A Novel Image Scrambling Technique Based On Information Entropy And Quad Tree Decomposition

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

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

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

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

Abstract

With the rapid increase of digital data exchange and increased usage of digital images, it is important to protect the confidential image data from illegal access. Digital image scrambling or encryption is the solution which transforms a meaningful image into a meaningless or disordered image in order to enhance the ability to confront attack and in turn improve the security. This paper presents a new scheme for digital image scrambling based on the principle of information entropy. The quad tree decomposition technique is used to hierarchically divide the image into blocks or regions for enforcing security at the block or region level of an image, which thus ensures the security of the entire image. The experimental results show that the proposed algorithm can successfully scramble the images, and the analysis of the algorithm also demonstrate that the scrambled images have good information entropy and low correlation coefficients thereby satisfying the requisite security.

Keywords: Image Encryption, Scrambling, Image Entropy, Image correlation, Image histogram, Quad tree

1. Introduction

With the huge growth of computer networks and the latest advances in digital technologies, a huge amount of digital data is being exchanged over various types of networks where digital images constitute a major chunk. Large parts of the data exchanged are confidential and personal thus demanding security during storage and transmission. The issues like bulky nature of an image and slow speed of traditional cipher, dependence of encryption on compression and thereby the existing tradeoff, intractable high redundancy that exists in images, and the inability of traditional ciphers to provide avalanche property required for image confidentiality emphasize the need to treat an image differently from text data with regard to confidentiality [14]. There have been several image scrambling schemes for protecting confidentiality of sensitive images basically through cryptographic and steganographic techniques [6]. An image scrambling scheme basically transforms an image into another unintelligible image. In spite of these efforts, analysis indicates that security level is still not strong for images and multimedia data in general [3,7,11]. Also these techniques barely consider the significant intrinsic properties of images. This indicates the need for content-based schemes which are simpler yet stronger for shielding confidentiality of digital images [14]. The proposed research is one such attempt to build simpler yet efficient security model for image confidentiality.

The rest of this paper is organized as follows. Section 2 presents the related work found in literature with regard to image scrambling. In Section 3, the proposed scheme for image scrambling based on entropy and quad tree structure is discussed. Section 4 contains the experiments carried out and the results obtained. Section 5 presents the thorough security analysis of the new proposed approach. Finally, Section 6 concludes the paper highlighting the research accomplishments and also proposing future directions.

2. Related Work

Conventional methods for image encryption such as Data Encryption Standard and Advanced Encryption Standard based on cryptography concept scramble an image by considering it as text data. Since Classical and modern cryptographic algorithms have been developed for the simplest form of data i.e., text and are not suitable for data such as images, several image scrambling schemes have been proposed [9,12]. There are image scrambling methods that offer lightweight scrambling, while others

offer strong form of encryption. Algorithms which provide different levels of security ranging from degradation to strong encryption are categorized under scalable algorithms [10]. Permutation based techniques are based on bit, pixel or block permutation [1,4]. In [2] a random combinational Image encryption approach with bit, pixel and block permutations is proposed. There are approaches to scramble an image in a transformed domain by scrambling the transform coefficients. Methods for scrambling all the pixels and transform coefficients with multiplicative or additive matrices are proposed which are considered as a generalization of the permutation-only encryption. Some image encryption schemes are based on the multi-round combination of secret permutations and pixel value substitutions [4]. Several chaos-based algorithms are also proposed for image encryption [5,8,11].

3. Proposed Approach

The proposed approach is based on the principle of image entropy which is one of the main statistical measures to assess the security levels of image scrambling techniques. The approach is a block permutation-based image scrambling technique. The objective is to make every image block heterogeneous by maximizing the entropy at the level of image blocks and thereby enforcing image scrambling. Here the concept of quad tree decomposition is employed to recursively scramble the image to impose image confidentiality.

3.1 Information entropy

Entropy, in an information sense is a measure of unpredictability. Entropy is proved to be a good method to express randomness or uncertainty of a random variable [15]. Here the concept of entropy is used in the sense of information theory (Shannon entropy), where entropy is used to quantify the minimum descriptive complexity of a random variable. For a digital image, Image Entropy indicates the amount of information contained in an image. It can be chosen as a measure of the detail provided by an image. Higher the value of entropy less is the information revealed. If all pixels in an image have the same gray level or the same intensity of color components, this image will present the minimal entropy value. On the other hand, when each pixel of an image presents a specific gray level or color intensity, the image will exhibit maximum entropy. This property of entropy provided in information theory implying that higher the entropy; lesser the information conveyed is conceptualized for image security perspective in the proposed approach. For a random variable X with n outcomes $\{x_1,\ldots,x_n\}$, the Shannon entropy, a measure of uncertainty denoted by H(X), is defined as[14,15]

$$H(X) = -\sum_{i=1}^{n} p(x_i) \log_b p(x_i) \quad (1)$$

where $p(x_i)$ is the probability mass function of outcome x_i.

The entropy E_n of an image is calculated as below:

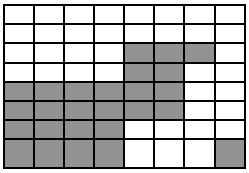
$$E_n = \sum_{i=0}^{255} (\mathrm{p(i)} * \log_2(1/\mathrm{p(i)})) \quad (2)$$

where, p(i) = Number of occurrence of pixel 'i' / Total number of pixels in the image

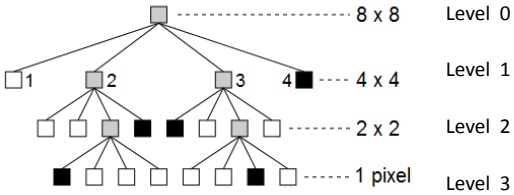
3.2 Quad Tree decomposition

A Quad Tree is a tree data structure in which each internal node has exactly four children. Each node in the tree either has exactly four children, or has no children (a leaf node). Quad trees are most often used to partition a two dimensional space by recursively subdividing it into four quadrants or regions [12,13]. The regions may be square or rectangular, or may have arbitrary shapes. Quad tree decomposition is an analysis technique that involves subdividing an image into blocks that are more homogeneous than the image itself. In conventional quad tree decomposition a square image is divided into four equal sized square blocks, and then each block is tested to see if it meets some criterion of homogeneity. If a block meets the criterion, it is not divided any further. If it does not meet the criterion, it is subdivided again into four blocks, and the test criterion is applied to those blocks. This process is repeated iteratively until each block meets the criterion.

Quad tree decomposition is depicted in Fig. 1. The root node represents the entire region/image. A node is split into four blocks if it does not meet the homogeneity criteria. Finally the leaf node represents image blocks which satisfy the homogeneity constraint. Fig.1 shows the decomposition of an 8 x 8 image to the extent of 1 pixel size starting from a block size of 8x8.



(a)



(b)

Fig. 1 An example of the Quad tree representation applied to an 8x8 block: (a) block decomposition (b) Quad tree representation of the block decomposition.

3.3 Proposed Algorithm

In the proposed method an image is divided into four equal sized blocks and the entropy of the blocks are computed. If the blocks do not meet the entropy criteria which tests for heterogeneity of the image at block level, blocks are further divided using quad tree decomposition. At every level *'k'*, blocks are made more heterogeneous by shuffling the smaller sized blocks at level *'k+1'* to achieve following objectives. i) Maximize the Entropy of the image blocks at level *'k'* ii) Balance the entropy of image blocks at level *'k'*. The information of shuffling of the blocks is maintained as metadata for the decryption process. The metadata is encrypted using some strong encryption algorithm. The metadata acts as a key for descrambling the image. The scrambled image can undergo further encryption using some conventional algorithm if one more level of security is required. The block diagram of the proposed approach is shown in Fig 2. The information extracted as metadata during the block permutation process contains the position of the block before permutation, the new position of the block after permutation, and the level of quad tree decomposition which can be expressed as a structure data type as below:

```
Struct Metadata { int position_before_swapping;
                  int position_after_swapping;
                  int decomposition_swapping;
                }
```

Two variants of the proposed approach based on how the swapping of blocks is done are as below:

i) Top-down approach.

ii) Bottom-up approach.

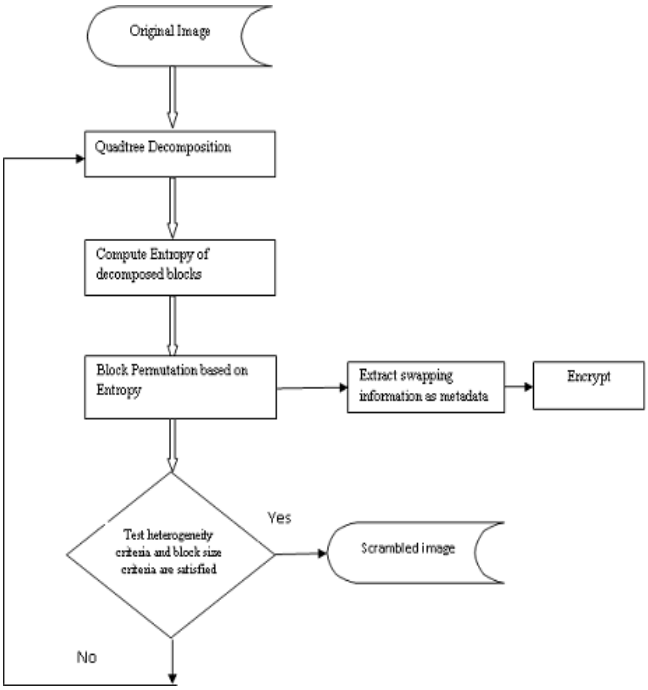


Fig. 2 Proposed Approach for scrambling

3.3.1 Top-down approach

In top-down approach, entropy balancing and swapping of image blocks starts from the first non-root parent level blocks and is directed down the quad tree. This approach results in an order where the image blocks swapped vary from bigger size to smaller size.

The outline of the algorithm for Top-down approach is as below:

Step 1: Using Quad tree decomposition technique split the image by dividing it into four blocks of equal size for two successive levels. (Fig.1)

Step 2: Initialize the starting level of parent node blocks for processing as lev = 1.

Step 3: Find the entropy of the parent node blocks at level lev.

Step 4: Sort the blocks at level lev based on their entropy values.

Step 5: Pair the parent blocks at level lev for balancing the entropy using the sorted vector of entropy obtained in step 4 as explained below.

Pairing is done between highest entropy parent block and lowest entropy parent block; next highest entropy parent block and next lowest entropy parent block and so on.

Step 6: Maximize the entropy of the parent blocks at level lev by swapping the children blocks at level lev+1 as below.

Determine the combination of children blocks between the pair of parent blocks which maximizes the sum of the entropy of the parent block pair, thereby maximizing the entropy of individual parent blocks. Swap selected children blocks.

Step 7: Recompute entropy of blocks at level lev. If all the blocks satisfies the entropy criteria in Eq. (3) or size of blocks at lev+1 is min_blocksize exit. Else decompose the blocks at level lev+1 whose parent blocks at level lev does not meet the criteria further into four blocks each by quad tree decomposition. Increment lev i.e., lev=lev+1. Repeat step 3 to step 7.

$$Entropy_{lev}^{i} >= threshold \quad (3)$$

Where 'i' indicate the block number and lev indicates the level in quad tree.
threshold indicates the entropy of image block at which the block is not decomposed further.

min_blocksize indicates the minimum block size at which quad tree decomposition is stopped.

3.3.2 Bottom-up approach

The other variant of the above algorithm is bottom-up approach where the entropy balancing and swapping of blocks is done starting from last parent node moving upward towards the root node of the quad tree. This approach results in an order where the image blocks swapped vary from smaller size to bigger size. The algorithm for bottom-up approach is as below:

Step 1: An image is recursively subdivided into four blocks of equal size until a specified block-size min_blocksize is reached. Let h be the height of the quad tree.

Step 2: Initialize the starting level of parent node blocks for processing as lev = h-1.

Step 3: Find the entropy of the parent node blocks at level lev.

Step 4: Sort the blocks based on their entropy values.

Step 5: Pair the parent blocks for balancing the entropy using the sorted vector of entropy obtained in step 3 as explained below.

Pairing is done between highest entropy parent block and lowest entropy parent block; next highest entropy parent block and next lowest entropy parent block and so on.

Step 6: Maximize the entropy of the parent blocks at level lev by swapping the children blocks at level lev+1 as explained below.

Determine the combination of children blocks between the pair of parent blocks which maximizes the sum of the entropy of the parent block pair, thereby maximizing the entropy of parent blocks. Swap selected children blocks.

Step 7: Recompute entropy of image blocks at level lev. If all the blocks satisfy the entropy criteria in Eq. (3) or if block size at level lev is equal to cut_off_size exit. Else decrement lev ie., lev=lev-1. Repeat step 3 to 6 for blocks which do not satisfy the entropy criteria.

cut_off_size indiacates the size of blocks at which the scrambling process can be terminated.

In both the approaches stated above, pairing of parent nodes (image blocks) in the fashion described above accomplishes the first objective i.e., balancing entropy of image blocks. The combination of blocks selected at the level of children nodes for swapping enforces the second objective which is to maximize the entropy of the image blocks.

3.3.3 Decryption or Descrambling process

To decrypt the image, the metadata which is encrypted using a strong encryption algorithm is decrypted and using this information the original image is obtained.

4. Experimental Results

The proposed image scrambling technique was tested on several images. Results obtained for standard Lena image of size 256x256 is shown in Fig. 3 and Fig. 4. The entropy criterion (threshold) is chosen as 8 which is the ideal possible entropy. Minimum block size (min_blocksize) at which quad tree decomposition is stopped is 4x4. For bottom-up approach, block size at which scrambling has to be stopped (cut_off_size) is chosen as 128x128.

5. Security Analysis of the Proposed System

A good image scrambling algorithm should be robust against all kinds of cryptanalytic, statistical, and brute-force attacks. To analyze the security of the proposed system, Entropy analysis, Histogram analysis and Correlation Coefficient analysis is carried out. Analysis of the proposed approach portrays that it is indeed strong against possible attacks.

5.1 Entropy Analysis

The proposed technique is based on the principle of information entropy which intends to maximize the entropy thereby increasing the security. Entropy analysis is done for image blocks of different size. Analysis indicates how entropy of image blocks are maximized as the image is decomposed and shuffling of blocks is carried out. Graphs indicate how concurrently along with maximization of entropy, balancing of entropy also happens during scrambling process at every level of quad tree decomposition. Entropy values of all the image blocks of original image and scrambled image in Fig. 5 and Fig. 6 for various block size indicate the accomplishment of balancing of entropy and maximization of entropy

5.2 Histogram Analysis

An image histogram can be used to measure the statistical similarity between the original image and the scrambled image. Histograms illustrate how pixels in an image are distributed by plotting the number of pixels at each intensity level. Histograms are drawn for all the blocks for different block size. It is evident from the results obtained that the block/region level histograms of the scrambled image compared to the original image is reasonably uniform and evenly spread across all possible intensity levels in the original image. So the scrambled image does not provide any hint to encourage statistical attack. A result of histograms of original image and scrambled image of few randomly chosen image blocks is given in Fig. 7.

5.3 Correlation Coefficient

Correlation Coefficient is a measure of correlation between two entities. The correlation coefficient between two horizontally/vertically adjacent image blocks in original image/scrambled image is analyzed by taking the average of correlation coefficients between all the adjacent pairs of horizontal/vertical image blocks.

The Correlation Coefficient between two image blocks A and B of size m x n is calculated using the expression:

$$r = \frac{\sum_m \sum_n (A_{mn} - \bar{A})(B_{mn} - \bar{B})}{\sqrt{\left(\sum_m \sum_n (A_{mn} - \bar{A})^2\right)\left(\sum_m \sum_n (B_{mn} - \bar{B})^2\right)}} \quad (4)$$

Where $\bar{A}$ = mean of A,

$\bar{B}$ = mean of B

In Table 1, higher value of correlation coefficient of original image indicates, image blocks in original image are highly correlated, whereas the reduced value of correlation coefficient of scrambled image indicate lesser correlation between image blocks. This is the desired property of any image scrambling technique.

Table 1: Average Correlation Coefficient of two adjacent image blocks (for block size of 4 x 4).

Orientation of Adjacent Image Blocks	Original Image	Scrambled Image	
		Top down	Bottom up
Horizontal	0.0986	0.0119	0.0265
Vertical	0.2979	0.0084	0.0128

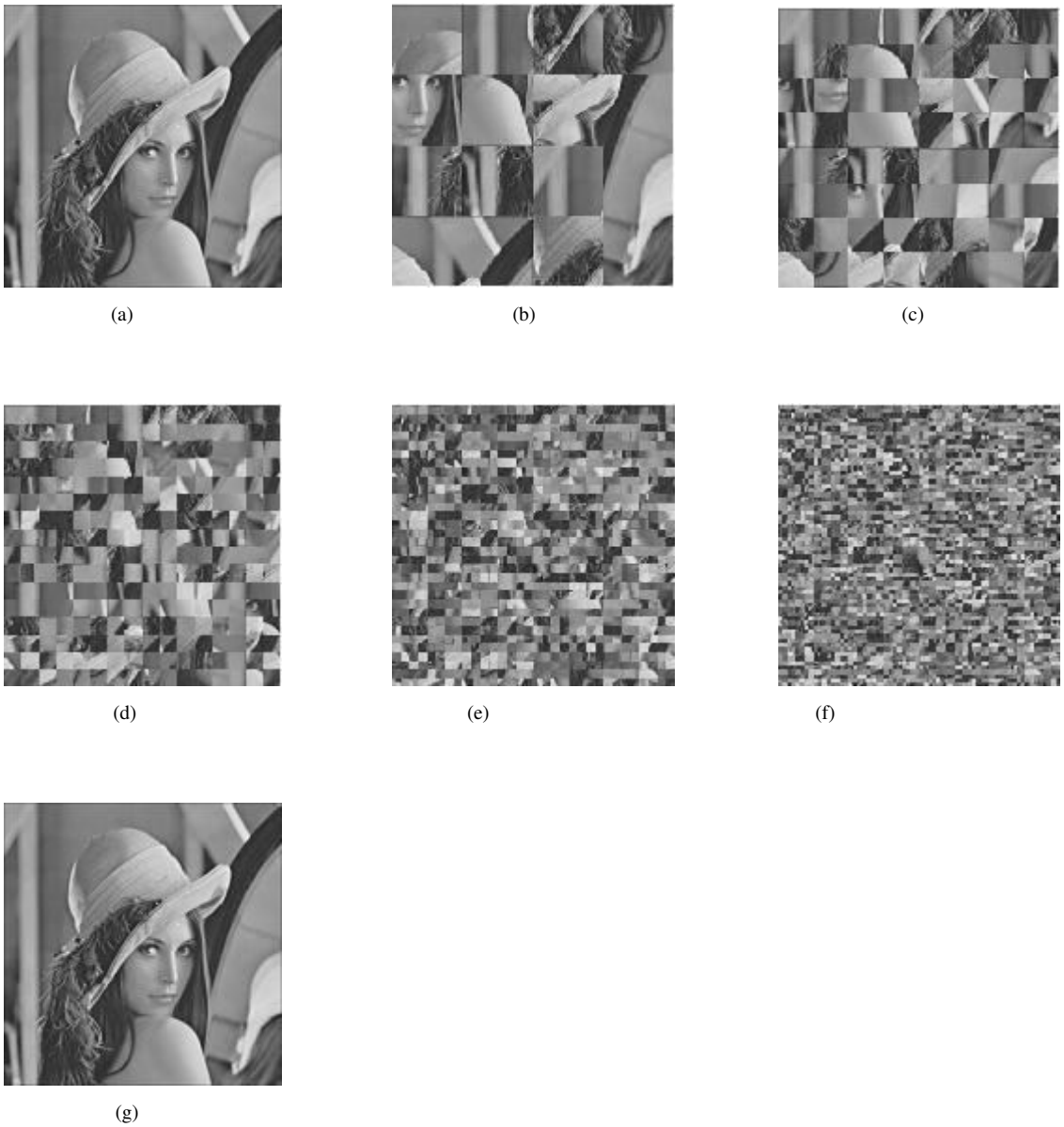
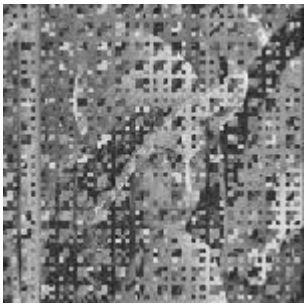


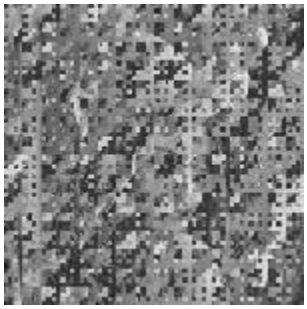
Fig. 3: Top down approach (a) Original image. (b) to (f) Scrambled image . (g) Decrypted image.

(a)

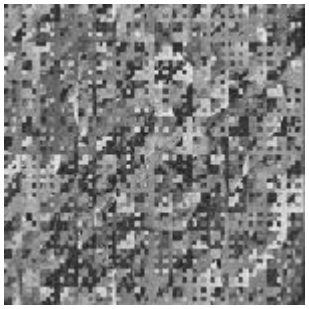
(b)



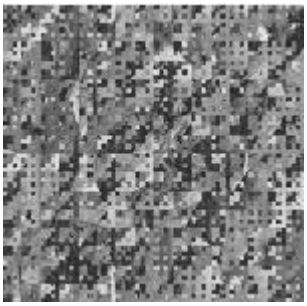
(c)



(d)



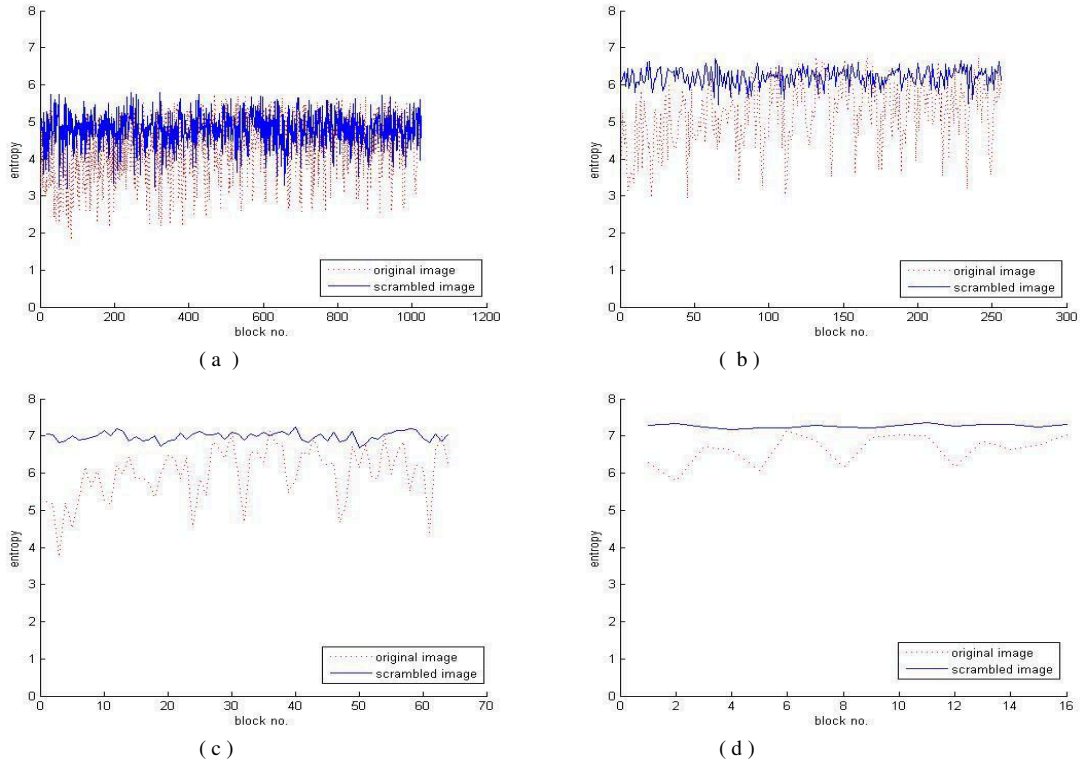
(e)



(f)

(g)

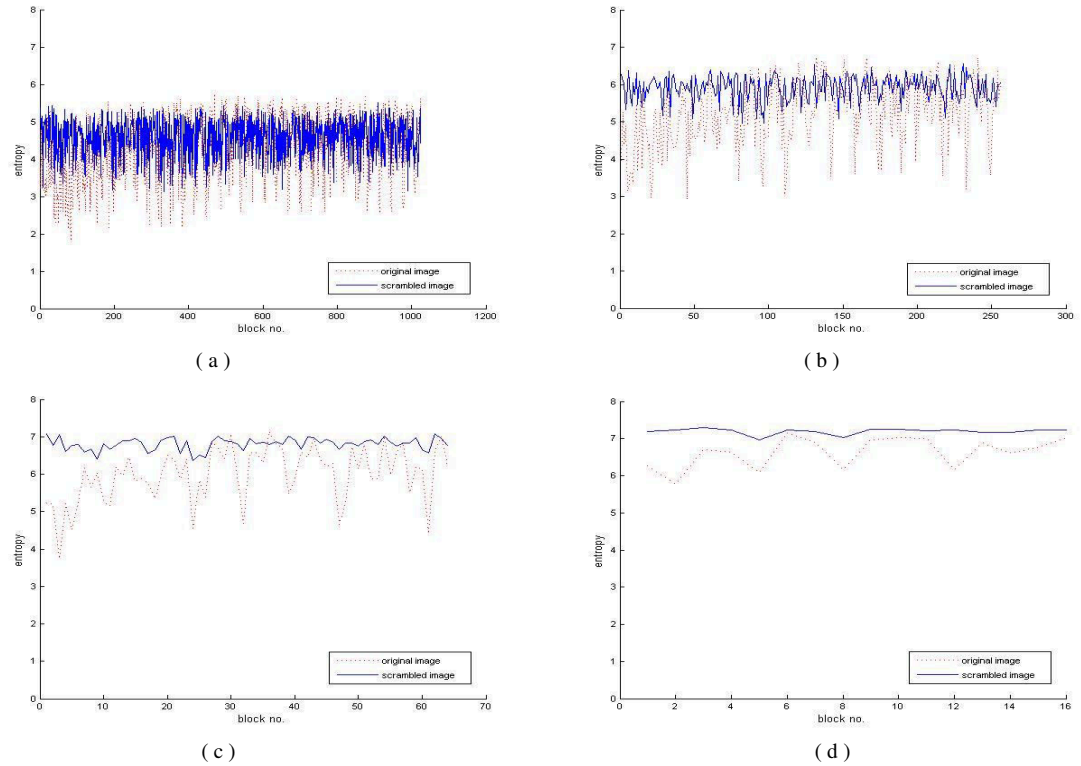
Fig. 4 Bottom-up approach (a) Original image (b) to (f) Scrambled image. (g) Decrypted image.



(a) (b)

(c) (d)

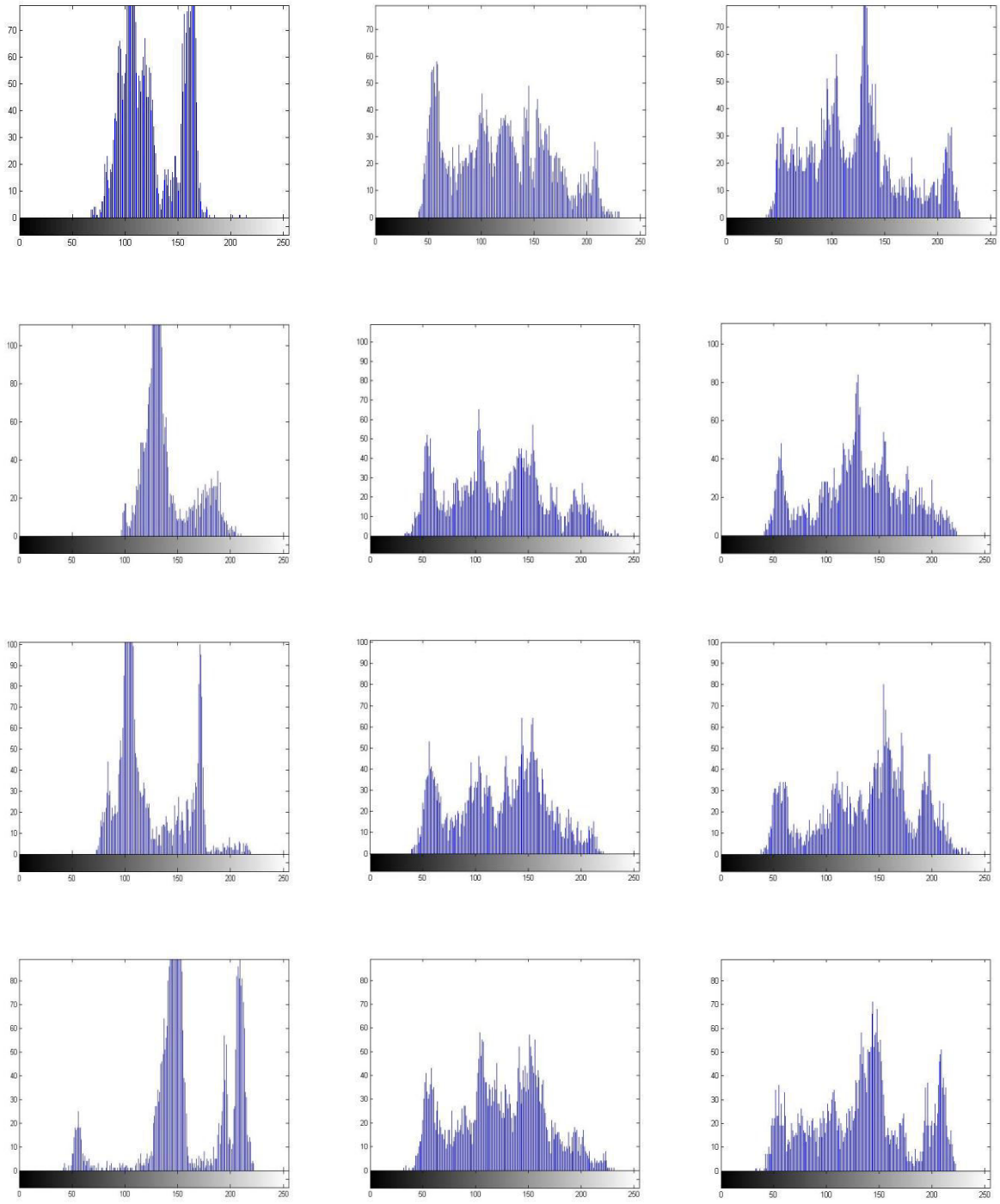
Fig 5. (a) to (d).Entropy of original image blocks and corresponding blocks in scrambled image for block size of 8x8, 16x16, 32x32 and 64x64 respectively.(Top-down approach).



(a) (b)

(c) (d)

Fig 6 (a) to (d) Entropy of original image blocks and corresponding blocks in scrambled image for block size of 8x8, 16x16, 32x32 and 64x64 respectively.(Bottom-up approach).



(a) (b) (c)

Fig. 7 (a). Histograms of image blocks of original image (b). Histograms of corresponding image blocks of scrambled image (top-down approach). (c). Histograms of corresponding image blocks of scrambled image (bottom-up approach)

6. Conclusion

In the proposed work the security of digital image is enforced via scrambling by making the image progressively heterogeneous region-wise. The quad tree decomposition technique is used for dividing the image into blocks or regions. Concept of information entropy which is a measure of the detail provided by the image is used as the foundation for scrambling by shuffling the image blocks. Further the proposed method, along with making the image heterogeneous region-wise also ensures that all the image regions are more or less equally heterogeneous by balancing the entropy of the image blocks. This implies that all the regions provide the same level of details and no particular region reveals more information. Experimental analysis carried out with various images has provided promising results. Security analyses of both top down and bottom up approach indicate that the proposed method satisfies the security criteria expected out of image scrambling technique. The proposed method provides one with an option to thrust aside the use of conventional encryption technique because of the agreeable security provided by block-based permutation of image blocks supervised by entropy principle. Further the proposed method provides the user with an option of varied security level to meet different security requirements, by choosing a threshold for entropy of image blocks, or by fixing the minimum size of image blocks at which the processing can be terminated during quad tree decomposition.

References

[1] M. A. Bani Younes and Aman Jantan, “Image Encryption Using Block-Based Transformation Algorithm”, IJCS, February 2008.
[2] A. Mitra, Y V. Subba Rao, and S. R. M. Prasnna, "A new image encryption approach using combinational permutation techniques," Journal of computer Science, vol.1, no. 1, 2006, pp.127
[3] I. Ozturk, I. Sogukpinar, "Analysis and comparison of image encryption algorithm," Journal of transactions on engineering, computing and technology December, vol. 3, 2004, pp. 38.
[4] Mohammad Ali Bani Younes and Aman Jantan, “An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption” IJCSNS, April 2008.
[5] Monisha Sharma and Manoj kumar kowar, “Image Encryption Technique using chaotic schemes: A review”, IJEST, 2010.
[6] Yuan-Hui Yu, Chin-Chen Chang and Iuon-Chang Lin, A new steganographic method for color and grayscale image hiding, Computer Vision and Image Understanding, Volume 107, Issue 3, September 2007.
[7] Qiudong Sun; Wenying Yan; Jiangwei Huang; Wenxin Ma, “Image encryption based on bit-plane decomposition and random scrambling”, 2nd International Conference on Consumer Electronics, Communications and Networks, 2012, pp. 2630 – 2633.
[8] Shou-Dong, Lu; Hui, Xu , “A New Color Digital Image Scrambling Algorithm Based on Chaotic Sequence”, International Conference on Computer Science & Service System , 2012.
[9] Alireza Jolfaei and Abdolrasoul Mirghadri, “ Survey: Image Encryption Using Salsa20”, IJCSI, International Journal of Computer Science Issues, Vol. 7, Issue 5, September 2010 pp 213-220.
[10] Shengbing Che; Zuguo Che; Bin Ma, “An Improved Image Scrambling Algorithm”, Second International Conference on Genetic and Evolutionary Computing, 2008, pp 495 – 499.
[11] A. Akhavan 1, A. Samsudin 1 and A. Akhshani, “On the Speed of Image Encryption with Chaotically Coupled Chaotic Maps", IJCSI, International Journal of Computer Science Issues, Vol. 9, Issue 3, No 3, May 2012
[12] T. Markas and J. Reif, "Quad tree structures for image compression applications", Information Processing & Management, vol. 28, no. 6, 1992, pp. 707-721.
[13] G. M. Hunter and K. Steiglitz,, “Operations on images using quad trees,” IEEE Trans. on Pattern Analysis and Machine Intelligence, vol. 1, no. 2, 1979, pp. 145-153.
[14] Furht , Kirovsk, Multimedia Security Handbook, 2005.
[15] Gonzalez, R.C., R.E. Woods, S.L. Eddins, Digital Image Processing, Second Edition, Prentice Hall, 2007.

Prabhudev Jagadeesh, is an Associate Professor in the Department of Computer Science and Engineering, Adithya Institute of Technology, Coimbatore, India. He completed his B.E degree in Computer Science and Engineering in 1997 from University of Mysore and M.Tech degree in Software Engineering in 2001 from VTU, Belgaum, India. Currently he is pursuing his PhD at University of Mysore, Mysore, India. He has over 15 years of teaching and research experience. His areas of research include Computer Vision and Information Security.

Dr. P Nagabhushan (BE-1980, M.Tech.1983, PhD-1989) is presently Professor, Department of Studies in Computer Science and also Chief Nodal Officer, Credit based choice based Education, University of Mysore. He is an active Researcher in the areas pertaining to Pattern Recognition, Document Image Processing, Symbolic Data Analysis and Data Mining. Till now he has successfully supervised 20 PhD candidates. He has over 400 publications in journals and conferences of International repute. He has chaired several international conferences. He is a visiting professor to USA, Japan and France. He is a fellow of Institution of Engineers (FIE) and Institution of Electronics and Telecommunication Engineers (FIETE) India.

Dr. R.Pradeep Kumar is Professor & Head, Department of Computer Science and Engineering, Adithya Institute of Technology, Coimbatore, India. He holds PhD in Computer Science from University of Mysore. His areas of research include Image Processing, Video Analytics, Symbolic data, Knowledge Engineering. He is currently supervising 7 PhD candidates. He has served as Head of Training and R&D sections at TCS Chennai. He has more than 25 publications in his areas of research.