RESEARCHERID
THOMSON REUTERS

ISSN: 2277-9655
[Shunmugan* *et al.*, 6(7): July, 2017] Impact Factor: 4.116
IC™ Value: 3.00 CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

AN EFFICIENT JOINT ENCRYPTION AND COMPRESSION USING HOP AND PERMUTATION

S. Shunmugan[*1] & P. Arockia Jansi Rani[2]

[*1]Research Scholar, Dept of Computer Science and Engineering, ManonmaniamSundaranar University, Tirunelveli

[2]Associate Professor, Dept of Computer Science and Engineering, ManonmaniamSundaranar University, Tirunelveli

DOI: 10.5281/zenodo.823090

ABSTRACT

A new coding initiative is introduced "Visually lossless" coding in place of numerically lossless coding to reduce the piling space and lower data transmission. The question for introducing this new coding method arises due to the increased image sizes. Here we speak about the lossy compression method on encrypted image, which compresses the image with minute quality losses that cannot be detected. This lossy compression method includes DCT with RLEcompression, Hierarchical Oriented Prediction (HOP), uniform quantization, orthogonal matrix generation, negative sign removal and Huffman compression. The encrypted image is divided as elastic part, which is compressed using Xingpeng Zhang method and rigid part for which HOP method is used for compression. This method is tested in different type and size of images and the results are obtained. The results reveal that this method is much better than the existing compression methods. The bit rate reduction ratio of this method is 10.45% and the naked eye perception is visually lossless.

KEYWORDS: EJPEG, HOP, EHUFFMAN, Orthogonal matrix, Iterative encryption, RLE, DCT.

I. INTRODUCTION

Image processing requires a pile of data. The problem with image compression techniques is that the digital image has to be compressed in such a manner that the amount of space required should be reduced without affecting the quality of the image. The image is compressed in two ways: lossy and lossless methods. Lossless method presents an image which is equivalent to the original and in the case of lossy, the image in the original and reconstructed differ in quality.

The necessity for image encryption evolves because in the modern world image travels to diversified sectors. Hence to maintain confidentiality, encryption is required over and above compression. Access rights of an encrypted image lies only with authorized sources. Image security [4] is the process of controlling and protecting highly sensitive and confidential images. An image can be preprocessed and transformed to some intermediate form to be compressed with better efficiency, so as to avoid natural redundancy.

Image compression (only reduces the size and security is less) and encryption (plays vital role in securing the image both at rest and transit [5]) can be classified as "Compression-then-Encryption" and "Encryption-then-Compression". There are very less chance to access the image and the image size is more in the Later. Former has chance to access the image with reduced size. Encryption-then-Compression is represented in Fig. 1 and Compression-then-Encryption is represented in Fig. 2.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

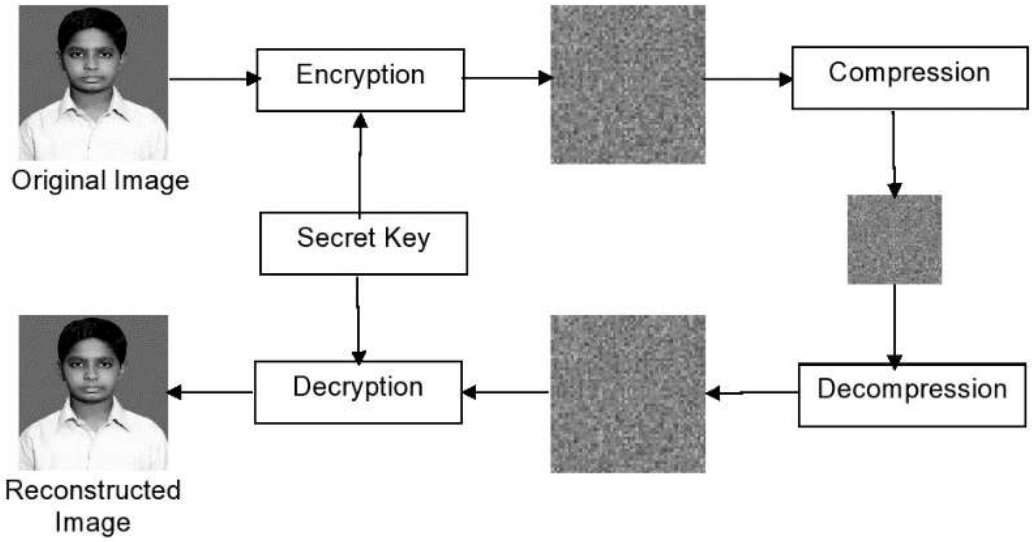

Fig.1. Encryption-then-Compression Scheme

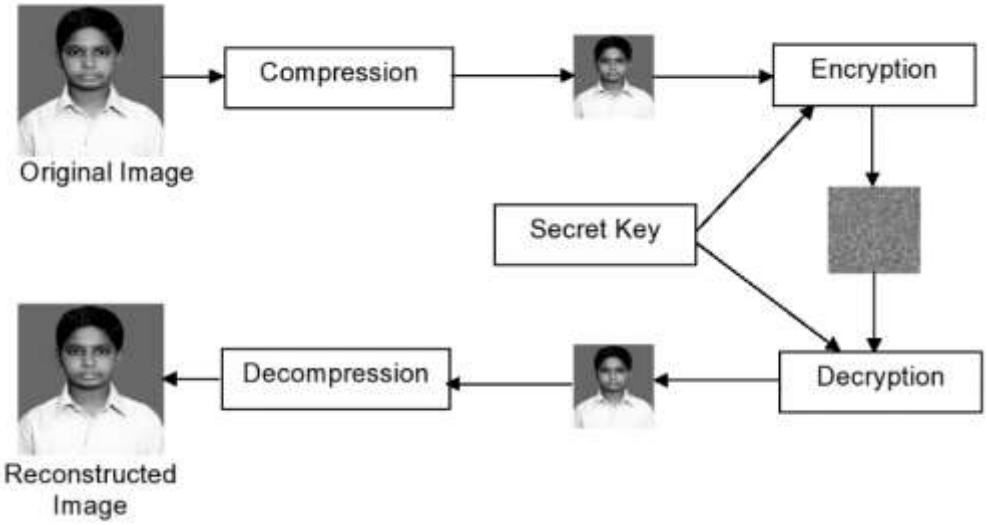

Fig.2. Compression-then-Encryption Scheme

This paper discusses how an image is compressed both in lossy and lossless methods with high security. For that the image is divided in to rigid data and elastic data. Rigid data is compressed using the lossless method and elastic data is compressed using the lossy method.

The rest of this paper is organized as follows: The related works are briefly discussed in Section II. The section III explains the proposed methodology. Section IV contains the analysis of the research work. Final section discusses the conclusion.

II. RELATED WORKS

The SCAN methodology presented by S.S. Maniccam and N.G. Bourbakis [6]. This method described the lossless compression and encryption of 512 x 512 gray scale images.

By applying the Independent Component Analysis (ICA) and Discrete Cosine Transform (DCT) technique Masanori Ito et al. [7] proposed a method by combining encryption and compression in which the an insignificant image covers the image to hide it and their mixtures to be transmitted in encryption. ICA algorithm is applied to reconstruct the original image. The DCT and simple low pass filter are used in the

compression. But in this method the quality of the reconstructed image is reduced, because the higher frequency components are cut off.

Sinha A. and Singh K. [8] introduced a method to encrypt the image using digital signature for the secured transmission.

Wei Liu et al. [9] developedstream cipher based Slepian-Wolf coding for encryption with progressive lossless reconstruction.

The image encryption algorithm proposed by V.Radha and D.Maheswari [10] consists of two parts: scrambling of plain-image and mixing operation of scrambled image using discrete states variables of chaotic maps and DCT is used for compression, which reconstructs the image with high security and great speed but its compression ratio is less.

Zhi-Hong Guan [11] developed an image encryption scheme, in which rearranging the pixel positions andmodifying the image pixel's grey values.

MitraA [12] used a random combinational image encryption approach using pixel, bit and block permutations.

J. Zhou [13] introduced an ImageCompression system in which a pair of encryption is done prior to image compression.

Riccardo Lazzeretti[14] developed lossless encrypted image compression with source coding and permutations.

Shannon [15], introduced a new compression-then-encryption method in which after reducing the interpixel redundancies, the DWT is applied. Finally AES is applied to encrypt the data.

The progressive compression method introduced by Wei Liu [16] adopted a new compression method with stream-cipher based encryption.

Shantanu D. Rane and Guillermo Sapiro [17] investigated and explained the application of JPEG-LS.

MarkosPapadonikolakis [18] proposed a new JPEG-LS compression with pipeline design with LOCO-I algorithm.

III. METHODOLOGY

A securedimage compression method is proposed in this paper. Fig.3. shows architecture of the proposed method.

The input image is reduced using uniform quantization, to reduce its size. Using the iterative encryption procedure, the image undergoes the process of encryption. Further the encrypted image is divided into rigid data and elastic data [1]. Visually lossless technique is applied to compress the rigid data whereas lossy compression method is applied in compressing elastic data.

For visually lossless compression the rigid data is divided into two parts namely L & H using the Hierarchical Oriented Prediction (HOP) [10]. The L part contains horizontal even index pixel and H part contains horizontal odd index pixel. It is blocked in to 5 x 5 window. Again L is divided into LH & LL. From L data $H_Prediction$and $V\_Prediction$ are calculated.$H\_Prediction$ is calculated using the horizontal pixels and $V\_Prediction$ is calculated using the vertical pixels.

$$H\_Prediction(i,j) = fix(\frac{sum}{12}) \quad (1)$$

$$V\_Prediction(i,j) = fix(\frac{sum}{12}) \quad (2)$$

where $i \in [0, L\_image\ height - 1]$
$j \in [0, L\_image\ width - 1]$
12 is the total number of pixels participated in the 5 x 5 window

Then,$H\_Error\ Image$ and$LH_Error\ Image$ are calculated.

$$H\_Error\ Image(i,j) = H(i,j) - H\_Prediction(i,j) \quad (3)$$

$$LH\_Error\ Image(i,j) = LH(i,j) - V\_Prediction(i,j) \quad (4)$$

where $H(i,j)\ is\ horizontal\ odd\ index\ data\ at\ the\ location\ i,j$
$LH(i,j)\ is\ horizontal\ odd\ index\ data\ at\ the\ location\ i,j$

The error information occupies one byte (8 bit) data storage. It may contain negative values. So one more bit is needed to store the error information. The following Equations are used to avoid the extra one bit to store negative information.

$$If\ (H\_ErrorImage(i,j) < 0.0) \quad (5)$$
$$H\_ErrorImage(i,j) = abs(H\_ErrorImage(i,j)) + 1$$
$$end$$
$$If\ (LH\_ErrorImage(i,j) < 0.0) \quad (6)$$
$$LH\_ErrorImage(i,j) = abs(LH\_ErrorImage(i,j)) + 1$$
end

The 7 bit data is converted into 8 bit sequence i.e. 7 bit data are placed continuously in the linear form. Then the continuous 8 bits are grouped as a single byte data and these data are used to form the integrated linear error information. Finally, LL and the integrated linear error information are combined to form a new rigid data.

The elastic data is compressed using Orthogonal Matrix Generation and Nearest Pixel calculation. The compressed elastic data and the new rigid data are concatenated and form the new compressed image. To increase the security it is again permuted. The Huffman compression is applied on the permuted data and get the final compressed data.

The compressed rigid data and the compressed elastic data are separated in the decompression section whereas Huffman decoding is applied on the compressed data. That data is inversely permuted to get LL, integrated linear information and compressed elastic data.

The 8 bit error sequence is converted back into 7 bit data sequence. The negative sign information is extracted from the LSB of the 7 bit data sequence using the Equation 6.

$$If\ (mod(H\_ErrorImage(i,j),2) == 1) \quad (7)$$
$$H\_ErrorImage(i,j) = H\_ErrorImage(i,j) * -1$$
$$end$$
$$If\ (mod(LH\_ErrorImage(i,j),2) == 1) \quad (8)$$
$$H\_ErrorImage(i,j) = LH\_ErrorImage(i,j) * -1$$
$$end$$

The predicted-LH is constructed using the original-LL using the HOP prediction. The reconstructed-LH is obtained by adding the predicted-LH and error-LH using Equation 9.

$$LH(i,j) = V\_Prediction(i,j) + LH\_Error\ Image(i,j) \quad (9)$$

The reconstructed-H is obtained by adding the predicted-H and error-H using Equation 10.

$$H(i,j) = V\_Prediction(i,j) + H\_Error\ Image(i,j) \quad (10)$$

The original-LL, reconstructed-H and the reconstructed-LH are used to generate the reconstructed-L.The reconstructed-L and the reconstructed-H are combined to reconstruct the final rigid data. The elastic data is decompressed using nearest pixel calculation and orthogonal matrix generation. Then the rigid data and elastic data are concatenated and the data is decrypted. Again that data is reverse quantized in order to the reconstruct the output image.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

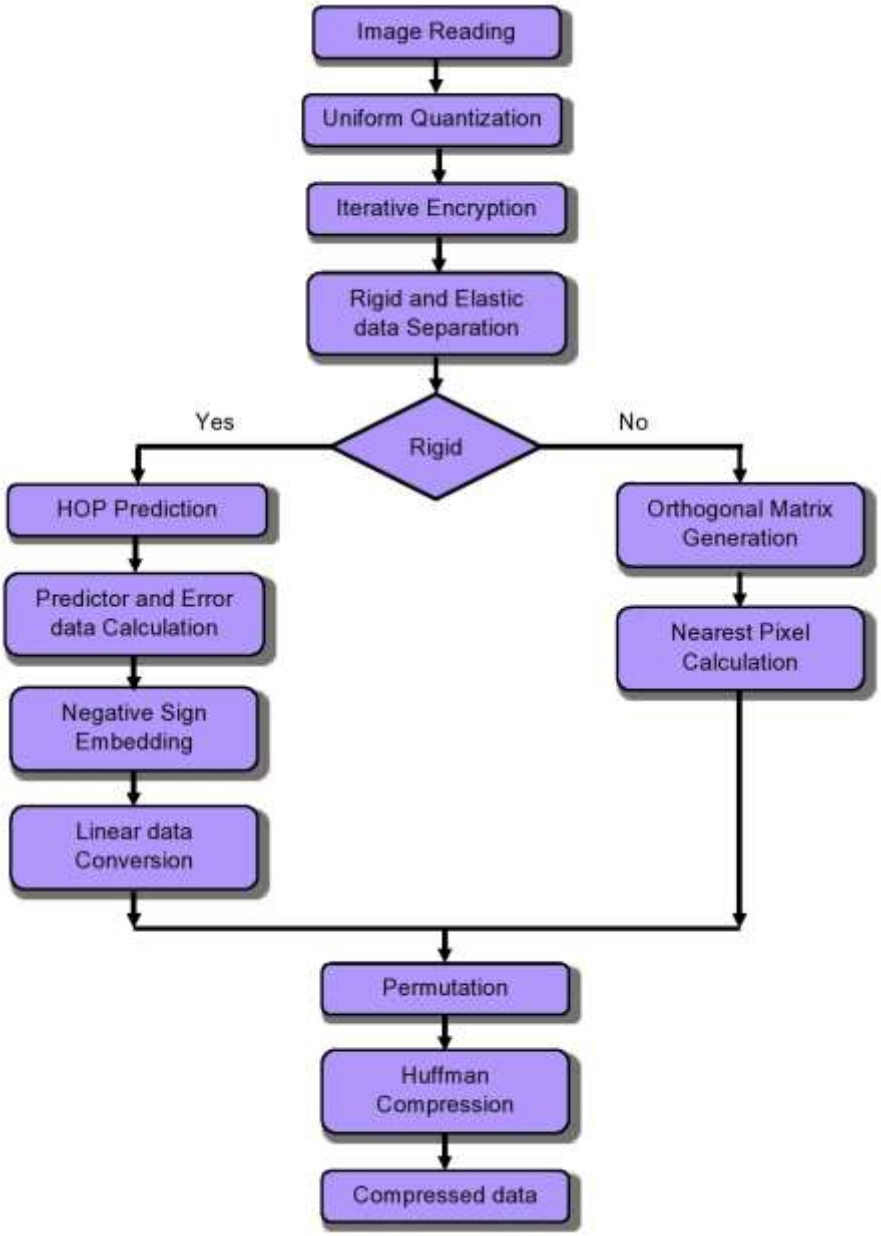

Fig.3. Proposed compression Scheme

IV. EXPERIMENTAL RESULTS

The performance of existing methods such as encrypted JPEG-LS, encrypted HUFFMAN and Ximpeng Zhang method are compared with that of the proposed method using a variety of experiments.

JPEG-LS [19], is one of the lossless coding of still images. The key function of this method is to use a lossless image coding which has lower complexity and better compression efficiency. In the process of implementation, the image is encrypted and it is compressed using JPEG-LS method. It is referred as the Encrypted JPEG method (EJPEG).

Huffman coding is a lossless data compression algorithm. The idea is to assign variable-length codes to input characters, lengths of the assigned codes are based on the frequencies of corresponding characters. The most frequent character gets the smallest code and the least frequent character gets the largest code. In the

implementation the Huffman coding is applied after the image encryption. It is referred as Encrypted HUFFMAN method (EHUFFMAN).

The DCT with RLE [1] method delivers a scheme for encrypted image compression in lossy manner. This methodology includes the components of joined image encryption with compression and joined decompression with decryption. In the decompression section Run-Length Encoding approach is proceeded.

A good system provides maximum secrecy with maximum fidelity using the least number of bits/symbol [20]. From Table 1, it can be inferred that the proposed work gives compression ratio around 2.0 for color images.

The Fig. 4shows various stages in compression. Intially the original image is read and displayed. Subsequently its Red channel images are displayed. Similarly the remaining Green and Blue chanel images are displayed.

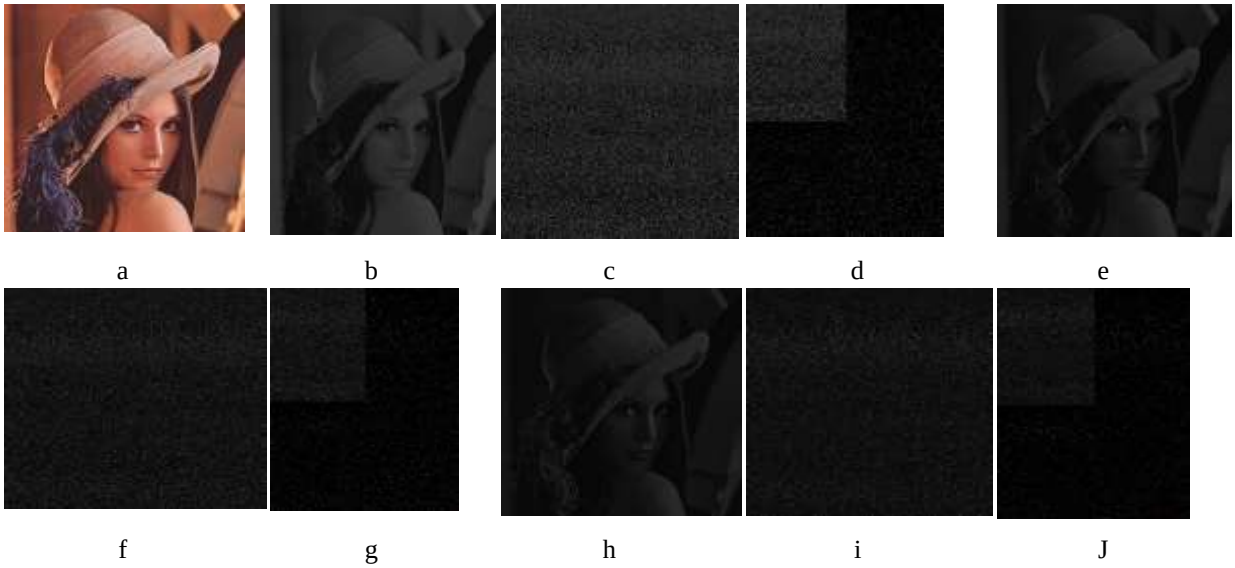

Fig.4. Compression stage:
a. Original color image b. Red channel color image c. Encrypted Red channel d. HOP Red channel e. Green channel color image f. Encrypted Green channel g. . HOP Green channel h. Blue channel color image i. Encrypted Blue channel j. HOP Blue channel

The Fig. 5shows various stages in decompression. Intially the compressed HOP Red chaneel image is displayed. Subsequently decrypted Red channel image and Enhanced Red channel image is dispayed. Similarly the remaining Green and Blue chanel images are displayed. Finally reconstrued image is displayed.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

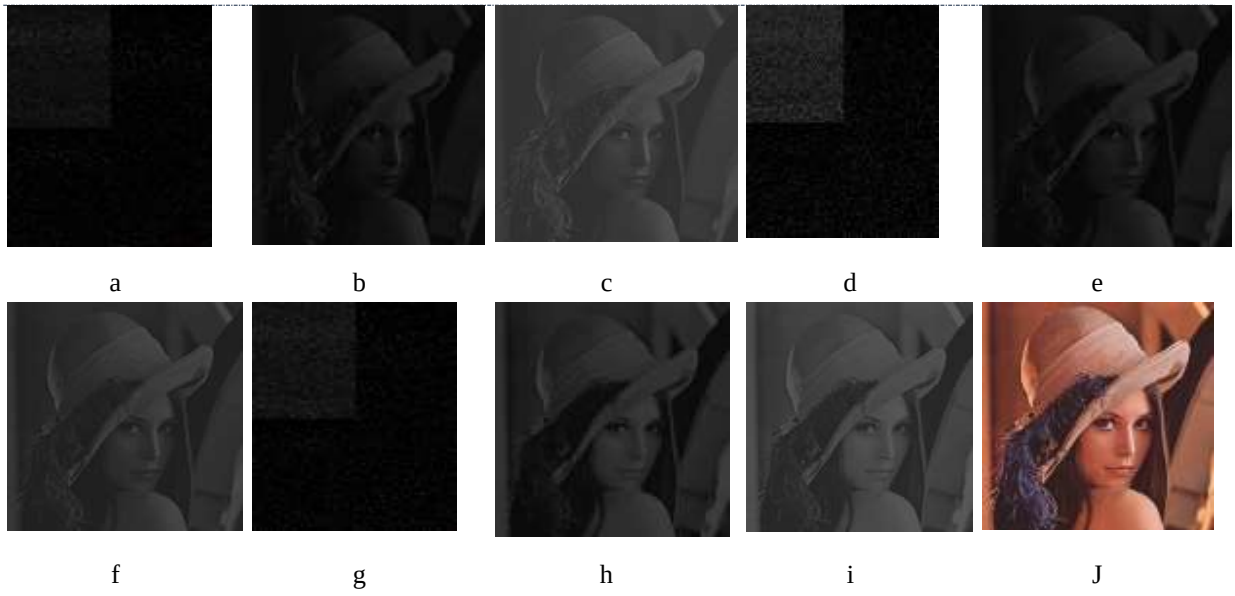

Fig.5. Decompression stage:
a. HOP Red channel b. Decrypted Red channel c. Enhanced Red channel d. HOP Green channel e. Decrypted Green channel f. Enhanced Green channel g. . HOP Green channel h. Decrypted Blue channel i. Enhanced Blue channel j. Reconstructed Image

The performance of the proposed work is compared in terms of compression ratio for 35.4db PSNR values and the results are tabulated in Table 1.

Table 1. Performance analysis with CR for PSNR 35.40 db

Image Name	Algorithm	CR
Lena.bmp	EJPEG	1.5445
	EHUFFMAN	1.2348
	DCT with RLE	1.4538
	Proposed	**2.0774**
Peppers.bmp	EJPEG	1.5374
	EHUFFMAN	1.2345
	DCT with RLE	1.4863
	Proposed	**2.6191**

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

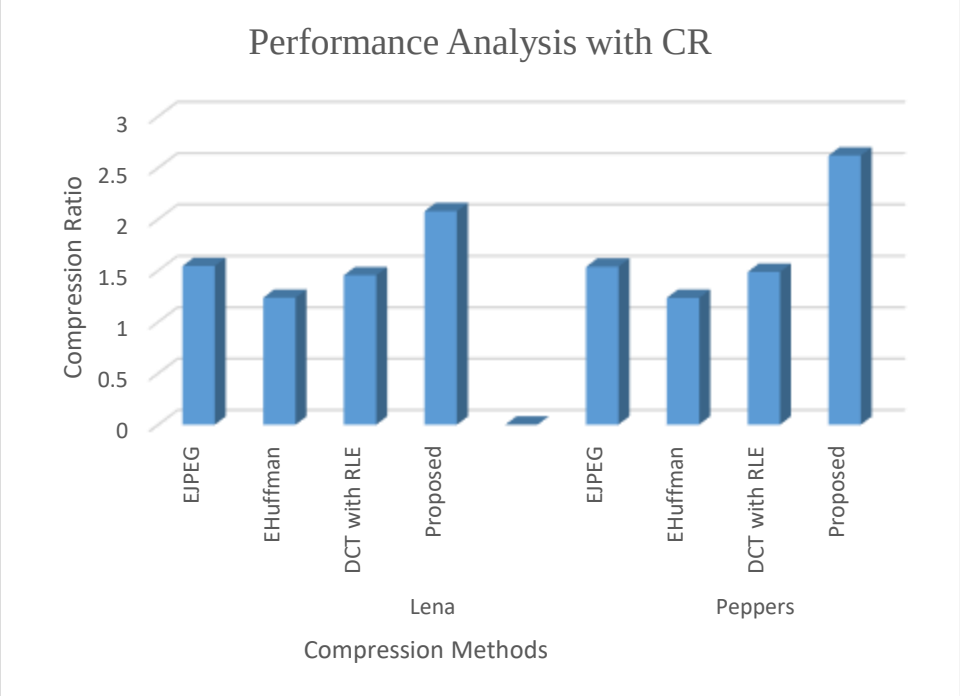

Fig.6. Compression Ratio performance analysis

In the Table 1 the compression ratio of the proposed system is compared with the existing EJPEG, EHUFFMAN and DCT with RLEmethods and the results are plotted in Fig. 6. From Table 1 and Fig. 6, it can be inferred that the proposed method gives better gain in compression ratio. These four CR values are computed against the constant Peak Signal to Noise Ratio (PSNR) value 34.60 db. The term CR means Compression Ratio and it is calculated using Equation 11.

$$CR = \frac{BS_{OI}}{BS_{RI}} \tag{11}$$

where $OI\ is\ original\ Image$
$RI\ is\ reconstruted\ Image$
$BS\ is\ byte\ size$

Table 2. Performance analysis with compression and decompression time consumption

Image Name	Algorithm	Time Taken	
		CTT	DTT
Lena.bmp	EJPEG	1.0608	0.7176
	EHUFFMAN	1.3414	0.4668
	DCT with RLE	3.1418	3.8581
	Proposed	**6.5513**	**7.4361**
Peppers.bmp	EJPEG	1.1246	0.9642
	EHUFFMAN	1.6112	0.8431
	DCT with RLE	3.4112	3.9321
	Proposed	**6.7119**	**7.4532**

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

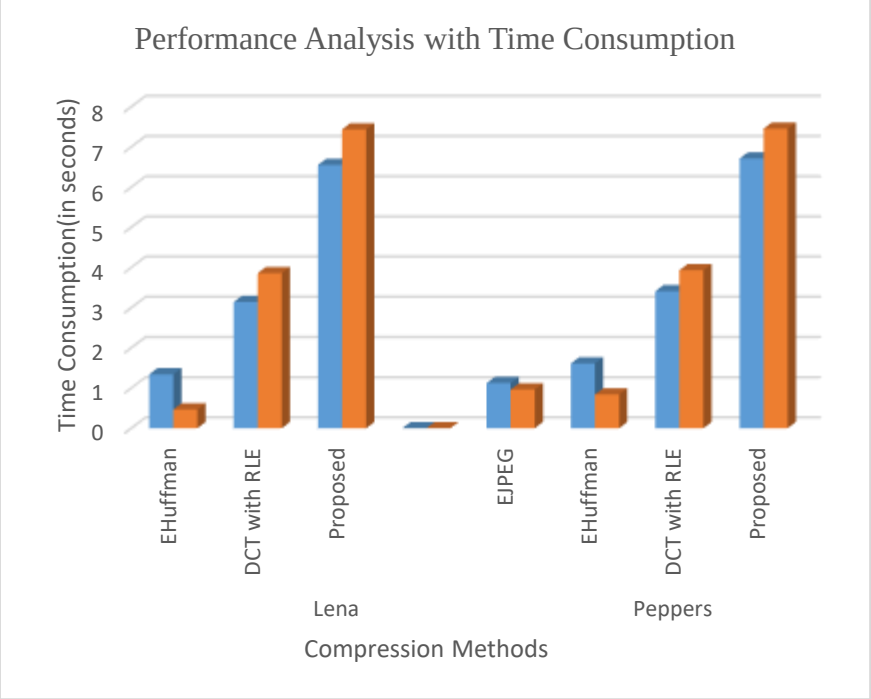

Fig.7. Time consumption performance analysis

the existing EJPEG, EHUFFMAN and DCT with RLEmethods and the results are shown. The time taken for both compression and decompression are little high in the proposed system but it provides better compression ratio and image quality. So these time taken variations are reasonable and can be acceptable. In this table the term CTT represents Compression Time Taken and the term DTT represents Decompression Time Taken.

Table 3. Performance analysis with MSE and PSNR for CR value 1.38

Image Name	Algorithm	MSE	PSNR(db)
Lena.bmp	EJPEG	499.205	11.5
	EHUFFMAN	168.56	25.86
	DCT with RLE	162.61	26.02
	Proposed	**93.02**	**28.45**
Peppers.bmp	EJPEG	198.021	51.16
	EHUFFMAN	116.95	27.45
	DCT with RLE	58.12	30.49
	Proposed	**38.03**	**32.33**

In the Table 3 and Fig. 8, the Mean Square Error (MSE) and PSNR performance measures are taken in account to make the performance analysis. From this table and figure it is proved that the proposed method reaches the lowest MSE and the highest PSNR compared with existing methods. The lowest MSE and the highest PSNR gives higher visual quality. The MSE is calculated using the Equation 12 and the PSNR is calculated using the

Equation 13

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(OI_{i,j} - RI_{i,j}\right)^2 \quad (12)$$

$$PSNR = 10\ log_{10}\left(\frac{255^2}{MSE}\right) \quad (13)$$

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

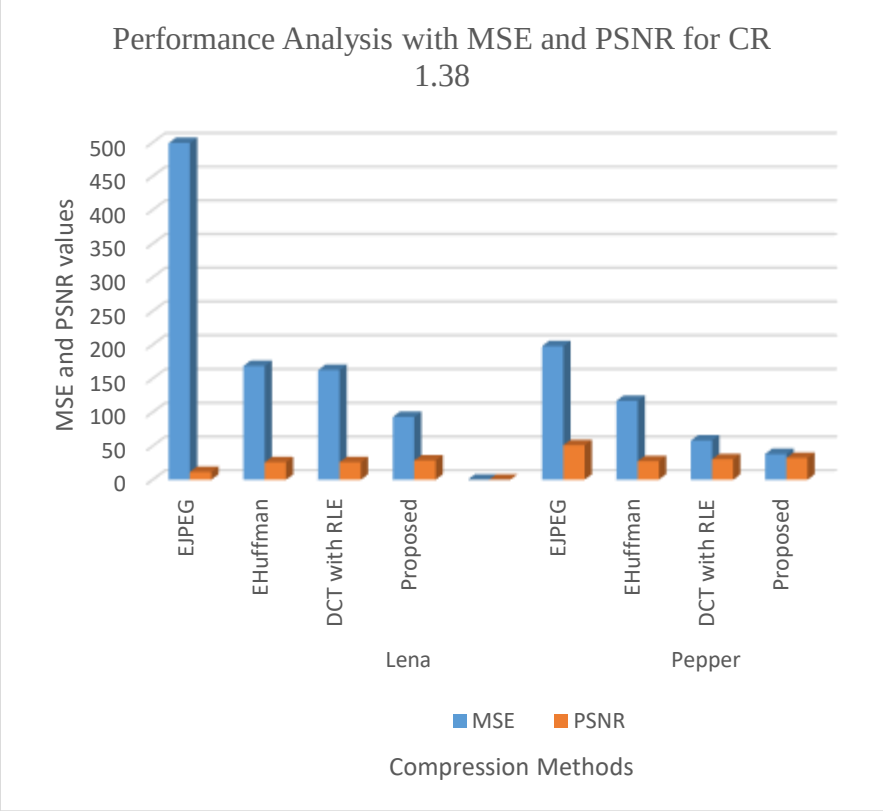

Fig.8. MSE and PSNR performance analysis.

V. CONCLUSION

The proposed method aims to compress the encrypted color images. The permutation based encryption is used in this paper. This joint encryption with compression method includes prediction based rigid data encoding, seven bit storage and negative sign removal processes. This paper improves the compression ratio by 10.45%. This method is suitable for image security applications. By considering the overall performance metrics, this paper concludes that the proposed method is better than the existing methods. In future enhancement the seven bit compressed storage can be improved to (n-k) bit compressed storage

VI. REFERENCES

[1] Xinpeng Zhang, "Lossy Compression and Iterative Reconstruction for encrypted images", IEEE transactions on Information forensics and security, vol. 6, no. 1, March 2011.
[2] Jonathan Taquet and Claude Labit, "Hierarchical Oriented Predictions for Resolution Scalable Lossless and Near-Lossless Compression of CT and MRI Biomedical Images", IEEE transactions on Image processing, vol. 21, no. 5, May 2012.
[3] Abdul Razzaque and V. Thakur, "Image Compression and Encryption: An Overview", International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 5, July - 2012 ISSN: 2278-0181.
[4] Dr. V.K. Govindan, B.S. Shajeemohan "An in intelligent text data encryption and compression for high speed and secure data transmission over internet", IEEE transactions on Information forensics and security, vol. 9, no. 3, May 2013.
[5] James Kelley and Roberto , "An analysis of image compression techniques", IEEE transactions on Image processing, vol. 14, no. 3, May 2014
[6] S. S. Maniccam, and N. G. Bourbakis, "SCAN Based Lossless Image Compression and Encryption"‖ IEEE 0-7695-0446-9/99, pp. 490-499, 1999
[7] Masanori Ito, Noboru Ohnishi, AymanAlfalou and Ali Mansour, "New Image Encryption And Compression Method Based On Independent Component Analysis", 678-1-2144-2957-4/IEEE, 2007
[8] Sinha, K. Singh, "A technique for image encryption using digital signature," Source: Optics Communications, vol.218, no. 4, 2003, pp.224-234.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

[9] Wei Liu, Wenjun Zeng, Lina Dong and Qiuming Yao, "Resolution-progressive Compression of Encrypted Grayscale Images", 425-1-1344-3257-4/I EEE, 2008
[10] V.Radha, D.Maheswari, "Secured Compound Image Compression Using Encryption Techniques", 978-1-4244-5967-4/ IEEE 2010
[11] G. Zhi-Hong, H. Fangjun, and G.Wenjie, "Chaos - based image encryption algorithm," Department of Electrical and computer Engineering, University of Waterloo, ON N2L 3G1, Canada. Published by: Elsevier, 2005, pp. 153-157.
[12] 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, p.127, 2006.
[13] J. Zhou, X. Liu, and O. C. Au, "On the design of an efficient encryption-then-compression system," in Proc. ICASSP, 2013, pp. 2872–2876.
[14] R. Lazzeretti and M. Barni, "Lossless compression of encrypted grey- level and color images," in Proc. 16th Eur. Signal Process. Conf., Aug. 2008, pp. 1–5.
[15] C.E. Shannon, "A mathematical theory of communication," Bell system technical journal, Vol. 27, No. 3, pp. 379, 1948.
[16] Wei Liu, Wenjun Zeng and Qiuming Yao "Efficient Compression of Encrypted Grayscale Images", TIP-04646-2008, pp.1-6.
[17] Shantanu D. Rane and Guillermo Sapiro "Evaluation of JPEG-LS, the New Lossless and Controlled-Lossy Still Image Compression Standard, for Compression of High-Resolution Elevation Data", IEEE Transactions on Geoscience And Remote Sensing, vol. 39, no. 10, October 2001, pp. 2298-2306.
[18] MarkosPapadonikolakis, VasilleiosPantazis and Athanasios P. Kakarountas "Efficient High-Performance ASIC Implementation of JPEG-LS Encoder" 978-3-9810801-2-4/DATE07 © 2007 EDAA
[19] Diego Santa cruz, and TouradjEbrahimi "An Analytical study of JPEG 2000 Functionalities" IEEE transactions on Image processing, vol.2, pp.49-52,Sep 2000.
[20] On compressing encrypted Data, Mark Johnson and Daniel Schonberg, IEEE transactions on signal processing, vol. 52, No.10, October 2004.

CITE AN ARTICLE

Shunmugan, S., & Rani, P. J. (2017). AN EFFICIENT JOINT ENCRYPTION AND COMPRESSION USING HOP AND PERMUTATION. *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY*, *6*(7), 194-205. doi:10.5281/zenodo.823090