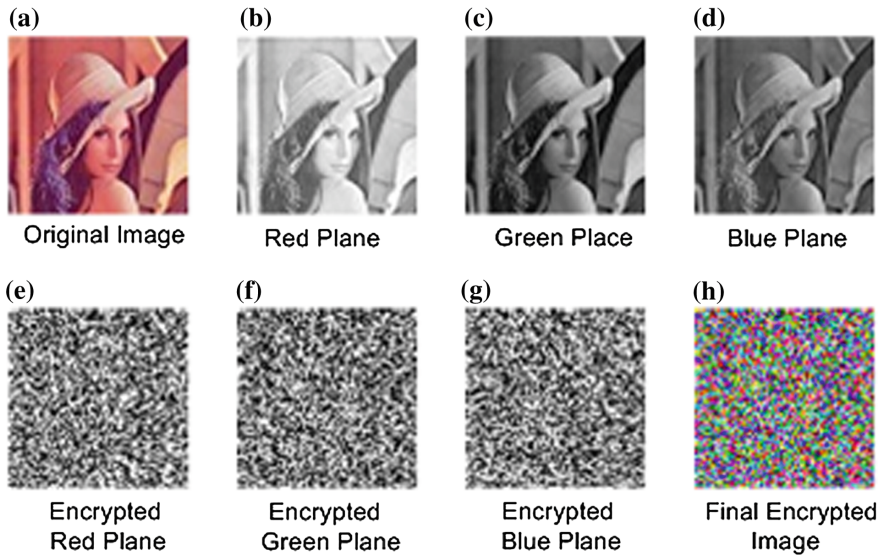


Fig. 6 Results for image encryption using cross chaos map

$$Z(X, Y) = \begin{cases} X_{i+1} = 1 - \mu * (Y_i)^2 \\ Y_{i+1} = \cos(k * \cos^{-1} X_i) \end{cases}; \quad X, Y \in [-1, 1] \quad (6)$$

where,  $\mu, k$  are the control parameters of the system.  $X_0$  and  $Y_0$  are the initial conditions. The  $M \times M$  color image is broken down into 3 planes (RGB). For each plane, two chaotic sequences are generated. The system works better for  $\mu = 2$  and  $k = 6$  [10, 11]. The 1D sequences  $X$  and  $Y$  are reconstructed to form row and column matrices respectively, which are multiplied together to generate  $K$ , one  $M \times M$  matrix. Finally, this matrix is quantized using the same quantization function discussed in earlier. The encrypted result from all the 3 planes are concatenated to form a single encrypted image for one plane.

The original image can be recovered by providing the appropriate system parameters and initial conditions. Here, we have taken  $\mu = 2, k = 6, X_0 = 0.64$  and  $Y_0 = 0.76$ . The detail of image encryption using cross chaos map is shown in Fig. 6.

### 3 Comparative Analysis of Security

The security level of the above implemented 2D chaotic maps need to be checked. We do this comparative analysis by calculating 2 parameters: NPCR (number of pixel change rate) and UACI (unified average change intensity). Differential attack analysis shows relationship between original image and encrypted image. NPCR is used to check how a change in single pixel in original image brings about a

significant change in the encrypted image [12]. Let's take two images,  $P$  and  $Q$  with a difference of only one pixel. We define another matrix,  $K$  such as:

$$K(i,j) = \begin{cases} 0, & \text{if } P(i,j) = Q(i,j) \\ 1, & \text{if } P(i,j) \neq Q(i,j) \end{cases} \tag{7}$$

NPCR can be calculated as:

$$NPCR = \frac{\sum_{i,j} K(i,j)}{a \times b} \times 100 \% \tag{8}$$

where,  $a$  and  $b$  are the height and width of both images  $P$  and  $Q$ . UACI calculates the percentage of different pixels in both the images [12]. This can be calculated as:

$$UACI = \frac{\sum_{i,j} \frac{|P(i,j)-Q(i,j)|}{255}}{a \times b} \times 100 \% \tag{9}$$

Table 1 shows the values obtained after the simulation of NPCR and UACI together calculated using Eqs. (8) and (9).

The result shows that the value of NPCR is around 99 % and UACI is around 33 %. The higher the average value of NPCR and UACI, the better is the chaotic map.

$$Average = \frac{NPCR + UACI}{2} \tag{10}$$

Table 2 shows average values of NPCR and UACI for each of the chaotic maps using the values from Table 1. The result shows that Arnold 2D Cat map is better than other maps.

**Table 1** NPCR and UACI values

	2D logistic map	Henon map	Baker map	Arnold cat map	Cross chaos map
NPCR	98.92	99.12	99.34	99.60	99.56
UACI	33.50	32.67	32.62	33.00	32.96

**Table 2** Average of NPCR and UACI

	2D Logistic map	Henon map	Baker map	Arnold cat map	Cross chaos map
Average	66.21	65.89	65.98	66.30	66.26



## 4 Conclusion

In this paper, we have used different version of 2D chaotic maps to encrypt the color images. The involvement of several control parameters in 2D chaotic maps makes them more robust and thus provides higher security than 1D chaotic map. NPCR and UACI values assure the security nature of these maps. Though cryptography has some limitations, still it is growing up at a very good pace. Every now and then, we are introduced to a new, secure and fast chaotic algorithm. Although we can't say that this kind of cryptography is best and will stand up to all the real attacks, still we consider that 2D chaotic cryptography. In future, will solve the security and copyright issues over transmission of digital images. These encryption methods will be applicable for watermarking techniques soon in near future. These maps can also be enhanced in higher dimension to increase the efficiency; thus, making transmission of digital images via various communication media more secure.

## References

1. Pisarchik, A.N., Zanin, M.: Chaotic map cryptography and security, encryption: methods, software and security, vol. 4. Nova Science Publishers, New York, pp. 1–28 (2010)
2. Sethi, N., Sharma, D.: A novel method of image encryption using logistic mapping. *Int. J. Comput. Sci. Eng.* **1**(2), 115–119 (2012)
3. Cheng, J., Guo, J.: A new chaotic key-based design for image encryption and decryption. In: *International Symposium on Circuits and Systems*, vol. 4, pp. 49–52. IEEE (2000)
4. Abuhaibal, I.S.I., Abuthraya, H.M., Hubboub, H.B., Salamah, R.A.: Image encryption using chaotic map and block chaining. *Int. J. Comput. Netw. Inf. Secur.* **7**, 19–26 (2012)
5. Jolfaei, A., Mirghadri, A.: An image encryption approach using chaos and stream cipher. *J. Theor. Appl. Inf. Technol.*, 117–125 (2010)
6. Yadava, R.K., Singh, B.K., Sinha, S.K., Pandey, K.K.: A new approach of colour image encryption based on Henon like chaotic map. *J. Inf. Eng. Appl.* **3**(6), 14–20 (2013)
7. Fridrich, J.: Symmetric ciphers based on two-dimensional chaotic maps. *Int. J. Bifurcation Chaos* **8**(6), 1259–1284 (1998)
8. Peterson, G.: Arnold's cat map, *Math 45. Linear Algebra*, pp. 1–7 (1997)
9. Ahmad, M., Alam, M.S.: A new algorithm of encryption and decryption of images using chaotic mapping. *Int. J. Comput. Sci. Eng.* **2**(1), 46–50 (2009)
10. Pradhan, C., Rath, S., Bisoi, A.K.: Non blind digital watermarking technique using DWT and cross chaos. In: *International Conference on Communication, Computing and Security*, vol. 6, pp. 897–904. *Procedia Technology*, Elsevier, Amsterdam (2012)
11. Pradhan, C., Bisoi, A.K.: Robust watermarking using chaotic variations of AES in DWT domain. In: *International Conference on Computational Intelligence and Information Technology*, pp. 445–451. IET (2013)
12. Jiansheng, M., Sukang, L., Xiaomei, T.: A digital watermarking algorithm based on DCT and DWT. In: *International Symposium on Web Information Systems and Applications*, pp. 104–109 (2009)