*I.J. Image, Graphics and Signal Processing,* **2012, 2, 16-22**
Published Online March 2012 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijigsp.2012.02.03

# A Technique for Image Encryption with Combination of Pixel Rearrangement Scheme Based On Sorting Group-Wise Of RGB Values and Explosive Inter-Pixel Displacement

Amnesh Goel
Amity School Of Engineering & Technology, Amity University, Noida (U.P.), India
Email : amneshgoel7@gmail.com

Nidhi Chandra
Amity School Of Engineering & Technology, Amity University, Noida (U.P.), India
Email : srivastavanidhi8@gmail.com

*Abstract* - **Encryption is used to prevent data from unauthorized access and with the appalling headway in network technology seen in the past decade; it has become the need of time to encrypt the images before sending over open network. Though researchers has proposed contrastive methods to encrypt images but correlation between pixels RGB value play a imperative part to guess for original image. So, here we introduce a new image encryption method which first rearranges the pixels within image on basis of RGB values and then forward intervening image for encryption. Experimentally it has shown that pixel rearrangement is enough from image encryption point of view but to send image over open network; inter-pixel displacement algorithm is applied to dispense more armament to image before transmission.**

*Index Terms :* **RGB, Image Encryption, Rearrangement, Inter-Pixel, correlation, sorting.**

## I. INTRODUCTION

As the communication network usage has increased due to its low cost and high availability, encryption methods are required to encrypt the information before sending it to open network [1]. Looking towards the stealing of data from open network and usage of that data in non-social manner, it is the need of time to prevent the data from unauthorized access during the flow of data over network. High network bandwidth at low cost avow users to send multimedia content over network which can subsist of textual data, images, videos etc. and here the need of encryption comes into picture. Mostly images are vastly used in today's world to represent information in various domains varying from corporate world, health care, document organization, military operations etc.

Images are widely used for authorization propose to differentiate between authorized and unauthorized users. For this propose the organization keeps the recorded images into databases. Although different database companies all already providing their security control but relying on database security is not enough. Hence, need of image encryptions comes into picture to store images after encrypting them. Not only the authorization domain is using database to store images but also it is better to scan historical sign documents, agreements, and other similar kind of documents which are usually hard to keep safe for further long period of time. In this way, image encryption domain is spreading its roots in most of fields with the advancement in technology.

Image encryption mechanism should indemnify that the cipher image generated after encryption process can only convert into the plain image by providing the key which is used in encryption and on receiver end, the receiver should be able to convert cipher image into plain image without loss of information. Looking on the network usage in day to day life, it has become the need of time to encapsulate image encryption process in the transmission process itself so that all images which will flow over network are encrypted in nature and accordingly image decryption process should encapsulate at the receiver end before taking image into actual use.

Correlation between neighboring pixel values in the image makes the image decryption process or guessing of plain image from cipher image bit easy. As different types of data have independent characteristics like data replica, bulk data capacity and high correlation between pixel values; the image encryption methods should be different from textual encryption and therefore it is difficult to follow the traditional encryption methods for images. So, it is important to reduce the correlation between pixels and increase entropy value before image transmission over network and in order to reduce correlation, we are introducing pixel rearrangement scheme before encryption.

This paper is organized into 7 sections. Section 2 discusses the related papers on the title. Section 3 describes the proposed methodology while section 4 explains the architecture of proposed method. Section 5 describes the algorithm which is proposed in this paper and section 6 shows the experimental results based on the algorithm proposed. Section 7 focus on the further scope of work in this area.

## II. Related Work

*Block Encryption*

Block encryption methods are based on the encryption of image block by block [2]. Image is first divided into pre-calculated size of blocks and then theses blocks are encrypted within its boundaries one at a time. Block encryption methods also helps to reduce the correlation property of pixel and increase entropy value but calculation of block size differs from method to method.

*Secure Image Data by Double encryption [3]*

Jayant Kushwaha and Bhola Nath Roy proposed image encryption technique where encryption is done by first doing at pixel level and then at block level. This paper focused towards reducing the correlation between pixel values. They used public key cryptography method for encryption; pixel values are encrypted using their position and then blocks were encrypted by using the public key of receiver. Although, they could not show any experimental result for this approach and pixel encryption scheme was also not explained.

*Image Encryption Using Block-Based Transformation Algorithm [4]*

Mohammad Ali Bani Younes and Aman Jantan proposed image encryption technique where encryption is done by first at block level and then using Blowfish method to encrypt image. According to this paper, they first divided the whole image into number of blocks and then they did rearrangement of blocks within image before applying Blowfish method. This paper also tried to reduce correlation between pixel values and they used key scheme for rearrangement of blocks within image. This key need to send to receiver to get the plain image back.

*An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption [5]*

Mohammad Ali Bani Younes and Aman Jantan proposed image encryption technique by first dividing the image into 4 x 4 pixel block and then these blocks were rearranged into a permuted image using a combination of permutation technique. This permuted image later on encrypted using the RijnDael Algorithm. This paper also tried to reduce correlation between pixel values by rearrangement of blocks within image.

*A New Image Encryption Approach Using Block Based Transformation Algorithm [6]*

Aditee Gautam, Meenakshi Panwar and Dr.P.R Gupta proposed image encryption technique by diving image into blocks and then encryption was performed. They did not keep fix block size and gave result with variable block sizes but they were unable to explain the procedure of block rearrangement. This block rearrangement was chosen to reduce the correlation property of pixel. For the encryption purpose they used Blowfish method.

*Image Encryption based on Inter Pixel Displacement of RGB Values inside Custom Slices [7]*

This paper was proposed which was further extension of work of Inter-Pixel displacement of the RGB attributes of a Pixel by making the 4 slices and shuffling of those slices before encryption. Slices were made from the center of image and these four slices were diagonally inter exchanged before doing actual image encryption to reduce the correlation between pixels but making slices of image from the center was not that effective to reduce correlation and block size should be small. By taking the slices from the center of image divides the image into only 4 blocks and more blocks can be generate by divided image into more smaller parts. Although shuffling of slices was a confusing feature which was proposed under this algorithm.

*Stream Encryption*

Steam encryption method is works on bit level or byte level rather than at block level. These methods generate infinite cryptographic key streams to encrypt one bit or one byte in one slot. Different chaotic papers [8] [9] were used this method for image encryption.

*A New Chaotic Key-Based Design for Image Encryption and Decryption [10]*

Jui-Cheng and Jiun-In Guo proposed image encryption decryption algorithm in which gray level of each pixel is XORed or XNORed bit-by-bit to one of the two predetermined keys. This paper kept focus on three main factors i.e. high security, low computation and no distortion.

*Image Encryption Based on Explosive Inter Pixel Displacement of the RGB Attribute of a Pixel [11]*

In this method focus was more on the inter pixel displacement rather than just manipulation of pixel bits value and shifting of pixel completely from its position to new position. RGB value of pixel was untouched in this method, but R value of pixel jumps to another location horizontally and vertically same as in chaotic method. In the similar manner, G and B values of pixel

also shift from its position in both direction and jumping factor depends on confidential key. Number of horizontal and vertical manipulation of values depend on key and gap between pixel is also defines from key. So, key value increases in this case because it contains dual value, one for gap between pixel and second for number of horizontal and vertical movement order. Hence, in this method the RGB value of pixel goes to different positions which is most difficult for anyone to retrieve original image without knowing the key.

Considering the inter pixel displacement method which talks about the inter pixel displacement of RGB values in circular manner in both horizontal and vertical direction. Circular shift is performed in such a way that loss of RGB values is 0. For example is image is of dimension 1600*1200 or of any dimension and key value is 50 for R then first R value will be in 51 column and 2nd R value will be in 52 column and so on so forth. Similarly, for 1551 column the R value will jump into first column of image. Same circular fashion repeats with G and B but with different key value and same pattern repeats in vertical shift. But drawback of this method is continuous working of algorithm on whole image in one go. Hence, in improvement of this method, slicing scheme was introduced where one image is divided into few slices and then algorithm was applied which lead to more confusing property in encryption method.

## III. Proposed Methodology

Proposed image encryption method completes in two steps i.e. pixel rearrangement within image using sorting method and in second step image is encrypted using inter- pixel displacement algorithm. For the pixel rearrangement, all the pixels of image are first stored in an array where array sorting is performed. By the sorting method, all the pixels are get compound sort in ascending order of any value i.e. R, G, B and the top we gets 0, 0, 0 pixel if present and 255, 255, 255 in the last position if present. Precedence of sorting is independent of value i.e. R, G, B because the motivation for sorting was reducing the correlation between pixel values. This correlation method by arranging the pixel values in sorting order is better than block shifting as discussed in earlier section.

This array which consists of sorted pixel on basis of RGB value is back transferred to form an image of original length and width size which will then have pixels in ascending order starting from 0, 0, 0 to 255, 255, 255 (both pixel are subject to present in plain image). Now, this image is used for the encryption purpose using the explosive inter-pixel displacement algorithm which has already discussed.

## IV. Proposed Architecture

Architecture for the proposed system is shown in fig 1.

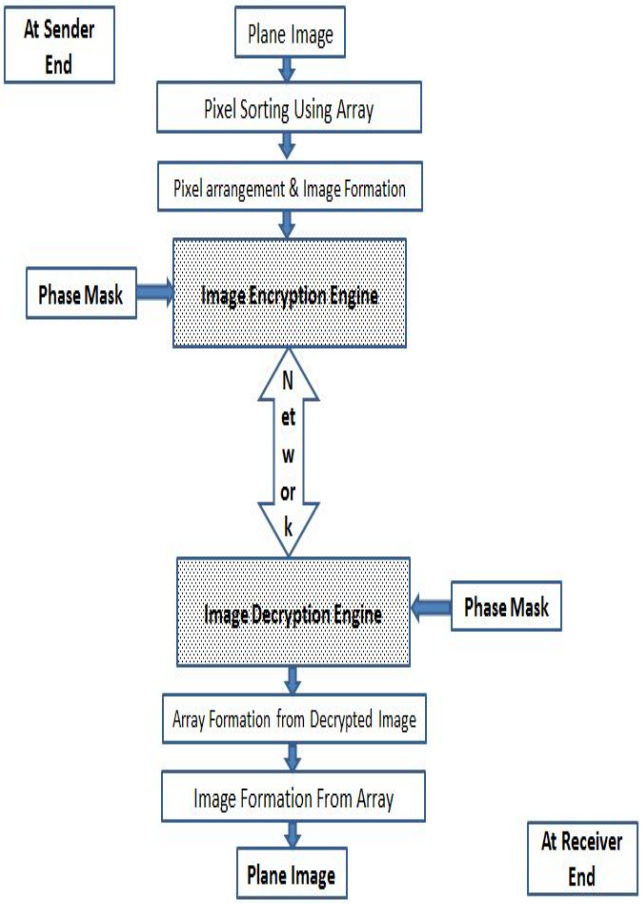



Figure 1 Architecture of proposed method for image encryption.

Architecture shows the image encryption method proposed in this paper. Plain image is first sorted using an array then this array is used to form an intermediate image which is passed for image encryption engine where inter-pixel algorithm is applied to convert a plain image into cipher image. Reverse of this procedure is shown at the receiver end.

## V. Algorithm

***Pixel_ReArrangement()***

1 Start
2 img = input plain image.
3 rows, cols = size of img.
4 create array of (rows*cols , 5)
5 transfer img pixel values into array for complete image
    array(,1)=R value
    array(,2)=G value
    array(,3)=B value
    array(,4)=x position
    array(,5)= y position

6 sort this array
7 img = form an image using this array
8 Invoke ImageEncryption(img, rows, cols)
9 End

Pixel rearrangement algorithm will be responsible for reducing the correlation between pixel values by arranging pixels in a sorted manner within image by using their RGB values and experimental result proves the reduced correlation. To perform this arrangement of pixels, this algorithm filches an image and enumerates its length, width and from its length and width; it calculates the total no of pixels in image. Once we know the number of pixels in image, then an array is created of same length equal to no of pixels in image and then each row of array is assigned with the each pixel of image. When all pixels of image will get shift to array then this array is sorted and this is compound sort which makes further sorting at group-wise; means if 20 pixels starts from 120 value for R then all these pixels will be grouped together and further if these pixels have same value of G and B then groups will made on G and B also.

When these pixels will be get sorted in an array then this array is used for forming image again in sequence starting from first pixel to last and by doing this, 0, 0, 0 pixel value will be occupy first pixel (1, 1) in new image and pixel value 255, 255, 255 will get last pixel location in image (pixel 0, 0, 0 and 255, 255, 255 are subject to available in original image).

***ImageEncryption (e,x,y)***

1 Start
2 Supply PM[ ] array
3 Initialize Counter=1, initJump= Any Arbitrary Integer
4 Loop while PM[counter] is not NULL
  if PM[counter]=0
    Invoke HORIZONTAL_Shift(e,x,y,αr[counter], αg[counter], αb[counter])
    Increment counter by 1.
  Endif
  if PM[counter] = 1
    Invoke VERTICAL_Shift(e,x,y,αr[counter], αg[counter], αb[counter])
    Increment counter by 1.
  Endif
 Endloop
5 End

The ImageEncryption() method takes image with its coordinate limits and started performing encryption process by deploying the shifting of R G B components among the pixels. The PM[] array called as Shift pattern mask array consists of binary digits 1's and 0's. The length of this array is the total number of vertical and horizontal shifts done in the encryption process. Each 1 triggers a circular vertical shift and a 0 triggers the invocation of circular horizontal shift. The PM[ ] can be made a part of the key or else supplied separately. With the increase in the length of the mask, the security as well as running time for encryption process increases linearly.

The ImageEncryption() method uses another set of arrays namely αr[counter], αg[counter], αb[counter] which holds in it the different integers for R, G and B component shifts. This ensures that in each successive row, the displacement of a component doesn't remain a constant. Else it will result in the simple circular shift of the entire color component and hence it becomes a favorable condition for the cryptanalyst since guessing the shift of a single row is enough to know by how much are the other rows also shifted. The same entity is also used in the HORIZONTAL_Shift function also to provide a wider scattering of the R G B components from its native pixel position.

***VERTICAL_Shift(e,x,y, αr[counter], αg[counter], αb[counter])***

1 Start
2 Input image with its coordinate limits x1 to x2, y1 to y2.
3 αr[counter], αg[counter], αb[counter]
4 ΔR= initJump + αr[counter]
5 ΔG= initJump + αg[counter]
6 ΔB= initJump + αb[counter]
7 Loop and Repeat steps for ColC = x1 to ColC= x2
  Do Circular Vertical Shift of R values at ColCth column by ΔR pixels
  Do Circular Vertical Shift of G values at ColCth column by ΔG pixels
  Do Circular Vertical Shift of B values at ColCth column by ΔB pixels
  ΔR = ΔR + αr[counter]
  ΔG = ΔG + αg[counter]
  ΔB = ΔB + αb[counter]
 Endloop
8 Return

***HORIZONTAL_Shift(e,x,y,αr[counter], αg[counter], αb[counter])***

1 Start
2 Input image with its coordinate limits x0 to xmax and y0 to ymax.

3 αr[counter], αg[counter], αb[counter]
4 ΔR= initJump + αr[counter]
5 ΔG= initJump+ αg[counter]
6 ΔB= initJump + αb[counter]
7 Loop and Repeat steps for RowC = y1 to RowC= y2
Do Circular Horizontal Shift of R values at RowCth row by ΔR pixels
Do Circular Horizontal Shift of G values at RowCth row by ΔG pixels
Do Circular Horizontal Shift of B values at RowCth row by ΔB pixels
ΔR = ΔR + αr[counter]
ΔG = ΔG + αg[counter]
ΔB = ΔB + αb[counter]
Endloop
8 Return

## VI. Experimental Result & Histogram Analysis

For the experimental purpose this algorithm is executed in Matlab 6.0.1 software on three different images of variable pixel sizes and following results were obtained by running this algorithm.

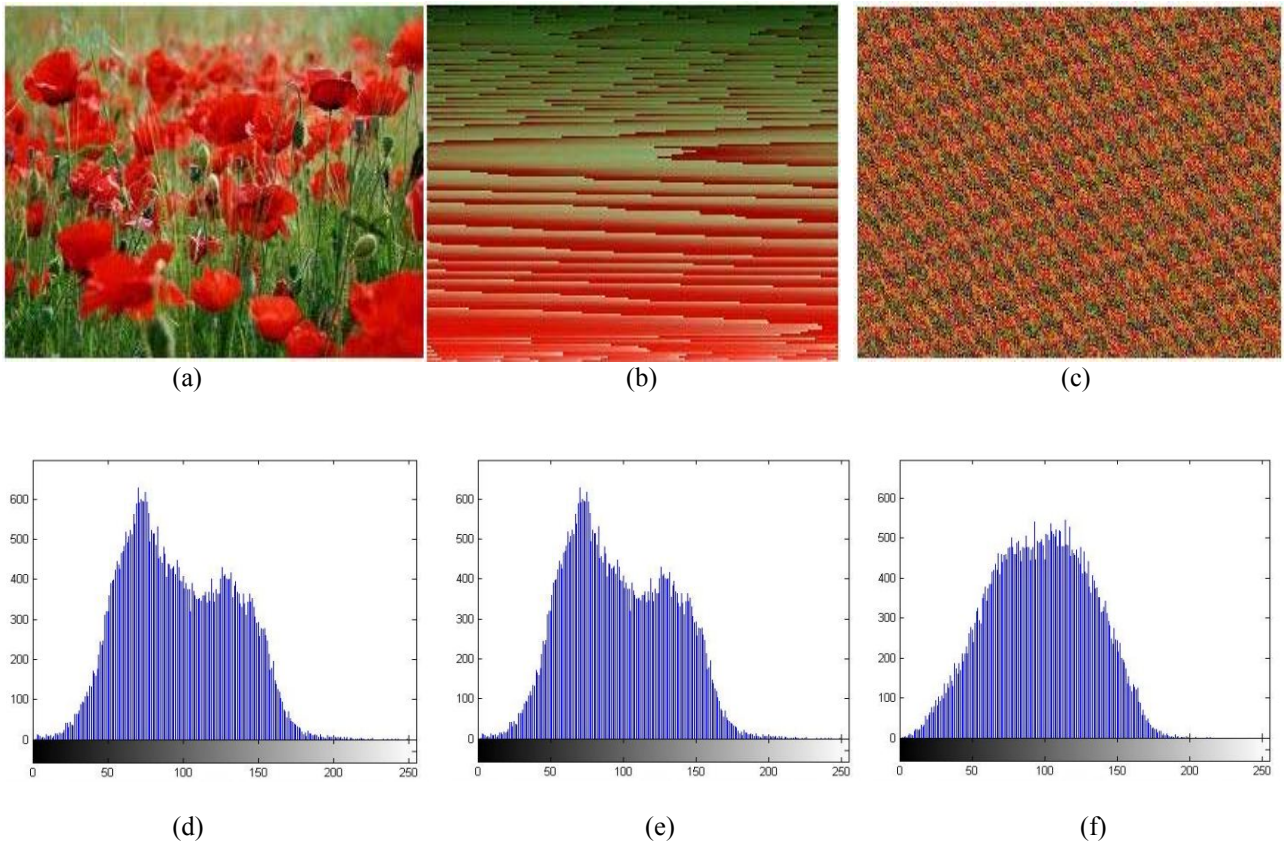
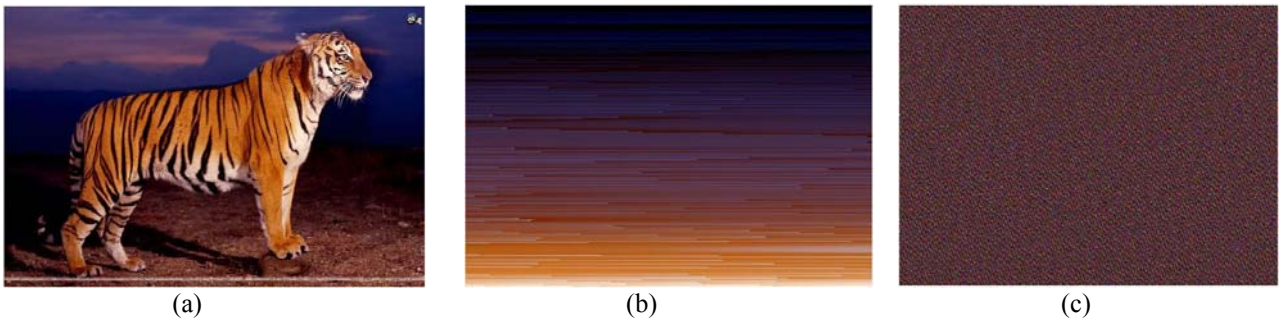



Figure 2 (a) Plain image size of 284 x 117 (b) Image obtain after pixel rearrangement (c) Cipher Image (d) Histogram of plain image (e) Histogram of image obtain after pixel rearrangement and (f) Histogram of Cipher image.



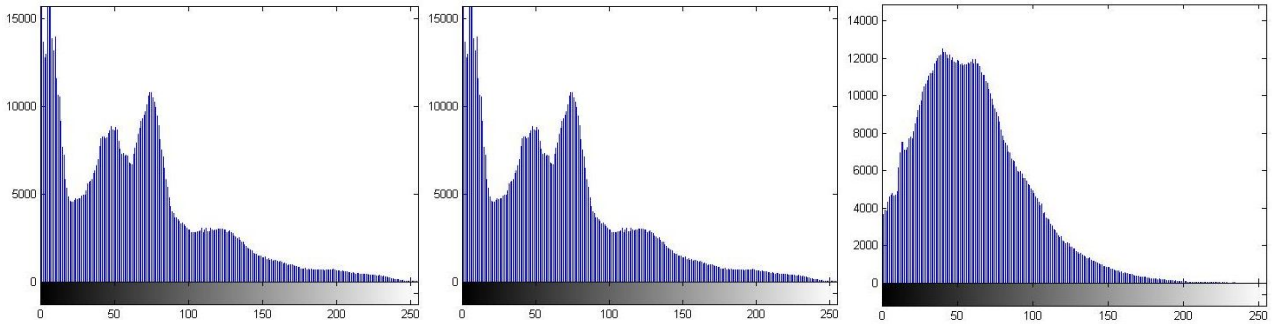



Figure 3 (a) Plain image size of 1200 x 800 (b) Image obtain after pixel rearrangement (c) Cipher Image (d) Histogram of plain image (e) Histogram of image obtain after pixel rearrangement and (f) Histogram of Cipher image.

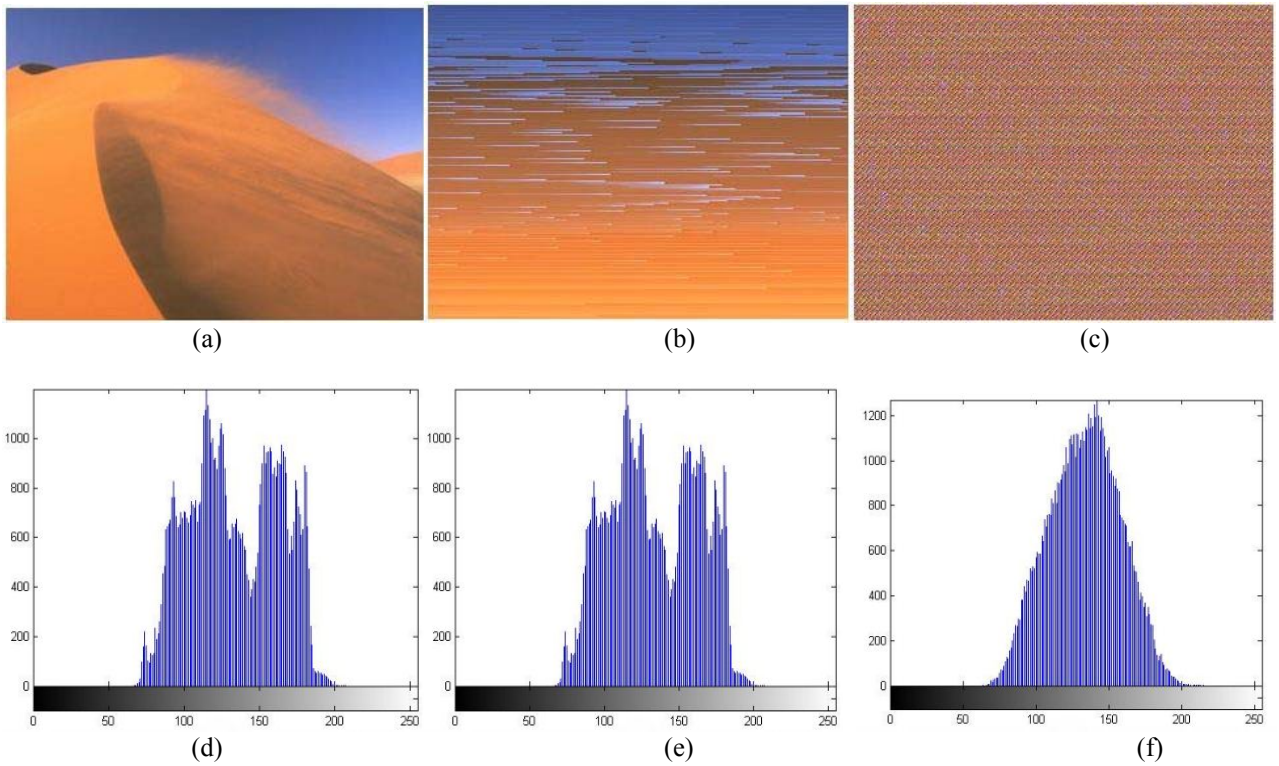



Figure 4 (a) Plain image size of 320 x 240 (b) Image obtain after pixel rearrangement (c) Cipher Image (d) Histogram of plain image (e) Histogram of image obtain after pixel rearrangement and (f) Histogram of Cipher image.

Proposed algorithm was tested on three different size images of pixels 284 x 117, 1200 x 800 and 320 x 240 and result obtain is shown in figure 2, 3 and 4 respectively. Part (b) of each figure shows the image which is obtained after applying pixel rearrangement which is proposed to reduce the correlation between pixel values such that images should not guess by neighboring pixel. Although image encryption model is based on this methodology that no one other than authorized user can guess about cipher image. So, by looking at part (b) of each figure, this can conclude that correlation is negligible because it is not possible to calculate the neighbor 8 pixel for any pixel. Further histogram of each image is shown which shows the difference in the plain image and cipher image and histogram for plain image and intermediate image is same because there is only pixel rearrangement while in plain image and cipher image there is inter-pixel displacement.

## VII. Conclusion and Scope of Future Research

In this paper we presented new algorithm for image encryption by using sorting of pixels as per their RGB values and arranging them group-wise which helped to reduce the correlation between pixels and increased entropy value. Experimental results were taken out on Matlab 6.0.1 and this is a lossless image encryption algorithm with results. Histogram of plain image and cipher image is also carried out. Further inter pixel algorithm can be used with another confusing property

to result in better image encryption technique. This work can be further extended by using the pyramidal block scheme for image encryption with inter pixel scheme.

## REFERENCES

[1] Information available via www at http://en.wikipedia.org/wiki/Open_communication.

[2] Jakimoski, G. and L. Kocarev. 2001. ―Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps ‖. IEEE Transactions on Circuits and Systems—I: Fundamental Theory and Applications. 48(2): 163-169.

[3] Jayant Kushwaha and Bhola Nath Roy, "Secure Image Data by Double encryption", International Journal of Computer Applications (0975 – 8887), Volume 5– No.10, August 2010.

[4] Mohammad Ali Bani Younes and Aman Jantan, "Image Encryption Using Block – Based Transformation Algorithm" IAENG, 35:1, IJCS_35_1_03, February 2008.

[5] Mohammad Ali Bani Younes and Aman Jantan, "An Encryption Approach Using a Combination of Permutation Technique Followed by Encryption" IJCSNS, vol 3 no 4, April 2008.

[6] Aditee Gautam, Meenakshi Panwar and Dr.P.R Gupta, "A New Image Encryption Approach Using Block Based Transformation Algorithm", (IJAEST) International Journal Of Advanced Engineering Sciences And Technologies, Vol No. 8, Issue No. 1, 090 - 096 @ 2011, ISSN: 2230-7818.

[7] Amnesh Goel, Reji Mathews & Nidhi Chandra, "Image Encryption based on Inter Pixel Displacement of RGB Values inside Custom Slices", International Journal of Computer Applications (0975 – 8887), Volume 36– No.3, December 2011.

[8] Socek, D., Shujun Li, Magliveras, S.S. and Furht, B, "Enhanced 1-D Chaotic Key-Based Algorithm for Image Encryption", First International Conference on Security and Privacy for Emerging Areas in Communications Networks, 2005:406-406.

[9] Deergha Rao and K. Gangadhar, "Modified Chaotic Key-Based Algorithm for Image Encryption And Its VLSI Realization", International Conference on Digital Signal Processing, 2006.

[10] Jui-Cheng Yen, and Jiun-In Guo, "A New Chaotic Key-Based Design for Image Encryption and Decryption", IEEE International Symposium on ISCAS 2000, Geneva, pp. IV-49-IV-52, May. 2000.

[11] Reji Mathews, Amnesh Goel, PrachurSaxena & Ved Prakash Mishra, "Image Encryption Based on Explosive Inter-pixel Displacement of the RGB Attributes of a PIXEL", Proceedings of the World Congress on Engineering and Computer Science 2011 Vol I WCECS 2011, October 19-21, 2011, San Francisco, USA. ISBN: 978-988-18210-9-6.

Amnesh Goel is pursuing M.Tech in Computer Science and Engineering at Amity School of Engineering & Technology, Amity University, Noida. He has received MCA, M.Sc degree from Maharshi Dayanand University, Rohtak in 2010 and 2009 respectively. He has done BCA and B.Sc from IGNOU, Delhi and Chaudhary Charan Singh University, Meerut respectively in 2007. He has more than 2 years' experience in administration. His current research includes in Image Encryption, MANET, sensor network and Data Mining.

Ms. Nidhi Chandra has more than 7 years' experience in academic and Software Development. She is M.Tech from CDAC NOIDA, affiliated from GGSIPU, Delhi. Presently she is working as Assistant Professor at Amity University Noida. She has Worked with Tata Unisys and CDAC Noida. Her research interest includes Natural Language Processing, Assistive Technology and Semantic Web Based Application.