REVERSIBLE IMAGE DATA HIDING WITH CONTRAST ENHANCEMENT

Pratima B. Choudhari[1], Mr. M. S. Sadavarte[2]

[1]M.Tech student, Electronics and Telecommunication Engineering, Government College of Engineering, Jalgaon, Maharashtra, India
[2]Professor in Electronics and Telecommunication Engineering, Government College of Engineering, Jalgaon, Maharashtra, India

---***---

Abstract *- Digital communication has become an essential part of infrastructure nowadays, a lot of applications are Internet based and in some cases it is desired that communication be made secret. Consequently, the security of messages has become a fundamental issue. The existing system such as the Difference Expansion and Expansion Embedding are most commonly used techniques but suffers from undesirable distortion which makes these methods unsuitable or less reliable. The techniques used in proposed system is to achieve Reversible data hiding. The message is embedded into cover image and then the cover image is transmitted.*
In proposed system one first contribution is a histogram shifting modulation which adaptively takes care of the local specificities of the image content. By applying it to the image prediction-errors and by considering their immediate neighborhood, the scheme we propose inserts data in textured areas where other methods fail to do so. This method inserts the payload in the textured area and thus reduces the distortion and it also increases the embedding capacity of the cover image. In that way, the message embedder and extractor remain synchronized for message extraction and image reconstruction. After extraction of message from the image proposed system chieve a peak signal-to-noise ratio (PSNR) of about 1–2 dB greater than the original image.

Key Words: Reversible Data Hiding, Histogram Shifting, Peak Signal to Noise Ratio, Mean Squared Error.

1. INTRODUCTION

Reversible Data Hiding (RDH) has been intensively studied in the community of signal processing. Also referred as invertible or lossless data hiding, RDH is to embed a piece of information into a host signal to generate the marked one, from which the original signal can be exactly recovered after extracting the embedded data. The technique of RDH is useful in some sensitive applications where no permanent change is allowed on the host signal. In the literature, most of the proposed algorithms are for digital images to embed invisible data or a visible watermark.

Digital communication has become an essential part of infrastructure nowadays, a lot of applications are Internet based and in some cases it is desired that communication be made secret. Consequently, the security of messages has become a fundamental issue. The techniques is available to achieve this goal is Reversible data hiding technique , the message is transformed into some other form and then the embedded message is transmitted. In reversible data hiding , the data is embedded in a cover file and the cover file is transmitted. This paper proposed a system that combines the effect of these two methods to enhance the security of the data This proposed system' embeds the data with a RDH algorithm and then embeds the secrete data in a cover file. The cover carrier is an image.

To evaluate the performance of a RDH algorithm, the hiding rate and the marked image quality are important metrics. There exists a trade-off between them because increasing the hiding rate often causes more distortion in image content. To measure the distortion, the peak signal-to-noise ratio (PSNR) value of modification of image histogram provides less embedding capacity. In contrast, the more recent algorithms manipulate the more centrally distributed prediction errors by exploiting the correlations between neighboring pixels so that less distortion is caused by data hiding. Although the PSNR of a marked image generated with a prediction error based algorithm is kept high, the visual quality can hardly be improved because more or less distortion has been introduced by the embedding operations. For the images acquired with poor illumination, improving the visual quality is more important than keeping the PSNR value high. Moreover, contrast enhancement of medical or satellite images is desired to show the details for visual inspection.

2. LITERATURE REVIEW

Up till now more work or research has been done in reversible data hiding techniques. Lots of efficient techniques are proposed till. The work done in reversible data hiding techniques are as follows:

We know it is very difficult to vacate the room losslessly from encrypted images. So by considering this in [2] Kede Ma, Weiming Zhang, Xianfeng Zhao, Nenghai Yu and Fenghua Li has proposed a technique for embedding the data in reversible manner using reserve room before encryption.Vacating room from the encrypted images losslessly is sometimes difficult and not efficient, so if we reverse order of encryption and vacating room, i.e., reserving room before image encryption, the RDH tasks in encrypted images would be more natural and much easier which gives the novel framework, reserving room before encryption (RRBE). There are some standard RDH algorithms available which are ideal for reserving room before encryption and can be easily applied to Framework RRBE to achieve better performance compared with techniques from Framework VRAE. This is because in this new framework, follow the customary idea that first lossless compresses the redundant image content (e.g., using excellent RDH techniques) and then encrypts it with respect to protecting privacy.

In [8] Wen-Chung Kuo, Po-Yu Lai, Lih-ChyauWuu has proposed a adaptive reversible data hiding method. A new scheme based on histogram and slope method enhancing the data hiding capacity and also the efficiency increases and maintains the high quality of image.

In [3] Kuo-Ming, Wen-Kai Su, Ting-Wen Chen, Li-Ming Chen has proposes the method which is the combination of data hiding, half-toning and vector quantization technique. In this the embedding of gray scale image in other image is done. This scheme is work as follows:

a) Image compression from gray scale to half tone using half-toning process.

b) Computation of difference between original image and the image on which we perform operations.

c) Then VQ compression compress the difference obtain in above and embed it with secret data.

José .R; Abraham .G, in [4] proposed the method in which a reversibly data hiding in encrypted gray scale image is done in separable manner. Encryption of the image is done by content owner using encryption key by permuting the pixels. Data hiding is done by using data hiding key using histogram modification method.

Malik, Anjali Sardana, Jaya in [5] has proposed another different approach for visual cryptography which consist of three steps:

1.Sieving 2. Division 3. Shuffling to generate random shares. The advantage of this is that minimal computation requirement to generate the binary secret image without loss of quality of image.

Yi-Hui Chen, Ci-Wei lan and Chiaio-Chih Huang in [6] have proposed the another different approach for visual cryptography is authentication mechanism. In this two procedures are there :

a) Encryption procedure

b) Decryption procedure

Cryptography is an art of securely transferring the message from sender to receiver. It uses the key concept for encryption the message information known as cryptography. It is used when communicating over the untrusted media such as internet. Cryptography is the technique that used in securely transfers the information with the use of algorithm which is un-readable by the third-party. Decryption of secret image and authenticated image is obtain by difference expansion.

3. REVERSIBLE DATA HIDING

Fig. 1 shows procedure of the proposed reversible data hiding system. First step is to find predictive error $e_{x,y}$values of image.The block that is classified to calculate prediction error is considered to be 3*3 matrix with 9 pixel points. Then generate histogram of predictive errors. The classical Histogram Shifting method is slightly modified in order to obtain a quality data embedded image. The histogram shifting here is dynamically applied. When histogram shifting is applied dynamically on prediction errors it is called 'dynamic prediction error histogram shifting. The histogram shifting here is dynamically applied. When histogram shifting is directly applied to pixels it is called the 'pixel histogram shifting' and when it is applied dynamically on prediction errors it is called 'dynamic prediction error histogram shifting. These modulations will modify only one pixel in the block that has been classified. Generally the data hiding introduces distortion. This distortion is reduced by the dynamic predictive error histogram shifting algorithms and it increases the quality of the embedded image. The payload is usually in the form of a binary sequence. The underflow and overflow problems are also considered and avoided in our proposed system. The delta gray values are added while shifting the pixels by using the pixel histogram shifting and thus the risk of overflow can be avoided.

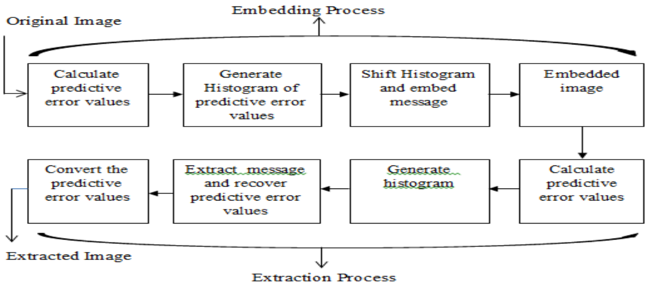

Original Image
Embedding Process
Calculate predictive error values
Generate Histogram of predictive error values
Shift Histogram and embed message
Embedded image
Convert the predictive error values
Extract message and recover predictive error values
Generate histogram
Calculate predictive error values
Extracted Image
Extraction Process

Fig. 1 procedure of the proposed reversible data hiding system.

3.1 Algorithm for message embedding

1. Load input image
2. Calculate Prediction error of input image
3. Plot histogram of prediction error
4. Select carriers from histogram of prediction error
5. Convert message into binary bits
6. Embed message in carriers

Following flowchart gives details of message embedding process.

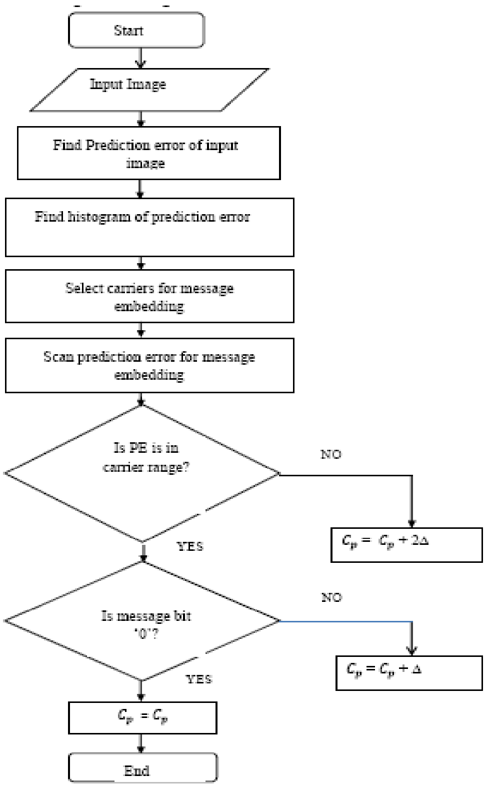

Start
Input Image
Find Prediction error of input image
Find histogram of prediction error
Select carriers for message embedding
Scan prediction error for message embedding
Is PE is in carrier range?
NO
$C_p = C_p + 2\Delta$
YES
Is message bit '0'?
NO
$C_p = C_p + \Delta$
YES
$C_p = C_p$
End

Fig. 2 Flow Chart for Message Embedding

3.2 Prediction Error

In proposed block diagram first step is to find prediction error. This means that the prediction-error neighborhood is not derived from the original image but from a copy of it where pixels for embedding are replaced by their predicted-values. An alternative to this strategy is to compute the prediction-error neighborhood using the block of nine pixel neighbors.

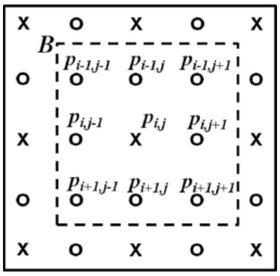


Fig.3 Pixel Neighborhood for Prediction

Above figure 3 shows Pixel neighborhood for prediction in a 3* 3 pixels block B, $P_{i,j}$ is estimated through its nine nearest neighbors.. From here on, we work with the image prediction-error. Considering the pixel block in Figure 3.5 the prediction-error of the pixel is given by

$$e_{i,j} = P_{I,J} - \hat{p} I, J \qquad (1)$$

where $\hat{p} I, J$ is the predicted value of $P_{I,J}$ derived from its eight nearest neighbor pixels :

$$\hat{p} i, j = (\sum_{i,j=1}^{3} P_{I,J} - P_{2,2}) / 8 \qquad (2)$$

It is important to notice that $P_{I,J}$as well as all pixels identified by 'x' in Fig.3.5 are modified after embedding. As a consequence, the prediction-error neighborhood of $P_{I,J}$ will also vary if it is computed based on eq. (2)

3.3 Histogram of Prediction Errors

Next procedure is to find histogram of the prediction error. A histogram is an accurate graphical representation of the distribution of numerical data. It is an estimate of the probability distribution of a continuous variable (quantitative variable) and was first introduced by Karl Pearson. It is a kind of bar graph. To construct a histogram, the first step is to "bin" the range of values that is, divide the entire range of values into a series of intervals—and then count how many values fall into each interval. The bins are usually specified as consecutive, non-overlapping intervals of a variable. However, a bounding box-based ground truth is far from accurate, as also stated by Wang and Li.

$$n = \sum_{i=1}^{k} m_i \qquad (3)$$

Where, n = the total number of observations

K = total number of bins

Histograms plots how many times (frequency) each intensity value in image occurs. Example: Image (left) has 256 distinct gray levels (8 bits) . Histogram (right) shows frequency (how many times) each gr ay level occurs.

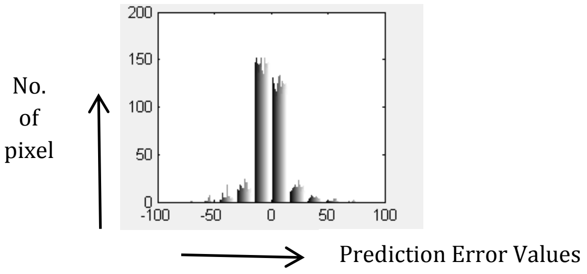


Fig.4 Histogram of Prediction Error for Input Image

3.4 Classical And Dynamic Histogram Shifting

There are two types of histogram shifting first one is classical histogram shifting and another is dynamic histogram shifting. Out of these two types dynamic histogram shifting is more efficient.

3.4.1 Basic HS Modulation Principles

The basic principle of Histogram Shifting modulation, in a general case, consists of shifting a range of the histogram with a fixed magnitude , in order to create a 'gap' near the histogram maxima. Pixels, or more generally samples with values associated to the class of the histogram maxima , are then shifted to the gap or kept unchanged to encode one bit of the message, i.e., '0' or '1'. As stated previously, we name samples that belong to this class as ―carriers. Other samples, i.e., ―noncarriers, are simply shifted. At the extraction stage, the extractor just has to interpret the message from the samples of the classes and and invert watermark distortions (i.e., shifting back shifted value). Obviously, in order to restore exactly the original message.

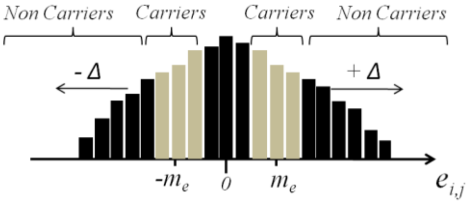


Fig 3.5 Dynamic Histogram Modulation Applied on Predict Errors

3.6 Cassification Of Carriers

The prediction-error can thus be HS modulated as illustrated in the figure 3.11. In that case, prediction-errors which do not belong to the carrier-class = [-Δ , Δ] are considered as ―non carriers and are shifted of + Δ / -Δ depending on their sign (+Δ if >= ; -Δ if <= 0). Prediction-errors within the class = [-Δ , Δ] the carriers are used for embedding is left unchanged to encode '0' or shifted to the range [-2 , -Δ] or [Δ , 2Δ], depending on its sign, to encode '1'. Notice that, even though message insertion is conducted in the prediction-error, it is the image pixels which are modulated.

$$C_c = Max\ (h) - 1 \qquad (4)$$

$$C_c = Max\ (h) + 1 \qquad (5)$$

Where , C_c = Carriers selected for message embedding

Max(h) = Maximum peak of the prediction error histogram

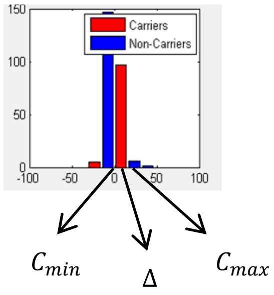


Fig.3.6 Carriers Range and Area for Input Image

3.5 Text To Binary Conversion

The data to be embedded will be in the form of character. So, at first text will be converted into ASCII codes then into binary bits and then binary bits will get embedded into the image using equations.

3.6 Message Embedding

Carriers are classified from the histogram of prediction error of pixel values. Then the secret image converted into binary sequence. For example a, ascii value of 'a' is 97 is converted into binary numbers like 01100001, Embed this binary values in carriers. Finally we get distortion less embedded image.

$$Cp = \begin{cases} Cp & if\ b = '0' \\ Cp + \Delta & if\ \ b = '1' \end{cases} \qquad (6)$$

And if the prediction error is not in the range of carriers then use following formula to change central pixel value.

$$Cp = Cp\ + 2\ \Delta \qquad (7)$$

Where, Cp = Central pixel value
Δ = Carrier range

$$\Delta = C_{max} - C_{min} \qquad (8)$$

Where C_{max} = maximum value of carrier range
C_{min} = minimum value of carrier range

3.7 Message Extraction Process

When data receiver acquires the data embedded image, he can completely extract the hidden information as well as recover the original image without loss. It can be performed with an inverse operation on the data hider side. We consider the block of nine pixels where $P_{i\ ,j}$ is a center pixel as shown in the fig.

3.7.1 Algorithm for extraction of message

The algorithm for extraction of message is as follows

1. Load data embedded image
2. Calculate prediction error of data embedded image.
3. From the values of prediction error find out message bit whether it is '0' or '1'by applying equations.
4. Covert binary bits into characters.
5. Prevention of overflow and underflow.

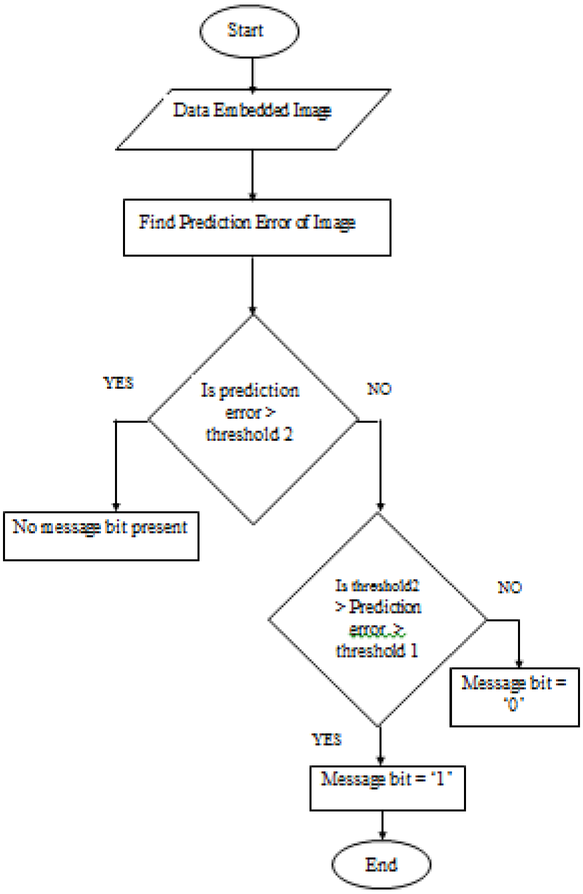

Start
Data Embedded Image
Find Prediction Error of Image
Is prediction error > threshold 2
YES
NO
No message bit present
Is threshold2 > Prediction error ≥ threshold 1
NO
Message bit = '0'
YES
Message bit = '1'
End

Fig. 7 Flow Chart for Message Extraction

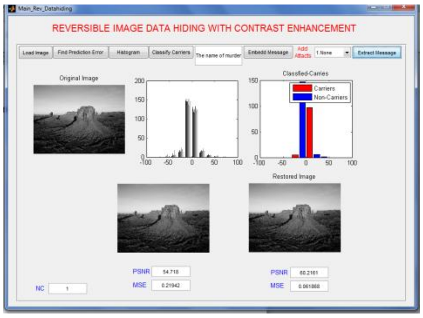
$$Cp = \begin{cases} 1 & if \quad C_{min} + \Delta < P_e < C_{min} + 2\Delta \\ 0 & if \quad C_{min} < P_e < C_{min} + \Delta \\ no\ message\ bit & if \quad C_{min} + 2\Delta < P_e \end{cases} \tag{9}$$

3.8 Experimental Results And Analysis

The experiment is performed on various images of different dimensions in order to hide secret information. The information that we want to hide is in the form of character, which is embedded into each of these images. The result of experiment is compared based on the following image quality metrics:

- Peak Signal to Noise Ratio (PSNR)
- Mean Square Error (MSE)
- Embedding Capacity

High PSNR value and low MSE value signifies the good quality of image. The MSE and PSNR are the most widely used metrics in the literature that's why we use them.



The name of murder

1.None

PSNR 54.718

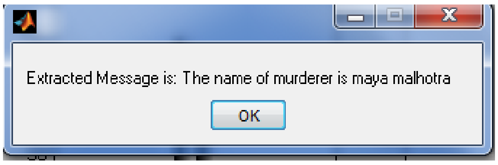
MSE 0.21942

PSNR 60.2161

MSE 0.061868

NC 1

Fig. 8 Figure Showing Result of Message Embedding



Extracted Message is: The name of murderer is maya malhotra

Fig.9 Extracted Message

Fig. 9 shows that extracted message is same as message Embedded in Image

3.9 Experimental Analysis Of Quality Of Restored Image

The PSNR computes the peak signal-to-noise ratio, in decibels, between two images. This ratio is often used as a quality measurement between the original and a Restored image. The higher the PSNR, the better the quality of the restored, or reconstructed image. The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two error metrics used to compare image quality.

Table 1 Comparative Analysis of Mean Squared Error for Different Images

Input Image	Data Embedded Image MSE	Restored Image MSE
Desert	0.1109	0.0302
Lena	1.9615	0.2471
Baboon	3.4521	3.4521
Lighthouse	0.2601	0.2601

Table 2 Comparative Analysis of Peck Signal to Noise Ratio

Input Image	Data Embedded Image PSNR(dB)	Restored Image PSNR(dB)
Desert	57.68	63.33
Lena	45.20	54.20
Baboon	42.75	50.76
Lighthouse	53.97	58.96

Table 2 shows comparative Analysis of Peck Signal to Noise Ratio of data embedded image and restored image after extraction of data. In table it is shown that Peck Signal to Noise Ratio of restored image is greater than data embedded image. If Peck Signal to Noise Ratio is more then noise introduced in image will be less. That means distortion in image will be less.

4 CONCLUSION

In the proposed work the embeder and extractor remain integrated because the extractor will salvage the same reference image. Reversible data hiding is based on dynamic prediction error, histogram shifting reduces the distortion and also improve the security of the original image. The proposed system providing embedding capacity of 64 characters that is 512 binary bits. A dynamis histogram shifting is used to improve capacity and fidelity of the image. The experimental results have shown that the contrast image can be enhanced by increasing PSNR value. Moreover, the original image can be exactly recovered without any additional degradation. Thus, we can say that the proposed algorithm has made the image contrast enhancement reversible. Improving the algorithm robustness, and can be used in the medical and satellite images with the better visibility.

REFERENCE

[1] Dawen Xu, Rangding Wang, and Yun Q. Shi, Fellow, IEEE "Data Hiding in Encrypted H.264/AVC Video Streams by Codeword Substitution" IEEE Transaction On Information Forensics and Security, Vol. 9, NO. 4, April 2014 applied to machine vibration analysis," in Proc. ASCI, 1999, pp. 398–405.

[2] Kede Ma. Weiming Zhang, Xianfeng Zhao, Nenghai Yu,Fenghua Li, "Reversible Data Hiding in Images by Reserving Room Before Encryption", IEEE Trans on Information Forensics and security, Vol. 8, No. 3, March 2013

[3] Kuo-Ming Hung, Wen-Kai Su, Ting-Wen Chen, Li-Ming Chen, "Reversible Data Hiding Base on VQ and Halftoning Technique", International Conference on Microelectronics, Communication and Renewable Energy (ICMiCR-2013).

[4] Jose, R.; Abraham, G, "A separable reversible data hiding in encrypted im age with improved performance", Emerging Research Areas and 2013 International Conference on Microelectronics, Communications and Renewable Energy(AICERA/ICMiCR), 2013 Annual International Conference l'IEEE 2013.

[5] Siddharth Malik, Anjali Sardana, Jaya, "A Keyless Approach to Image Encryption", 2012 international conference on Communication systems and Network Technologies l'2012 IEEE

[6] Yi-Hui Chen, Ci-Wei lan and Chiao Chih Huang, " A verifiable Visual Cryptography Scheme", Fifth International Conference and Evolutionary Computing l' IEEE 2011

[7] D. Coltuc, "Improved embedding for prediction-based reversible watermarking," IEE E Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 873–882, Sep. 2011.

[8] Wen Chung Kuo, Po Yu Lai, Lih Chyau Wuu, "Adaptive Reversible Data Hiding Based on

[9] Histogram", 10th International Conference on Intelligent Systems Design and Application, l' IEEE 2010 (2002) The IEEE website. [Online]. Available: http://www.ieee.org/

[10] W. Pan, G. Coatrieux, N. Cuppens, F. Cuppens, and C. Roux, "An additive
and lossless watermarking method based on invariant image approximation and Haar wavelet transform," in Proc. IEEE EMBC Conf., Buenos Aires, Argentina, 2010, pp. 4740–4743.

[11] H. J. Hwang, H. J. Kim, V. Sachnev, and S. H. Joo, "Reversible watermarking method using optimal histogram pair shifting based on prediction and sorting," KSII, Trans. Internet Inform. Syst., vol. 4, no. 4, pp. 655–670, Aug. 2010.

[11] C. H.Yang andM.H. Tsai, "Improving histogram-based reversible data hiding by interleaving predictions," IET Image Process., vol. 4, no. 4, pp. 223–234, Aug. 2010.

[12] Jiantao Zhou, Weiwei Sun, Li Dong,Xianming Liu, Oscar C. Au,and Yuan Yan Tang, "Secure Reversible Image Data Hiding over Encrypted Domain via Key Modulation", IEEE transactions on circuits and systems for video technology,2015

[13] Kede Ma, Wei. Zhang, Xianfeng Zhao, "Reversible data Hiding in Encrypted Images by reserving Room before encryption", IEEE trans. On information forensics and security, vol,8 No.3 , march 2013.