ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

REVERSIBLE DATA HIDING IN ENCRYPTED IMAGES USING HISTOGRAM AND CIPHERING TECHNIQUE

Surendra Rodge*, Bhushan Bawankar

* Department of Information Technology,Yeshwantrao Chavan College of Engineering,Nagpur,India
Department of Information Technology,Yeshwantrao Chavan College of Engineering,Nagpur,India

ABSTRACT

In today's world information worth more than anything so it needs to be protected during communication and other modes of exchanging information. The aim of our work is to implement data hiding efficiently in the images. For providing security to the image embedded with secret information we take help of histogram shifting and encryption techniques. So that it will be beneficial for security of the data and efficiently transmission of data to the receiver. Improving data hiding capacity in the images, reversibility, and security are the key components of the proposed work. These two techniques we used for data hiding provide good security and also improves the data hiding capacity in the images. with better data hiding capacity. We also gets good PSNR values.

KEYWORDS: Reversibility, Encryption, Histogram Shifting, Security

INTRODUCTION

Information worth more than money so it needs to be protected and transferred safely to the recipient. So the aim of the proposed work is to provide security to the images by encrypting the image and hide the secret information behind the image using some modification in the pixel value of the images by histogram shifting method so as to efficiently transfer the data to the receiver by embedding it into the images. There are a number of other applications driving interesting the subject of information hiding like in military application, medical and other areas where information has very much importance. There are number of techniques for hiding the information. Some of the techniques are LSB (least significant bit) method, histogram shifting, predictive error method, pixel value differencing method, differential expansion method. Data hiding also depend upon the capacity of image i.e. how much data should be embedded into the image. Capacity is inversely proportional to the quality of image. As during data hiding some of the pixels of the image are modified if the large number of pixels are modified the image quality becomes degraded So to maintain the quality of image at receiver end up to certain level we are going to modify only certain area of the images which worth less with respect to other area of the image. For increasing the data hiding capacity we are going to divide image into number of blocks and perform the embedding operation.

Reversible data-hiding techniques can be performed in three domains, namely, the spatial domain, frequency domain and compressed domain [6]. Two sets, set of the embedded data and another set of the cover media data are linked in data hiding process. Reversible data hiding is one kind of information hiding techniques where the aim is not only to extract the secret message but also the cover itself should be restored without loosing the cover content [1],[2]. The number of algorithm has been proposed for data hiding into the image. The algorithms can be categorized into different classes like compression-embedding framework, difference expansion, and histogram shifting [2].

Our proposed work is based on the combining two different techniques proposed earlier in order to improve security of images embedded with data. The two techniques combined are the ciphering and histogram modification technique. Stream cipher technique is used for encrypting the image. In this technique X-OR operation is performed between image pixel value and key value which results into enciphering of the image.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

The other technique is histogram shifting technique used to hide data into the image by modifying the histogram. In this technique the image is divided into number of tiles and obtained the maximum (peak intensity) and minimum (zero intensity) frequency in the histogram of each tile. Then the histogram of each tile is shifted between its minimum and maximum frequency. In order to maximize the data hiding capacity, data is then inserted at the pixel level with the largest frequency. To embed the data The zeros and peaks of the histograms of the image tiles are then relocated. As a result of embedding grey values of some pixels are modified [8].

Some of the benefits of histogram shifting are RONI, High payload , Higher objective quality , Higher subjective quality, Narrower histogram [8]

Region of Non-Interest (RONI): The data hiding is performed in the region which is less important compared to other regions. For this reason the image is divided into number of tiles based on the information available to embed. In the broader histogram of the whole image reduce the data hiding capacity as the minimum frequency may not be zero. In the narrower histograms of the image tiles, the minimum frequencies are more likely to be zero. Narrower histograms offer more options while selecting the most suitable pairs of peaks–zeros.

EXISTING TECHNIQUES

The process of embedding information into cover media, such as an image, audio or video then the process referred as data hiding. There is number of algorithms which are used to hide data into the images. Fabien A. P. Petitcolas, Ross J. Anderson, Markus G. Kuhn [5] discuss different information hiding technique in their survey. They discuss number of areas where information hiding given much importance also discuss different information hiding technique and categorize them as shown in figure

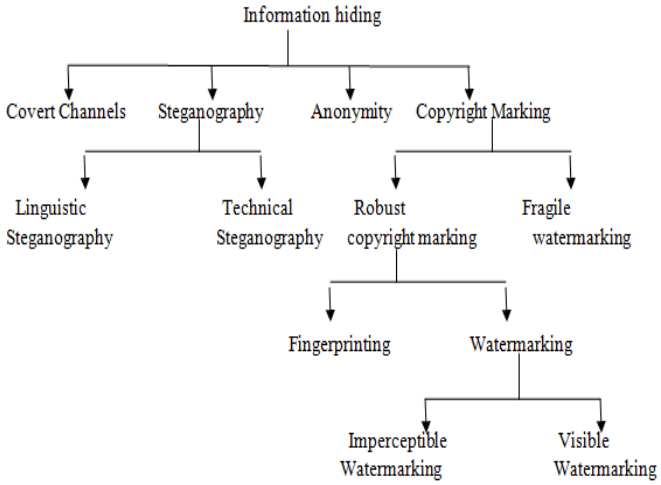

Figure 1: Categorization of information hiding technique [5].

Xinpeng Zhang proposed data hiding using encryption and least significant bit (LSB) substitution algorithms. Zhang discuss an effective means of privacy protection through encryption. In order to securely share a secret image with the recipient, the sender may encrypt the image before transmission so that opponent not able to read the content. For example, consider military images where information has much importance. The image has been encrypted for protecting the privacy of confidential information. The sender may aim to embed (hide information) the information into the corresponding encrypted images and also hopeful that the original content which are embedded in image can be recovered without any error after decryption along with the original image. Zhang obtained the values of PSNR as 37.9 dB [3].

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

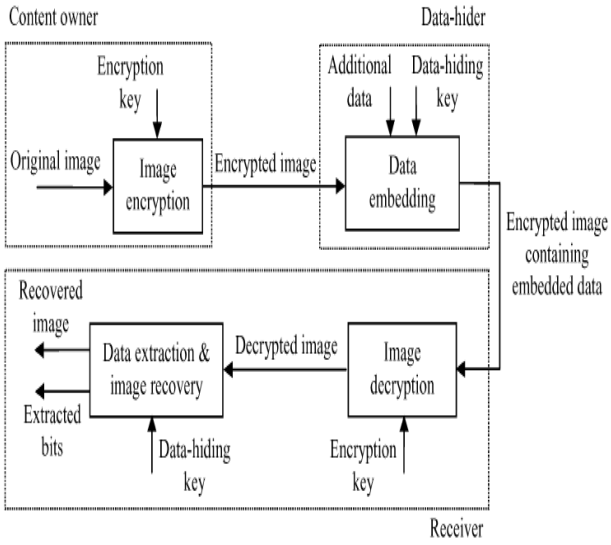

Figure 2: Scheme proposed by Xhang [3] Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, and

Wei Su discuss data hiding algorithm based on histogram shifting technique. Algorithm discuss is based on finding the zero intensity (minimum frequency) points of the histogram image tile and slightly modifies the pixel grayscale values by shifting the histogram between maximum and minimum frequency to embed data into the image. Authors propose a new reversible data embedding technique, which can embed a large amount of data (5–80 kb for a 512× 512 ×8 grayscale image) while keeping high visual quality for images. Authors guaranteed that the PSNR of the marked image versus the original image is higher than 48 dB [1].

Mehmet U. Celik, Gaurav Sharma, A. Murat Tekalp, Eli Saber discuss high capacity, low distortion , reversible data hiding technique, upon extraction of the embedded information this technique helps in the exact recovery of the original host signal. Authors proposed LSB (least significant bit) modification method as the underlying irreversible (lossy) embedding technique. This technique modifies the lowest levels- instead of bit planes- of the host signal to accommodate the payload information. In the second part, a lossless data embedding algorithm for continuous-tone images is built on the generalized LSB modification method. This spatial domain algorithm modifies the lowest levels of the raw pixel values as signal features. They got PSNR value as 51 db which decreases with the increase in the number of bit planes [4].

M. Fallahpour, D. Megias, M. Ghanbari uses somewhat similar kind of algorithm to embed data into the image using histogram shifting technique. They have performed histogram shifting on medical image to hide patient's data [8].

Wei-Liang Tai, Chia-Ming Yeh, and Chin-Chen Chang, Fellow, IEEE proposed method based histogram modification of pixel difference. In order to improve data hiding capacity of image authors used histogram modification technique using pixel differences. They also proposed the use of a binary tree structure to eliminate the requirement to communicate pairs of peak and zero points. Histogram shifting technique can also be used to prevent overflow and underflow. The PSNR values are 48 dB for level zero which decreases with the increase in tree levels[6].

Kede Ma, Weiming Zhang, Xianfeng Zhao, Member, IEEE, Nenghai Yu, and Fenghua Li proposed method of data hiding by reserving room before performing encryption on the image. Room is reserved using traditional algorithm before encryption and thus it is easy for the data hider to reversibly embed data in the encrypted image. Data extraction and image recovery are free of any error. Authors obtained results that show increased payload capacity of image with the PSNR value 40 dB [7].

PROPOSED WORK

The proposed work is based on the concept of secure data transfer over the network. In our work we are going to combine the two techniques proposed by

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

different authors for secure data transfer through images. One technique is encryption used by Zang for encrypting the image. Another technique ia used by Ansari and his teammates which is based on histogram shifting. The aim behind using these two techniques is to improve the security while transferring the information.

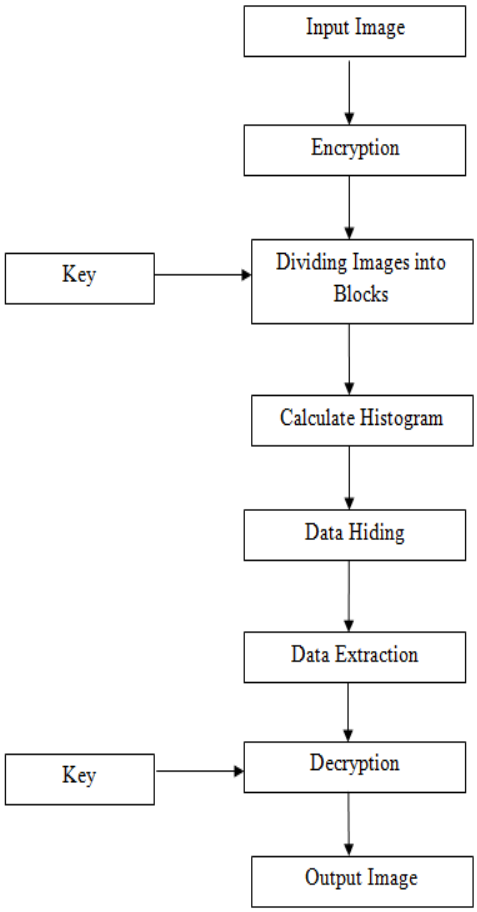

Figure 3: Flowchart of proposed work

In our proposed scheme data process through four phases as encryption, data hiding, data extraction and decryption. Encryption is performed using stream cipher i.e. X-OR operation is performed between image pixel bits and the encryption key. The same key is then used for the decryption.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

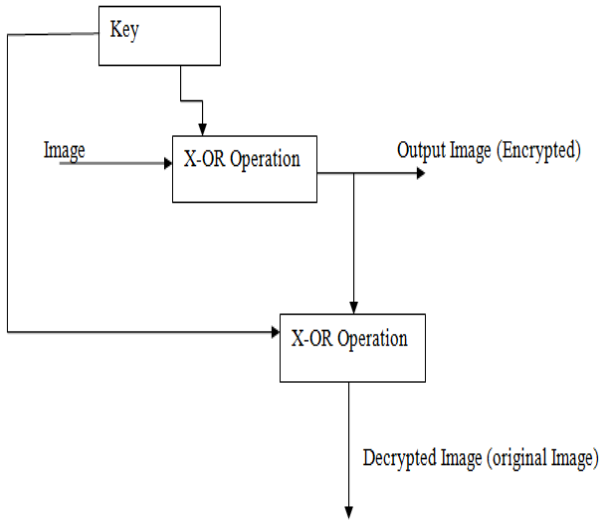

Figure 4: Encryption and Decryption operation

Data embedding is performed by histogram shifting algorithm used by Ansari and his teammates. The same concept is used by M. Fallahpour and his teammates as they perform operation of image division into block of tiles before embedding the data.

Following algorithms used by ANsari and Fallpour [8][1]

Algorithm for hiding the data:

1. Divide image into N_b non-overlapping image tiles. Then for each image tile intensity histogram of is obtained and the steps 2–4 are iteratively executed.
2. For a given number of n (peak, zero) pairs in each image tile, the pairs are chosen such that the image quality is either maximized or according to any other criteria such as perceptual quality.
3. The following iterations are executed n times for i =1 : n.

For pair (Pi, Zi) the image tile is scanned and the conditions are checked:

(a) If Pi > Zi, the grey values of the pixels between Zi + 1 and p_i are reduced by one (shif the range of the histogram to the left). This creates a gap at grey level Pi. Then the image tile is re-scanned and if the corresponding secret bits are '1'the values of the pixels with grey value of Pi − 1 are incremented by 1 otherwise they will not be modified.

(b)If Zi > Pi, the grey values of the pixels between Pi + 1 and Zi − 1 are incremented by one. As a result of this a gap is created at grey value Pi + 1. After that the image tile is re-scanned and check if the corresponding bits of to be embedded data are '1' then the values of the pixels with grey value of pi are increased by 1, Otherwise they will not be altered.

Algorithm for extracting the data:

To extract the secret message from a marked image and the lossless recovery of the host image following steps are performed..

1. The image is divided into N_b image tiles then they are rank in their order of priority. Then for each image tile steps 2–3 are repeatedly executed.

2. The following iterations are executed n times for i =1 : n.

For pair (Pi, Zi) the image tile is scanned and the conditions are checked:

(a) If Pi > Zi, the pixel with grey value Pi indicates that the embedded data bit was 1 and it should not be modified. However, its grey value has to be increased by 1 if the grey value of current pixel is equal to Pi − 1, it means that the embedded data bit was 0. After that, the grey values of all pixels with grey values between Zi and Pi − 2 need to be increased by one.

(b) If Zi > Pi, the pixel with grey value Pi indicates that the embedded data bit was 0 and they do not need to be modified. However, its grey value is reduced by 1 if the grey value of current pixel is equal to Pi + 1 as it indicates that the embedded data bit was 1. Hence the

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

grey values of all pixels with grey values between Pi + 2 and Zi are reduced by 1.

EXPERIMENTAL RESULTS

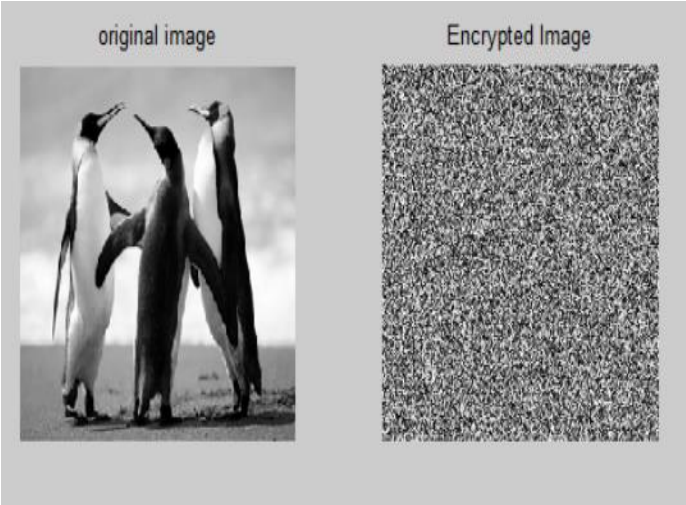

Figure 5: Result of Encryption operation

The snapshot shows the original image along with the encrypted image which is encrypted using stream cipher encryption algorithm.

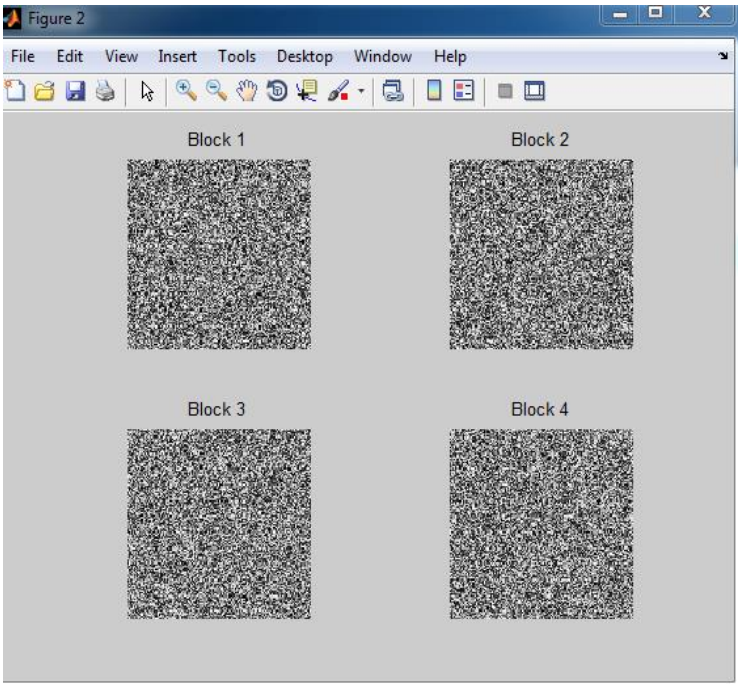

Figure 6: Result of division of image into tiles

Above snapshot shows the result of dividing image into number of blocks. We can divide the image into

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

any number block but with the increase in the image block results in increasae of overhead of combining them according to their proper location

.

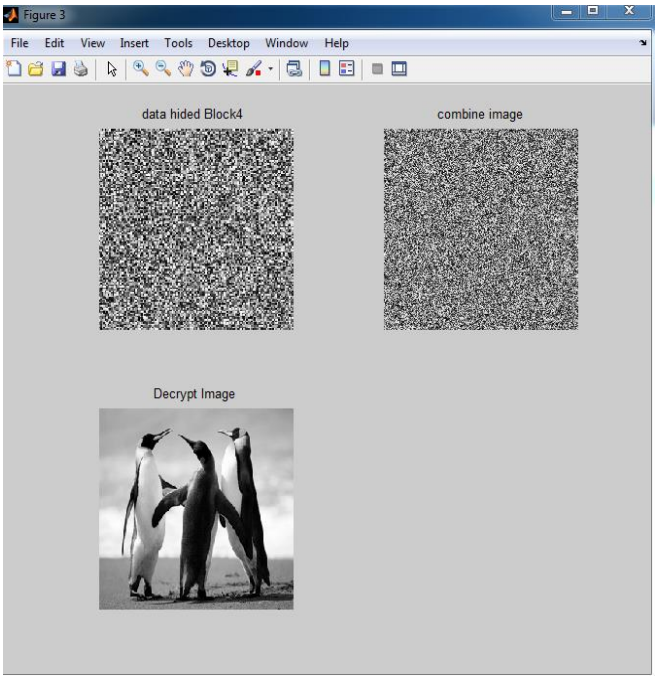

Figure 7 : Data hiding and Decryption operation

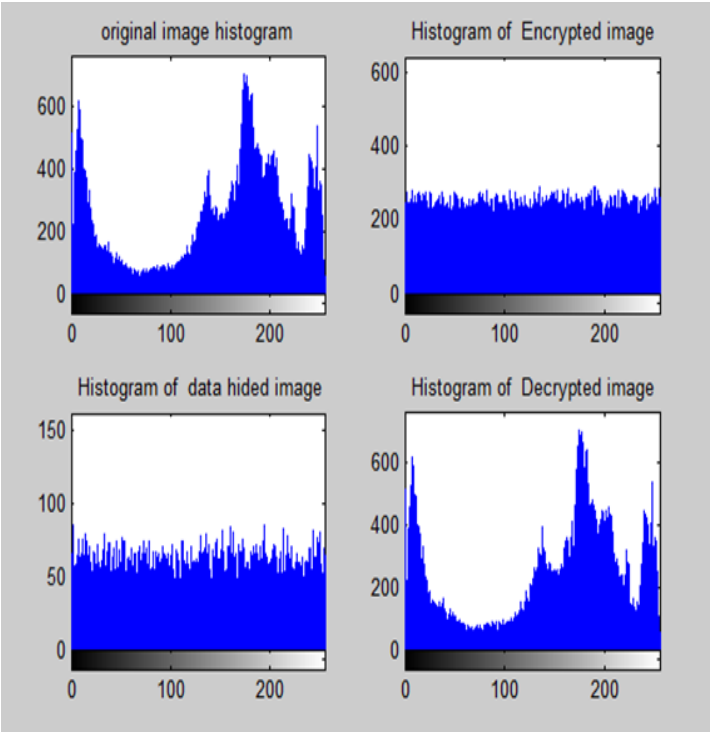

Figure 8: Histograms

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

The above snapshot shows the different histograms obtained at different level of image proccessing in the proposed scheme. Histogram is the count of pixels plotted against the intensity values of the pixel.

Image	PSNR	Payload(in bits)
Pepper	53.35	5,460
Lena	53.39	7,301
Baboon	53.41	8,782
Boat	53.36	5,421
House	53.35	5,421

Table 1: PSNR Values for different payload

CONCLUSION

Use of encryption and histogram shifting technique for data hiding may improve the security of the image also improves the data hiding performance of the image. The proposed technique can be applied to any kind of image. Technique we are going to implement preserves the image quality at the receiver end after extracting data if data is hidden into the region of non-interest that is area which does not contain much information (important information). The algorithms used are quite simple, and the execution time is rather short. The PSNR values obtained is around 51.30 dB.

REFERENCES

1. Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, and Wei Su, "Reversible Data Hiding", *IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY*, VOL. 16, NO. 3, MARCH 2006
2. Weiming Zhang, Xiaocheng Hu, Xiaolong Li, and Nenghai Yu,"Recursive Histogram Modification: Establishing Equivalency Between Reversible Data Hiding and Lossless Data Compression" *IEEE TRANSACTIONS ON IMAGE PROCESSING*, VOL. 22, NO. 7, JULY 2013.
3. XipengZang ,"Separable Reversible Data Hiding in Encrypted Image," *IEEE transactions on information forensics and security*, vol. 7, no. 2, april 2012.
4. M.U. Celik, G. Sharma, A.M. Tekalp and E. Saber, "Lossless generalized-LSB data embedding*",* IEEE 2002.
5. Fabien A. P. Petitcolas, Ross J. Anderson, And Markus G. Kuhn,"Information Hiding—A Survey," *proceedings of the ieee*, vol. 87, no. 7, july 1999.
6. Wei-Liang Tai, Chia-Ming Yeh, and Chin-Chen Chang, Fellow, IEEE "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.
7. Kede Ma, Weiming Zhang, Xianfeng Zhao, *Member, IEEE*, Nenghai Yu, and Fenghua Li ,"Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption*", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*, VOL. 8, NO. 3, MARCH 2013 553.
8. M. Fallahpour, D. Megias, M. Ghanbari ,"Reversible and high-capacity data hiding in medical images", *Published in IET Image Processing* doi: 10.1049/iet-ipr.2009.0226
9. J. Tian, "Reversible data embedding using a difference expansion, "*IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 890–896, Aug. 2003.
10. C.-C. Chang, C.-C.Lin, and Y.-H. Chen, "Reversible data-embedding scheme using differences between original and predicted pixel values," *IET Inform. Security*, vol. 2, no. 2, pp. 35–46, 2008.
11. W. Zeng, "Digital watermarking and data hiding: technologies and applications," in *Proc. Int. Conf. Inf. Syst., Anal. Synth.*, vol. 3, 1998, pp. 223–229.
12. W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," *IBM Syst. J.*, vol. 35, no. 3–4, pp. 313–336, 1996
13. Weiming Zhang, Xiaocheng Hu, Xiaolong Li, and Nenghai Yu," Recursive Histogram Modification: Establishing Equivalency Between Reversible Data Hiding and Lossless Data Compression", *IEEE TRANSACTIONS ON IMAGE PROCESSING*, VOL. 22, NO. 7, JULY 2013.
14. W. Bender, D. Gruhl, N. Morimoto, A. Lu," Techniques for data Hiding", *IBM SYSTEMS JOURNAL*, VOL 35, NOS 3&4, 1996.
15. Che-Lun Pan, Wien Hong, Jeanne Chen, Tung- Shou Chen," Multilevel Reversible Data Hiding using modification of prediction

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

errors", *International Journal of Innovative Computing, Information and Control*, Volume 7,Number 9 September 2011.

16. Yongjian Hu, Member, IEEE, and Byeungwoo Jeon, Senior Member, IEEE," Reversible Visible Watermarking and Lossless Recovery of Original Images", *IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY*, VOL. 16, NO. 11, NOVEMBER 2006
17. Franc¸ois Cayre, Caroline Fontaine, and Teddy Furon "Watermarking Security: Theory and Practice", IEEE TRANSACTIONS ON SIGNAL PROCESSING, VOL.XX, NO.Y, XYZ 2005