Digital Image Encryption based on Chaotic Map and Circulant Matrix

Anand Ballabh Joshi and Abdul Gaffar

Department of Mathematics and Astronomy,
University of Lucknow, Lucknow-India

anandiitd.joshi@gmail.com, abdul266gaffar@gmail.com

Abstract

Security of digital images is a major concern when they are used on public channels such as internet. Many digital image encryption methods have been proposed in recent past years. Chaotic maps are very effective for cryptography due to their effects of ergodicity, sensitivity to initial and control parameters. In this paper, we proposed an encryption algorithm for digital images based on chaotic map and circulant matrix. The method is based on the well known confusion and diffusion concepts of cryptography. Confusion is performed by permutation of rows and columns of digital image using the chaotic sequence as a key. Diffusion is performed by decomposing the image pixel matrix into different sub-matrices and adding these sub-matrices with the sub-matrices generated by circulant matrices. Statistical and security analysis are also given in this paper to support the robustness of the proposed method.

Subject class [2010]:53D15, 53A20, 53C25.
Keywords: Cryptography, plaintext, ciphertext, digital image, chaotic map and circulant matrix.

1 Introduction

Activity of exchanging information and thoughts over a space is known as communication. Secure communicaton involves protecting this exchange of information from intruders. Some mechanism needs to be provided in order to achieve this security. Cryptography [1, 2] provides much needed data security. Cryptography is a technique that involves converting intelligible data such as text, pictures, audio and video into an unintelligible form in order to protect from attackers. It is probably the most important means to provide secure communication. The intelligible data in a cryptosystem is called plaintext and its encrypted unintelligible form is known as ciphertext. Any encryption algorithm takes plaintext and a secret key as input and produces the ciphertext as output. The secret key is known only to sender and reciever. Here digital images are used as digital data. Among various digital image encryption methods, the chaos based image encryption method is a family of methods that are believed to be good for encryption purposes.

As chaotic system [5, 6, 7, 8] has high sensitivity to its initial value, high sensitivity to its control parameter (r) and ergodicity, it is considered as a good candidate for cryptography. The paper is organised as follows: Section 2 gives a brief description about chaotic map, circulant matrix, Toeplitz matrix; Section 3 gives architecture of the proposed cryptosystem; Section 4 discusses about encryption and decryption process of the proposed method; Section 5 gives proposed algorithm for encryption and decryption; Section 6 gives demonstration of the procedure while security anlysis and statististcal anlysis of the proposed cryptosystem are given in section 7 and section 8 respectively. Finally section 9 concludes the paper.

2 Prelimanaries

2.1 Digital Image

An image is a two-dimensional function f(x, y) where x and y are spatial (plane) co-ordinates and the amplitude of 'f' at any pair of co-ordinates (x, y) is called intensity or gray level of the image at that point. When x, y and the amplitude values of 'f' are all finite, we call an image a digital image.

2.2 Chaotic Map

In mathematics, a chaotic map is a map that exhibits some sort of chaotic behaviour. Maps may be parameterized by discrete time or a continuous time parameter. Discrete map usually take the form of iterated functions. Chaotic maps often occur in the study of dynamical system [3, 4].
For example, the logistic map (i.e. a non-linear return map) given by

$$x_{n+1} = r x_n(1 - x_n)\ ;\ n \in \mathbb{N} \cup \{0\},\ x_n \in [0,1]\ and\ r \in [0,4] \tag{2.1}$$

is a chaotic map for $r \geq 3.57$

Here x_0 is the initial value and r is the control parameter of the map.

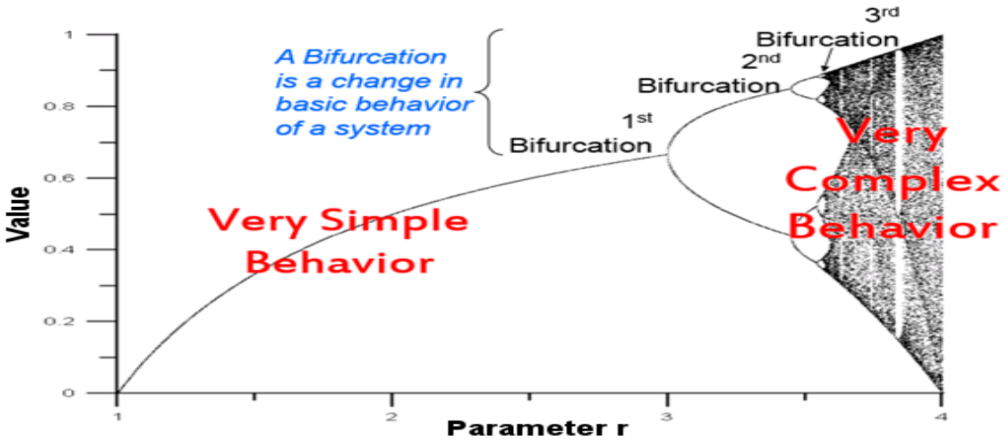
Bifurcation diagram:- It shows the possible long term values of a map according to the control parameter (r), see figure 1 below.
We have following cases depending on the value of r :

Case 1. When $r \simeq 3.57$:- Period doubling region ends and chaos begins.

Case 2. When $r \simeq 3.83$:- Small period tripling window opens up.

Case 3. When $r \simeq 3.86$:- Period tripling cascade ends and chaos resumes.

Case 4. When $r \simeq 4.0$:- Chaos reigns!!!



Bifurcation diagram of the logistic map

Fig. 1

2.3 Toeplitz Matrix

It is named after Otto Toeplitz, is a matrix in which each descending diagonal from left to right is constant. It is also known as Diagonal-Constant matrix.
For example,

$$A = \begin{bmatrix} a & b & c & d & e \\ f & a & b & c & d \\ g & f & a & b & c \\ h & g & f & a & b \\ i & h & g & f & a \end{bmatrix}$$

2.4 Circulant Matrix

In linear algebra, a circulant matrix [9], is a special kind of Toeplitz matrix in which each row vector is rotated one element to the right relative to the preceding row vector.
For example,

$$B = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_5 & a_1 & a_2 & a_3 & a_4 \\ a_4 & a_5 & a_1 & a_2 & a_3 \\ a_3 & a_4 & a_5 & a_1 & a_2 \\ a_2 & a_3 & a_4 & a_5 & a_1 \end{bmatrix}$$

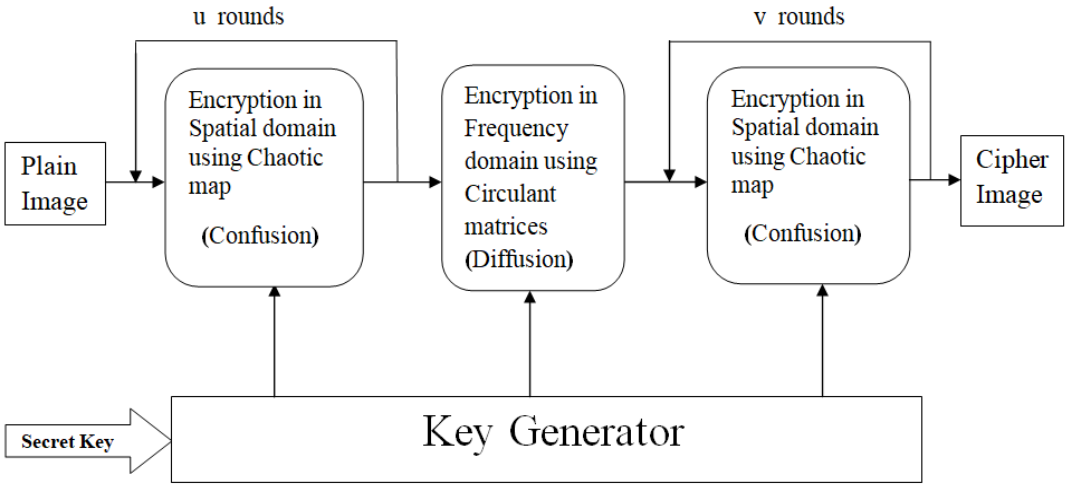


Fig. 2: **Architecture of proposed cryptosystem**

3 Architecture of the Proposed Cryptosystem

The typical architecture of the proposed cryptosystem is given in figure 2. There are three stages in the proposed cryptosystem. The confusion stage permute the pixels without changing their values (i.e. encryption in spatial domain) while diffusion stage modifies the pixel values sequentially (i.e. encryption in frequency domain). Keys for the proposed cryptosystem are generated using the chaotic map (see, equation 1) and the circulant matrices.

4 Encryption and Decryption Process

In the proposed cryptoystem, security of RGB images is based on the two famous concept of cryptgraphy viz. confusion (row and column shuffling) and diffusion (pixel value modification). Encryption is done in three stages. In stage 1, confusion is performed and to decorrelate relationship between adjacent pixels, there are u permutation rounds where u is a fixed positive integer. In stage 2, partially encrypted image pixel matrix of size m $\times$ n is decomposed into $\frac{mn}{s^2}$ blocks (sub-matrices) of size s each and then diffusion is performed on these $\frac{mn}{s^2}$ blocks. In stage 3, again confusion is done and to achieve satisfactory level of security, the process is repeated for v rounds, where v is a fixed positive integer. Proposed algorithm is applied on red (R), green (G) and blue (B) components of an RGB image data in encryption and decryption process. The procedure of encryption and decryption algorithm applied on RGB image is given in figure 3 and figure 4 respectively.

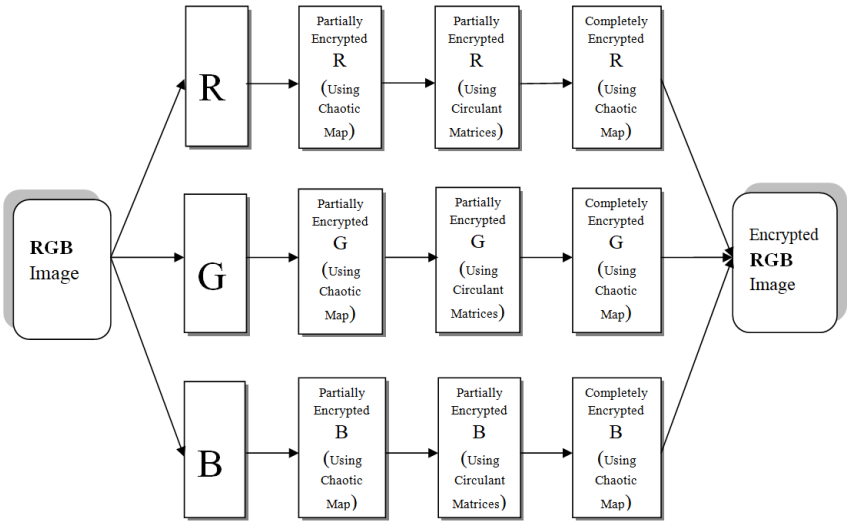


Fig. 3: Encryption procedure for each comoponent of RGB image

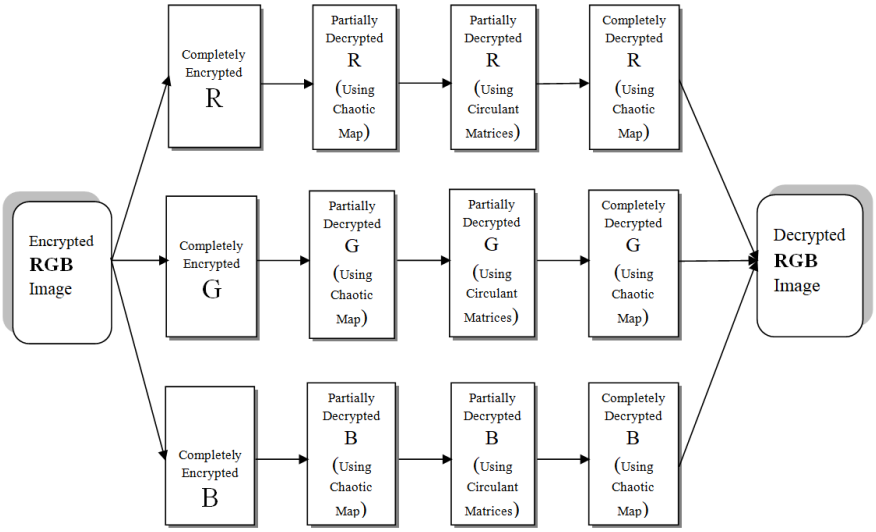


Fig. 4: Decryption procedure for each comoponent of RGB image

5 Proposed Algorithm for Encryption and Decryption

5.1 Encryption Algorithm

Let us consider an image of size m × n.

Stage 1

Step 1. Generate a chaotic sequence with the help of chaotic map; remove first 'm' elements and take 'p' elements from the sequence, where p = $max\{m, n\}$. Let $\{x_1, x_2, ..., x_p\}$ be p elements of the chaotic sequence.
Step 2. Convert these $\{x_1, x_2, ..., x_p\}$, p elements into integers by multiplying by 10^4

i.e. $y_i = x_i \times 10^4$; i = 1, 2,..., p

Step 3. Calculate $z_i = y_i \pmod{p}$; i = 1, 2,..., p
Step 4. Add 1 to each z_i i.e. $d_i = 1 + z_i$; i = 1, 2,..., p. Let D = $\{d_1, d_2, ..., d_p\}$ where $d_i \in \{1, 2, ..., p\}$ for each i = 1, 2,..., p
Step 5. Form a set, say A, of distinct elements of set D and let A = $\{d_1, d_2, ..., d_j\}$; j ≤ p and replace repeating elements (if any) of set D by elements of the set F − A, where F = $\{1, 2, ..., p\}$.
Step 6. Let $\pi = \{q_1, q_2, ..., q_p\}$ be permutation of p elements generated using step 5. Now, three cases arise :

Case 1. If m > n then p = m, these p elements $\{q_1, q_2, ..., q_m\}$ of π are used as a key for row shuffling and first n elements of π are used as a key for column shuffling.

Case 2. If m < n then p = n, these p elements $\{q_1, q_2, ..., q_n\}$ of π are used as a key for column shuffling and first m elements of π are used as a key for row shuffling.

Case 3. If m = n then p = m = n, these p elements $\{q_1, q_2, ..., q_p\}$ are used as a key for row and column shuffling.
Step 7. Repeat step 6 for u rounds, where u is a some fixed positive integer .

Stage 2

Step 8. Decompose the pixel matrix obtained in step 7 into $\frac{mn}{s^2}$ blocks (sub-matrices) of size s each such that s | m & s | n and if s ∤ m or s ∤ n, use padding.
Step 9. Generate t chaotic sequences, where t = min$\{\frac{m}{s}, \frac{n}{s}\}$, whence q elements are taken from each sequence, where $q = max\{m, n\}$.
Step 10. Divide these q elements into $\frac{q}{s}$ equal sub-arrays of size s each and form circulant matrices, in this way we have $\frac{mn}{s^2}$ circulant matrices. Let $k_1, k_2, ..., k_{\frac{mn}{s^2}}$ be first rows of $\frac{mn}{s^2}$ circulant matrices respectively then these are used as keys for diffusion.

Stage 3

Step 11. Perform confusion on the image obtained in step 10 for v rounds, where v is a some fixed positive integer, using key of stage 1 i.e. π.
Image obtained in step 11 is the required encrypted image.

5.2 Decryption Algorithm

Step 1. Reciever recieves the encrypted image.
Step 2. Calculate π^{-1} and perform v round permutation using key π^{-1}.
Step 3. Decompose the image obtained in step 2 into $\frac{mn}{s^2}$ blocks of size s each and operate additive inverse of circulant matrices on these blocks, whose first rows are $k_1, k_2, ..., k_{\frac{mn}{s^2}}$ respectively.
Step 4. Again perform u round permutation using key π^{-1}.

6 Demonstration of the Procedure

In the proposed method, we have taken an RGB Lena image of size $256 \times 256 \times 3$ pixels, (m = 256, n = 256) for experimental analysis, which is given in figure 5(a).

Encryption process:- First we generate a sequence using a chaotic map given by equation (1), in which first 256, (m = 256) elements are removed and 256, (p = max{256, 256} = 256) elements are taken and generate a permutation π using stage 1 of algorithm given in section (5.1). We perform confusion on red (R), green (G) and blue (B) components using key π. The permutation π is applied for u = 15 rounds to get the partially encrypted components.
Now, we decompose the partially encrypted R, G, B components into 16, ($\frac{mn}{s^2} = 16$) blocks of size 64×64, (s = 64) each and perform encryption using stage 2 of algorithm given in section (5.1) on these blocks and the encryption process is illustrated below:-
We generate 4 chaotic sequences ($t = \min\{\frac{256}{64}, \frac{256}{64}\} = 4$), from which 256, (q = max{256, 256}) elements are taken from each and then divide these 256 elements into 4, ($\frac{q}{s} = 4$) equal sub-arrays of size 64, (s = 64) each and create circulant matrices of these 64 elements. In this way we have created 16 circulant matrices which are used for diffusion. Let R_1 denotes partially encrypted red component (PERC) of size 256×256 pixels. Let $b_1, b_2, ..., b_{16}$ denotes 16 blocks of PERC and $k_1, k_2, ..., k_{16}$ be 16 keys (i.e. circulant matrices). The encryption method is given as

$$c_i = (b_i + k_i) \bmod 256 \ ; \ i = 1, 2, ..., 16$$

Now, we combine these blocks (c_i's) to form a component, which is again partiallly encrypted. Similarly, we do this for partially encrypted green and blue components respectively. We again perform confusion using the key π already generated and to achieve satisfactory level of security, we repeat this process for v = 20 rounds, finally we concatenate all these 3 components to get a finally encrypted RGB Lena image.
Illustration of the process is given in figure 5 (a - d).

Decryption process:- We split the encrypted RGB Lena image (Fig.5(e)) into R, G, B components and then we perform confusion using permutation π^{-1} (given in step 2 of section 5.2) for v = 20 rounds to get the partially decrypted R, G, B components. Now diffusion is performed using step 3 of section 5.2 on the partially decrypted R, G, B components and the process is given as follows :
Let c_i ; i = 1,..., 16 denotes blocks of partially encrypted red component and $k_1, k_2, ..., k_{16}$ be 16 keys then decryption method is given by

$$b_i = (c_i - k_i) \bmod 256 \ ; \ \text{i} = 1,..., 16$$

Now, we combine these partially decrypted red blocks (b_i's) to get a partially decrypted red component. Similarly, we do the above process for partially encrypted green and blue components respectively. Again we perform confusion using permutation π^{-1} already generated, on these partially decrypted R, G, B components for u = 15 rounds to get the completelty decrypted R, G, B components which on concatenating gives the completely decrypted RGB Lena image. Illustration of the process is given in figure 5 (e - h).
We have also applied the above proposed method on two more images. The experimental results are given in figure 6.

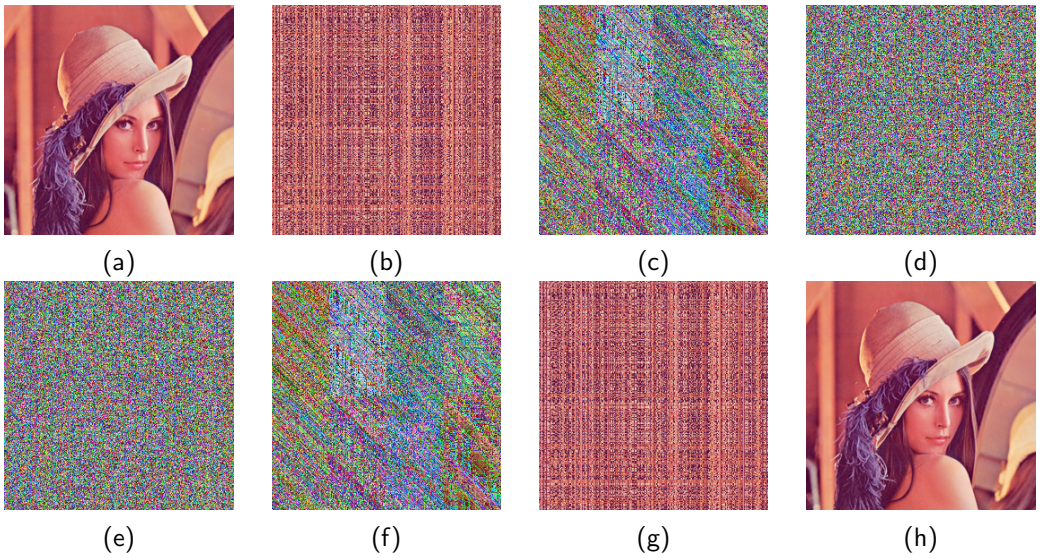


Fig. 5: Results:-**(a)** Original Lena image **(b)** Partially encrypted image (u = 15 rounds) **(c)** Partially encrypted image using circulant matrices **(d)** Completely encrypted image (v = 20 rounds) **(e)** Encrypted image **(f)** Partially decrypted image (v = 20 rounds) **(g)** Partially decrypted image using circulant matrices **(h)** Completely decrypted image (u = 15 rounds)

7 Security Analysis of the Proposed Method

7.1 Key Space Analysis

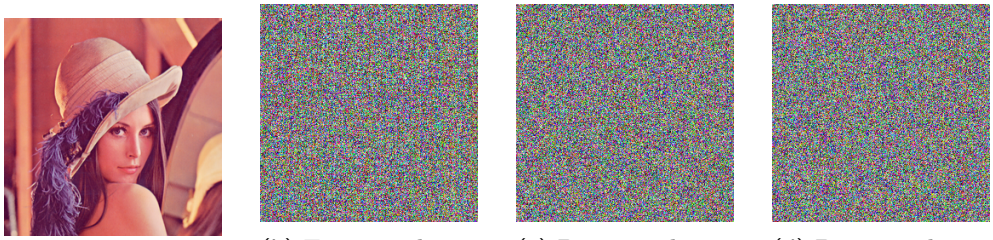
The key space of the cryptosystem refers to set of all possible keys that can be used to generate a key for encryption. A secure encryption should have a large key space to resist attacks. Large key space of the cryptosystem provides robustness against brute-force attack, known-plaintext attack, chosen-ciphertext attack etc. In the proposed method, chaotic map is used, which has two parameters r and x_0. As $r \in [3.57, 4]$ and $x_0 \in [0, 1]$, there are uncountable possibilities for parameters r and x_0. Also, $\frac{mn}{s^2}$ circulant matrices are used, which can be arranged in $(\frac{mn}{s^2})!$ ways . So key space is very large.

(a) Original rose (b) Encrypted rose (c) Original tiger (d) Encrypted tiger

Fig. 6

7.2 Sensitivity Analysis

The robustness of the cryptosysytem is fully based on the sensitivity of keys. To prevent the attacker from breaking the cryptosystem, high sensitivity is required. In the proposed method, chaotic map is used which is highly sensitive to initial value x_0. If someone tries to decrypt the encrypted image with approximate value of x_0 (not exact), the resulting image will be totally different from original image. Figure 7(b) is the encrypted image of Lena image using initial value $x_0 = 0.675279$. Figure 7(c) is obtained when a very small change is made in initial value i.e. change of -0.000001 while figure 7(d) is obtained when change of $+0.000001$ is made at decryption process. We can see from figur 7 that the image decrypted using a key with very small change in initial value does not give any information about the original image. So our proposed method is highly sensitive and is suitable for encryption.



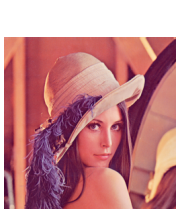
(a) Original Lena image (b) Encrypted image using $x_0 = 0.675\mathbf{279}$ (c) Decrypted image using $x_0 = 0.675\mathbf{278}$ (d) Decrypted image using $x_0 = 0.675\mathbf{280}$

Fig. 7

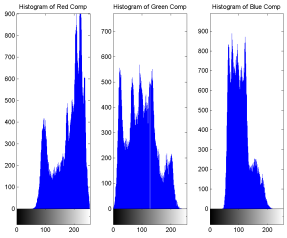
8 Statistical Analysis

8.1 Histogram Analysis

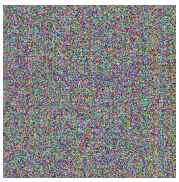
An RGB image histogram is a graphical representation of the pixel intensity distribution of the image. Therefore, an image histogram provides a clear illustration of how the pixels in an image are distriuted, by plotting the number of pixels at each intensity level. Since a good image encryption method tends to encrypt a plaintext image to a random like, it is desired to see uniformly distributed histogram for the image and is one of the important factor which supports robustness of the cryptosystem. Figure 8(b) and figure 8(d) shows the histogram of R, G, B components of the original Lena image (Fig.8(a)) and the encrypted Lena image (Fig.8(c)) respectively.



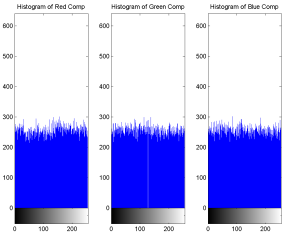
(a) Lena image



(b) Histogram of Lena image



(c)Encrypted image



(d) Histogram of encrypted image

Fig. 8

8.2 Mean Square Error, Peak Signal-to-Noise Ratio analysis and Correlation Coefficient

The commonly used measures for comparing the original image and encrypted image are the mean square error (MSE), peak signal-to-noise ratio (PSNR) and correlation coefficient. For good encryption, high MSE value, low PSNR value and correlation coefficient value close to 'zero' is desired.
The MSE between original image and encrypted image is calculated using the formula:

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[g(i,j) - f(i,j)]^2 \tag{8.1}$$

where M, N denotes number of rows and columns of image matrix and g(i, j) and f(i, j) denotes pixel value of encrypted and original image respectively.

The PSNR between original and encrypted image is given by the following formula:

$$PSNR = -10log_{10}\frac{MSE}{S^2} \tag{8.2}$$

where S denotes maximum possible pixel value of image. In particular, if a pixel is represented by 8 bits then S=255.

The correlation coefficient (C_r) of red (R), green (G) and blue (B) components of original image and encrypted image is computed by

$$C_r = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}(A_{mn}-\overline{A})(B_{mn}-\overline{B})}{\sqrt{[\sum_{i=1}^{m}\sum_{j=1}^{n}(A_{mn}-\overline{A})]^2[\sum_{i=1}^{m}\sum_{j=1}^{n}(B_{mn}-\overline{B})]^2}}. \tag{8.3}$$

where $\overline{A}$ and $\overline{B}$ are the mean of encrypted and original images respectively. The correlation coefficient between two images vary from -1 to $+1$, i.e. $-1 \leq C_r \leq +1$. Two images A and B have a strong positive linear correlation if the correlation coefficient C_r is close to $+1$, have negative linear relationship if C_r is close to -1 and have no relationship between two images if C_r is close to 'zero'. The MSE, PSNR and C_r values of R, G and B components between original Lena image (Fig.5(a)) and completely encrypted Lena image (Fig.5(d)) are given in the table 1.

Here high MSE, low PSNR and correlation coefficient values show that original image is

Components of RGB image	**MSE**	**PSNR**	**Correlation**
RED	1.0729×10^4	7.8591	-2.67×10^{-2}
GREEN	8.8920×10^3	8.6748	1.08×10^{-2}
BLUE	6.9411×10^3	9.7505	2.00×10^{-2}

Tab. 1: Statistical analysis of Lena image

completely changed.

8.3 Correlation Analysis

The correlation coefficient between two adjacent pixels x and y is calculated using the formula:

$$C_{xy} = \frac{cov(x,y)}{\sigma_x \times \sigma_y} \tag{8.4}$$

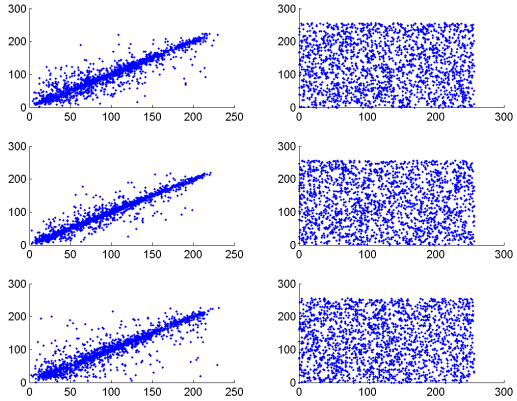
where cov(x, y) is the covariance between pixels x and y; σ_x and σ_y are standard deviation of pixels x and y respectively. The correlation coefficient for the plain image has positive value tending towards 1 as neighbouring pixels have similar range pixel values. The correlation for encrypted image has value moving away from positive 1 as neighbouring pixels have dissimilar pixel values. Table 2 shows correlation coefficient of original Lena image and the encrypted image along horizontal, vertical and diagonal components of R, G, B components.

Graphical correlation plot for original Lena and encrypted image along horizontal, vertical and diagonal components is given in figure 9.

Components of RGB image	**Plain image**			**Encrypted image**		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
R	0.9528	0.9761	0.9285	0.0005	0.0284	−0.0030
G	0.9360	0.9669	0.9111	0.0045	0.0044	−0.0029
B	0.9181	0.9484	0.8892	0.0044	0.0423	0.0036

Tab. 2: Correlation analysis of Lena image

(a) **Lena image** (b) **Encrypted im**



(c) **Horizontal, Vertical and Diagonal pixel distributions of Fig.(a) and Fig.(b) respectively**

Fig. 9

Here we see that the pixel intensity distributions of the encrypted images is uniformly distributed in the domain, which is completely different from pixel distributions of the original image. So no information can be obtained from encrypted image, hence it is secured from attacks.

9 Conclusion

In the proposed paper, a novel approach has been presented for encryption and decryption. The security of RGB images has been done with the help of chaotic map and circulant

matrices. We have demonstrated the encryption and decryption process. The security and statistical analysis also has been discussed. Moreover, histogram analysis, high MSE, low PSNR and correlation coefficient values as illustrated in the proposed paper, indicate that our proposed method is sufficient for security of RGB (digital) images.

References

[1] Rivest, Ronald L.(1990), "Cryptography". In J.Van Leeuwen. *Handbook of Theoretical Computer Science.* 1.Elsevier.

[2] Bellare, Mihir; Rogaway, Phillip (21 September 2005), "Introduction", *Introduction to Modern Cryptography.* p. 10.

[3] Alligood KT, Sauer TD, Yorke JA., *"Chaos: An introduction to dynamic system"*, Springer, 1996.

[4] Devaney R., *"Chaos, Fractals and Dynamics: Computer experiments in Mathematics"*, Addison Wesley, 1989.

[5] Mao Y.B., Chen G., *"Chaos based image encryption"*, Springer, Verlag, 2003.

[6] J.Fridrich, *"Image encryption based on chaotic maps"*, in IEEE Int. Conf. Systems, Man and Cybernatics, **2**.1105-1110 (1997).

[7] Patidar V., Pareek N.K., Purohit G., Sud K.K., *"A robust and secure chaotic standard map based pseudorandom permutation substitution scheme for image encryption"*, Optics Communications, vol. 284(19), pp. 4331-4339, 2011.

[8] Zhang Z.X., Cao T., *"A chaos based image encryption scheme with confusion and diffusion architechture"*, Communication in Computer and Information Science, vol.152, pp. 258-263, 2011.

[9] Davis, Phillip J., *"Circulant matrices"*, Wiley, New York, 1970 ISBN 0471057711.