



Secure Reversible Data Hiding Method Based on Histogram Shifting and XOR Based Transformation

Krati PandeyM-tech scholar & LNCT, Bhopal,
India**Shraddha Pandit**Assistant Professor & LNCT, Bhopal,
India

Abstract: When a data hiding technique is used, the secret data needs to be embedded in a cover image. This embedding causes a distortion of the cover image and reduces its quality due to the different pixel values of the cover image. The distortion and the quality issues are seen mainly in sensitive images. To resolve this problem Reverse Data Hiding (RDH) research has become a trend currently. The Reverse Data Hiding technique is being used to improve the distortion of sensitive images and improve their quality. In this paper, we propose a unique secure Reversible Data Hiding technique based on Histogram Modification and X-OR Transform. This technique comprises of 3 phases; data embedding, image encryption, and data extraction/image-recovery. Histogram shifting is used for hiding the secret data into a coloured image and X-OR based operation is used for encryption of image in order to achieve secure point of view. When we do this the data extraction is non-separable from the content decryption. We have tested the proposed reverse data hiding technique for different samples (hiding capacities) and the results prove that this technique has a lot of potential and delivers astonishing results. During experimentation we found that the proposed technique supports high capacity rate reach up to approximately 0.2 bits/pixel which is above 10% of the size of the input image at PSNR above 120dB for the output signal.

Keywords— Affine Transform, Histogram Modification, Reversible Data Hiding (RDH), Stego image, Cover image, PSNR.

I. INTRODUCTION

Data hiding is the approach by which some data is hidden into a cover media. The data may be any text related to the image such as authentication data or author information. At the receiver side it prerequisite is able to extract the hidden data. In some high-precision applications such as medical, military and remote sensing, it is highly desired that the original image should be perfectly regained after data extraction. A data hiding technique satisfying this requirement is known as reversible data hiding. They are also called invertible, lossless or distortion free data hiding [1].

Data hiding is usually transacted by an inferior assistant or a channel administrator. The proprietor of the image cannot trust the assistant or channel administrator completely. In such cases, when the proprietor needs to keep the secrecy of the image, he may first encrypt the image using an encryption key. The channel administrator, without any knowledge about the original image content, has to conceal hide data into the encrypted image using a data hiding key. It is also desired that the receiver can extract the hidden data and recover the original image in a separable manner. Separable means that if the receiver is having the data hiding key only, he can extract the data, but cannot decrypt the image. If he is having encryption key only, it is attainable to decrypt the image, but cannot extract the hidden data. If the receiver is having both keys, he can extract the hidden data and recover the original image [2].

Most of the performance on data hiding techniques are not reversible. Reversible data hiding can be done in many ways like, Integer-to-Integer Wavelet Transform[3-4], Difference expansion[5-7], and Histogram modification[8-12]. There are a different number of schemes [13-14] which performs data hiding and encryption jointly. In some of them, a part of cover is used to carry supplementary data and rest of the cover is encrypted.

The main goal of this proposed work is to implement a Histogram shifting (HS) based Reversible Data Hiding (RDH) method that can endow a high embedding capacity with lowest distortion. A content owner takes the histogram of original image. After that data hider hides the additional data into the image using data hiding key and with the help of encryption key, encrypts the image that the receiver does not know about the original content. With an encrypted image containing additional data, a receiver can only get the contents of the image after decryption according to the encryption key, and then extract the embedded data and find again the original image according to the data-hiding key. In the technique, the data extraction is non-separable from the content decryption.

The organization of this paper is as follows. In the next section, basic difference between separable and non-separable Reversible data hiding is described. Section 3 defines the proposed methodology followed by block diagram of proposed methodology in section 4. We define objective visual quality measurements to simulate human perception model in Section 5. Section 6 gives the results of proposed method as in like of PSNR, NPCR and Embedding rate using cover image and recovered image. Some clear problems of image steganography related to transform domain and some interesting direction that may be worth future research are discussed in Section 7.

II. SEPARABLE V/S NON-SEPARABLE REVERSIBLE DATA HIDING

A. Separable Reversible Data Hiding

The scheme of reversible data hiding is the separable reversible data hiding (RDH). Here the separable means to separate i.e. we can separate something. The main notions of separable reversible data hiding (RDH) is that we can extract the genuine image by using the encryption key and the extraction of the payload data by using the data hiding key.

Both parts are separated from each other. It means that if we have the data hiding key then we can extract the hidden data but cannot reorganize the original image and we can construct the image same as the original if we have the encryption key but cannot read the hidden data. We need both keys to read the whole received data.

B. Non-Separable Reversible Data Hiding

Another method of reversible data hiding is Non-separable Reversible Data hiding (RDH). In this method the content owner first encrypts the image using encryption key then passes it to the data hider. One who hides data then embedded some supplementary data in the image using the data hiding key. The main characteristics of Non-Separable Reversible Data hiding is differ from Separable Reversible Data hiding from here. At the receiver side we need both keys that is encryption key and the data hiding key to extract the genuine data and the original image.

III. PROPOSED METHODOLOGY

We proposed an efficient non-separable reversible data hiding in encrypted image. The proposed method is divided into four phases:

- A. Data Embedding Phase
- B. Image Encryption Phase
- C. Image Decryption Phase
- D. Data Extraction Phase

The contents owner embeds the secret data in the image and encrypts the whole image using encryption key. Upon receiver receiving decrypts image using the key and extracts the data and recovers genuine image. Data hiding scheme along with data extraction and image recovery is depicted in section A and D respectively. Encryption and decryption technique is depicted in section B and section C respectively.

A. Data Embedding Phase

This is the first procedure of embedding. First Input a color image X with L bits per pixel. Shift the histogram from both sides by 1 unit. Note that the information of histogram shifting is recorded as general bookkeeping information that will be embedded into the image itself with payload.

Generate histogram of original image and find the values of maximum (MAX) and minimum (MIN) points. A MAX point is the color value having maximum number of pixels in the image. A MIN point is the color value having minimum number of pixels in the image

Data are embedded into pixels with color value equal to MAX. The pixel positions with color value equal to MIN are stored as overhead information that will be hidden into the image along with pure data.

Determine the Max point P and Min point Q from the histogram.

Scan the whole image from left to right and top to bottom and perform the following conditions.

$$y_{ij} = \begin{cases} x_{ij} + 1 & \text{if } x_{ij} > P \text{ and } x_{ij} \leq Q \\ x_{ij} & \text{otherwise} \end{cases}$$

where y_{ij} is the modified value of pixel at location (i,j). If $x_{ij} = P$, modify x_{ij} according to the message bit

$$y_{ij} = \begin{cases} x_{ij} + b & \text{if } x_{ij} = P \end{cases}$$

where b is a message bit to be embedded.

This process is applied to the entire color plane that is R-G-B color plane.

After changing and modifying the pixels value of original image X we obtain the stego image Y and it is ready for encryption.

B. Image Encryption

To encrypt the image we substitute the pixel values to different value using 32 bit X-OR operation technique with four 8-bit keys. XOR operation fractures the correlation between adjacent pixels of an image.

The Stego image Y is divided into 2 pixels \times 2 pixels blocks. The image pixel is contained by every block B i,j of Y is encrypted using block level XOR operation by four eight bit sub key K1, K2, K3 and K4 is given below respectively.

$$E_{1,1} = Y_{1,1} \oplus K_1$$

$$E_{1,2} = Y_{1,2} \oplus K_2$$

$$E_{2,1} = Y_{2,1} \oplus K_3$$

$$E_{2,2} = Y_{2,2} \oplus K_4$$

where $E_{i,j}$ is the pixel value at ith and jth location in block inside the encrypted image. The encrypted image by using the XOR operation is called by cipher image E.

After applying the X-OR operation on whole image color plane we get encrypted stego image E. and now it is transformed by sender to receiver.

C. Image Decryption

To extract data from encrypted stego image E it is necessity to decrypt first. To do this the one who receives decrypts the encrypted image. So, we use the same key sequence as in encryption phase using and the initial conditions.

We have an Encrypted Stego image E of size $M \times N \times 3$ with pixel locations ranging from (1, 1) to (M, N). Next Step is to performs the block level X-OR operation on encrypted stego image E by using the X-OR operation. Again we divided E into 2 pixels \times 2 pixels blocks. Then image pixel contained by every Block Bij of E is Decrypted using block level X-OR operation by same four eight bit keys (K1, K2, K3, and K4) as followed:

$$Y_{1,1} = E_{1,1} \oplus K_1$$

$$Y_{1,2} = E_{1,2} \oplus K_2$$

$$Y_{2,1} = E_{2,1} \oplus K_3$$

$$Y_{2,2} = E_{2,2} \oplus K_4$$

where $Y_{i,j}$ is the pixel value at ith and jth location in block inside pixel of decrypted stego.

D. Data Extraction

Now receiver can extracts the data from decrypted image Y. the recipient extracts message bits from the decrypted stego image by scanning the image in the same order during the embedding. The message bit b is possibly be extracted by

$$b = \begin{cases} 1 & \text{if } y_{ij} = P+1 \\ 0 & \text{if } y_{ij} = P \end{cases}$$

where y_{ij} denotes the pixel value of decrypted stego image at location (i,j). The original pixel value of x_{ij} can be restored by:

$$x_{ij} = \begin{cases} y_{ij} - 1 & \text{if } y_{ij} > P \text{ and } y_{ij} \leq Q \\ y_{ij} & \text{otherwise} \end{cases}$$

Extract the overhead information from the extracted message. If a value 1 is determinate (assigned) in the location i, restore x_i to its original state by shifting it by 1 unit; otherwise, no shifting is required.

IV. PROPOSED BLOCK DIAGRAM

The Block diagram of embedding process is divided into the individual blocks such as Message encryption, Histogram Calculation, Histogram Shifting, Message Embedding and X-OR Operation shown in Fig. 1.

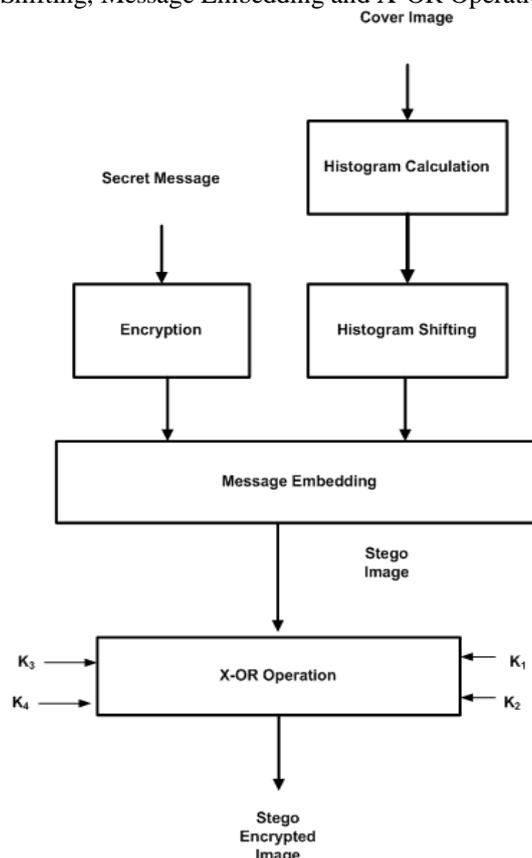


Fig.1 The general Structure of the Proposed Hiding Scheme

Fig.2 presents the sketch of proposed message Recovery system, here the input is the encrypted stego image in which data is hidden and output is the recovered message from the input stego image.

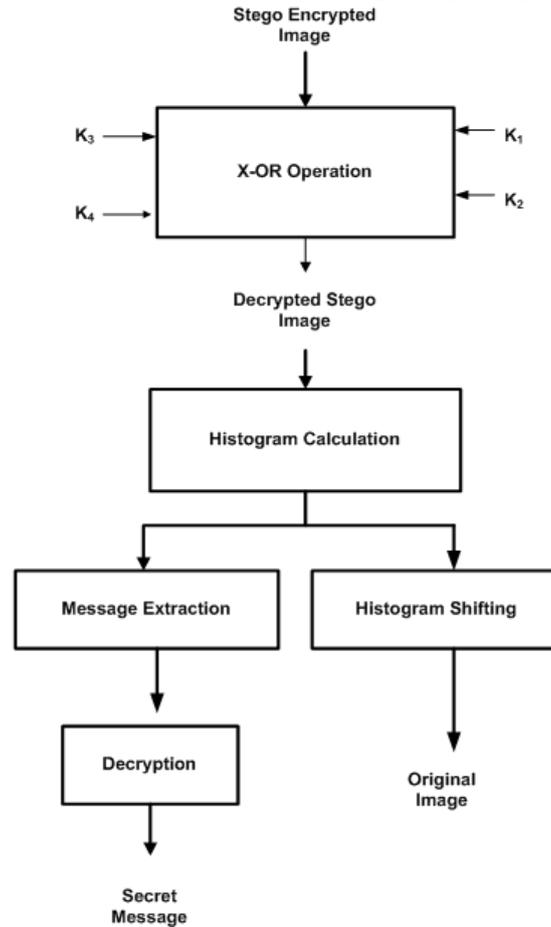


Fig.2 Sketch of the Message Recovery Algorithm.

V. QUALITY MEASUREMENT

The quality of the encrypted image is measured by calculation of certain evaluation measurement metrics. These metrics gives the comparison ratio between the original image and the modified image. The quality may be assessed/obtained on the basis of these values. The metrics used in this paper are as follows: Mean Square error (MSE), peak signal- to-noise ratio (PSNR), Number of Pixel Change Rate (NPCR), Correlation Coefficient (CC) and Embedding ratio in BPP.

A. Mean square error (MSE)

MSE is one of the frequently used quality measurement technique followed by PSNR. The MSE can be defined as the measurement of average of the squares of the difference between the intensities of the Encrypted image and the original image. It is mostly used because of the mathematical observance it offers. It is represented as:

$$MSE = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N (C(i, j) - C'(i, j))^2$$

where $C(i, j)$ is the original image and $C'(i, j)$ is the encrypted image. A large (major) value for MSE means that the image of poor quality.

B. Peak signal to noise ratio (PSNR)

The PSNR describes the measure of reconstruction of the encrypted image. This metric is used for discriminating between the cover image and encrypted image. The advantage of this measure is easy computation. It is formulated as:

$$PSNR = 20 \log 255^2 / MSE$$

A low value of PSNR shows that the constructed image is of poor quality.

C. Number of pixel Change rate (NPCR)

Aggressor tries to find out a relation between the plain image and the cipher-image, by learning how differences in an input can affect the resultant difference at the output in an attempt to determine the key. Trying to make a slight

change such as modifying one pixel of the encrypted image, aggressor observes the change of the plain-image. To testing the influence of one pixel change on the entire encrypted image by the proposed algorithm (technique), two common measures are used.

Number of Pixel Change Rate (NPCR)

$$NPCR = \frac{\sum_{i,j} D(i, j)}{W \times H} \times 100\%$$

C1 and C2: two ciphered images, whose corresponding original images have only one-pixel difference. C1 and C2 have the exact same size.

C1(i, j) and C2(i, j): grey-scale values of the pixels at grid (i,j).

D(i, j): determined by C1(i, j) and C2(i, j), if C1(i, j) = C2(i,j), then, D(i, j) = 1; otherwise, D(i, j) = 0. W and H: columns and rows of the image.

D. Bit rate/Embedding Ratio

Bit rate shows the number of bit hided per pixel in image and it is describe as below.

Embedding Capacity = Total number of pixel;

$$Bitrate = \frac{Embedding\ Capacity}{Total\ number\ of\ pixels} (bits\ per\ pixel)$$

VI. EXPERIMENT RESULT

Proposed techniques are implemented on Windows PC having Intel 2.4 GHz processor and 2GB RAM, and run using MATLAB 2009a. The tests were performed with a colored standard testing image Lena and other cover image depicted in Figure 3. All the cover images are colored image (RGB) and the dimension of all the image is 512× 512 pixels shown in Fig 3. The embedded data is a text file of size (2528B).

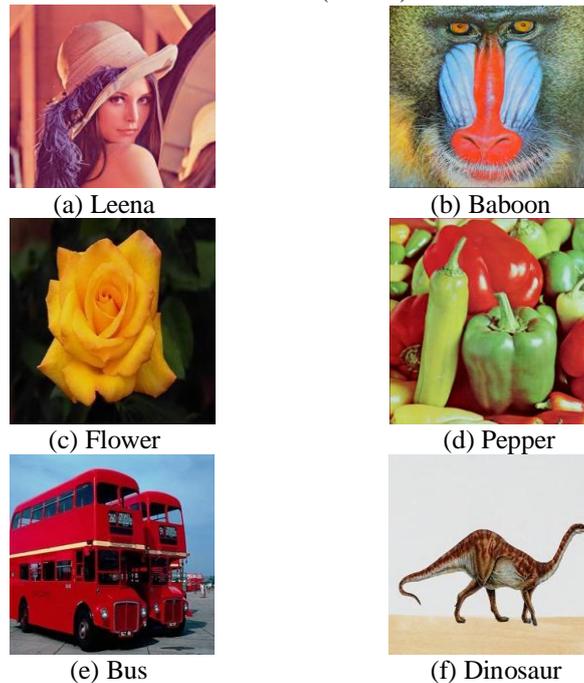


Fig. 3 Text Images of size 512×512

A. Quality Parameter Calculation

The Average quality parameters between the corresponding pixels values of the eight encrypted images Lena, Baboon, Pepper, Boat, Man, Butterfly, Cat, and Airplane are tabulated in Table 1.

Table 1 Quality Parameter Calculation of proposed method on different images.

Parameters Images	PSNR 1 (155.9811)	Embedded Ratio (BPP) (0.0512)	NPCR (100)	PSNR 2 (17.8183)
Lena	176.2164	0.0165	100	20.6089
Baboon	125.7975	0.0171	100	21.0599
Pepper	174.7523	0.0136	100	19.50
Flower	141.9135	0.0319	100	14.1715
Dinosaur	176.2164	0.2169	100	14.9132
Bus	140.9909	0.0166	100	16.6568

We know that higher the values of PSNR, better is the quality of the stego image. PSNR greater than 30 dB is considered to be an acceptable quality stego image, and from the table it is clear that PSNR1 of proposed method is greater than 30 dB (Avg. 56.2656) so we can say that the proposed method gives better stego image quality. Fig. 4 shows the PSNR graph of proposed method on different images.

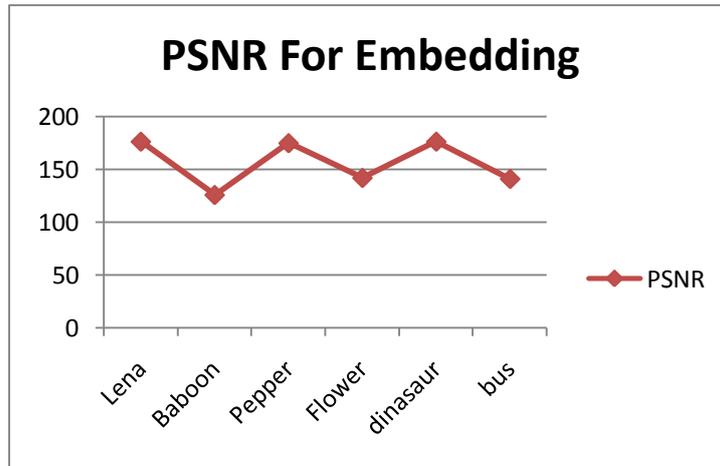


Fig. 4 Show PSNR Calculation of proposed method on different images.

We know that lower the values of PSNR, better is the quality of the encrypted image. PSNR less than 30 dB is considered to be an acceptable quality encrypted image, and from the table it is clear that PSNR of proposed method is less than 30 dB (Avg. 17.8183) so we can say that the proposed method gives better encrypted image quality. Fig 5 shows the PSNR graph of proposed method on different images.

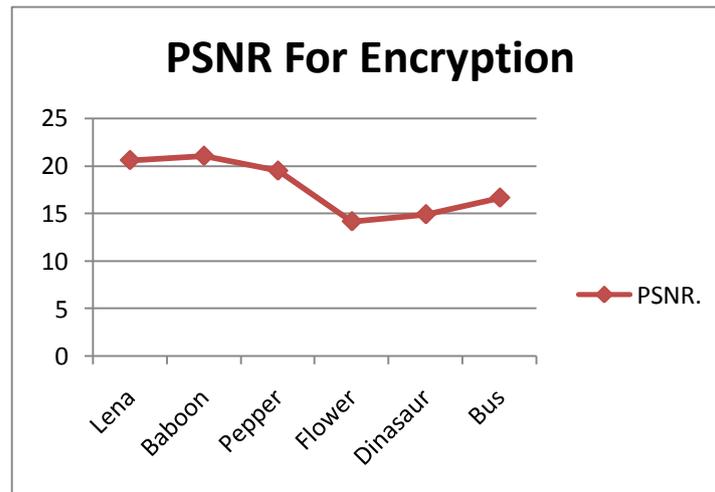


Fig. 5 Show CC Calculation of proposed method on different images.

B. Comparative Analysis

We take the plain image Lena as an example to do 20 times of experiments, in each experiment randomly beget the secret key, and then calculate the PSNR and Embedding Ratio of produced Stego images. The average value of PSNR, Embedding ratio are tabulated in Table II. From Table II, we can say that PSNR are better than that are obtained using the other considered methods. According to the proposed method the image having highest correlation between the adjacent pixels will have the highest embedding capacity and the image with lower correlation between pixels have lower embedding capacity. We can also see from Tables II that the plain image is highly correlated in horizontal, vertical and diagonal directions, so embedding ratio is higher than other methods. Fig 6 and Fig 7 shows the comparison graph of proposed method with other considered method with respect to PSNR and Embedding Rate respectively.

Table II comparative analysis of proposed Data Hiding technique

Methods	PSNR	Embedding Rate
W. Tai et.al. [10]	48.3245	0.05545
V. Suresh et.al. [13]	54.1733	0.00497
R Jose et.al. [14]	52.9996	0.01731
G. Coatrieux, [12]	55.7200	0.08123
Proposed Method	55.8286	0.05120

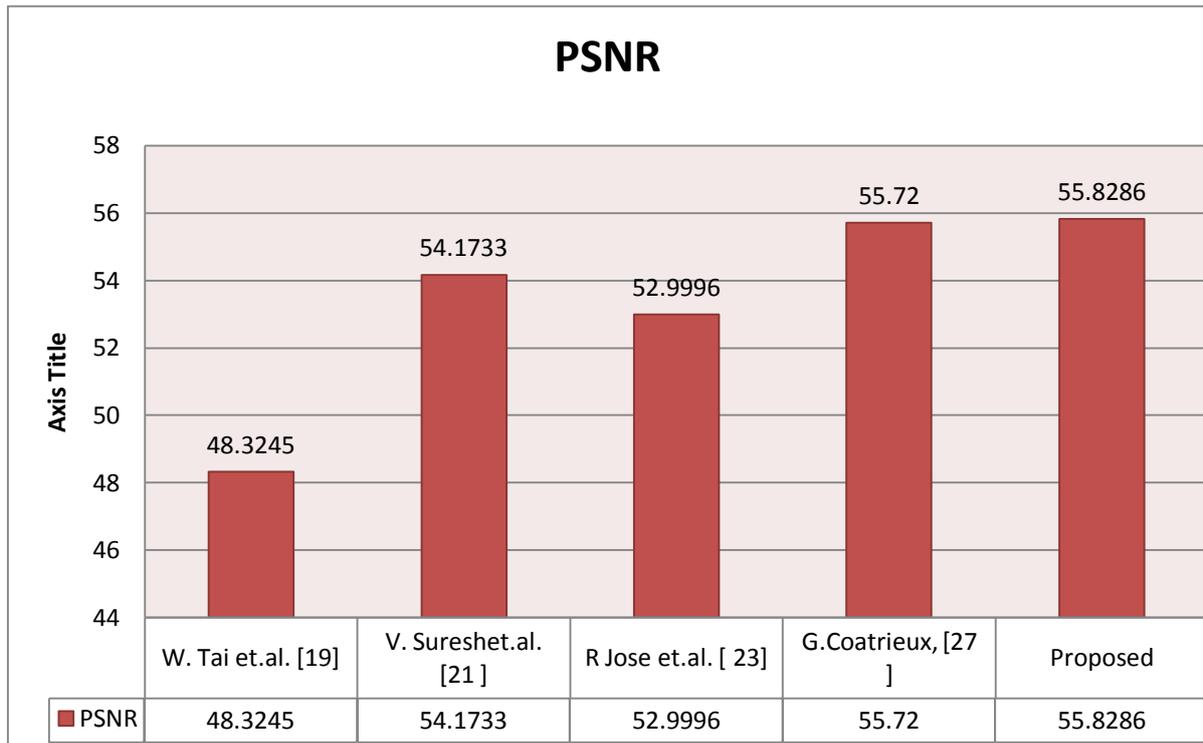


Fig. 6 Average PSNR comparison with different image RDH Methods.

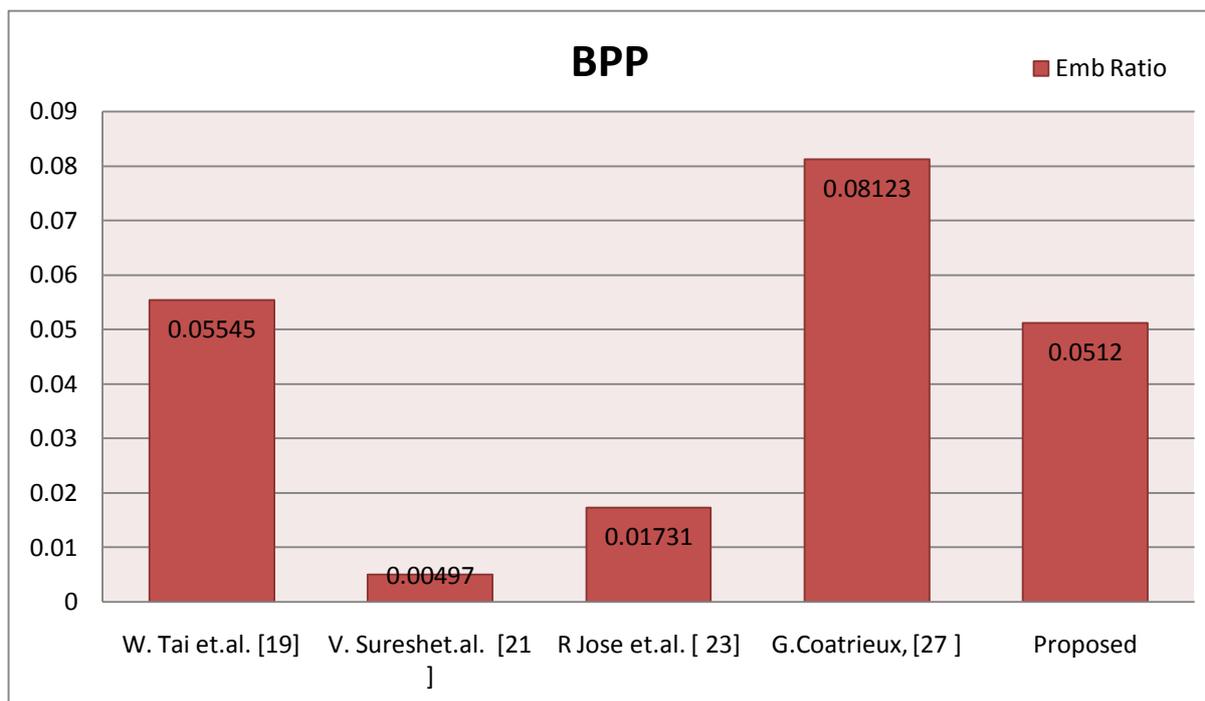


Fig. 7 Shows average Correlation between pixel values and compare different RDH Methods.

VII. CONCLUSION

The aim of this research paper is to increase RDH capacity and to show how image quality of the stego images can be improved using the RDH Technique. In this research paper, we proposed a novel and secure Reverse Data Hiding technique based on Histogram Modification and X-OR Transform. This technique comprised of 3 phases; data embedding, image encryption, and data extraction/image-recovery. When we follow the proposed technique data extraction is non-separable form from the content decryption.

We have tested the proposed reverse data hiding technique for different samples (hiding capacities) and the results prove that this technique has a lot of potential and delivers astonishing results. From the experimentation we found that the proposed technique supports high capacity rate reach up to approximately 0.2 bits/pixel which is above 10% of the size of input image at PSNR above 120 dB for output signal.

The technique which we have proposed here has a lot of scope and still need to record the extra information for restoring the cover image. The wasting capacity of extra information can reduce in the future. In future, this technique can also be implemented for video sequences by separating them into individual frames.

ACKNOWLEDGMENT

We are very much thankful to all the authors which are mentioned in this paper as we are referring their research to proposed paper.

REFERENCES

- [1] Zaidoon Kh., AL-Ani, A.A.Zaidan, B.B.Zaidan and Hamdan.O.Alanazi,” Overview: Main Fundamentals for Steganography “, journal of computing, volume 2, issue 3, March 2010.
- [2] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, “Reversible data hiding,” IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.
- [3] J. Fridrich, M. Goljan, and R. Du, “Lossless data embedding-new paradigm in digital watermarking,” Eur. Assoc. Signal Process. J. Appl. Signal Process., vol. 2002, no. 2, pp. 185–196, Feb. 2002.
- [4] Zou, Y. Q. Shi, Z. Ni, and W. Su, “A semi-fragile lossless digital watermarking scheme based on integer wavelet transform,” IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 10, pp. 1294–1300, Oct. 2006.
- [5] S. Lee, C. D. Yoo, and T. Kalker, “Reversible image watermarking based on integer-to-integer wavelet transform,” IEEE Trans. Inf. Forensic Secur., vol. 2, no. 3, pp. 321–330, Sep. 2007.
- [6] J. Tian, “Reversible data embedding using a difference expansion,” IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.
- [7] A. M. Alattar, “Reversible watermark using the difference expansion of a generalized integer transform,” IEEE Trans. Image Process., vol. 13, no. 8, pp. 1147–1156, Aug. 2004.
- [8] H. J. Kim, V. Sachnev, Y. Q. Shi, J. Nam, and H. G. Choo, “A novel difference expansion transform for reversible data embedding,” IEEE Trans. Inf. Forensic Secur., vol. 3, no. 3, pp. 456–465, Sep. 2008.
- [9] M. Fallahpour and M. H. Sedaaghi, “High capacity lossless data hiding based on histogram modification,” IEICE Electron. Exp., vol. 4, no. 7, pp. 205–210, Apr. 2007.
- [10] C. C. Lin, W. L. Tai, and C. C. Chang, “Multilevel reversible data hiding based on histogram modification of difference images,” Pattern Recognit., vol. 41, pp. 3582–3591, 2008.
- [11] Wei-Liang Tai, Chia-Ming Yeh, and Chin-Chen Chang, “Reversible Data Hiding Based on Histogram Modification of Pixel Differences”, Ieee Transactions On Circuits And Systems For Video Technology, Vol. 19, no. 6, June 2009.
- [12] P. Tsai, Y. C. Hu, and H. L. Yeh, “Reversible image hiding scheme using predictive coding and histogram shifting,” Signal Process., vol. 89, pp. 1129–1143, 2009.
- [13] Gouenou Coatrieux, Wei Pan, Nora Cuppens-Boulahia, “Reversible Watermarking Based on Invariant Image Classification and Dynamic Histogram Shifting”, IEEE Transactions On Information Forensics And Security, Vol. 8, no. 1, january 2013.
- [14] V. Suresh, C. Saraswathy, “Separable Reversible Data Hiding Using Rc4 Algorithm” IEEE International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME) February 2013.
- [15] Rintu Jose, Gincy Abraham, “Separable Reversible Data Hiding in Encrypted Image with Improved Performance”, IEEE International Conference on Microelectronics, Communication and Renewable Energy, 2013.