ISSN: 0975-766X
CODEN: IJPTFI
Available Online through *Research Article*
www.ijptonline.com

A SECURE IMAGE CRYPTOSYSTEM USING 2D ARNOLD CAT MAP AND LOGISTIC MAP

[1]R. Sujarani, [2]D. Manivannan
[1]Assistant professor, Department of Computer Science, Srinivasa Ramanujan Centre, SASTRA University, Kumbakonam 612002, India.
[2]Senior Assistant Professor, School Of Computing, SASTRA University, Thanjavur 613401, India.
Email: rsujarani@src.sastra.edu

Received on 18-08-2016 *Accepted on 25-09-2016*

Abstract

Background/ Objectives: To design a new image cryptosystem using chaotic maps for providing secure communication of images.

Methods/Statistical Analysis: The proposed scheme is the combination of confusion and diffusion process. In confusion part, the position of the pixels are shuffled by using the new index position generated by the Arnold cat map. In diffusion phase each pixel in the shuffled image is substituted by another value using the sorted index value of the chaotic sequence generated by the two dimensional (2D) logistic map and the neighbourhood pixels. Security analysis of the proposed scheme has done by using histogram analysis, correlation coefficient and information entropy analysis.

Findings: Combination of chaotic maps for image cryptosystem provides better security at less computational time and complexity with huge key space. The analysis part and the statistical result demonstrates that the proposed cipher has sufficient encryption effect to attack against differential and statistical attacks.

Application/Improvement: The proposed cipher can be applicable for different format of images such as GIF, bmp, TIFF, JPG and also it can be applied for DICOM images.

Keywords: Arnold cat map, chaos, image encryption, logistic map, pseudo random numbers.

1. Introduction: In today's scenario, the usage of images has become very popular in many applications like military, medical, social media and industries. Sensitive images are communicated through insecure networks. So, there is a great demand for encryption algorithms to securely transfer the images over the communication media. Images are encrypted in two forms either by disturbing the intensity of the pixels (Spatial domain) 1,2 or disturbing the frequency of pixels in image(Frequency domain)3,4. Images have some inherent properties, such as high data redundancy, high relationship

among pixel value and usually large in size. Because of these features, some conventional encryption techniques are challenging to use and slow the encryption process. To provide solution to this problem chaos based image cryptosystem has emerged as a new field in cryptography. Chaos system has some inherent properties such as determinism, randomness, sensitivity to initial condition and ergodicity, these properties make the chaos a very popular in the field of image encryption. Various image encryption algorithm using chaos has been proposed 5–7. Chaos based image cipher is the combination of confusion and diffusion process. In confusion process the position of the pixel values are changed and in diffusion process the value of the pixels are changed. An image encryption algorithm8 has proposed using logistic map. Another map which is more related to logistic map is a tent map. In9 some changes has done in tent map to have a high chaotic range, they combine the logistic, tent and sine map to form tent- sine map which has excellent chaotic behaviour and used for the substitution process of image encryption. A new encryption scheme10has proposed using Chebyshev map which has excellent chaotic properties. However, all of them used one dimensional chaotic maps , the random numbers generated by these chaotic map are chaotic only for the limited range, again the same set of sequence are repeated. To overcome these limitations two dimensional chaotic maps were invented, which generate more random numbers. In another scheme11 authors used Chirikov-taylor map for generating pseudo random numbers used for confusing the image. A novel image encryption12has proposed using the Henon map for permutation and spatiotemporal chaos for substitution. In the image encryption concept13 authors used the discretized baker map for shuffling the image. In our proposed scheme we have used Arnold cat map14 for confusion process and the confused image is diffused using two dimensional (2D) logistic map15, which increases the security of the proposed scheme. To increase the diffusion result, image pixel values are diffused using both logistic map and the neighbourhood pixel values. This paper is ordered in the succeeding form. Section 2 discusses the basics of generalized Arnold cat map and 2D logistic map. Proposed chaos based image cryptosystem is presented in section3. Result and security level analysed in section 4. Conclusion part discussed in section 5

2. Basic concept of proposed scheme

2.1. **Arnold cat map:** Arnold cat map is one of the most discrete systems, which provide chaotic behavior. In 1960 Vladmir Arnold invented this chaotic map, he tested this map using cat image, so he named this as Arnold cat map16.The Arnold cat map is explained by the following Eq. (1).

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N \quad (1)$$

In the above equation x and y are the position of pixels in origin image while (x',y') is the chaotic sequence denoted as random position of the pixel value created by the cat map. P and q are system parameters, N represents the height or width of the image. By using the Arnold cat map the position of the pixel values(x, y) of original image is changed to position (x',y'). So, by using cat map iteratively all the pixel positions are modified and finally we get the permutated image which is ready for the diffusion process. Figure 1. shows the result of permutated image which obtained by using

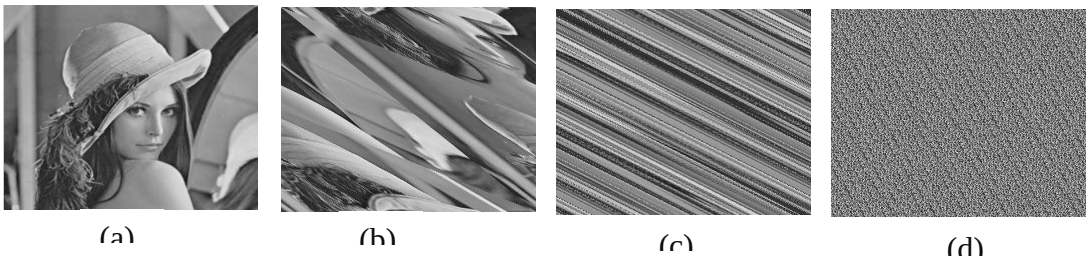

Figure 1. Image Permutation (a) origin image (b) result of 1st iteration of permutation (c) output of 2nd iteration (d) 10th iteration-final permutated image

Arnold cat cap with 10 iterations.

2D Logistic map

The expanded form of one dimensional logistic map is a 2D logistic map. It provides large key space and increases the dependency of system parameters.The chaotic sequence generated by this map has a great amount of chaotic behavior17. The 2D logistic map is defined in Eq. (2).

$$\begin{aligned} x_{i+1} &= \beta_1 x_i(1-x_i) + \gamma_1 y_i^2 \\ y_{i+1} &= \beta_2 y_i(1-y_i) + \gamma_2(x_i^2 + x_i y_i) \end{aligned} \quad (2)$$

β1, β2, γ1 and γ2 are system control parameters. The 2D logistic map is in chaotic behavior only when the system parameters are in the range of 2.75≤ β1, β2 ≤ 3.45 and 0.15 ≤ γ1, γ2 ≤ 0.21, the initial values x0 and y0 must be in the range between 0 and 1. It can produce two chaotic sequences within the range [0, 1]. Chaotic sequences generated by a map is greatly sensitive to initial values, a small variation in these parameters will change the result of decryption. In 2D

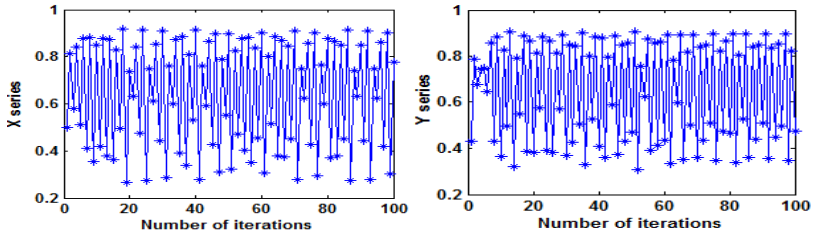

Figure. 2. Randomness of chaotic series x and y

logistic map 6 keys are used. So it is not possible for the attacker to apply the exhaustive attack to get the origin image. The analysis of the randomness of the chaotic sequences of the 2D logistic map is shown in Figure. 2.

3. Proposed encryption scheme

The proposed image cryptosystem is the combination of two major steps, image confusion and diffusion. In confusion the position of the pixel values are scattered by utilizing the chaotic numbers generated by the Arnold cat map and in diffusion process each pixel of the scattered image is converted into another value by using x and y series generated by the 2D logistic map. The overall view of the proposed image cryptosystem is shown in Figure 3.

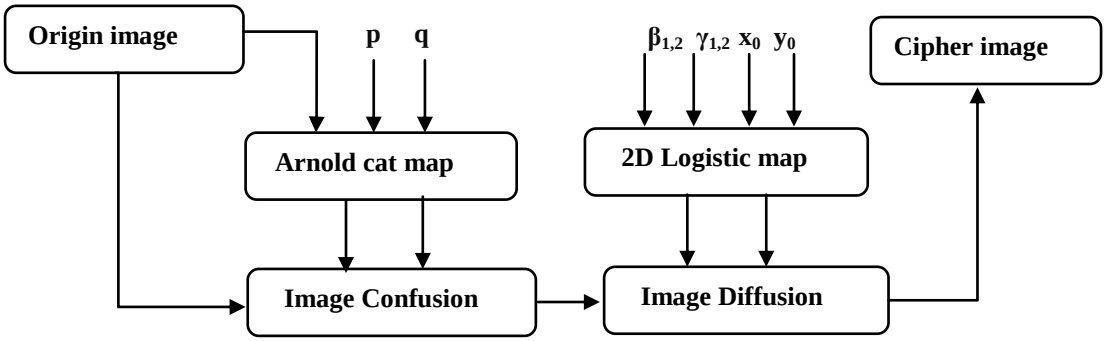

Figure 3. Overall view of the proposed image cryptosystem

The proposed encryption scheme contains 6 steps, which are discussed as follows.

Step1: Select any grayscale image I(m,n) as the original image, where n,m denotes number of rows and columns of images.

Step 2: Produce new pixel positions x'={ x1,x2,x3,x4……Xm} and y'={ y1,y2,y3,y4…….yn } using Arnold cat map.

Step 3: Shuffle the image by using the method given below

Ix(i),y(j) ⇔ Ix'(i),y'(j) i= 1,2,3……m; j=1,2,3……n;

As the result of this step, we get the confused image I'(m,n)

Step 4: Generate two chaotic sequences ={ x**1,**x**2**,x**3**,x**4**…X**mxn**} and Y={ y**1,**y**2**,y**3**,y**4**….y**nxm**}using 2D logistic map by applying the key parameters.

Step 5: Sort the generated chaotic sequence X, Y as follows:

[sx,ix] = sort(X); sx and sy are the new sorted sequence

[sy,iy] = sort(Y); ix and iy are the index values of X and Y

Step 6: The confused image I'(m,n) is diffused by using the following procedure

For i=2:m

For j=2:n

I f (mod(j,2)==0)

I''(i,j) = I'(i-1,j-1) (xor) ix(k) k=1,2,3……..(m* n)/2;

Else

I''(i,j) = I'(i-1,j-1) (xor) iy(k) k=1,2,3……..(m* n)/2;

End

End

At the end of this step encrypted image I''(m,n) has generated.

For retrieving the origin image from the cipher image, reverse process of the proposed encryption process can be used.

4. Experimental result

Here, we have taken the standard grayscale Lena image (256 X 256) as the original image for the projected scheme. We have developed the experiment using Matlab 13. The initial values and key parameters we have taken for generating chaotic sequence is β1=3.13, β2=2.94, γ1=0.17, γ2=0.14, x0=0.17, y0=0.40. In addition to these keys include the number of iteration of Arnold cat map and the system parameters p and q are also used as secret keys, for our experiment we have chosen the iteration value as 10 and for p and q we have taken the size of the origin image. Figure 4. Shows the result of proposed scheme. The result shows that there is no connection between the origin image and the cipher image.

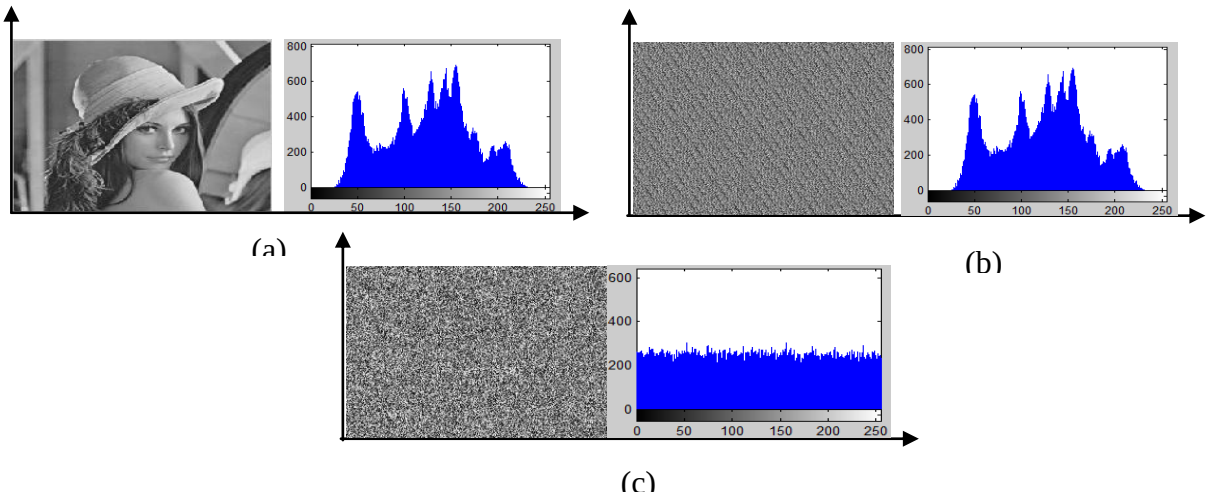

Figure 4. (a) Origin image and its histogram (b) Confused image and its histogram (c) Final diffused image and its histogram

So, it is difficult to get the original image by applying differential attack.

5. Security Analysis

5.1. Key space analysis

Good cipher must have a large key space 18. Here, we are using six different keys they are β1, β2 γ1, γ2, x0, y0. If we have taken the precision value as 10-14, then the size of the key is 1084. In addition to these keys include the number of iteration value and system parameters p and q for Arnold cat map is also used as keys. So, totally 9 keys are used in our scheme. Hence, size of the key is sufficient to fight against differential attack.

5.2. Gray histogram analysis

We have compared the histogram of the origin and encrypted image to analyse the security level. Figure.5 (a) and (b) shows the histogram of the input and cipher image. From the figures it is clearly identified that the pixel values of the origin and ciphered image has low similarities. So, it is challenging for the attackers to apply statistical attack for hacking the original image.

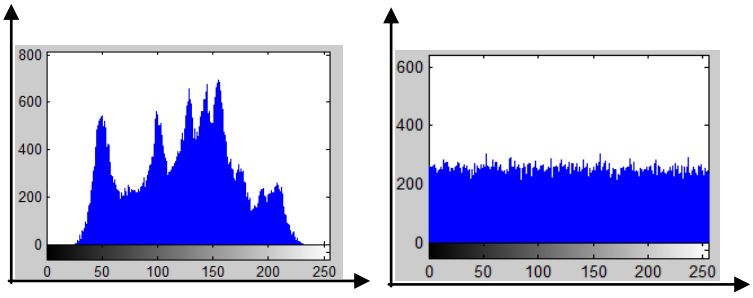

Figure 5. (a) Origin Lena image histogram
(b) Ciphered Lena image histogram

5.3. Correlation coefficient analysis

All pixels in the origin image are highly related with its neighborhood pixels in all directions. A good image cipher should generate the ciphered image with no such relationship in the neighborhood pixels 19. The correlation coefficient analysis is the best way for finding the eminence of the projected encryption algorithm 20. To check the correlation among the two neighborhood pixels in origin image and cipher image, we have selected 3840 pairs of pixels from each direction (horizontal, vertical, diagonal) from the origin and cipher image. And so, correlation coefficient is computed by utilizing the following Eq. (3).

$$Exp(x) = \frac{1}{N}\sum_{i=0}^{n} x_i$$

$$D(x) = \frac{1}{N}\sum_{i=0}^{n}(x_i - Exp(x))^2$$

$$Covar(x,y) = \frac{1}{N}\sum_{i=0}^{n}(x_i - Exp(x))(y_i - Exp(y))$$

$$r_{xy} = \frac{covar(x,y)}{\sqrt{D(x)} \times \sqrt{D(y)}} \qquad (3)$$

The correlation coefficient of the original image and the cipher image of each direction is given in Figure 6. Figure 6 (a) shows the correlation between the pixels of three direction of the origin Lena image. Figure 6(b) show the correlation between the pixels of ciphered Lena image.

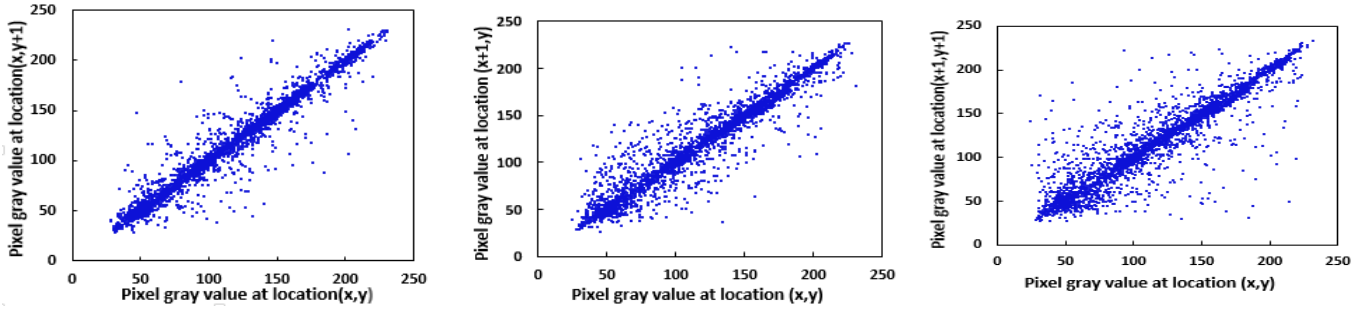

Figure 6. (a) Correlation of pixels in original Lena image

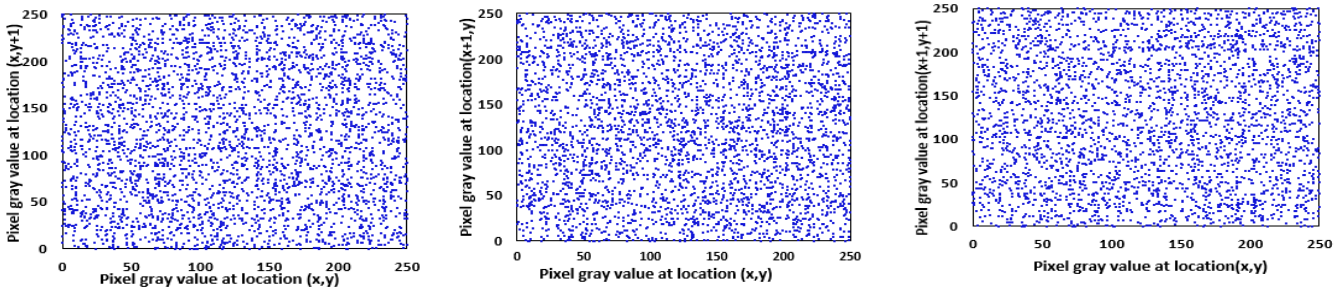

Figure 6. (b) Correlation of pixels in ciphered Lena image

The correlation coefficients of the different origin and cipher image are presented in Table 1. Based on the result shown in Table 1, it is clear, that the correlation between the pixel values of the cipher image has nearest value to 0. So the projected image cryptosystem has good encryption effect.

Table 1: correlation coefficient of images.

Input image	Horizontal	Vertical	Diagonal
Lena:			
Origin image	0.9413	0.9699	0.9155
Cipher image	0.0086	-0.0016	0.0039
Boat:			
Origin image	0.8951	0.9229	0.8418
Cipher image	-0.0015	-0.0059	0.0011

Camera man:			
Origin image	0.9292	0.9577	0.9000
Cipher image	0.0017	0.0021	0.0017

5.4. Information entropy

To find the level of uncertainties of information in image, information entropy can be used. It evaluate the scattering of pixel values in the image. If the pixel values are distributed evenly then the entropy value is high. It is described in following Eq. (4).

$$E(I) = \sum_{i=0}^{n} P(I_i) log_2 P(I_i) \qquad (4)$$

Ii is the ith pixel value of the n size gray image. P(Ii) is the probability of Ii. 8 is the entropy value of the images which are generated randomly. A good cryptosystem must have the entropy value as 8. Table 2 shows the result of entropy of the proposed scheme. From the result it is clear that the encrypted image entropy is very close to 8. Hence the proposed cipher is efficient to fight against statistical attack.

Table 2: information entropy of images.

Image	**Entropy**	
	Origin image	**Cipher image**
Lena	7.4436	7.9973
Boat	7.1770	7.9970
Camera man	7.0922	7.9963

6. Conclusion

Here, we projected an image cryptosystem by combining two chaotic maps. The image is scrambled by using Arnold cat map and the scrambled image is diffused by using XOR between index value of the chaotic sequence produced by 2D logistic map and the previous pixel value. The result analysis shows that the proposed scheme has sufficient encryption effect, huge key space. The proposed scheme can directly apply to color image cryptosystem.

References

1. Chattopadhyay D, Mandal M K. Symmetric key chaotic image encryption using circle map. *Indian J Sci Technol*. 2011,4(5),pp. 8-11.

2. Vijayaraghavan R, Sathya S, Raajan NR. Security for an image using bit-slice rotation method-image encryption. *Indian J Sci Technol*. 2014,7,pp. 1-7.
3. Tamilselvi R, Ravindran G. Image Encryption using Pseudo Random Bit Generator Based on Logistic Maps with Radon Transform. *Indian J Sci Technol*. 2015;8(11). doi:10.17485/ijst/2015/v8i11/71763.
4. Parthasarathy MB, Srinivasan B. Increased Security in Image Cryptography using Wavelet Transforms. *Indian J Sci Technol*. 2015;8(12). doi:10.17485/ijst/2015/v8i12/62433.
5. Liu Y, Tong X, Hu S. A family of new complex number chaotic maps based image encryption algorithm. *Signal Process Image Commun*. 2013;28(10):1548-1559. doi:10.1016/j.image.2013.07.009.
6. Zhang X, Shao L, Zhao Z, Liang Z. An image encryption scheme based on constructing large permutation with chaotic sequence. *Comput Electr Eng*. 2014;40(3):931-941. doi:10.1016/j.compeleceng.2013.08.008.
7. Wang X, Liu C, Zhang H. An effective and fast image encryption algorithm based on Chaos and interweaving of ranks. *Nonlinear Dyn*. 2016. doi:10.1007/s11071-015-2590-3.
8. Ye G. Image scrambling encryption algorithm of pixel bit based on chaos map. *Pattern Recognit Lett*. 2010;31(5):347-354. doi:10.1016/j.patrec.2009.11.008.
9. Bao L, Zhou Y, Chen CLP, Liu H. A New Chaotic System for Image Encryption. *Signal Processing*. 2012;3(3):69-73.
10. Liu H, Wang X. Triple-image encryption scheme based on one-time key stream generated by chaos and plain images. *J Syst Softw*. 2013;86(3):826-834. doi:10.1016/j.jss.2012.11.026.
11. Patidar V, Pareek NK, Sud KK. Commun Nonlinear Sci Numer Simulat A new substitution – diffusion based image cipher using chaotic standard and logistic maps. *Commun Nonlinear Sci Numer Simul*. 2009;14(7):3056-3075. doi:10.1016/j.cnsns.2008.11.005.
12. Zheng Y, Jin J. A novel image encryption scheme based on H??non map and compound spatiotemporal chaos. *Multimed Tools Appl*. 2014;74(18):7803-7820. doi:10.1007/s11042-014-2024-0.
13. Fu C, Li WJ, Meng ZY, Wang T, Li PX. A symmetric image encryption scheme using chaotic baker map and lorenz system. *Proc - 9th Int Conf Comput Intell Secur CIS 2013*. 2013:724-728. doi:10.1109/CIS.2013.158.
14. Zhang W, Wong K wo, Yu H, Zhu Z liang. An image encryption scheme using reverse 2-dimensional chaotic map

and dependent diffusion. *Commun Nonlinear Sci Numer Simul*. 2013;18(8):2066-2080. doi:10.1016/j.cnsns.2012.12.012.

15. Zhang Q, Liu L, Wei X. Improved algorithm for image encryption based on DNA encoding and multi-chaotic maps. *AEU - Int J Electron Commun*. 2014;68(3):186-192. doi:10.1016/j.aeue.2013.08.007.
16. Prusty AK, Pattanaik A, Mishra S. An image encryption & decryption approach based on pixel shuffling using Arnold Cat Map & Henon Map. *ICACCS 2013 - Proc 2013 Int Conf Adv Comput Commun Syst Bringing to Table, Futur Technol from Around Globe*. 2014:1-6. doi:10.1109/ICACCS.2013.6938729.
17. Seyedzadeh SM. A novel color image encryption algorithm based on spatial. *Nonlinear Dyn*. 2015:511-529. doi:10.1007/s11071-015-2008-2.
18. Ye G, Wong KW. An efficient chaotic image encryption algorithm based on a generalized arnold map. *Nonlinear Dyn*. 2012;69(4):2079-2087. doi:10.1007/s11071-012-0409-z.
19. Carmen P, Ricardo L. Notions of Chaotic Cryptography : Sketch of a Chaos Based Cryptosystem. 2009.
20. Somaraj S, Hussain MA. Performance and Security Analysis for Image Encryption using Key Image. *Indian J Sci Technol*. 2015,8(35),pp.6-9.