TJ-ACA: An Advanced Cryptographic Algorithm for Color Images using Ikeda Mapping

Taranjit Kaur[#1], Reecha Sharma[#2]

[1#]*M.tech Student, UCoE, Punjabi University, Patiala, Punjab, India*
[2#]*Assistant Professor, UCoE, Punjabi University, Patiala, Punjab, India*

***ABSTRACT*— Presently, cryptography of images is of high concern due to highly confidential information contained in it. Image encryption is difficult as compared to text encryption because of high correlation among pixels and bulk information capacity. A newly proposed algorithm based on symmetric key algorithm, TJ-ACA, an advanced cryptographic algorithm will make use of pixel position alteration, and pixel intensity surrogation through which a visually changed image i.e. encrypted image is obtained. In this algorithm, ikeda mapping and various methods are used to get highly secure image. To increase the security ikeda mapping is done at five different values instead of single value. This proposed algorithm is applicable for color images and also for images on which steganography has been applied and by this method we get lossless decrypted image. This method resists Brute Force attack. TJ-ACA can be applied to all sizes images which can be used in medical, aerial application.**

Keywords – Ikeda mapping, image Cryptography, pixel intensity surrogation, statistical analysis.

I. INTRODUCTION

Day-by-day, technology is increasing leading to many elevations in communication, but on the other hand many security issues are also there. Because with the growing technology, attackers also keep on developing new techniques to crack the encryption techniques. So timely, there is great need to develop new cryptographic methods to ensure that the confidentiality of original information is at no threat. Even in medical applications and defence systems security of information is prior. Any leakage of information proves to be highly disastrous.

Cryptography is a process of transforming readable information to non-readable form because the information is sent over insecure channel. 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]. The image encryption 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.

These two algorithms play a crucial role in steganography.

- In visually changed based algorithm, encrypted image is made so non-readable that human eye can't decrypt any part of image.

The image encryption algorithms can also be classified: (i) lossy algorithm, where decrypted image contains small amount of distortion. This decrypted image is used in applications where fine details in image are not required, (ii) lossless algorithm, where high image quality and fine details in image is required [2]. Features of image encryption may be summarized as follows:

- Bulk capacity generally makes encrypted image data week enough to attacks via cryptanalysis. Based on this, the user can gain enough cipher image samples even from a single image for statistical analysis.
- Due to high redundancy and adjacent pixels of image having similar grayscale intensities or image blocks have similar patterns, which usually embed the image with certain patterns result in secret leakage.
- Due to strong correlation among the adjacent pixels of image data, it makes fast data shuffling quite difficult. The ciphered image should not provide any information about the original image. To fulfil this requirement the ciphered image should be presented as randomly as possible.

- In almost every case, the data is compressed before it is stored or transmitted due to huge amount of image data and their very high redundancy. That is why security requirements in the data compression system are a very attractive approach. The main challenge is how to ensure reasonable security while reducing the computational cost without degrading the compression performance [15].

This paper is organised as in section I, general guidelines related to cryptography and literature survey is discussed. In section II, proposed algorithm is discussed. In section III, decryption process is defined. In section IV, security analyses of results are discussed. In section V, conclusion and future scope is discussed.

Suli Wu and Yang Zhang [4] proposed an algorithm based on Shifting and Exchanging Rule of Bi-column Bi-row Circular Queue which removes the defect of regularity .Xiaojun Tong and Minggen Cui [5] proposed an algorithm based on new compound chaos by selecting one of the two one-dimensional chaotic functions randomly. Alireza Jolfaei and Abdolrasoul Mirghadri [6] proposed an algorithm based on combination of pixel shuffling and A5/1 algorithm , which uses external key for the chaotic henon and Baker's map. Sahar Mazloom and Amir Masud Eftekhari – Moghadam [7] presented an Algorithm composed of new symmetric image cipher based on confusion –diffusion architecture for color images by chaotic 2D standard map and 1D logistic map. In 2011, Sesha Pallavi Indrakanti andP.S.Avadhani [8] proposed an algorithm compose of three steps: image encryption , key generation phase , identification process based on random pixel permutation with the motivation to maintain the quality of the image. Somdip Dey [9], [10] has proposed many cryptographic methods for image encryption.

In this paper, the proposed algorithm is symmetric key algorithm which uses same cluster at both sender and receiver side to encrypt and decrypt images.

The steps used in the 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.

The basic idea for the step1, 2 is taken from Somdip Dey [3] to produce a key cluster and bits rotation with modifications.

II. PROPOSED ENCRYPTION ALGORITHM

In the proposed algorithm, firstly cluster is made which is further used in the encryption stages.

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 RGB 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 RGB layers and are placed in sub-cluster at the respective 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 to their further uses. E.g. a single digit number is obtained as:

Number = 54786
5+4+7+8+6=30
3+0=3
single digit number = 3

1) 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 position same 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 position of pixel's row number will be taken). E.g. let "abcdefgh" is the binary equivalent of pixel intensity and 5 is the element of cluster at the same row number as that of pixel. The rotation to left is done as:
  Old intensity = a b c d e f g h
  After rotation to left by 5 units,
  New intensity = f g h a b c d e
- *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.
  Old pixel value = 135
  Binary equivalent = 10000111
  1's complement at even places = 11010010
  New pixel value = 210

2) 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 for encryption to permutate 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 doffing equations as A 2D real equations of ikeda map are:

$$x_{n+1} = 1 + u(x_n cost_n - y_n sint_n) \quad (1)$$
$$y_{n+1} = u(x_n sint_n + y_n cost_n) \quad (2)$$

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

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

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.

3) ROW-ROW and COLUMN-COLUMN FUSION

In this step, individual rows are XORed with other rows. The difference between two rows position taken for XORing is 20. E.g. let difference between two rows position be 2. Suppose a matrix of multiple rows and single column I staken as:

Old matrix =
a
b
c
d
e
f
g

After XORing two rows,

New matrix =
a⊕c
b⊕d
c⊕e
d⊕f
e⊕g
f
g

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 2. And a matrix of single row and multiple columns are supposed as :

Old matrix =
a b c d e f g

After XORing two columns,

New matrix =
a⊕c b⊕d c⊕e d⊕f e⊕g f g

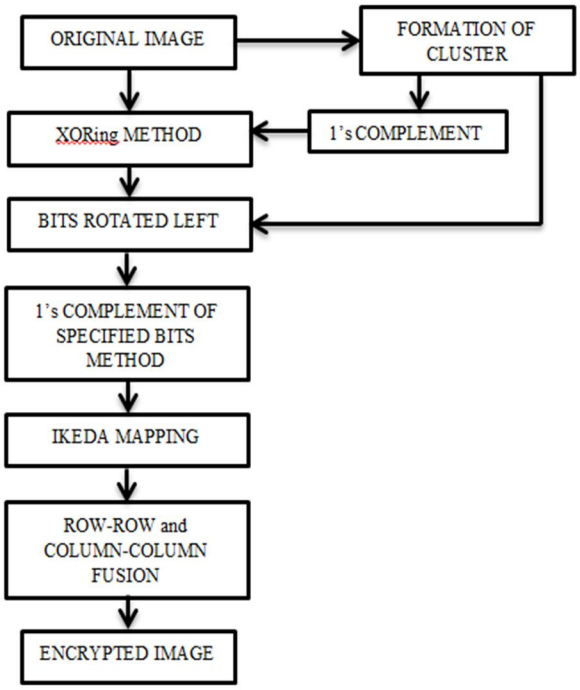


Fig. 1. Block diagram of Encryption algorithm

Cluster is concatenated with the encrypted image and is send over communication channel. Here, a drawback occurs of increase in bandwidth for communication.

III. DECRYPTION 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 is used for decrypting images. At receiver's side, cluster is extracted from the received image and the left image is used for the decryption process. In the proposed algorithm, lossless image is obtained. The decryption process is as follows:

1) 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.

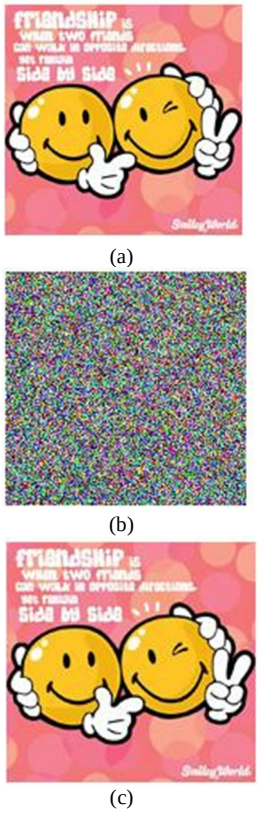
2) IKEDA MAPPING

Ikeda equations are applied.

3) 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.



(a) (b) (c)

Fig. 2. (a)Original image, (b) Encrypted image , (c)Decrypted image.

IV. SECURITY ANALYSIS

The proposed algorithm is strong enough to withstand various kinds of well-known attacks such as known-plain image attack, cipher image-only attack, chosen-cipher image attack , statistical attack and exhaustive key (brute force)attacks. Statistical analysis has been performed for the proposed image cryptography algorithm on suji.jpg image of 450 X 210 pixels. Histogram of encrypted images at various encryption stages, correlation coefficients of original image with respect to encrypted image and of original image with respect to decrypted image and scatter plot of plain image and cipher image is plotted [7]. A 3D plot is drawn for pixel position number, pixel values of original image and pixel value of encrypted image. Information entropy for original, encrypted and decrypted image is calculated.

1. Histogram of encrypted images:

Histograms are the graphs which show pixels of each color intensity level are distributed in graph. The histogram of original image and encrypted image should be totally different. So that intruder's do not get any knowledge about the original image. Image histogram is same for pixel position alteration process but it totally differ, if values of pixels are changed.

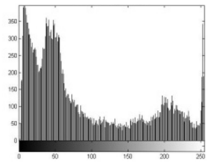
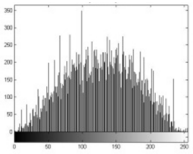
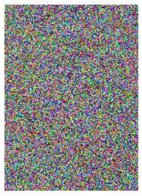
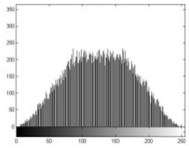
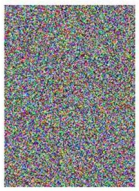
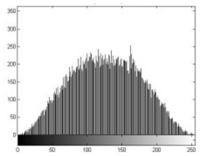
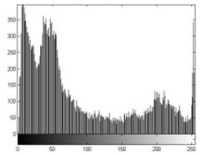
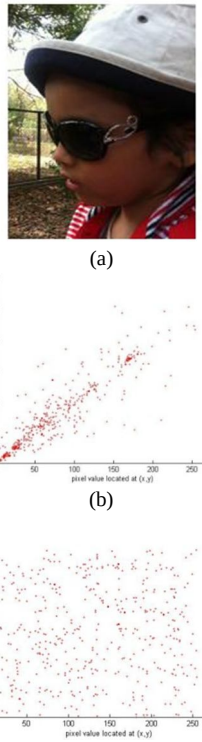
Stages	Images	Histogram
Original image		
Encryption stage 1		
Encryption stage 2		
Encryption stage 3		
Decrypted image		

Table. 1. Histograms at various stages.

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 perfect positive correlation. Cipher image, shows almost zero or near to zero correlation means no correlation.



(a)

(b)

(c)

Fig. 3. (a) Original image, (b) Scatter plot of plain(original) image ,(c) Scatter plot of cipher (encrypted) image.

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. Its value ranges from -1 to 1. Zero correlation coefficient means there is no relationship between two images. Same correlation coefficient value of original image with decrypted image shows that lossless cryptography has taken place.

$$rho = \frac{\sum_m \sum_n (A_{mn} - A')(B_{mn} - B')}{\sqrt{(\sum_m \sum_n (A_{mn} - A')^2)(\sum_m \sum_n (B_{mn} - B')^2)}} \quad (4)$$

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

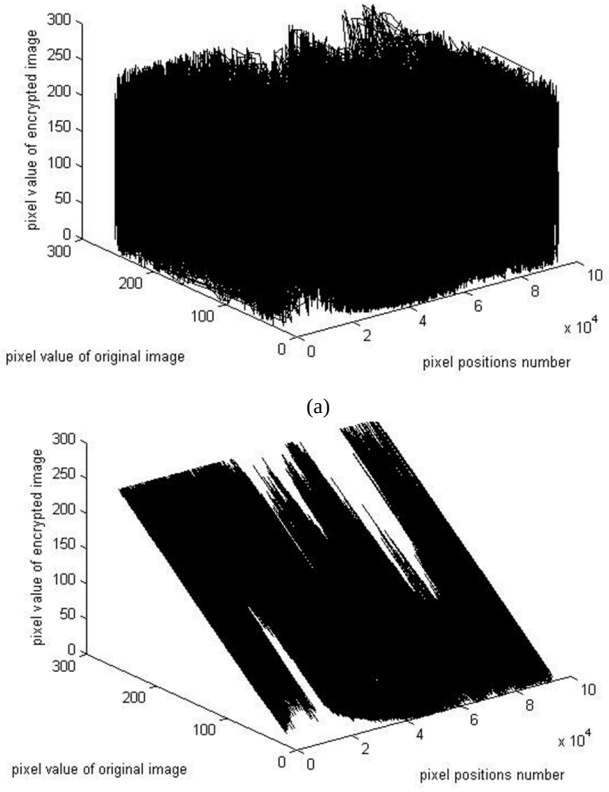
Correlation Coefficient of original input image with :	
Encrypted image	7.1515e-004 = 0.00071515
Decrypted image	1

Table. 2. Correlation coefficient values between original images and encrypted and decrypted images .

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

3. 3D Plot:

A 3D plot is drawn for pixel position number, pixel values of original image and pixel value of encrypted image. In fig 4 (a), plots shows the randomness in the encrypted image, as the pixels points are distributed all over the plot without any sequence. This also shows that there are good enough variations between pixel intensities of original and encrypted image 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.



(a)

(b)

Fig. 4. (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 suji.jpg image.

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. 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]:

$$H(m) = \sum_{i=1}^{N-1} p(m_i) log_2 \frac{1}{p(m_i)} \quad bits \qquad (5)$$

Information Entropy	
Original image	7.6344
Encrypted image	7.9883
Decrypted image	7.6344

Table. 3. Information Entropy values of original, encrypted and decrypted images.

V. CONCLUSION AND FUTURE SCOPE

In the proposed cryptographic algorithm, encryption is accomplished by three stages after the formation of cluster, a key array. The algorithm is derived by keeping in mind the pixel position alteration, pixel intensity surrogation and visually changed method of encryption. This algorithm works well for color images, producing highly secure encrypted images and produces lossless decrypted images. Thus maintaining the confidentiality of images. To increase the security ikeda mapping is done at five different values instead of single value. Algorithm can be used for any type of images (secret, medical, aerial) encryption as well as for text encryption. A drawback is there of increase in bandwidth for communication. Various statistical analysis are done to calculates its quantative values. The algorithm TJ-ACA can be further extended by doing more work on pixel position alteration and pixel intensity surrogation encryption methods.

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 Sibu, " 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).