2015 International Conference on Communication, Information & Computing Technology (ICCICT), Jan. 16-17, Mumbai, India

Probabilistic Triangular Shuffling Approach in DWT Based Image Compression Scheme

Afshan Mulla*, Jaypal Baviskar†, Swapnil Wagh‡, Neha Kudu§ and Amol Baviskar¶
*† ‡Department of Electrical Engineering, Veermata Jijabai Technological Institute, Mumbai 400019, India
§ Department of Electronics Engineering, Dwarkadas J. Sanghvi College of Engineering, Mumbai 400056, India
¶ Department of Electronics Engineering, Universal College Of Engineering, Kaman Road, Thane, India
*afshan.m.mulla@ieee.org, †jaypal.j.baviskar@ieee.org, ‡swapnil.wagh@gmail.com,
§nehakudu@gmail.com, ¶amol.baviskar@universal.edu.in

***Abstract*—In the image processing domain, researchers all over the world aim at designing algorithms which posses the feature of facilitating multiple advantages amalgamated in one scheme *viz.* compression, fusion, enhancement, security *etc.* In various classified applications such as military, medical, forensics *etc,* the image databases are huge and contain a lot of information. Hence, compression of these high-quality images and securing these databases becomes imperative. This paper proposes a Discrete Wavelet Transform (DWT) guided image compression as well as image security technique. The RGB color images are converted into *textured images* by exploiting DWT properties and thereby facilitating image compression. Since this process is reversible, the colors in the image are retrieved back from the texture patterns. In addition, the security of the image is enhanced based on a novel *probabilistic triangular shuffling* scheme. The overall proposed algorithm assists in achieving 67-70% compression ratio and improved security. Evaluating the performance of the algorithm, various graphs pertaining to PSNR, MSE, probability of security breach are realized.**

Keywords - **Image processing, image compression, image security, Discrete Wavelet Transform (DWT), probabilistic, triangular shuffling, color image, texture pattern, compression ratio, security.**

I. Introduction

Securing an image over the network to forestall unauthorized eavesdropping and compressing images based on lossy or lossless approach, are the cardinal aim for the researchers. With significant enhancement in visual intelligence and image investigation methods, image data is used in various sensitive applications such as military surveillance, forensic investigation, medical-care *etc.* In these applications, huge classified image databases are maintained that are liable to be hacked by the attackers. Depending upon the application spectrum, suitable compression [7] [9] [11] and security algorithms should be implemented. Tremendous efforts have been conceded in the past [1] for the development of security algorithms focusing on visual data such as high redundancy, strong correlation between adjacent pixels *etc.* Usually chaotic encryption standards are popular [2] [3] because of their density function feature, which is dispersed and distributed due to small key space. In [4] Lian *et al.* demonstrated a novel block cipher based on the implementation of logistic map in the diffusion process. The need for image security is aggravated by the fact that the existing standard symmetric ciphers do not adapt to inherent image features, as mentioned by Mao *et al.* and Qiao *et al.* in [5] [6]. Hence, this paper proposes a unique technique to provide *probabilistic triangular shuffling* of segmented blocks. This approach yields robust performance and mitigates the probability of the attacker getting hold of authorized access to the images in the database.

In addition to security, the vast image databases demand storage of data with minimum memory requirement and limited bandwidth utilization. Hence, the need for algorithms facilitating compression, is imperative. The application area discussed above contain images that posses high quality. Hence, they stipulate large bandwidth requirement, memory storage and more transmission time. Since, colored images exploit network bandwidth and demand more computational time, they can be converted to gray-scale. Doing so minimizes the basic requirements, but many discrete colors when transformed to gray-scale exhibit approximately similar brightness. This is because each color varies from 0-255 level of gray, vanishing their visual incongruity *eg.* light blue and light green. This creates ambiguity at the recipient side while reproducing the original colored images. The solution to these issues are resolved in this paper.

This paper proposes an extremely unique algorithm that facilitates improvement in security of images, as well as it engenders compression without hampering the quality of the image. It is guided by a novel method for transforming RGB color images to *textured* images. This is achieved by replacing certain sub-bands generated *via* DWT by chrominance information. Creating unique texture patterns for each color, even if they have same luminance component and mapping them to high frequency low visibility feature, it assigns unique texture patterns [8] to every individual color. Converting color images to textured images provides compression. The security aspect is enhanced by exploiting properties of matrix and random signal synthesis. A unique scheme based on probability, segmentation and shuffling is implemented, in order to create a synthesized image.

The paper is organized as follows; Section II explains the novelty of the proposed security algorithm by describing the triangular shuffling method in detail. Section III presents the proposed algorithm, which deals with an altogether new image security and compression scheme, for ensuring bandwidth efficiency and enhanced safety. Section IV evaluates and discusses the various image analysis parameters and renders security performance. Section V concludes the paper by summarizing the overall idea.

II. Image Security: Probabilistic Triangular Shuffling Approach

Securing image databases, so as to forestall attackers accessing the data has aggravated the demand for image security algorithms. This paper presents a Probabilistic Triangular Shuffling (PTS) algorithm to provide shambling of pixels based on the properties of matrices and a probabilistic approach. It offers a robust computational method, but an extremely reliable one. Since images are naturally of 2 dimensions, they are competently converted into 2D vector matrices. In this technique, the matrices are operated with processes pertaining to segmentation and division of individual blocks into unique triangular sections, and then performing random pixel shuffling algorithm. The process for triangular shuffling is explained in Fig.1.

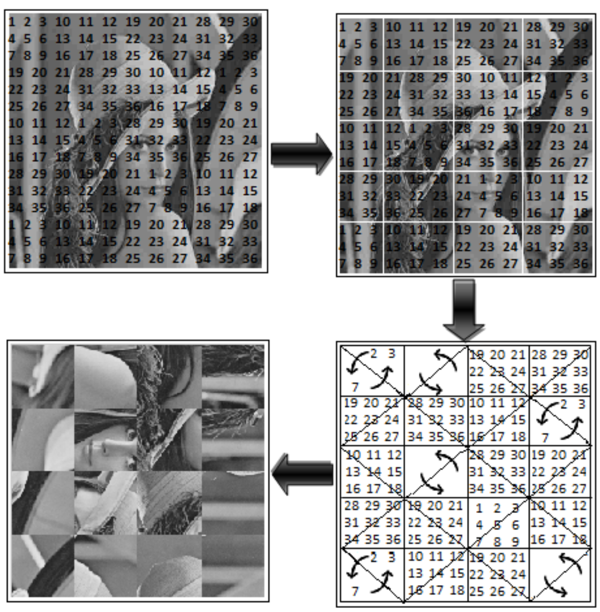

Fig. 1. Triangular Shuffling process on Images

Each of the block in the segmented image is subjected to alternating forward or reverse triangular division operation. The two half sections thus formed are then interchanged by performing Left to Right (LR) or Right to Left (RL) triangular shifting. The image thus created is subjected to a probabilistic shuffling algorithm which generates a chaotic image. The segmented image is diffused to the shuffled and bit-plane separation of the original textured image. The pixels in the image are shuffled, in order to prevent the attacker from accessing the image details. With a rapid image securing procedure and high degree of safety performances, the proposed scheme provides a potential alternative to digital image storage in a various applications *viz.* in national security control, or in crime prevention, payment system, detection, and forensics. The technique is expected to provide flat responses in histogram plots between actual and shuffled images. The algorithm assisting the above explained operation is illustrated in Algorithm 1.

1. Data: Input the image; nS= no. of segment
2. initialization;
3. for *nS = 4,16,32,64,128...* **do**
  Execute Segmentation Algorithm
end
4. Select each segment block randomly
5. if *segment == even* **then**
  Perform Right to Left triangular shuffling
end
6. if *segment == odd* **then**
  Perform Left to Right triangular shuffling
end
7. Initialize new image matrix
8. Perform Horizontal row concatenation for row segment block
9. for *Segmentation completed* **do**
  Perform Vertical concatenation of horizontal block segments
end
10. if *Segmentation incomplete* **then**
  Goto line 8
end
11. Display Shuffled Image by mapping matrix

Algorithm 1: Algorithm for Triangular Shuffling of Images

III. Implementation of Image Compression and Security Algorithm

The algorithm suggested in this paper is suitable for huge image databases containing colored RGB images. The processing technique discussed in further sections involve image compression scheme based on an extremely unique DWT subband replacement technique, whereas the security algorithm achieves enhanced reliability of protecting the images through execution of triangular shuffling scheme. Fig. 2 delineates the implemented scheme in detail.

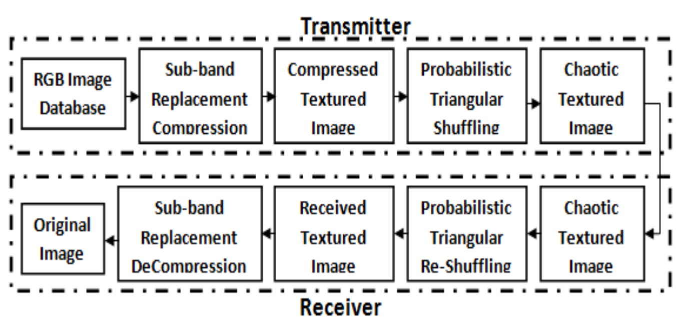

Fig. 2. Image Compression and Security Enhancement System

978-1-4799-5522-0/15/$31.00 ©2015 IEEE

A. Image Compression: Mapping of Color image to Textured Image

Compressing color images require processing on any two planes out of the three *viz.* Red, Blue and Green (RGB) planes. Another important plane is the luminance (Y) plane which provides the brightness information. The Sub-band Replacement DWT based image compression scheme assists in compressing RGB color images, by creating textured images. They also posses the reversibility feature for retrieving original colors back from the texture patterns. The procedure is explained by taking Fig. 3 as test image.

Fig. 3. Test Image

- The *RGB* color-space of the image is transformed into *YCbCr* color-space.
- The luminance (Y) component is considered for applying 2-level discrete wavelet transform (2-level DWT).
- The sub-bands generated by the DWT operation contains approximation co-efficients (LL sub-band) and detailed co-efficients (LH, HL and HH sub-bands). The detailed co-efficients provide edge information and are available in both the DWT levels.
- Since, the main aim is to embed the chrominance (color) information in this image, the sub-bands in the first level of DWT *viz.* LH1 and HL1 are *replaced* by the chrominance (Cb & Cr) planes respectively.
- The image thus created is processed with 2-level Inverse DWT (I-DWT).
- This results in creation of a textured image, which consist of texture patterns that are essential in determining the colors in the image.

Fig.4 demonstrates the procedure for creating texture image. This textured image is the compressed version of the original color image and contains chrominance information mapped to high frequency low visibility patterns. It does not create a lookup table for mapping colors, but embeds additional information by replacing sub-bands, thereby facilitating compression.

B. Image Security: Triangular Shuffling Scheme

The generated textured image is processed with probabilistic triangular shuffling algorithm. The procedure facilitates enhanced security by producing images shown in Fig.5. In order to produce a chaotically shuffled image, the proposed

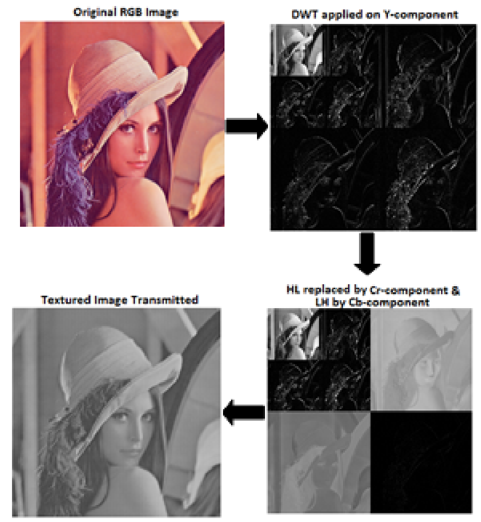

Fig. 4. Creation of compressed textured image

algorithm shambles the textured image with a probabilistic approach, explained in section II. This mitigates the probability of the attacker intercepting the image.

The compressed textured image generated by the compression scheme is segmented into 2x2 or 4x4 or 8x8 or 16x16 blocks. The size of the block determines the level of security offered by the algorithm. Smaller the size of the block, more secure is the image. After creating block segments, each alternate block is divided diagonally into forward or reverse divisions, creating triangular sections. These sections are shuffled probabilistically to generate secured image, which is difficult to decode by the attacker. This chaotic image is then transmitted over the link. The shuffled image being chaotic in nature, shows high sensitivity to security keys, and a adequately huge key-space to resist the brute attack.

Fig. 5. a) Compressed Textured Image, b) Shuffled Textured Image

C. Reshuffling at Authenticated receiver side and Retrieving color image

The algorithm is designed for a two layered secure network. The key generation and distribution is presumed to be performed prior to the image transmission process. The chaos created in the textured image is corrected at an authenticated

978-1-4799-5522-0/15/$31.00 ©2015 IEEE

Fig. 6. Retrieval of RGB Image at Authenticated user side

user side by using suitable key. The received textured image is subjected to the wavelet transform (DWT). On achieving the sub-bands, the chrominance (Cb& Cr) components are retrieved. For a RGB image to be recreated, the luminance component (Y) should be recovered. Since the Cb & Cr components are obtained from the 1st level DWT, the image is interpolated by 2nd level HL and LH sub-bands as depicted in Fig.6. This image is then processed with I-DWT, and the luminance component (Y') is retrieved. By obtaining the Y', Cb and Cr planes, the RGB image is recuperated faithfully.

IV. Result and Performance Evaluation

In order to evaluate the performance of the proposed algorithm, the simulations are executed in MATLAB. The key for correcting the shuffled textured image into actual textured image is given by the Diffe-Hellman rule multiplied by the size of segmented sub-image (2x2, 4x4, 8x8 *etc.*) and its positions. Hence, the security key is in the format $S * 2M$; where 'S' is significant and 'M' is an exponent. The recovered image

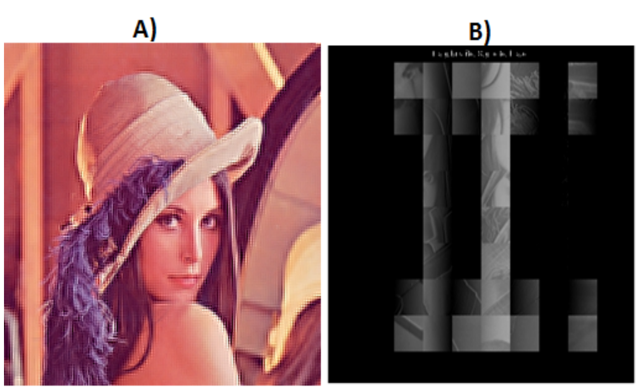

Fig. 7. a) Faithful reconstruction with valid key, b) Unfaithful reconstruction with invalid key

if decrypted with a wrong-key creates an entirely confused reconstruction, and the original RGB image cannot be extracted. Fig. 7 demonstrates faithful and unfaithful reconstruction of images. Only with valid keys and accurate chrominance information, the RGB image can be recovered.

A. Image Security Aspect

The image histogram provides information about the number of pixels in an image at different intensity levels. Each plane of the image exhibits 256 levels for signifying intensity. Graphically, the histograms display 256 numbers with distribution of pixels amongst luminance values. The intensities of original textured image in the histogram are contributed with different values, as compared to shuffled textured image histogram shown in Fig.8.

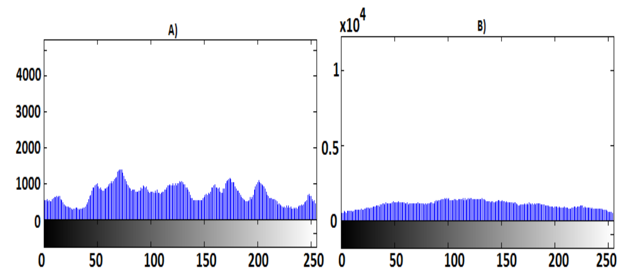

Fig. 8. a) Histogram of Original Textured Image, b) Histogram of Shuffled Textured Image

The histogram for actual textured image shows distribution of intensity levels varying with the pixels. The histogram indicating flat response for shuffled textured image creating chaos and confusion for the attacker, signifies that the luminance values are uniformly contributed over all the intensity range.

B. Fidelity of Retrieving Accurate RGB color image

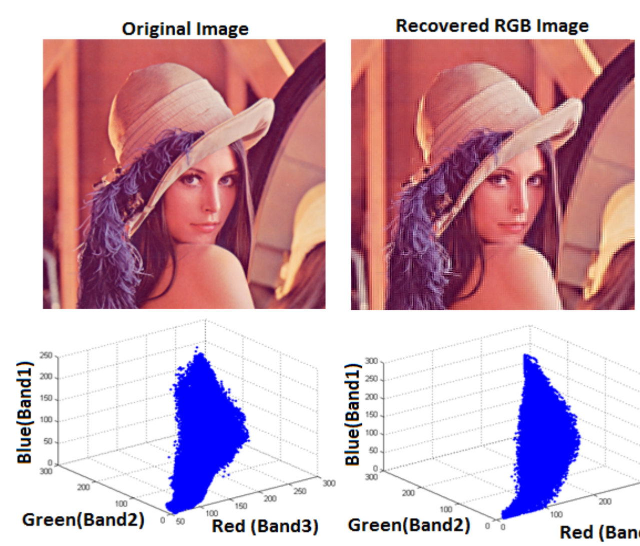

Fig. 9. a) RGB Plot of Original Color Image, b) RGB Plot of Recovered Color Image

978-1-4799-5522-0/15/$31.00 ©2015 IEEE

In order to verify the faithful reconstruction of RGB images after the creation of compressed textured image & reshuffling it to transmit over the link, and finally reconstructing it; the RGB Plot for original and resurrected images are plotted. Fig. 9 demonstrates the similarity between the two images and it is apparent that the original & the reconstructed images are identical with no pixel loss owing to complete bit-plane separation and combinations. It is observed that certain edges are spread, due to exploiting HL & LH sub-bands, that contain edge information.

C. Analysis of Image Quality Parameters

The algorithm offers significant compression along with enhanced security. The technique should provide high compression ratio with minimum quality degradation. Also, it should offer acceptable Peak Signal to Noise Ratio (PSNR) at correspondingly low Mean Square Error (MSE) values. If these requirements are satisfied, only then it can be considered as an efficient scheme for compression. As a result, the evaluated PSNR and MSE are plotted against bits per pixel (bpp) shown in Fig.10 and Fig.11.

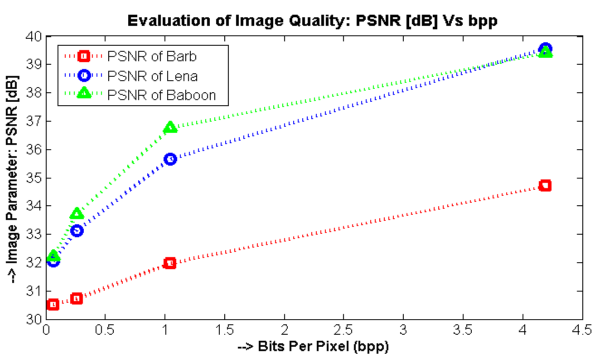

Fig. 10. PSNR [dB] v/s bpp

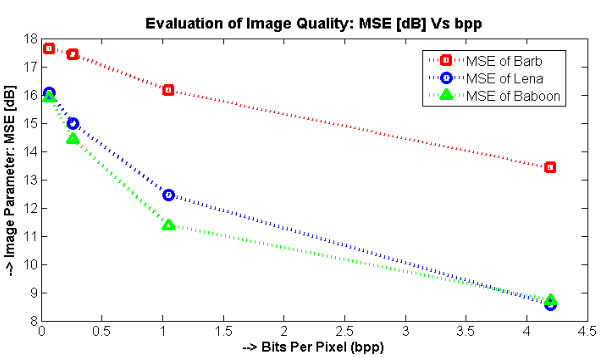

Fig. 11. MSE [dB] v/s bpp

The MSE signifies that the reconstruction of color images is achieved without hampering the quality. Table 1 illustrates the compression ratio achieved for selected standard images *viz.* lena, baboon, barb *etc.* The compression ratio achieved ranges from 60% to 75%.

TABLE I
ANALYSIS OF IMAGE COMPRESSION RATIO

Parameters	Image 1	Image 2	Image 3
Original size	4.4297Mb	6.3666Mb	4.8804Mb
Textured size	50.867Kb	63.163Kb	65.062Kb
CR	63.083	69.793	75.0113

D. Probabilistic Evaluation for Security Enhancement

In this approach, the triangular shuffling is carried out on the image to be transmitted. The number of segments and the triangular shuffles (either Left to Right or vice-versa) are cardinal factors to strengthen the security. In case of *Brute Force Attack* [10], number of attempts would increase drastically with increase in the permutations. The graph of number of segments of image v/s number of attempts in Brute Force attack is depicted in Fig.12. The number of permutations is evaluated by the formula;

$$N =^n \mathrm{P}_r \tag{1}$$

where, N= Number of permutations
n= Number of segments in an Image
r= Required number of segments

The case discussed in this paper requires same no. of segments as the total number of segments available, in order to avoid any loss of data. Hence, the number of permutations can be estimated by;

$$N =^n \mathrm{P}_n = n! \tag{2}$$

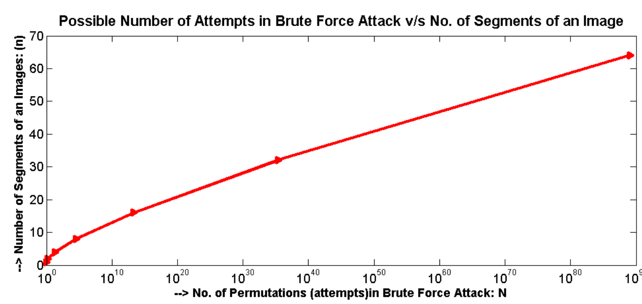

Fig. 12. Number of segments of image v/s number of attempts (permutations) in Brute Force attack

Along with the permutations, another factor contributing to the probability of success is the probability of acquiring the correct image from the shuffled one. The graph of probability (P) v/s number of attempts in Brute Force attack is depicted in Fig. 13 The probability of failure (P) is given by;

$$P = \frac{1}{Number\ \ of\ \ Permutations\ \ (N) * 2!} \tag{3}$$

It can be observed that, linear increase in the number of segments results into the exponential increase in the number of permutations (refer Fig.13). Also, it drastically decreases the probability of acquiring correct image by the attacker. Hence, triangular shuffling approach provides th third layer of the security in transmission of images over the network.

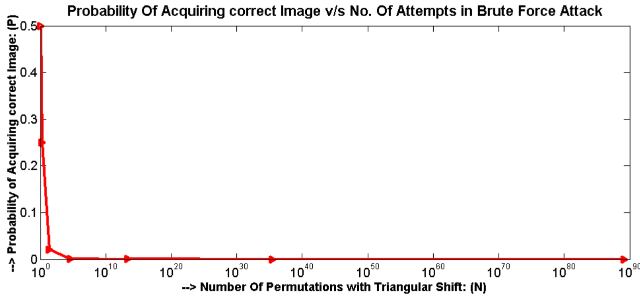

Fig. 13. Probability of acquiring the correct image v/s Number of attempts

V. Conclusion

The algorithm implemented in this paper facilitates enhanced security as well as quality conscience compression ratio. It is based on an extremely unique method known as *Probabilistic Triangular Shuffling Approach in DWT Based Image Compression Scheme.* The algorithm efficiently maps RGB images to unique texture patterns in a three plane format. The creation of patterns on the image assists in adding confusion and chaos with the image, since it is further processed with a probabilistic triangular shuffling algorithm. The overall algorithm facilitates improved security, in terms of preventing the attacker from acquiring the information and features of the images in the database. The probability of the attacker retrieving the correct images is very probabilistic in nature, which is illustrated with appropriate histograms and other plots. Also, this technique offers acceptable compression ratio, maintaining good PSNR value, thereby mitigating errors. Overall, the Probabilistic Triangular Shuffling Approach based on DWT Sub-Band Replacement technique is highly reliable and competitive algorithm in image processing domain.

Acknowledgement

We would like to thank our friends for their crucial help in our work. We are also thankful to our institute Veermata Jijabai Technological Institute, Mumbai, India for providing the facilities to carry out our research.

References

[1] Baviskar J., Mulla A., Baviskar A., et.al, Adaptive Matrix Design For LDPC Based Image Processing System," *International Conference on Advances in Computing, Communications and Informatics (ICACCI), Delhi, India,2014,* vol.,no., pp.2374-2379, 24-27 Sept.2014

[2] Baviskar A., Ashtekar S., and Chintawar A., "Performance Evaluation of High Quality Image Compression Techniques," *International Conference on Advances in Computing, Communications and Informatics (ICACCI), Delhi, India,2014,* vol., no., pp.1986-1990, 24-27 Sept, 2014

[3] Mulla A., Baviskar J., Baviskar A., et.al, Image Compression Scheme Based on Zig-Zag 3D-DCT and LDPC Coding, *International Conference on Advances in Computing, Communications and Informatics (ICACCI), Delhi, India,2014,* vol., no., pp.2380-2384, 24-27 Sept, 2014

[4] A. Uhl, A. Pommer, Image and video encryption, Springer, USA, 2005

[5] X. G. Wu, H. P. Hu B. L., and Zhang. Analyzing and Improving a Chaotic Encryption Method. Chaos, Solitons and Fractals, 22(2):367373, 2004

[6] T. Yang. A Survey of Chaotic Secure Communication Systems. Journal of Computational Cognition, 2(2):81130, 2004

[7] S. G. Lian, J. Sun, and Z. Wang. A Block Cipher Based on a Suitable Use of Chaotic Standard Map. Chaos, Solitons and Fractals, 26(1):117129, 2005

[8] Y. Mao, G. Chen, Chaos-based image encryption, *In Eduardo Bayro-Corrochano, editor, Handbook of Computational Geometry for Pattern Recognition, Computer Vision, Neural Computing and Robotics.* Springer-Verlag, Heidelberg, April 2004

[9] L. Qiao, K. Nahrsted, Comparison of MPEG Encryption Algorithms, *Computers and Graphics Journal,* Vol. 22, No. 4, pp.437-448, 1998

[10] Mulla Afshan, Namrata Gunjikar, and Radhika Naik, Comparison of Different Image Compression Techniques. *International Journal of Computer Applications 70, no. 28 (2013)*

[11] Baviskar J., Mulla A., Baviskar A., et.al, Sub-Band Exchange DWT Based Image Fusion Algorithm for Enhanced Security,*International Conference on Advances in Computing, Communications and Informatics (ICACCI), Delhi, India,2014,* vol., no., pp.534-539, 24-27 Sept, 2014