IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 2, April-May, 2013
ISSN: 2320 - 8791
www.ijreat.org

A Novel Color Image Scrambling Technique Based on Transposition of Image-Blocks between RGB Color Components

Prabhudev Jagadeesh[1], P. Nagabhushan[2] and R. Pradeep Kumar[3]

[1] Adithya Institute of Technology, Anna University
Coimbatore-641048, India.

[2] Department of Studies in Computer Science, University of Mysore
Mysore-570006, India

[3] Adithya Institute of Technology, Anna University
Coimbatore-641048, India

Abstract

Digital images comprise the major portion of data that is being exchanged over communication network. A higher level security has to be provided when digital images are personal or confidential. Traditionally Encryption is used to disguise data making it incomprehensible to unauthorized observers. However inherent features of image data such as bulky nature, high redundancy and high correlation among pixels warrant the need to treat an image in a different way from text data with regard to confidentiality. In this paper a block-based image scrambling technique for RGB color images is proposed with the objective to improve information entropy and correlation among image blocks criteria. In the proposed method hierarchical decomposition of the RGB planes of an image into equal-sized blocks is followed by an efficient shuffling of image blocks across the three color planes. Transpositions of image blocks also accomplish the substitution property. Experimental results show significant decrease in correlation between adjacent blocks in all color components together with the increase in entropy.

Keywords: *RGB color components, Entropy, Scrambling Encryption, image histogram*

1. Introduction

The security of multimedia data in digital distribution networks is generally provided by encryption, which transforms a plaintext message into unintelligible ciphertext. Classical and modern ciphers have all been developed for the simplest form of data i.e., text and thus are not suitable for encrypting image data which has certain intrinsic properties like bulky nature, intractable high redundancy and higher correlation among pixels. Several image scrambling schemes for shielding confidentiality of sensitive images basically through cryptographic and steganographic techniques have been proposed. In spite of these efforts, analysis indicates that security level is still not tough for images and multimedia data in general. Moreover most of the works in literature are systems that have been designed for gray scale images that are then independently applied on the RGB color components. By considering the RGB components together rather than in isolation the proposed work is an effort to build simpler yet efficient security model for enforcing confidentiality of color images.

The rest of this paper is organized as follows. Section 2 presents the related works found from literature basically with regard to color image scrambling. Section 3 presents the overall architecture and proposed algorithms. Section 4 illustrates the experimental results and the various security analyses carried out on the proposed algorithms. Finally, Section 5 concludes the paper highlighting the accomplishments.

2. Related work

Since Classical and modern cryptographic algorithms have been developed for basically text data and are not suitable for images, several image scrambling schemes have been proposed[1,11] considering the intrinsic characteristics of images. Image encryption techniques can be categorized as spatial domain methods or frequency domain methods. Basically most encryption schemes are constructed using three methods namely permutation, substitution and combination of both. Most of the works in literature with regard to color image encryption are schemes that have been designed for gray scale images that are then separately applied on the RGB color components and very few works can be found solely designed for color images. To explore some of the representative work, in [4], the encryption process is applied on RGB components of the image's pixel instead

of the pixels itself using another image as a key. The corresponding RGB components in plain image and key image go through diffusion process followed by permutation of RGB components of ciphered image. In [5] an image is decomposed into its RGB components and then the shifting and permutations on these elements are performed based on a key. The inter-pixel shifting of R, G, and B values provides minimum clues for guessing out the light and shade profiles of the original plain image. In [7] a method to encrypt color images using optical encryption systems is proposed where the color image converted to indexed image format is encoded to stationary white noise with two random phase masks. Several chaos-based algorithms are also proposed for image encryption [3,8,12] because of the non-periodic, non-linear and non-convergent nature of chaos signals. In [6] a novel chaos-based image encryption algorithm to encrypt color images by using a coupled two dimensional Piecewise Nonlinear Chaotic Map and a masking process is proposed. In [10] an image scrambling technique based on information Entropy using quad tree decomposition is proposed where a grayscale image is scrambled region-wise. In [9] a Visual Cryptography which exploits the halftone technology and color decomposition is proposed.

3. Proposed technique

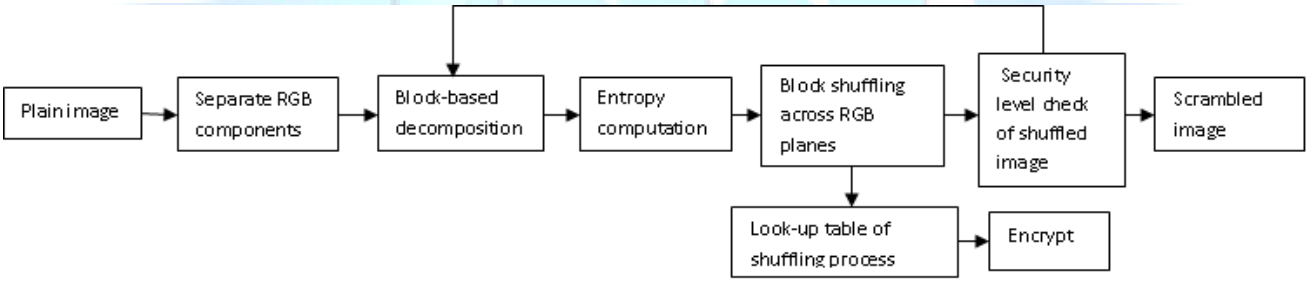


Fig. 1 Proposed Scheme for Scrambling

From information security viewpoint if the information content of an image is highly unpredictable then lesser information is revealed. The objective should be to increase the uncertainty on the expected value of a pixel in an image. The information theory concept 'Entropy' which is a measure of the uncertainty in a random variable and which also quantifies the expected value of the information contained in a message can be used to accomplish the proposed scheme. Keeping this as the fundamental theme the proposed approach attempts to convert an image which is perceived to be homogeneous into a heterogeneous image by supervised shuffling of smaller image blocks contained by the image/image block. The objective is to make the image more and more heterogeneous by successive decomposition followed by shuffling of image blocks. For this at each level an image/image block is divided into four equal sized blocks. The blocks are supposedly more homogeneous than the image itself. As depicted in fig after the image is decomposed into four smaller sized blocks based on the entropy which is a measure of heterogeneity, the block shuffling is carried out. Shuffling of a subset of blocks among four blocks at each level will result in a more heterogeneous image block at the previous level. Apart from maximizing the heterogeneity factor, at each level of decomposition the entropy of the image blocks also gets normalized making blocks more or less equally heterogeneous. The process is continued until the required level of security is obtained or the minimum size of the blocks is reached. During the shuffling process a look-up table is generated which is a record of the shuffling information of blocks. This look-up table is used during decryption as a key to reconstruct the original image. Only the look-up table is encrypted using a strong encryption technique. The scrambled image can go through further encryption using some conventional

algorithm if one more level of security is preferred. Three techniques are proposed based on the above theme.

3.1 Method 1

Here an RGB image is separated into R, G and B components. The proposed algorithm is applied considering all the three color components together where shuffling of image blocks take place within and also across the three color components.

Algorithm 1
Input: Plain image, minimum block size
Output: Scrambled RGB image
Step 1: Separate the R, G, and B components of the image into three images I_R, I_G and I_B.

Step 2: Split images I_R, I_G and I_B each into four equal-sized images (parent image blocks).

Step 3: Find the entropy of each block using equation 1. Let E be the sorted array of image blocks based on entropy of individual image blocks.

$$E_n = \sum_{i=0}^{255} (\mathrm{p(i)} * \log_2(1/\mathrm{p(i)})) \quad (1)$$

Step 4: Pair image blocks E_i and E_{n+1-i} for i=1, 2 ,…., *n* for all *n* image blocks.

Step 5: Divide the image blocks (parent image blocks) further into four equal-sized blocks (child image blocks).

Step 6: Between each pair of image blocks (parent image blocks) perform shuffling of image blocks (child image blocks) by swapping a subset of blocks from one parent block with a subset of blocks from other parent block in the pair such that the sum of entropy of the parent block nodes is maximized thereby making the blocks more heterogeneous.

Step 7: Extract the swapping information in a look-up table which is used as key for decryption of scrambled image.

Step 8: Now with child image blocks as parent image blocks repeat step 3 to step 7 until the image block is decomposed into blocks of minimum block size.

Step 9: Combine the scrambled I_R, I_G and I_B images to obtain the scrambled RGB image.

3.2 Method 2

Here the RGB image is first converted to grayscale image and then the proposed algorithm is applied on grayscale image. The block permutation generated for the grayscale image is then applied separately to all the three color components to obtain the scrambled image.

Algorithm 2
Step 1: Convert an RGB image into grayscale image by forming a weighted sum of the R, G, and B components: 0.2989 * R + 0.5870 * G + 0.1140 * B.

Step 2: Split the grayscale image into four image blocks of equal size (parent image blocks).

Step 3: Perform step 3 to step 8 of Algorithm 1.

Step 4: Apply the block permutation generated for the grayscale image available in look-up table separately to all the three color components.

Step 5: Combine the scrambled I_R, I_G and I_B images to obtain the scrambled RGB image.

3.3 Method 3

Here the proposed algorithm is applied to R, G and B components of the image individually to obtain a scrambled image.

Algorithm 3
Step 1: Separate the R, G, and B components of the image into three images I_R, I_G and I_B.

Step 2: For each image component I_R, I_G and I_B perform step 3 to step 8 of Algorithm 1 separately.

Step 3: Combine the scrambled I_R, I_G and I_B images to obtain the scrambled RGB image.

3.3 Decryption process

To decrypt a scrambled image, the look-up table which acts as the key is first decrypted and using the shuffling information available in the look-up table the original image is obtained.

4. Experimental Results and Security Analysis

Several images have been tested by using the proposed image scrambling scheme. The results tested on a RGB image of size 512x512 is indicated in Fig.2 – Fig.6. The various algorithms are investigated by scrambling an image up to a minimum block size of 2x2. Fig. 2 shows the different levels of decomposition. To test the

robustness of the proposed scheme, security analysis was performed. In order to resist statistical attacks, the scrambled images should possess certain random properties. A statistical analysis has been performed by calculating the histograms, the entropy and the correlation coefficient for the plain image and the scrambled image.

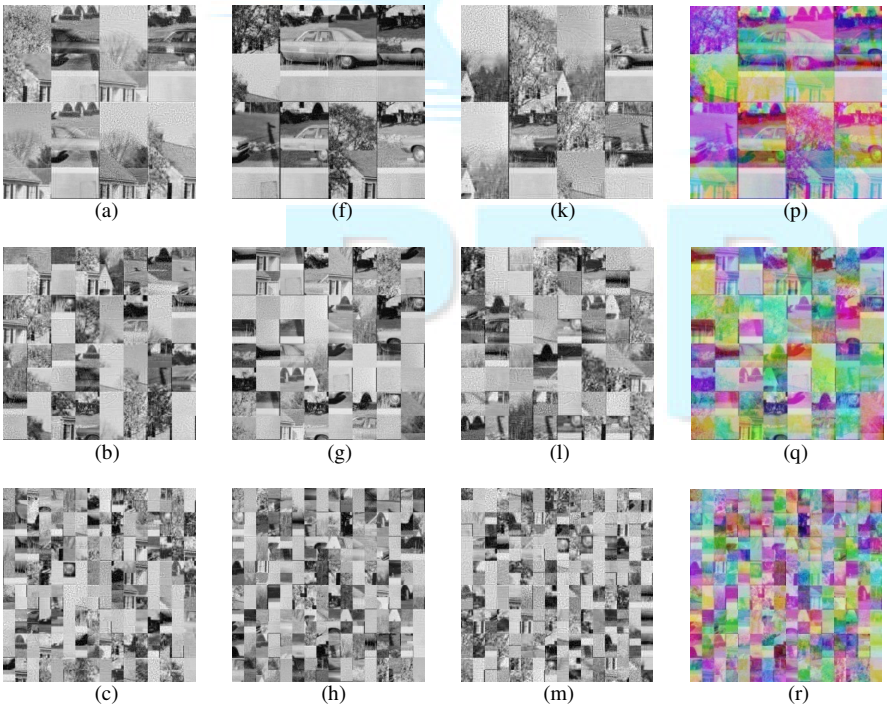
The correlation analysis was performed between the two adjacent image blocks of both plain image and scrambled image to analyze correlation between image blocks in vertical and horizontal directions. Correlation coefficient is a measure of correlation between two entities. The correlation coefficient between two adjacent image blocks in an image is analyzed by taking the average of correlation coefficients between all the adjacent pairs of image blocks. The Correlation Coefficient between two image blocks A and B of size m x n is calculated using the expression in equation 2.

$$r = \frac{\sum_m \sum_n (A_{mn} - \bar{A})(B_{mn} - \bar{B})}{\sqrt{\left(\sum_m \sum_n (A_{mn} - \bar{A})^2\right)\left(\sum_m \sum_n (B_{mn} - \bar{B})^2\right)}} \quad (2)$$

Where $\bar{A}$ and $\bar{B}$ are the mean of A and B respectively.

Another Security analysis carried out is histogram analysis. An image histogram illustrates how pixels in an image are distributed by plotting the number of pixels at each intensity level. For the proposed work histogram analysis is carried for image blocks of various sizes. It is apparent from the representative histograms of image blocks of size 128x128 indicated in Fig.6, that the histogram of the final encrypted image is fairly uniform and is considerably different from that of the original image thus not revealing any clue for statistical attack.

Entropy analysis is also done for image blocks of different size to analyze the security level. As the image is decomposed and the proposed algorithm is applied the entropy of the blocks gets maximized at every level. Entropy analysis carried on for image blocks of different size is indicated in Fig.7 From the graphs it is clear that the property of maximization of entropy happens more or less equally for all the blocks thereby ensuring that all the blocks exhibit the same security level. Further it is evident from the results obtained, that method 1 of image scrambling across RGB planes gives better results compared to the other two approaches.



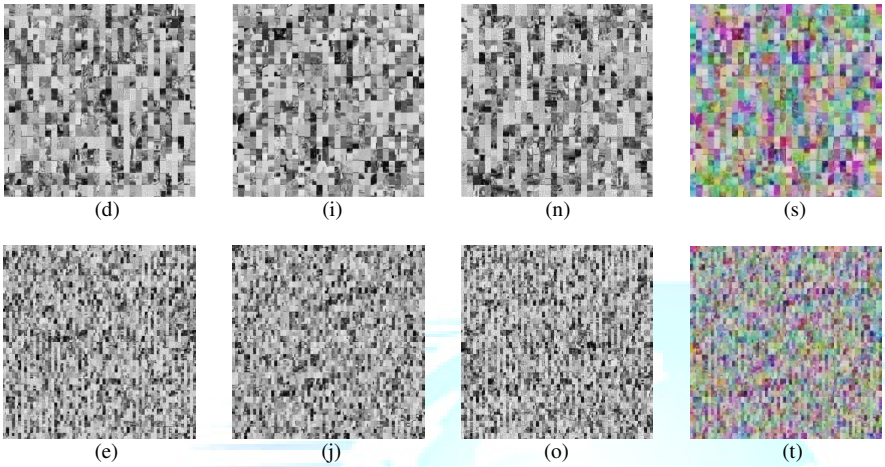


Fig. 2 (a) - (e) Scrambled R component. (f) - (j) Scrambled G component. (k) - (o) Scrambled B component. (p) - (t) Scrambled RGB image (Method 1)

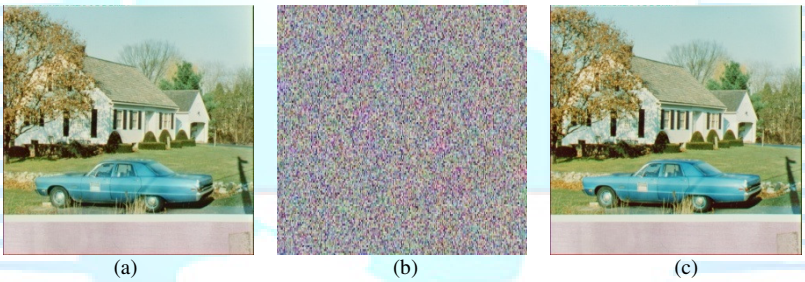


Fig. 3 (a) Original image of size 512x512 (b) Scrambled image (c) Decrypted image (Method 1)

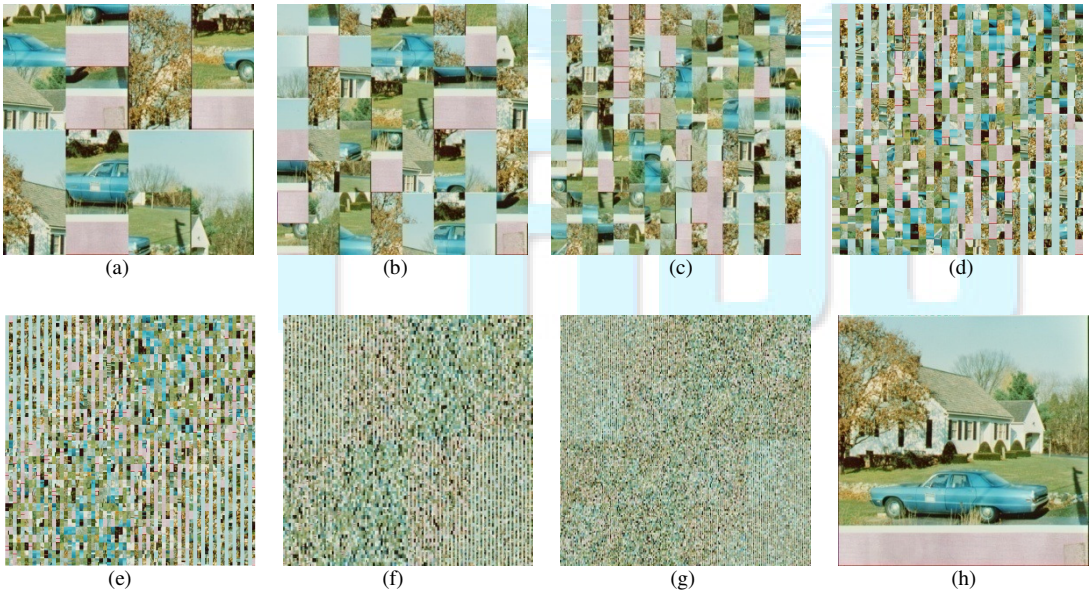
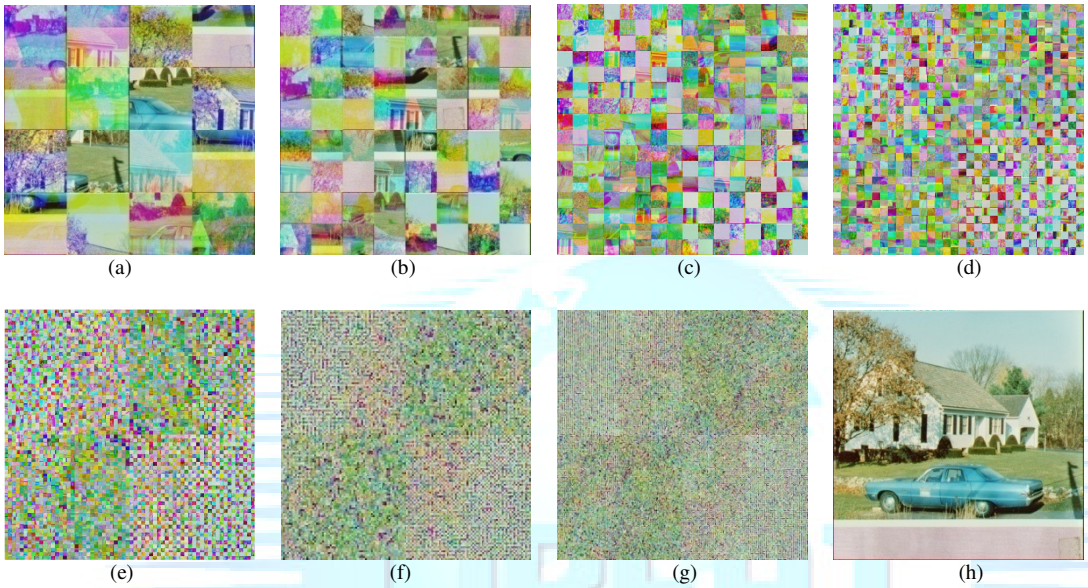


Fig. 4 (a) to (g) Scrambled images. (h) Decrypted image (Method 2)



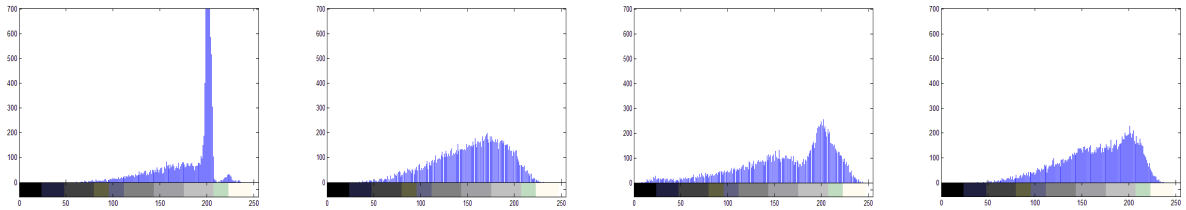
(a) (b) (c) (d)

(e) (f) (g) (h)

Fig. 5 (a) to (g) Scrambled images. (h) Decrypted image (Method 3)

Table 1. Correlation Coefficient of plain image and scrambled image

Direction of adjacent image blocks	Plain image	Scrambled image		
		Method 1	Method 2	Method 3
Horizontal	0.1593	0.0066	0.0162	0.0995
Vertical	0.1008	0.0655	0.0964	0.0822



(a) (d) (g) (j)

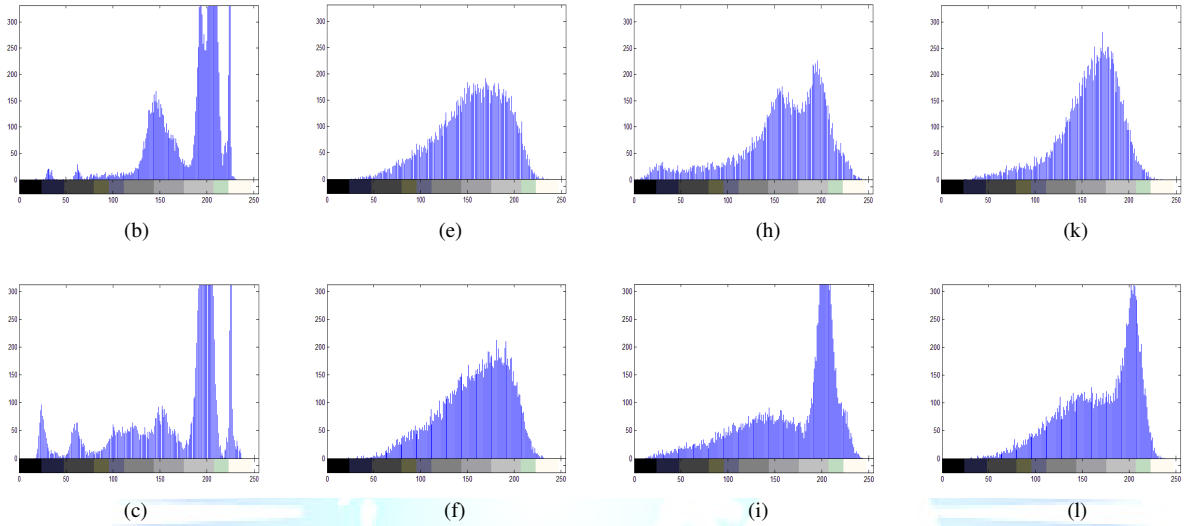


Fig. 6 (a) to (c) Histogram of image blocks (128x128) of plain image. (d) to (f) Histogram of image blocks of scrambled image(method 1). (g) to (i) Histogram of image blocks of scrambled image(method 2). (j) to (l) Histogram of image blocks of scrambled image(method 3)

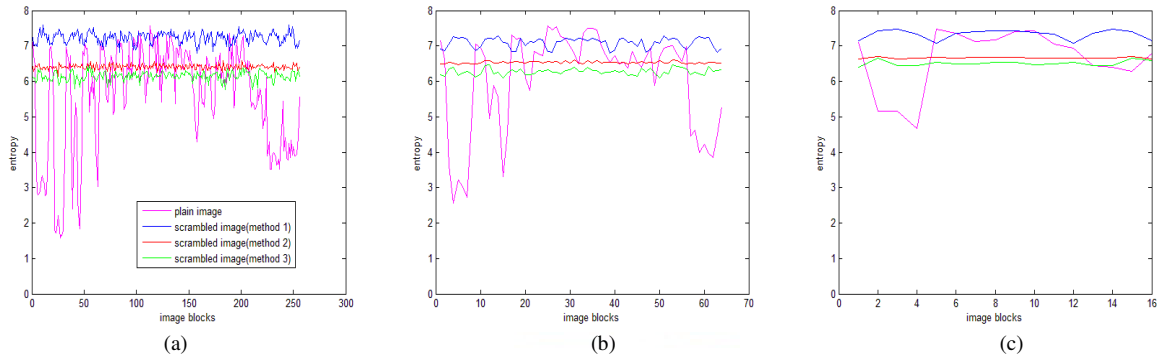


Fig. 6 Entropy of original image blocks and corresponding blocks in scrambled image. (a) 32x32 blocks. (b) 64x64 blocks. (c) 128x128 blocks.

5. Conclusion

Based on decomposition of image into smaller size blocks and able permutation of image blocks across the RGB components a simple yet efficient scheme for scrambling true color RGB image has been developed. The proposed scheme strives to scramble the image by making the image more heterogeneous at each step. The inter shuffling of blocks between R, G and B components also brings in the substitution property desired in a good scrambling algorithm. Experimental analysis carried out with various test images has provided promising outcomes. Security analyses of all the three variants point out that the proposed method satisfies the major security criteria of image scrambling technique. Providing one with the choice to select the minimum block size at which point scrambling can be stopped, a different security levels or a form of light-weight encryption can be provided to meet the diverse security necessities.

References

[1] Furht , Kirovsk, Multimedia Security Handbook, 2005.
[2] Gonzalez, R.C., R.E. Woods, S.L. Eddins, Digital Image Processing, Second Edition, Prentice Hall, 2007.
[3] Mintu Philip, Asha Das, "Survey: Image Encryption using Chaotic Cryptography Schemes" International Journal of Computer Applications, 2011.
[4] Nashwan A. Al-Romema1, Abdulfatah S. Mashat, Ibrahim AlBidewi, "New Chaos-Based Image Encryption Scheme for RGB Components of Color Image", Computer Science and Engineering 2012, pp 77-85
[5] Reji Mathews , Amnesh Goel , Prachur Saxena, 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 IWCECS 2011, October 19-21, 2011, San Francisco, USA.
[6] Seyed Mohammad Seyedzadeh , Sattar Mirzakuchaki " A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map", Signal Processing Volume 92, Issue 5, May 2012, pps 1202–1215.
[7] S. Zhang and M.A. Karim, "Color image encryption using double random phase encoding", microwave and optical technology letters. Vol. 21, No. 5, June 5 1999, pp. 318-322.
[8] Zhu, Z., et al., "A chaos-based symmetric image encryption scheme using a bit-level permutation", Information Sciences, 2011. 181(6): pp 1171-1186.
[9] Young Chang Hou, "Visual cryptography for color images", The journal of Pattern Recognition society, 2003, pp 1619-1629.
[10] Prabhudev Jagadeesh, Nagabhushan, Pradeep Kumar, "A Novel Image Scrambling Technique Based On Information Entropy And Quad Tree Decomposition", International Journal of Computer Science Issues ,Vol.10,Issue 2,No. 1, March 2013.
[11] Alireza Jolfaei and Abdolrasoul Mirghadri, " Survey: Image Encryption Using Salsa20," IJCSI, Vol. 7, Issue 5, September 2010 pp 213-220.

[12] Shou-Dong, Lu Hui, Xu , "A New Color Digital Image Scrambling Algorithm Based on Chaotic Sequence", International Conference on Computer Science & Service System , 2012.