

# Image Cryptography by TJ-SCA: Supplementary Cryptographic Algorithm for Color Images

Taranjit Kaur, Reecha Sharma

**Abstract**— In this paper extended version of TJ-ACA: advanced cryptographic algorithm is proposed named as TJ-SCA: supplementary cryptographic algorithm for color images through which we get white blank encrypted image (no preview is available) in frequency domain, which makes brute force and various other attacks futile. Thus, maintaining the confidentiality of original images. In this proposed algorithm, 2-D fast Fourier transform, ikeda mapping and various methods are used to get highly secure image. Through, this algorithm lossless decryption is possible and is also applicable for images on which steganography has been applied.

**Index Terms**— 2-D fast Fourier transform, 3-D plot, ikeda mapping, image Cryptography, logarithmic transform, pixel intensity surrogation, security definitive tests.

## 1 INTRODUCTION

Outstanding growth in communication leads to development of new techniques, simultaneously increasing threat for information security. Transmission of information over network forges intruders to acquire information directly and clearly through images. Therefore, information security has become a crucial and indispensable matter of contention. Information which is to send has to be so unreadable that intruder cannot decrypt it.

Cryptography main objective is providing security to information which is possible in the following aspects:

- **Privacy:** Confidentiality of information is maintained. The transmitted message should be sensible to only the intended receiver. Privacy is achieved through encryption of plain-image and decryption of the cipher-image.
- **Integrity:** Protection against information modification. Information must arrive at the receiver as it was sent.
- **Authentication:** Receiver is assured of sender's identity and that an intruder has not sent the message.
- **Non-Repudiation:** Receiver must be able to prove that a received message came from a specified sender only. The burden of proof falls on the receiver [17].

The image cryptography algorithms are classified in three types: (i) pixel position alteration based algorithm, (ii) pixel intensity surrogation based algorithm, (iii) visually changed based algorithm [1]. The proposed algorithm is designed while keeping in mind the entire three image cryptographic algorithm.

In pixel position alteration based algorithm, pixel positions are altered by applying certain logic. In pixel intensity surrogation based algorithm, intensity value of the pixels is changed. In visually changed based algorithm, encrypted image is made so unreadable that human eyes can't decrypt any part of the image.

Cryptography is done in two ways: (i) symmetric (private) key cryptography, where only single key is used to do encryption and decryption, (ii) asymmetric (public) key cryptography, where one key is used to do encryption and other key is used to do decryption [3].

A newly proposed algorithm is supplementary to TJ-ACA [18]. The proposed algorithm is symmetric key algorithm which uses same cluster and same scaling constant (used in logarithmic transform) at both sender and receiver side to encrypt and decrypt images.

The steps used in the supplementary proposed algorithm to encrypt the images are:

Step 1: Formation of Cluster.

Step 2: Pixel intensity reformation.

Step 3: Ikeda Mapping.

Step 4: RR-CC Fusion.

Step 5: 2-D Fast Fourier Transform.

The basic idea for the step 1, 2 is taken from Somdip Dey [3] to produce a key cluster and bits rotation with modifications. Steps 1, 2, 3 and 4 are of TJ-ACA: advanced cryptographic algorithm [18].

## 2 PROPOSED ENCRYPTION ALGORITHM

### 2.1 Formation of Cluster

Digital color image consist of red, green and blue image layers. Cluster is a key array, having elements of single digit value. All the intensities of each row of each Red (R), Green (G) and Blue (B) layer are added individually to produce a number. All digits of a number are added to again produce a number. This process repeats again and again until a single digit number is obtained. This single digit number is placed in a sub-cluster. Thus, single digit numbers is produced for each row of R G B layers and are placed in sub-cluster at the respec-

• Taranjit Kaur is currently pursuing M.Tech (student) in electronics and communication engineering in Punjabi University, UCoE, Patiala, Punjab, India. E-mail: taranjit1988@gmail.com

• Reecha Sharma is currently Assistant Professor in Punjabi University, UCoE, Patiala, Punjab, India. E-mail: richa\_gemini@yahoo.com

tive processed row number. To produce the final cluster which is the actual key array, elements of three sub-clusters at same positions are XORed and addition of digits of number is done till single digit number is obtained. Thus, a key is ready. E.g. a single digit number is obtained as:

$$\begin{aligned} \text{Number} &= 46823 \\ &4+6+8+2+3=23 \\ &2+3=5 \end{aligned}$$

$$\text{Single digit number} = 5$$

## 2.2 Pixel Intensity Reformation

In this step, intensities of image are changed. In case of steganography, this step is must to keep the confidentiality of information. This step is further divided into three functions as:

- XORing METHOD: image pixels are XORed with 1's complement of cluster elements at the same position as that of pixel's row number.
- BITS ROTATED LEFT: value of each pixel is converted to its binary equivalent and is rotated to left by the element value units of cluster (element residing at the same position as that of pixel's row number will be taken). E.g. The rotation to left by 3 units of a number is done as:

$$\begin{aligned} \text{Old intensity} &= 59 \\ \text{Binary equivalent} &= 00111011 \\ \text{After rotation to left by 3 units} &= 11011001 \\ \text{New intensity} &= 217 \end{aligned}$$

- 1's COMPLEMENT OF SPECIFIED BITS METHOD: in this method, 1's complement of bits is taken, only of bits pertaining at even places in binary equivalent of pixel value. e.g.

$$\begin{aligned} \text{Old pixel value} &= 59 \\ \text{Binary equivalent} &= 00111011 \\ \text{1's complement at even places} &= 01101110 \\ \text{New pixel value} &= 110 \end{aligned}$$

## 2.3 Ikeda Mapping

The ikeda map is a discrete time dynamical system. This was proposed by ikeda as a paradigm of light going across a non-linear optical resonator (ring cavity containing a non-linear dielectric medium). This map is use to determine the saturation reactions of nonlinear dielectric medium [16]. This mapping is used to encrypt image by permutating the pixel values in an image. Suppose old pixel position  $(x_n, y_n)$ . New pixel position  $(x_{n+1}, y_{n+1})$  is obtained from ikeda mapping equations are:

$$x_{n+1} = 1 + u(x_n \cos t_n - y_n \sin t_n) \quad (1)$$

$$y_{n+1} = u(x_n \sin t_n + y_n \cos t_n) \quad (2)$$

Where,  $u$  is an ikeda parameter whose value lies from 0-1 and shows chaotic behaviour, and  $t_n$  is calculated as:

$$t_n = 0.4 - 6/1 + x_n^2 + y_n^2 \quad (3)$$

In the proposed algorithm, five different values of ikeda parameter 'u' are taken. These are:

$$u = 1, 0.85, 0.65, 0.45, 0.25$$

Values are exchanged between old and new pixel position. However, at certain new pixel positions which are beyond the image matrix at that point no change to row number is made, and always last column is taken.

## 2.4 Row-Row and Column-Column Fusion

In this step, individual rows are XORed (Exclusive OR) with other rows. The difference between two rows position taken for XORing is 20. E.g. let difference between two rows position be 3. Suppose a matrix of multiple rows and single column is taken as:

$$\begin{array}{l} \text{Old matrix} = \\ a \\ b \\ c \\ d \\ e \\ f \\ g \end{array}$$

After XORing two rows,

$$\begin{array}{l} \text{New matrix} = \\ a \oplus d \\ b \oplus e \\ c \oplus f \\ d \oplus g \\ e \\ f \\ g \end{array}$$

Now, individual columns are XORed with other columns. The difference between two columns position should have to be 20. E.g. if difference between two columns position be 3. And a matrix of single row and multiple columns are supposed as:

$$\begin{array}{l} \text{Old matrix} = \\ a \ b \ c \ d \ e \ f \ g \end{array}$$

After XORing two columns,

$$\begin{array}{l} \text{New matrix} = \\ a \oplus d \ b \oplus e \ c \oplus f \ d \oplus g \ e \ f \ g \end{array}$$

## 2.5 2-D Fast Fourier Transform

In this step, 2-D fast Fourier transform, swapping of blocks and logarithmic transform of each R G B layers of image is taken. To reduce the computations and time, fast Fourier transform is taken instead of discrete Fourier transform. A Fast Fourier Transform (FFT) is an efficient way to compute the discrete Fourier transform (DFT) and it's inverse. Fourier transform decompose an image into its sine and cosine components. Image is transformed from spatial domain to frequency domain, in which each particular frequency represents pixel intensity. Image in spatial and frequency domain are of same size [12]. 2-D discrete Fourier transform is given as:

$$F(u, v) = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) e^{-j2\pi(ux/M + vy/N)} \quad (4)$$

Where,  $F(u, v)$  is transformed image in frequency domain and  $f(x, y)$  is a digital image of size  $M \times N$  in spatial domain, and discrete variables  $u$  and  $v$  in the ranges,  $u=0,1,2,\dots,M-1$  and  $v=0,1,2,\dots,N-1$ . Now, divide the image is four equal blocks (as shown in fig. 1) and rearranges by swapping the first block with the third and the second block with the fourth block.

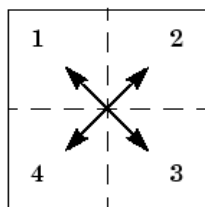


Fig. 1. Block swapping way.

The frequency domain image has a much greater range than the image in spatial domain. So, by logarithmic transformation dynamic range of an image can be compressed by replacing each pixel value with its natural logarithm value. The logarithmic mapping of 'q' to 'p' is given by:

$$p = c \log(1 + q) \tag{5}$$

Where, c is scaling constant and is chosen so that the maximum output value is 255 (providing an 8-bit format). That means if R is the value with the maximum magnitude in the input image, c is given by:

$$c = 255 / \log(1 + |R|) \tag{6}$$

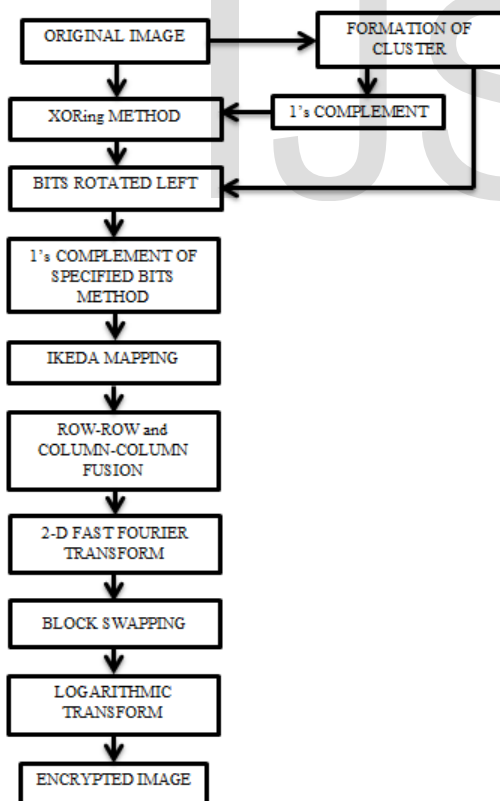


Fig. 2. Block diagram of Encryption algorithm

Same cluster and same scaling constant (in logarithmic transform) values are used for both encryption and decryption. Therefore, this algorithm is symmetric key cryptography.

### 3 DECRYPTIOM PROCESS

Decryption process is the reverse of encryption process, in this encrypted image is decrypted. As it is the symmetric key algorithm, so same cluster and same scaling constant values are used for decrypting images. In the proposed algorithm, loss-less decrypted image is obtained. The decryption process is as follows:

#### 3.1 Inverse 2-D Fast Fourier Transform

Firstly, inverse logarithmic transform is taken by same scaling constant values as used during encryption. Then, swapping of first block with third block and second block with the fourth block is done. Lastly, inverse 2-D fast Fourier Transform is taken. Digital image  $f(x,y)$  is obtained by taking inverse 2-D discrete Fourier transform of image in frequency domain  $F(u,v)$  as [12]:

$$f(x,y) = \frac{1}{MN} \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} F(u,v) e^{j2\pi(ux/M + vy/N)} \tag{7}$$

For  $x=0,1,2,\dots,M-1$  and  $y=0,1,2,\dots,N-1$ . Equation (4) and (7) constitute the 2-D discrete Fourier transform pair.

#### 3.2 ROW-ROW and COLUMN-COLUMN FUSION

In this firstly, column-column are XORed starting from last column having gap of 20 columns, then row-row are XORed starting from last row with gap of 20 between two rows.

#### 3.3 IKEDA MAPPING

Ikeda mapping equations are applied.

#### 3.4 PIXEL INTENSITY REFORMATION

Operations are applied in reverse order as:

- 1's complement of specified bits method.
- Bits are rotated to right by cluster element units of the same row number position.
- Xoring method: XORing of pixels with the 1's complement of cluster element (of same position) is done.



Fig. 3. (a)Original image, (b) Encrypted image (c) decrypted image.

### 4 SECURITY DEFINITIVE TESTS


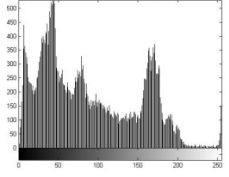

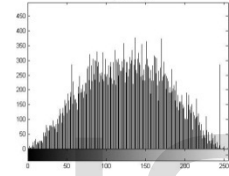

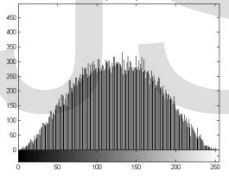

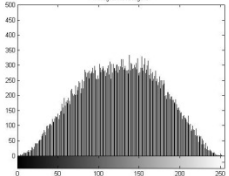
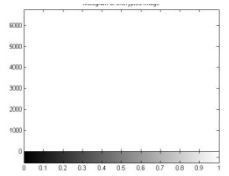

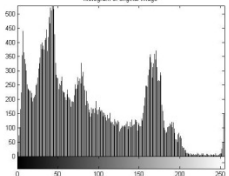
In the proposed algorithm, we neither get any preview of encrypted image nor histogram. Therefore, algorithm is strong enough to withstand various kinds of attacks like known-plain image attack, cipher image-only attack, chosen-cipher image attack, statistical attack and exhaustive key (brute force) at-

tacks. Statistical analysis has been performed for the proposed image cryptography algorithm on suraj.jpg image of  $188 \times 230$  pixels. Histogram, correlation coefficient, scatter plot, 3D plot and Information entropy is computed.

**4.1 Histogram of encrypted images:**

Histogram is a graph showing the number of pixels in an image at each different intensity value found in that image.

TABLE. 1. HISTOGRAMS AT VARIOUS STAGES.

Stages	Images	Histogram
Original image		
Encryption stage 1		
Encryption stage 2		
Encryption stage 3		
Encryption stage 4	--NO IMAGE PREVIEW--	
Decrypted image		

For an 8-bit grayscale image there are 256 different possible intensities, and so the histogram will graphically display 256 numbers showing the distribution of pixels amongst those grayscale values. The horizontal axis of the graph represents the grayscale values, while the vertical axis represents the number of pixels of that particular grayscale intensity. The histogram of original image and encrypted image should be totally different.

**4.2 Scatter plot and Correlation Coefficient:**

Scatter plots shows correlation between two pixels graphically. Here, Scatter plots has been plotted to show correlation between two horizontally adjacent pixels of original and encrypted image. Plain image shows strong positive correlation. Cipher (encrypted) image, shows no association (no correlation) [7].

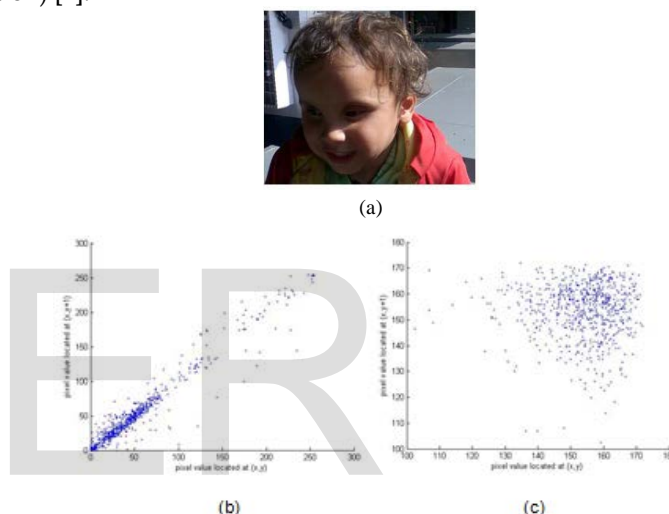


Fig. 4. (a) Original image, (b) Scatter plot of plain (original) image, (c) Scatter plot of cipher (encrypted) image.

*Correlation Coefficient*

Correlation Coefficient has been calculated by (4) that tell the amount of similarity between two images i.e. the input-encrypted images and original-decrypted images [7]. Its value ranges from -1 to 1. Zero correlation coefficient means there is no association between two images. 1 correlation coefficient means two images are same. -1 correlation coefficient means that two images are totally opposite. Same correlation coefficient value of original image with decrypted image depicts that lossless cryptography has taken place.

$$rho = \frac{\sum_m \sum_n (A_{mn} - A')(B_{mn} - B')}{\sqrt{(\sum_m \sum_n (A_{mn} - A')^2)(\sum_m \sum_n (B_{mn} - B')^2)}} \tag{8}$$

- Where, A: Original image
- B: Encrypted image
- A': mean of original image
- B': mean of encrypted image
- m: number of pixels in original image
- n: number of pixels in encrypted image

TABLE. 2. CORRELATION COEFFICIENT VALUES OF ORIGINAL IMAGES WITH ENCRYPTED AND DECRYPTED IMAGES.

Correlation Coefficient of original input image with :	
Encrypted image	-0.0022
Decrypted image	1

As the encryption stages increases , correlation coefficient values becomes closer to zero , means very less or almost no correlation between two images.

**4.3 3D Plot:**

A 3D plot is drawn for pixel position number, pixel values of original image and pixel value of encrypted and decrypted images. In fig 4 (a), plots shows the randomness between original and encrypted images pixel intensities lying at same position, means very less correlation. In fig 4 (b), plot shows the sequentially order points. In this algorithm, a lossless decrypted image is obtained. Thus, 3 D plot of original and decrypted image have high correlation among pixels of two images are clearly depicted.

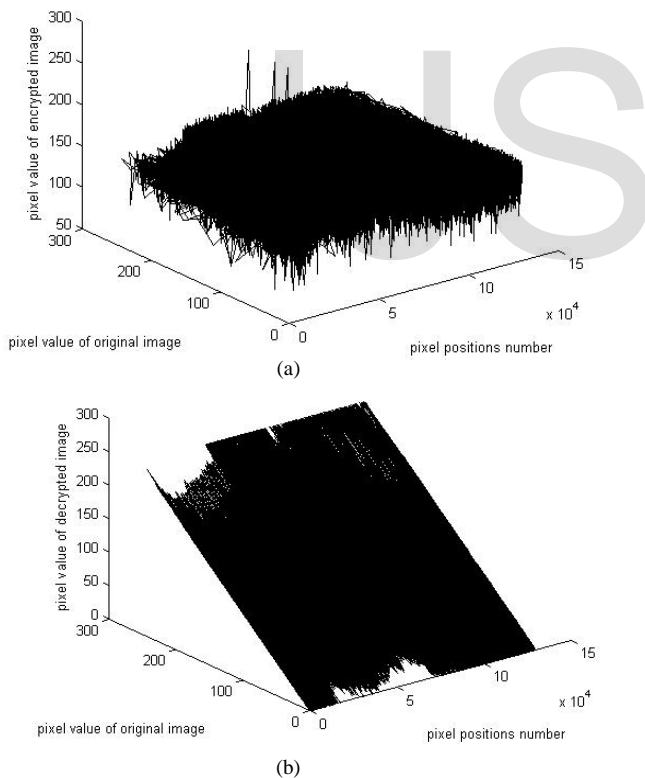


Fig. 5. (a) 3D plot for original image and encrypted image at their respective positions, (b) 3D plot for original image and decrypted image at their respective positions, of suraj.jpg image.

**4.4 Information Entropy Analysis:**

Information entropy is a statistical measure of randomness that can be used to characterize the texture of the input image. If entropy of encrypted image is less than entropy of plain image then image can be predicted and threatens its security.

However, when there is no variation in an image means any preview is not available, ultimately entropy is zero. Thus, becomes impossible for intruders to decrypt image. Entropy  $H(m)$  of a message source  $m$ , with  $P(m_i)$  represents the probability of symbol  $m_i$  and  $N$  is the total number of pixels in image and the entropy is expressed in bits can be calculated as [4,6]:

$$H(m) = \sum_{i=1}^{N-1} p(m_i) \log_2(1/p(m_i)) \text{ bits} \quad (9)$$

TABLE. 3. INFORMATION ENTROPY VALUES OF ORIGINAL, ENCRYPTED AND DECRYPTED IMAGES.

Information Entropy	
Original image	7.6807
Encrypted image	0
Decrypted image	7.6807

**5 CONCLUSION**

The algorithm is composed pixel position alteration, pixel intensity surrogation and visually changed method of encryption. This algorithm works well for color images, producing highly secure blank encrypted images (no preview available) and produces lossless decrypted images. Thus, maintaining the confidentiality of images. The proposed cryptographic algorithm, encryption is accomplished by four stages after the formation of cluster, a key array. Ikeda mapping is done at five different values instead of single value and 2-D fast Fourier transform of image is taken to make images more secure. Algorithm can be used for any type of images (secret, medical, aerial) encryption as well as for text encryption. Various security definitive tests are done, from which we conclude that obtain encrypted image has no histogram, no entropy.

**REFERENCES**

- [1] Ismet Ozturk and Ibrahim Sogukpinaar, "Analysis and Comparison of Image Encryption Algorithms", World Academy of Science, Engineering and Technology 3 2007 ,page no: 562-566.
- [2] Sara Tedmori and Nijad Al-Najwadi , "Lossless image Cryptography Algorithm Based on Discrete Cosine Transform", The International Arab journal of Information Technology , Vol. 9 ,No.5 ,September 2012, page no : 471-478.
- [3] Somdip Dey," SD-AEI: An Advanced Encryption Technique For Images" , An Advanced Combined Encryption Technique For Encrypting Images Using Randomized Byte Manipulation , pp. 68-73 , 2012.
- [4] Suli Wu and Yang Zhang , " A Novel Encryption Algorithm based on Shifting and Exchanging Rule of Bi-column Bi-row Circular Queue" ,International Conference on Computer -Science and Software Engineering , pp. 841-844 , 2008.
- [5] Xiaojun Tong and Minggen Cui "A Novel Image Encryption Scheme Based On Feedback and 3D Baker", 2008 IEEE.
- [6] Alireza Jolfaei and Abdolrasoul Mirghadri , "A novel image encryption scheme using pixel shuffler and A5/1", International Conference on Artificial Intelligence and Computational Intelligence, pp. 369-373 , 2010.

- [7] Sahar Mazloom and Amir Masud Eftekhari - Moghadam , " Color Image Cryptosystem using Chaotic Maps", 2011 IEEE.
- [8] Sesha Pallavi Indrakanti and P.S.Avadhani, "Permutation based Image Encryption Technique", International Journal of Computer Applications (0975 - 8887) Volume 28- No.8, 2011.
- [9] Somdip Dey, "SD-AEI: An Advanced Encryption Technique For Images" , An Advanced Combined Encryption Technique For Encrypting Images Using Randomized Byte Manipulation , pp. 68-73 , 2012.
- [10] Somdip Dey , " An Image Encryption Method: SD-Advanced Image Encryption Standard: SD-AIES " , International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(2): 82-88 .
- [11] Komal D Patel and Sonal Belani "image encryption using different techniques : A review" , International Journal of Emerging Technology and Advanced Engineering , ISSN 2250-2459, Volume 1, Issue 1, November 2011 ,pp. 30-34.
- [12] Rafael C.Gonzalez and Richard E.Woods , "Image Processing", Pearson, 2011.
- [13] Keerti Kushwaha and Sini Sibin, " PROPOSED MODEL OF IMAGE CRYPTOGRAPHY (A DESIGNING APPROACH FOR IMAGES SECURITY)", International Journal of Emerging Technology and advanced engineering, ISSN 2250-2459, ISO 9001:2008 certified journal, Volume 3, Issue 1, January 2013 , Page no : 144-149.
- [14] Hiral Rathod , Mahendra Singh Sisodia, and Sanjay Kumar Sharma, "A REVIEW AND COMPARATIVE STUDY OF BLOCK BASED SYMMETRIC TRANSFORMATION ALGORITHM FOR IMAGE ENCRYPTION", International Journal of computer technology and electronics engineering (IJCTEE) Volume 1, issue 2, ISSN 2249-6343 ,page no : 23-30.
- [15] Yaobin Mao and Guanrong chen, "CHAOS-BASED IMAGE ENCRYPTION".
- [16] K.Ikeda, Multiple-valued Stationary State and its Instability of the Transmitted Light by a Ring Cavity System, Opt. Commun. 30 257-261 (1979); K. Ikeda, H. Daido and O. Akimoto, Optical Turbulence: Chaotic Behavior of Transmitted Light from a Ring Cavity, Phys. Rev. Lett. 45, 709-712 (1980).
- [17] Behrouz A. Forouzan, 'Data Communication and Networking', Genuine Tata McGraw-Hill 2nd edition.
- [18] Taranjit Kaur and Reecha Sharma, "TJ-ACA: An Advanced Cryptographic Algorithm for Color Images using Ikeda Mapping", International Journal of Computer Trends and Technology (IJCTT) - volume4 Issue5-May 2013 , page no: 1295-1300.
- [19] Taranjit Kaur and Reecha Sharma, "Security Definitive Parameters for Image Encryption Techniques", International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 5, May 2013, page no: 109-112.