International Journal of Innovative Research in Technology and Science
ISSN: 2321-1156 www.ijirts.org Volume 11 Issue 2, March 2023

A Survey Paper on Reversible Data Hiding with Hierarchical Embedding for Encrypted Images

Ritik Gour[1], Amar Nayak [2]
Computer Science and Engineering Department, TITE, RGPV, MP, Bhopal, India
ritikgour631@gmail.com, amar.n1975@gmail.com

Abstract: Reversible data hiding (RDH) is a form of information hiding that allows both the host sequence and the embedded data to be recovered without losing the marked sequence. In addition to media annotation and integrity authentication, RDH has recently been innovatively used in various other fields. With the advancement of digital communication, computer technologies, and the Internet, ensuring information security is considered one of the most difficult challenges in communication to protect user data. Numerous reversible and steganographic techniques are available for hiding or securing data, such as text, images, and protocols, which can be secretly transmitted to a receiver. A powerful data security technique is reversible data hiding in encrypted images (RDHEI). As digital techniques for transmitting and storing images become more widespread, it is increasingly important to consider how to protect image confidentiality, integrity, and authenticity. Any text associated with the image, such as authentication or author information, could be used as data. The receiver must be able to recover both the hidden data and the original image. Reversible data hiding is a technique that meets this requirement by allowing the host image to be accurately recovered. This research paper extends the performance parameters used in encryption processes and analyses their security issues using the MATLAB tool. We compare our proposed technique to the existing RDHEI technique, not only in terms of embedding but also in other aspects.

Keywords: Reversible Data Hiding, Image Encryption, Image Decryption, Histogram Shifting, MSE Measure, PSNR Measure, security.

I. Introduction

Nowadays, digital media is efficiently stored with high quality in a wide range of everyday life, but it can easily be manipulated through computer systems. Therefore, digital data can be transmitted through data communication networks quickly and inexpensively without losing quality. With the distribution of digital multimedia over the World Wide Web, intellectual property rights are more threatened than ever due to the possibility of unlimited copying. In order to restrict easy data copying, encryption techniques can be used. However, encryption alone does not protect as decrypted data can be freely distributed or manipulated. This problem can be solved by hiding ownership data in the multimedia data, which can later be extracted to prove ownership. This technique is widely used in bank currency, where a watermark is embedded to check the note's originality. The same concept, watermarking, can be applied to digital multimedia content to check its authenticity [1].

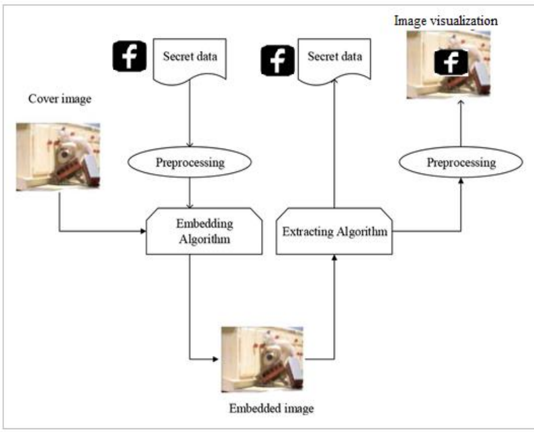

Figure1. reversible data hiding process

Secure image data-hiding techniques are used in the reversible data-hiding process, which also requires secret communication. This method involves hiding extra messages in cover media using a reversible approach to completely restore the original image and data cover content after extracting the hidden message's data or information. Image data hiding has traditionally been used for secret communication. In some important applications, the embedded carriers or images are encrypted to prevent the carrier or image from being analysed to reveal the presence of the embedment. In other applications, the carrier's owner or image may not want the other person, including the image data hider, to be familiar with the content of the image carrier before data hiding, such as in military images or secret medical images. Under this condition, the content or data owner must encrypt the content or data before passing it to the data hider for information or data embedment. The embedded message can be extracted, and the receiver can recover the original image. Many new reversible data-hiding schemes have been proposed, such as shifting the block histogram, data embedding based on 0 and 1 bits, and the difference expansion method using histograms. The lossless compression method in the difference expansion method produces less PSNR and more MSE than the BHS method [1]. Data hiding is a set of techniques used to securely store data in a host media with minimal degradation in the host, which can later be extracted. Steganography is a pro-security technique in which confidential data is embedded in a cover [2]. This method falls under reversible data hiding. In reversible data hiding, information bits are inserted by modifying the host signal, allowing for the lossless restoration of the original host signal after extracting the embedded information. However, recovering the exact original image is desirable in many fields, such as legal, medical, and military imaging. For instance, bank checks are scanned and protected with an authentication scheme based on reversible data hiding and sent through the Internet.

In most cases, watermarked documents are sufficient to distinguish the contents unambiguously. However, if any uncertainty arises, the possibility of recovering the original unmarked document is intriguing. Figure 1 depicts the block diagram of a basic reversible data-hiding system. Notably, the existing reversible data-hiding schemes are the most fragile. Imperceptibility and embedding capacity are the two significant properties of reversible data hiding. Imperceptibility pertains to the similarity measure between the stego and the cover image. In contrast, the embedding capacity measures the maximum number of information bits that can be embedded in the cover image. The performance of a reversible data-hiding technique is evaluated based on imperceptibility and embedding capacity [3].

1.1 Reversible Data Hiding in Encrypted Images

Reversible data hiding in an encrypted domain, or RDH-EI, involves embedding additional information into an encrypted image using any reversible data hiding method. The content owner encrypts the original image and sends it to the data hider using any encryption method. The receiver can extract the hidden data and decrypt the image. Some common reversible data hiding methods include LSB substitution, difference expansion, and histogram modification. Encryption can be categorised into two main types: symmetric encryption (private key cryptography) and asymmetric encryption (public key cryptography) [4]. The RDH-EI process involves the content owner, the data hider, and the receiver. The content owner encrypts the original image using an encryption key to obtain the encrypted image, and the data hider embeds data within the encrypted image using a data hiding key. The receiver extracts the embedded data from the encrypted image and performs image recovery. Image encryption executes an exclusive OR operation between the original and pseudo-random bits. The pseudo-random bits are generated using the encryption key, and the XOR results of various pixels are concatenated in an orderly manner.

Data embedding is executed by handing over the encrypted image to a data hider, who can embed extra data into the encrypted image by flipping a small part. First, the data hider segments the encrypted image into non-overlapping blocks of size s*s. For each block of size s2, the pixels are divided into two groups, s0 and s1, according to a data hiding key. If the data to be embedded is 0, the data hider flips the three least significant bits of the encrypted pixel in s0. And if the data to be embedded is 1, then the data hider flips the three least significant bits of the pixel in s1. The other encrypted data remains unchanged.

Data extraction and image recovery are performed by the receiver, who receives the encrypted image with the embedded data. The decryption operation is executed by performing an XOR operation between the bits of the encrypted image and the pseudo-random bits generated using the encryption key. The five most significant bits of each pixel are received correctly. For data extraction, the decrypted image is divided into different blocks, and the pixels of each block are divided into two parts, s0 and s1 [5].

1.2 Characterised of RDHEI

Reversible Data Hiding (RDH) is becoming increasingly popular due to its ability to restore the original image with minimal distortion and fair quality after extracting the hidden data. From a secure communication system perspective, RDH techniques involve embedding digital information in an image, which can only be extracted by an authenticated party to restore the original image. An information hiding system can be evaluated based on four different aspects: capacity, security, perceptibility, and robustness. Capacity refers to the amount of confidential information the cover media can accommodate. Security refers to the features implemented to protect against hackers' extraction of confidential information. Perceptibility is the ability to notice hidden information, while robustness is the ability to withstand modifications on the stego medium without distorting confidential information [6].

II. Related Work

Reversible Data Hiding (RDH) has existed for years, and researchers have proposed various RDH techniques on encrypted images to improve their characteristics. This section discusses different RDH methods on encrypted images that have been proposed. In the work of Yu, Chunqiang et al. [7], RDH on encrypted images is considered an effective data security technique. However, most of the state-of-the-art RDHEI methods fail to achieve desirable payload. The authors propose a new RDHEI method with hierarchical embedding to address this issue. The proposed method has two contributions. First, a novel hierarchical label map generation technique is proposed for the bit-planes of the plaintext image.

The hierarchical label map is calculated using a prediction technique and is compressed and embedded into the encrypted image. Second, hierarchical embedding is designed to achieve a high embedding payload. This embedding technique hierarchically divides prediction errors into three kinds: small-magnitude, medium-magnitude, and large-magnitude, which are marked by different labels. Unlike conventional techniques, pixels with small-magnitude/large magnitude prediction errors accommodate secret bits in the hierarchical embedding technique. In W. Puech et al. [8], an analysis of the local standard deviation of the marked encrypted images is proposed to remove the embedded data during the decryption step for multimedia protection based on encryption and watermarking algorithms. These algorithms rely on Kirchhoff's principle, where all algorithm details are known, and only the key to encrypt and decrypt the data should be kept secret. However, there are three main problems with block encryption methods. Firstly, when there are homogeneous zones, all blocks in these zones are encrypted similarly. Secondly, block encryption methods are not robust to noise due to the large size of the blocks. Lastly, data integrity is a concern. The combination of encryption and data hiding can solve these problems. Therefore, using this approach, a reversible data hiding method for encrypted images is able to embed data in encrypted images, decrypt the image, and rebuild the original image by removing the hidden data. However, it is impossible to use this approach when a high-capacity reversible data-hiding method for encrypted images is needed. In Q. Ying et al. [9], traditional reversible data hiding (RDH) aims to increase embedding payloads while minimising distortion using mean square error (MSE) as a criterion. However, imperceptibility can also be achieved through image processing. Therefore, the authors propose a novel RDH method with contrast enhancement (RDH-CE) using histogram shifting. Instead of minimising MSE, the proposed method generates marked images with good quality based on structural similarity.

The proposed method consists of two parts: baseline embedding and extensive embedding. In the baseline part, the least significant bits are merged to reserve spare bins, and additional data is embedded using a histogram-shifting approach with arithmetic encoding. The authors propose constructing the transfer matrix by maximising histogram entropy during histogram shifting. After embedding, the marked image containing additional data contrasts more than the original image. The authors propose concatenating the baseline embedding with an MSE-based embedding in the extensive embedding part. On the recipient side, the additional data can be extracted exactly, and the original image can be recovered losslessly. Compared to existing RDH-CE approaches, the proposed method achieves a better embedding payload. In Jun Tian et al. [10], reversible data embedding, also known as lossless data embedding, involves embedding invisible data into a digital image in a reversible manner. As a basic requirement, the quality degradation on the image after data embedding should be low. A captivating feature of reversible data embedding is the ability to remove the embedded data to restore the original image. A common approach of high-capacity reversible data embedding is to select an embedding area, such as the least significant bits of some pixels in an image, and embed both the payload and the original values needed for the exact recovery of the original image into such area. The authors employ a difference expansion (DE) technique, which discovers extra storage space by exploring redundancy in image content, to reversibly embed a payload into digital images. However, the main limitations of this method are the payload capacity limit and the visual quality of embedded images.

Furthermore, reversible data embedding is a fragile technique. When the embedded image is manipulated and/or lossy compressed, the decoder will identify it as inauthentic and original content restoration will not be possible. In Yu et al. [11] proposes work, reversible data hiding in encrypted images is proposed based on a novel separable and error-free approach using two-layer pixel errors. The original image is first divided into non-overlapping blocks and then permuted. A closed Hilbert curve is used to scan each block to obtain a one-dimensional pixel sequence that is encrypted with key transmission. The encrypted image is scanned in a closed Hilbert order to generate a one-dimensional encrypted pixel sequence during data hiding. The histogram of two-layer adjacent encrypted pixel errors embeds secret data by histogram shifting. Experimental results show the proposed scheme has a high payload and outperforms other reversible data-hiding schemes for encrypted images. Zhang et al. [12] propose a novel approach called RDHEI, which predicts some pixels before encryption to embed secret data in the prediction errors rather than embedding directly in encrypted images. As a result, some of the prediction errors will not be encrypted. Shuang Yi et al. [13] propose an improved approach for estimating the error for secret data embedding. Instead of randomly selecting pixels from the original image, half of the pixels are estimated to obtain the estimation errors, resulting in a significantly improved maximum embedding rate while maintaining a high image quality of the marked decrypted image.

The method first estimates a portion of the pixels using the remaining pixels to obtain estimation errors, which are then encrypted along with the remaining pixels. The data hider then embeds secret data into the encrypted estimation errors, and the image is scrambled using a sharing key. The secret data and the original image can be extracted and recovered separately at the receiver side using different security keys. Xu Wang et al. [14] reported an RDHEI using a correlation of sample and non-sample pixels. Sample pixels as reference points are used to calculate the prediction errors of non-sample pixels. A stream cypher is used to encrypt sample pixels, and a specific encryption procedure is planned to encrypt prediction errors of non-sample ones. Accordingly, a part of more frequent prediction errors is not encrypted. This procedure may be organised using a modified histogram shifting and difference expansion technique.

In this scheme, a part of prediction errors will not be encrypted. Zhaoxia Yin et al. [15] proposed and evaluated a new separable RDHEI framework. Additional data can be embedded into a cypher image previously encrypted using Josephus traversal and a stream cypher. A Block histogram shifting (BHS) approach using self-hidden peak pixels is adopted to perform reversible data embedding. Depending on the keys held, legal receivers can extract only the embedded data with the data-hiding key or decrypt an image very similar to the original image with the decryption key. They can extract both the embedded data and recover the original image error-free if both keys are available. The results demonstrate higher data embedding capacity, better decrypted-marked-image quality, error-free data extraction and accurate image reconstruction. Yin et al. [16] designed an RDHEI method based on multiple most significant bit predictions and Huffman coding (MMPHC), which compared the most significant bit (MSB) of the original pixel with the predicted pixel, used the bits of the same sequence as a label, and marked the pixel with a pre-defined Huffman code. However, experiments show that pre-defined Huffman encodings do not perform markup well. To take advantage of the correlation of adjacent pixels,

Table 1 Description of all RDHEI Related Work

Author Name	Year	Title	Description
Yu, Chunqiang et al. [7]	2021	Reversible data hiding with hierarchical	Low PSNR

		embedding for encrypted images	And high error rate (MSE)
W. Puech et al. [8]	2020	A Reversible Data Hiding Method for Encrypted Images	high error rate (MSE), block effect and low robustness
Q. Ying et al. [9]	2019.	Reversible Data Hiding with Image Enhancement Using Histogram Shifting	block effect based on block shifting Low PSNR And high error rate (MSE)
Jun Tian et al. [10]	2003	Reversible data embedding using a difference expansion	high error rate (MSE), block effect and low robustness
C. Yu et al., [11]	2018	Separable and Error-Free Reversible Data Hiding in Encrypted Image Based on Two-Layer Pixel Errors	Low PSNR And high error rate (MSE)
Zhang *et al.* [12]	2014	Reversibility improved data hiding in encrypted images	block effect based on block shifting Low PSNR And high error rate (MSE)
Shuang Yi et al. [13]	2015	An Improved Reversible Data Hiding in Encrypted Images	Low PSNR And high error rate (MSE)
Xu Wang et al. [14]	2016	Separable and error-free reversible data hiding in encrypted images	Not error free also has Low PSNR And high error rate (MSE)
Zhaoxia Yin et al. [15]	2016	Reversible Data Hiding in Encrypted Image Based on Block Histogram Shifting	block effect based on block shifting Low PSNR And high error rate (MSE)
Yin et al. [16]	2020	Reversible data hiding in encrypted images based on multi-MSB prediction and Huffman coding	Low PSNR And high error rate (MSE)
Zhang et al. [17]	2016	Reversible data hiding in encrypted images by reversible image transformation	Not properly encrypted image, low robustness quality image and more error
Puteaux et al. [18]	2018	An efficient MSB prediction-based method for high-capacity reversible data hiding in encrypted images	Not efficient MSB, low robustness quality image and more error
I. J. Cox et al. [19]	2007	Digital Watermarking and Steganography	Low PSNR And high error rate (MSE)
Nutan Palshikar et al. [20]	2014	Lossless Data Hiding using Histogram Modification and Hash Encryption Scheme	Lossless Data Hiding, low robustness quality image and more error
Mithu Varghese et al. [21]	2014	A Survey on Separable Reversible Data Hiding in Encrypted Images	block effect based on block shifting Low PSNR And high error rate (MSE)
Z. Ni et al. [22]	2006	Reversible data hiding	low robustness quality

			image and more error
L. R. Mathew et al. [23]	2014	Histogram Shifting based reversible data hiding	block effect based on block shifting Low PSNR And high error rate (MSE)
Rini.J et al. [24]	2013	Study on Separable Reversible Data Hiding in Encrypted Images"	Low PSNR And high error rate (MSE)
K. A. Navas et al. [25]	2008	DWT-DCT-SVD based watermarking	low robustness quality image and more error
Chauhan Usha et al. [26]	2016	Digital Image Watermarking Techniques and Applications: A Survey	block effect based on block shifting Low PSNR And high error rate (MSE)
Jiantao Zhou et al. [27]	2015	Secure Reversible Image Data Hiding Over Encrypted Domain via Key Modulation	Low PSNR And high error rate (MSE)
Ashwind S et al. [28]	2014	Secure Data Transmission Using Reversible Data Hiding	block effect based on block shifting Low PSNR And high error rate (MSE)
X. Zhang et al. [29]	2012	Separable reversible data hiding in the encrypted image,	Not properly encrypted image, low robustness quality
			image and more error
M.S Hwanga et al. [30]	2013	A reversible data hiding method by histogram shifting in high-quality medical images	low robustness quality image and more error

III. Problem Formulation

An effective technique is reversible data hiding in encrypted images (RDHEI). Existing approaches (RDHEI) face various issues, and one method for addressing the security issue is data hiding technology, which embeds the secret data imperceptibly into the cover media. However, the main problem is that the block binary embedding histogram process in existing approaches (RDHEI) does not increase PSNR values, has high MSE values, and does not support authentication. More multimedia files are stored and transmitted through the Internet. Data hiding is thought to be a proposed solution to these problems.

IV. Conclusion

Due to the reversibility of the carrier medium at the receiving end after secret data extraction, reversible data hiding methods have gained popularity. The performance of these methods can be assessed based on the image's visual quality and the algorithm's complexity. Data Hide various reversible data hiding techniques, including those for encrypted images requiring less PSNR computation. These techniques have three phases: image cryptography, data embedding, and data extraction/image recovery. The original pictures are encrypted using a cryptography strategy in the image cryptography phase. The data hider can then embed additional data without knowing the original image's content. Data extraction and image recovery can be done independently. Reversible data hiding techniques can conceal secret information within cover images and recover the cover image after the secret message has been extracted. RHD can be used on encrypted images to hide the original content from others. This paper has examined several methods to comprehend how information is embedded in graphical representations. The proposed binary bit embedding technique achieves perfect reconstruction of the original image by the content owner without the use of a data hider key, as well as increased PSNR and low MSE.

References

[1]. Zhang, X., Reversible data hiding in encrypted image. IEEE signal processing letters, 18(4), 255-258, 2011.

[2]. Puech, William, Marc Chaumont, and Olivier Strauss. "A reversible data hiding method for encrypted images." In security, forensics, steganography, and watermarking of multimedia contents X, vol. 6819, pp. 534-542. SPIE, 2008.

[3]. Ma, Kede, Weiming Zhang, Xianfeng Zhao, Nenghai Yu, and Fenghua Li. "Reversible data hiding in encrypted images by reserving room before encryption." IEEE Transactions on information forensics and Security 8, no. 3: 553-562, 2013.

[4]. Tai, Wei-Liang, 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 19, no. 6: 906-910, 2009.

[5]. Awrangjeb, Mohammad. "An overview of reversible data hiding." In Proceedings of the Sixth International Conference on Computer and Information Technology, pp. 75-79,2003.

[6]. Wang, Junxiang, Jiangqun Ni, Xing Zhang, and Yun-Qing Shi. "Rate and distortion optimisation for reversible data hiding using multiple histograms shifting." IEEE Transactions on Cybernetics 47, no. 2: 315-326, 2016.

[7]. Yu, Chunqiang, Xianquan Zhang, Xinpeng Zhang, Guoxiang Li, and Zhenjun Tang. "Reversible data hiding with hierarchical embedding for encrypted images." IEEE Transactions on Circuits and Systems for Video Technology 32, no. 2,451-466, 2021.

[8]. W. Puech, M. Chaumont and O. Strauss "A Reversible Data Hiding Method for Encrypted Images", SPIE, IS & T'08: SPIE Electronic Imaging, Security, Forensics, Steganography and Watermarking of Multimedia Contents, San Jose, CA, USA.

[9]. Q. Ying, Z. Qian, X. Zhang and D. Ye, "Reversible Data Hiding with Image Enhancement Using Histogram Shifting," in IEEE Access, vol. 7, pp. 46506-46521, 2019.

[10]. J. Tian, "Reversible data embedding using a difference expansion," IEEE Transaction on Circuits and Systems for Video Technology, Vol. 13, No. 8, August 2003. pp. 890 - 896.

[11]. C. Yu, X. Zhang, Z. Tang and X. Xie, "Separable and Error-Free Reversible Data Hiding in Encrypted Image Based on Two-Layer Pixel Errors," in IEEE Access, vol. 6, pp. 76956-76969, 2018.

[12]. W. Zhang, K. Ma, and N. Yu, "Reversibility improved data hiding in encrypted images," Signal Processing, vol. 94, no. 1, pp. 118-127, Jan. 2014.

[13]. Shuang Yi, Yicong Zhou" An Improved Reversible Data Hiding in Encrypted Images" Signal and Information Processing (ChinaSIP), 2015 IEEE China Summit and International Conference on, Pages:9, 2015.

[14]. D. Xu, and R. Wang, "Separable and error-free reversible data hiding in encrypted images," Signal Processing, vol. 123, pp. 9-21, Jun. 2016.

[15]. Zhaoxia Yin, Andrew Abel, Xinpeng Zhan, Bin Luo "Reversible Data Hiding in Encrypted Image Based on Block Histogram Shifting "Acoustics, Speech and Signal Processing (ICASSP), IEEE International Conference on,2129-2133, 2016.

[16]. Z. Yin, Y. Xiang and X. Zhang, "Reversible data hiding in encrypted images based on multi-MSB prediction and Huffman coding," IEEE Transactions on Multimedia, vol. 22, no. 4, pp. 874–884, 2020.

[17]. Zhang, Weiming, Hui Wang, Dongdong Hou, and Nenghai Yu. "Reversible data hiding in encrypted images by reversible image transformation." IEEE Transactions on Multimedia 18, no. 8: 1469-1479, 2016.

[18]. Puteaux, Pauline, and William Puech. "An efficient MSB prediction-based method for high-capacity reversible data hiding in encrypted images." IEEE Transactions on information forensics and Security 13, no. 7 1670-1681, 2018.

[19]. I. J. Cox, M. L. Miller, and J. A. Bloom, Digital Watermarking and Steganography, Morgan Kaufmann, 2nd edition, 2007.

[20].] Nutan Palshikar, Prof. Sanjay Jadhav, "Lossless Data Hiding using Histogram Modification and Hash Encryption Scheme", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 4, Issue 1, 2014.

[21]. Mithu Varghese, Teenu S Jhon, "A Survey on Separable Reversible Data Hiding in

Encrypted Images", International Journal of Computer Applications Advanced Computing and Communication Techniques for High-Performance Applications,0975 – 8887,2014.

[22]. Z. Ni, Y. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Transactions on Circuits and Systems for Video Technology, vol. 16, no. 3, pp. 354–362, 2006.

[23]. L. R. Mathew, A. C. Haran V., "Histogram Shifting based reversible data hiding", IJETT, pp. 482-485, 2014.

[24]. Rini. J, 4th Semester MTech, Dept. of Computer Science and Information Systems FISATAngamaly, Kerala, India "Study on Separable Reversible Data Hiding in Encrypted Images" International Journal of Advancements in Research & Technology, Volume 2, Issue 12, December-2013 Copyright © 2013 SciResPub. IJOART.

[25]. K. A. Navas, M. C. Ajay, M. Lakshmi, T. S. Archana, and M. Sasikumar, "DWT-DCT-SVD based watermarking," in Communication Systems Software and Middleware and Workshops, 2008. COMSWARE 2008. 3rd International Conference on, 2008, pp. 271–274.

[26]. Chauhan Usha, Singh Rajeev Kumar, "Digital Image Watermarking Techniques and Applications: A Survey", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 3, March 2016.

[27]. 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.

[28]. Ashwin S, Ganesh K, Gokul R and Ranjeeth Kumar C, "Secure Data Transmission Using Reversible Data Hiding", International Journal of Computer Science and Information Technologies, Vol. 5 Issue 2 pp. 861-1863, 2014.

[29]. X. Zhang, "Separable reversible data hiding in the encrypted image," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.

[30]. M.S Hwanga, L.Y. Tsengb, LC Huang, "A reversible data hiding method by histogram shifting in high-quality medical images", Journal of Systems and Software, Vol. 86, (3), pp. 716–727, 2013.