ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 1, January 2018

A Comprehensive Survey on Techniques of Reversible Data Hiding in Encrypted Images

Nilam N. Shaikh[1], Pratibha S. Rane[2], Prarthana M. Modak[2]

Asst. Professor, S.S.P.M.'s College of Engineering, Mumbai University, Mumbai, India[1,2,3]

ABSTRACT: Recently more attention is paid to reversible data hiding (RDH) in encrypted images, since it maintains the excellent property that the original image cover can be losslessly recovered after data embedded is extracted while protecting the image content's as confidential. In this survey paper different reversible data hiding methods are analyzed. All previous methods embed data by reversibly vacating room from the encrypted images, which may be subject to some errors on data extraction and/or image restoration. And the method by reserving room before encryption with a traditional RDH algorithm, it is easy for the data hider to reversibly embed data in the encrypted image. This paper also concerns with a method that embeds image/ text data invisibly into a video based on Integer Wavelet Transform and to minimize the mean square distortion between the original and watermarked image and also to increase Peak signal to noise ratio. The transmission and exchange of image also needs a high security. Cryptography is used to maintain security.

KEYWORDS: Reversible data hiding, image encryption, privacy protection, Data extraction.

I. INTRODUCTION

Data Hiding is the process to hide data (representing some information) into cover media. That is, the data hiding process links two sets of data, a set of the embedded data and another set of the cover media data. The relationship between these two sets of data characterizes different applications. For instance, in covert communications, the hidden data may often be irrelevant to the cover media. In authentication, however, the embedded data are closely related to the cover media. In these two types of applications, invisibility of hidden data is an important requirement. In most cases of data hiding, the cover media will experience some distortion due to data hiding and cannot be inverted back to the original media. That is, some permanent distortion has occurred to the cover media even after the hidden data have been extracted out.

In some applications, such as medical diagnosis and law enforcement, it is critical to reverse the marked media back to the original cover media after the hidden data are retrieved for some legal considerations. In other applications, such as remote sensing and high-energy particle physical experimental investigation, it is also desired that the original cover media can be recovered because of the required high-precision nature. The marking techniques satisfying this requirement are referred to as reversible, lossless, distortion-free, or invertible data image hiding techniques. Reversible data hiding facilitates immense possibility of applications to link two sets of data in such a way that the cover media can be losslessly recovered after the hidden data have been extracted out, thus providing an additional a venue of handling two different sets of data.

Data hiding is a technique which embeds data into digital media to communicate secret messages by slightly varying the content of the media, so that the embedding data is unnoticeable. Many anticipated techniques are data hiding are non-reversible which means the embedded media are distorted and cannot be restored. If the embedded media can be recovered through a specifically considered algorithm, then the data hiding technique is termed as reversible. When a digital image is used to embed data, the image that is used to carry data is called as the cover image and the image with the embedded data is called as the stego image. Images in certain applications like images in military, medical etc., allows no distortions. In these areas of applications, data hiding techniques gives a clarification to the deformation problem since the original cover image can be entirely recovered.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 1, January 2018

Reversible data hiding (RDH) in images is a technique, by which the original cover can be losslessly recovered after the embedded message is extracted. This important technique is widely used in medical imagery, military imagery and law forensics, where no distortion of the original cover is allowed. A number of reversible data hiding techniques have been proposed, and they can be roughly classified into three types: lossless compression based methods, difference expansion (DE) methods, and histogram modification (HM) methods. In practical aspect, many RDH techniques have emerged in recent years. Fridrich et Al, constructed a general framework for RDH. By first extracting compressible features of original cover and then compressing them losslessly, spare space can be saved for embedding auxiliary data. One reversible marking technique is watermarking .

The watermarking is a form of digital rights management that uses data embedded into a recording to secure the music(image) by identifying the computer or device attempting to play it and determining whether a license to play the music(image) exists on that device. These watermark programs can also transmit information about the consumer- for example, credit card numbers-back to the content owner, such as a record company or website. Digital watermarking is a technique which allows an individual to add hidden copyright notices or other verification messages to digital audio, video or image signals and documents. Such hidden message is a group of bits describing information pertaining to the signal or to the author of the signal (name, place etc) Another technique is histogram . In an image processing context, the histogram of an image normally refers to a histogram of the pixel intensity values. This histogram is a graph showing the number of pixels in an image at each different intensity value found in that image. The image is scanned in a single pass and a running count of the number of pixels found at each intensity value is kept. Then it is used to construct a suitable histogram Weiming Zhang, Biao Chen, and Nenghai Yu proposed a decompression algorithm [2]as the coding scheme for embedding data.

Three RDH schemes that use binary feature sequence as covers, i.e., one scheme for spatial images, one scheme for JPEG images, and pattern substitution scheme for binary images. Nosrati and some other people [3] present the paper Reversible Data Hiding:Principles, Techniques, and Recent Studies. In this primary techniques as the principles of RHD are talked. Pairwise logical computation data hiding technique (PWLC) and Data hiding by template ranking with symmetrical Central pixels(DHTC) technique. Lixin Luo, Zhenyong Chen, Ming Chen, Xiao Zeng, and Zhang Xiong suggested a method , [4] which can embed a large amount of covert data into images. It utilize the interpolation-error, the difference between interpolation value and corresponding pixel value, to embed bit “1” or “0” by expanding it additively or leaving it unchanged. Vasiliy Sachnev, Hyoung Joong Kim, Jeho Nam Sundaram Suresh, and Yun Qing Shi introduced a [5] Reversible Watermarking Algorithm Using Sorting and Prediction .

Here sorted prediction errors and, a reduced size location map allows to embed more data into the image with less distortion. Also sorting technique is used to record the prediction errors based on magnitude of its local variance. K.Shankar, Dr.C.Yaashuwanth develop the system [6] that uses the method RRBE (Reserving Room Before encryption) . This survey paper helps us to familiarize the technique. In [7] Dr. T. Bhaskara Reddy, Miss. Hema Suresh Yaragunti , Mr.T. Sri Harish Reddy , Dr. S. Kiran suggested an Effective Algorithm of Encryption and Decryption of Images Using Random Number Generation Technique and Huffman coding. Xinpeng Zhang did the [8] Reversible data hiding with optimal value transfer. In this the secret data, as well as the auxiliary information used for content recovery, are carried by the differences between the original pixel-values and the corresponding values estimated from the neighbors. Here, the estimation errors are modified according to the optimal value transfer rule. Another method [9] embeds image/ text data invisibly into a video based on Integer Wavelet Transform and to minimize the mean square distortion between the original and watermarked image and also to increase Peak signal to noise ratio. In Separable Reversible Data Hiding in Encrypted Image [10], a content owner encrypts the original uncompressed image using an encryption key. Then, a data-hider may compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate some additional data.

II. LITERATURE SURVEY

Lots of research has been done in the area of reversible data hiding. In last few years various efficient methods have been proposed for reversible data hiding. Some noticeable work in area of reversible data hiding is as follows:

In [7] . Bhaskara Reddy,et.al suggested an Effective Algorithm of Encryption and Decryption of Images Using Random Number Generation Technique and Huffman coding .In this paper, they implemented security for image.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 1, January 2018

They considered an image, read its pixels and convert it into pixels matrix of order as height and width of the image. Replace that pixels into some fixed numbers, generate the key using random generation technique .Encrypting the image using this key ,performing random transposition on encrypted image, converting it into one dimensional encrypted array and finally applied Huffman coding on that array , due this size of the encrypted image is reduced and image is encrypted again.The decryption is reverse process of encryption. Hence the proposed method provides a high security for an image with minimum memory usage. The main steps in the encryption algorithm is

Step 1 . Replace each pixel by fixed number values.
Step 2 .Generate the secrete key by using random generation technique
Step 3 . Huffman Coding.

The steps in image decryption is reverse of encryption Algorithm.

In [9] Subhanya R.J , Anjani Dayanandh N presented the paper " Difference Expansion Reversible Image Watermarking Schemes Using Integer Wavelet Transform Based Approach". In this project ,they present a new scheme of image watermarking to guard intellectual properties and to secure the content of digital images. It is an effective way to protect the copyright by image watermarking. The work concerns with the watermarking algorithm that embeds image/ text data invisibly into a video based on Integer Wavelet Transform and to minimize the mean square distortionbetween the original and watermarked image and also to increase Peak signal to noise ratio.Here the message bits (image) are (is) hidden into gray/color images. The size of secret data/image is smaller than cover image. To transfer the secret image/text confidentiality, the secret image/text itself is not hidden, keys are generated for each gray/color component and the IWT is used to hide the keys in the corresponding gray/color component of the cover image. The watermarks are invisible and robust against noise and commonly image processing methods.

Zhang [10] suggests a novel method for separable reversible data hiding .Here content owner first encrypts the original uncompressed image using an encryption key to produce an encrypted image. Then, the data-hider compresses the least significant bits (LSB) of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data. At the receiver side, the data embedded in the created space can be easily retrieved from the encrypted image containing additional data according to the data-hiding key. Since the data embedding only affects the LSB,a decryption with the encryption key can result in an image similar tothe original version. When using both of the encryption and data-hiding keys, the embedded additional data can be successfully extracted and the original image can be perfectly recovered by exploiting the spatial correlation in natural image.

In [11] C. Anuradha and S. Lavanya proposed a secure and authenticated descrete reversible Data hiding in cipher mages deals with security and authentication. In the first phase, a content owner encrypts the original uncompressed image using an encryption key. Then, a data hider may compress the least significant bits of the encrypted image using a data hiding key to create a sparse space to accommodate some additional data. With an encrypted image containing additional data, if a receiver has the data hiding key, receiver can extract the additional data though receiver does not know the image content. If the receiver has the encryption key, can decrypt the received data to obtain an image similar to the original one, but cannot extract the additional data. If the receiver has both the data hiding key and the encryption key, can extract the additional data and recover the original content without any error by exploiting the spatial correlation in natural image when the amount of additional data is not too large. It is also a drawback because if the receiver has any one key as known, and then he can take any one information from the encrypted data. In order to achieve authentication SHA-1 algorithm is being used.

Che-Wei Lee and Wen-Hsiang Tsai1[12] proposed a lossless data hiding method based on histogram shifting, which employs a scheme of adaptive division of cover images into blocks to yield large data hiding capacities as well as high stego-image qualities. The method is shown to break a bottleneck of data-hiding-rate increasing at the image block size of 8×8, which is found in existing histogram-shifting methods. Four ways of block divisions are designed, and the one which provides the largest data hiding capacity is selected adaptively.

Z. Ni, Y. Shi, N. Ansari, and S. Wei, has proposed a reversible data hiding algorithm[14].This algorithm can recover the original image without any distortion from the marked image after the hidden data have been extracted. It

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 1, January 2018

utilizes the zero or the minimum points of the histogram of an image and slightly modifies the pixel grayscale values to embed data into the image. It can embed more data than many of the existing reversible data hiding algorithms.

A non separable reversible data hiding method[15] proposed by Xinpeng Zhang ,is shown in Fig. 1.In this method, the data extraction is not separable from the content decryption. The additional data must be extracted from the decrypted image, so that the principal content of the original image is revealed before data extraction. If some has a data hiding key but not the encryption key, he cannot extract the information from the decrypted image containing additional data.

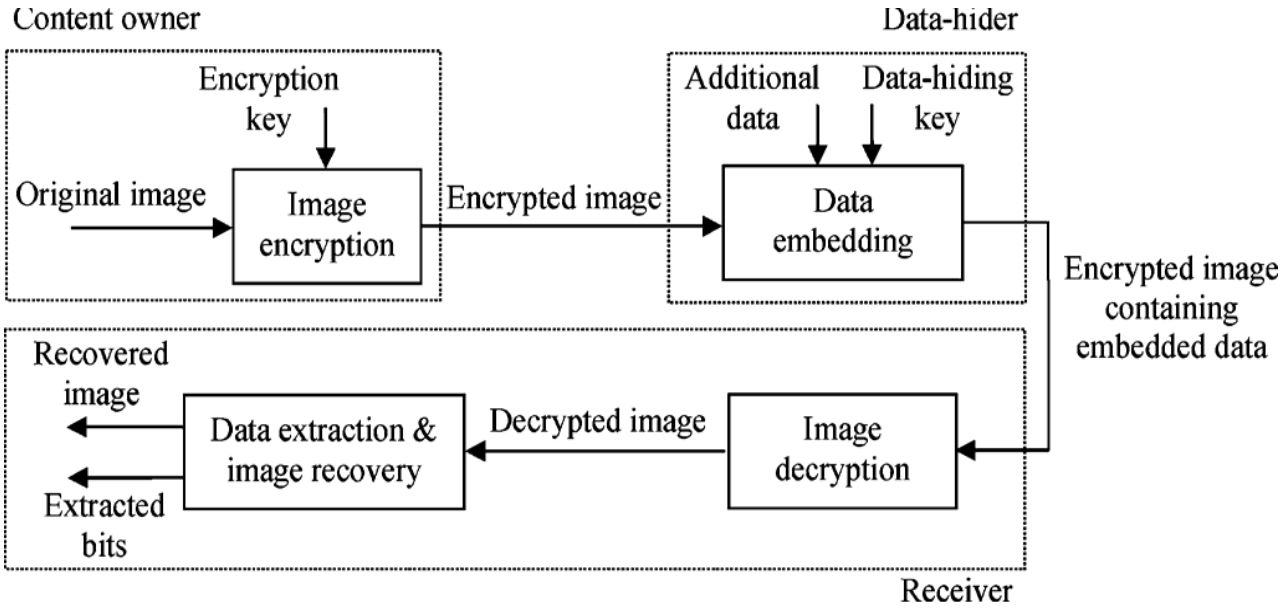

Fig. 1. A Non Separable Reversible Data Hiding method

Xinpeng Zhang has suggested, Separable Reversible Data Hiding in encrypted images [16]. As shown in Fig. 2, if the receiver has the data hiding key, he can extract the additional data though he does not know the image content. If the receiver has the encryption key, he can decrypt the received data to

obtain an image similar to the original one, but cannot extract the original data. If the receiver has the both the data hiding key and the encryption key, he can extract the additional data and recover the original content.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 1, January 2018

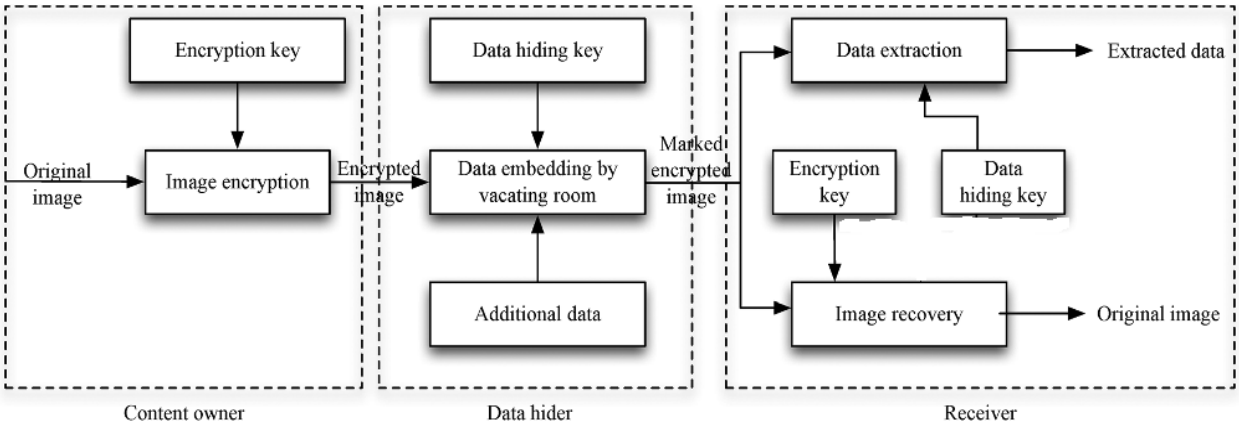

Fig. 2. A Separable Reversible Data Hiding method

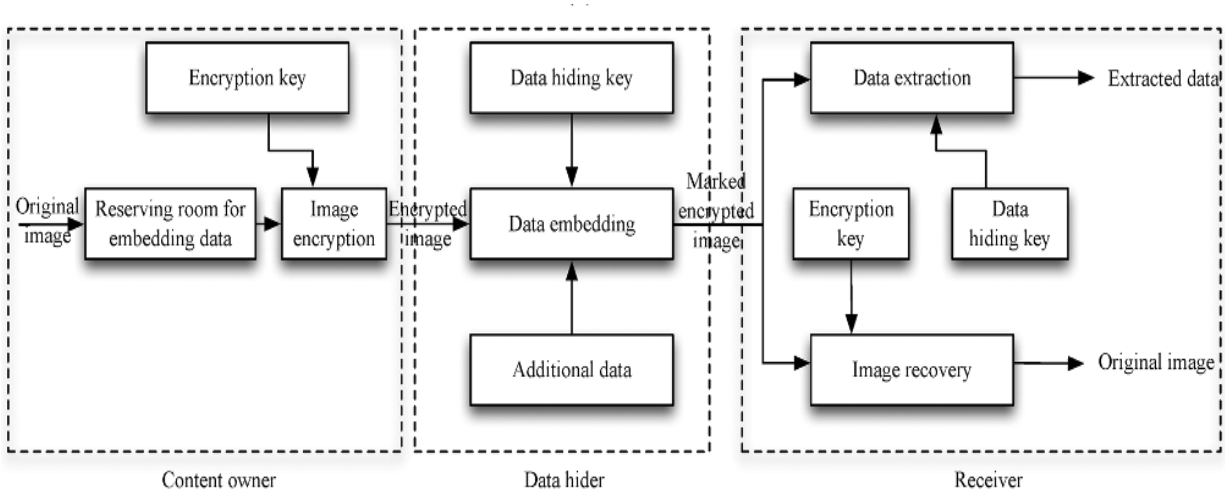

Fig.3 Reversible Data Hiding by Reserving Room Before Encryption

W. Hong, T. Chen, and H.Wu have proposed, an improved Reversible Data Hiding in Encrypted Images using Side Match[17]. The authors work exploit the pixels in calculating the smoothness of each block and consider the pixel correlations in the border of neighboring blocks.These two issues could reduce the correctness of data extraction. This method adopts a better scheme for measuring the smoothness of blocks, and uses the side-match scheme to further decrease the error rate of extracted-bits.

Reversible Data Hiding in encrypted images by Reserving Room Before Encryption [13] suggested by Kede Ma, Weiming Zhang, Xianfeng Zhao is shown in Fig.3.The method reserves room before encryption with a traditional RDH algorithm. Hence it is easy for
the data hider to reversibly embed data in the encrypted image. This method can achieve real reversibility, that is, data extraction and image recovery are free of any error.

III. SUMMARY

Reversible data hiding in encrypted images is a new topic drawing attention because of the privacypreserving requirements from cloud data management. Previous methods implement RDH in encrypted images by vacating room after encryption,as opposed to which we proposed by reserving room before encryption. Thus the data hider can benefit

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 1, January 2018

from the extra space emptied out in previous stage to make data hiding process effortless.The proposed method can take advantage of all traditional RDH techniques for plain images and achieve excellent performance without loss of perfect secrecy.

Furthermore, this novel method can achieve real reversibility, separate data extraction and greatly improvement on the quality of marked decrypted images. Also considers a new algorithm of encryption and decryption of images. This algorithm is based on Ceaser Cipher algorithm, random generation technique, concept of shuffling the rows i.e. rows transposition
and Huffman Encoding. Encryption and Decryption of an image by this algorithm protect the image from an unauthorized access.

IV. CONCLUSION

A survey on various reversible data hiding techniques is performed. Reversible data hiding schemes for encrypted image with a low computation complexity is analysed, which consists of image encryption, data hiding and data extraction/ image recovery phases. The original images are encrypted by an encryption strategy. So a study about an encryption strategy is performed. Although a data hider does not know the original content, he can embed the secret data into the encrypted image by modifying a part of encrypted data. So methods for data embedding are also noticed.

REFERENCES

[1] J. Fridrich and M. Goljan, “Lossless data embedding for all image formats,” in Proc. SPIE Proc. Photonics West, Electronic Imaging, Securityand Watermarking of Multimedia Contents, San Jose, CA,
USA,Jan. 2002, vol. 4675, pp. 572–583
[2] W. Zhang, B. Chen, and N. Yu, “Improving various reversible data hiding schemes via optimal codes for binary covers,” IEEE Trans.Image Process., vol. 21, no. 6, pp. 2991–3003, Jun. 2012.
[3] Nosrati * Ronak Karimi Mehdi Hariri,” Reversible Data Hiding:Principles, Techniques, and Recent Studies”. World Applied Programming, Vol (2), Issue (5), May 2012. 349-353ISSN: 2222- 2510©2011 WAP journal. www.waprogramming.com
[4] L. Luo et al., “Reversible image watermarking using interpolation technique,” IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 187–193,Mar. 2010.
[5]. V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y.-Q. Shi, “Reversible watermarking algorithm using sorting and prediction,” IEEE Trans.Circuits Syst. Video Technol., vol. 19, no. 7, pp. 989– 999, Jul. 2009.
[6] K.Shankar, 2Dr.C.Yaashuwanth” Data Hiding and Retrieval in Encrypted Images”. © 2014 IJEDR | Volume 2, Issue 1 | ISSN:2321-9939
[7] Dr. T. Bhaskara Reddy, Miss. Hema Suresh Yaragunti , Mr.T. Sri Harish Reddy, Dr. S. Kiran “ An Effective Algorithm of Encryption and Decryption of Images Using Random Number Generation Technique and Huffman coding” Hema Suresh Yaragunti et al,
Int.J.Computer Technology & Applications,Vol 4 (6),883-891
[8]. Xinpeng Zhang, Member, IEEE “Reversible Data Hiding With Optimal Value Transfer” IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 15, NO. 2, FEBRUARY 2013
[9]. Subhanya R.J (1), Anjani Dayanandh N (2)” Difference Expansion Reversible Image Watermarking Schemes Using Integer Wavelet Transform Based Approach”. International Journal of Engineering
Research and Applications (IJERA) ISSN: 2248-9622 International Conference on Humming Bird (01st March 2014)
[10]. X. Zhang, “Separable reversible data hiding in encrypted image,” IEEETrans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.
[11] C. Anuradha and S. Lavanya “A secure and authenticated reversible Data hiding in encrpted images” © 2013, IJARCSSE
[12] Che-Wei Lee1 and Wen-Hsiang Tsai1 “A Lossless Data Hiding Method by Histogram Shifting Based on an Adaptive Block Division Scheme” c 2010 River Publishers.
[13] 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, Mar. 2013
[14] Z. Ni, Y. Shi, N. Ansari, and S. Wei, “Reversible data hiding,” IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar,2006.
[15] X. Zhang, “Reversible data hiding in encrypted image”, IEEE Signal Process. Lett., vol.18, no.4, pp. 255-258, Apr.2011
[16] X. Zhang, “Separable reversible data hiding in encrypted image,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.
[17] W. Hong, T. Chen, and H.Wu, “An improved reversible data hiding in encrypted images Using side match”, IEEE Signal Process. Lett., vol. 19, no. 4, pp. 199–202, Apr. 2012.
[18] Weiming Zhang, Kede Ma, Nenghai Yu, “Reversibility improved data hiding in encrypted Images”, ELSEVIER Signal Process., 94 (2014) 118-127