Improved Reversible Image Encryption Data Hiding Algorithm and BHSEA

Swapnil Singh Thakur[1], Prof. Amit Thakur[2]

M. Tech. Scholar, Department of CSE, SVCST, RGPV, Bhopal, India[1]

Assistant Professor, Department of CSE, SVCST, RGPV, Bhopal, India[2]

Abstract: Describes the thought of Reversible Information Hiding (RDH) methodology is predicated on steganography. Recently loads of attention is paid to RDH in encrypted image. Security ought to be provided for the transmission of confidential and sensitive information over the network and insecure channel, loss in data happens. To secure the data, code the wrap information and introduce is secret information into cover media. therefore the protection of image and embedded data is maintained, Since RDH manages the outstanding secured property, and thus the first image are usually recovered with none loss, Reversible Information Concealing (RDH). At intervals the planned rule, bar chart Shifting (HS) is used for RDH, and thus the BHSEA methodology is employed for encryption. The BHSEA methodology performs four processes for encoding; Reversible info concealing can be a kind of info concealing techniques whereby the host image is usually recovered specifically. Being lossless makes this methodology acceptable for medical, military applications and cloud storage. In cloud storage, a content owner can code an image to preserve his/her privacy, and transfer the encrypted information onto cloud. Reversible information activity in encrypted image, which could recover the primary image with none distortion from the marked image once the hidden data, are extracted. Existing rule consists of varied hierarchical steps for the data embedding and thus the encryption. Therefore, the planned rule area unit usually acceptable for the stratified access system, where the permission is granted in keeping with the numerous access rights and planned algorithmic program up strength and authentication of image information concealing. Generation of encrypted image information, image information activity in encrypted into cover image, image information extraction and image information recovery. Projected technique may be a traditional BHSEA approach. n this process PSNR value is high in BHSEA compare to RIEDHA.

Keywords: Reversible data hiding, BHSEA, lossless data hiding, Image encryption, PSNR, MSE, data hiding capability, HS

I. INTRODUCTION

A reversible data hiding can recover the original image without any distortion from the marked image once the hidden information is extracted. The technique utilizes the zero or the minimum points of the bar graph of a picture. It modifies the constituent values to insert information into the image. It will insert more information than several of the present reversible information hiding techniques. it's established that the height signal/noise ratio (PSNR) of the marked image generated by the strategy. The PSNR is higher for all reversible information hiding techniques. Steganography is that the art of secret method of communication. During this reversible Steganography was used that is used to retain the first image even once the key message was embedded. This reversible information hiding will be used for medical, military, and legal applications, that don't permit any modification within the digital illustration of the quilt image because of the danger of misinterpretations. The property of changeability implies that the first type of the image, before the key bits were embedded, will be recovered utterly once the embedded bits area unit extracted [1]. Reversible information hiding will be used for medical, military, and legal applications, that don't permit any modification within the digital illustration of the quilt image because of the chance of misinterpretations. There are 2 main classes of reversible information hiding ways for pictures, i.e., ways supported distinction growth and ways supported bar graph shifting. during this work, the quilt image was divided into a series of no overlapping, neighboring constituent pairs, and also the distinction of every constituent try was doubled. Then, the doubled distinction was either kept reserved or changed in keeping with the parity of the embedding secret bit. On the receiver facet, the embedded secret information will be extracted simply from the Smallest Amount Important Bit (LSB) of the variations of the constituent pairs within the stego image. However the extra data of the placement map was required to resolve the underflow and overflow issues. Completely different from cryptography, the most goal of information of hiding is to hide the hidden data by the carrier media, in order that the hidden information is transferred while not drawing suspicions. The hiding algorithms area unit to keep up the natural look of the quilt media and to stay uninvolved folks from even thinking the data exists. To cover data within a picture, there are many accessible domains wherever steganography algorithms exploit like spatial domain or DCT domain. A copyright is protected through watermarking which is outlined as a method of

inserting data a picture [2]. A watermark is hidden information embedded into the first image. The watermark should be indiscernible. The watermarking has got to done by making invulnerability against varied sorts of attacks. Hit are carried out through each intentional and unintentional process per shaped on the image so as to delete the watermark or stop the identification of it. For past twenty years information hiding has emerged as interesting space of analysis. During this technique, secret information will be encoded into a canopy medium, and afterward facilitates the user to require out the embedded information from the stego medium for varied applications. Reversible information hiding that embeds essential information into pictures then on. Sender side, the information is embedded by the reversible remodel .The receiver side; the information is extracted by the converse transform [3].
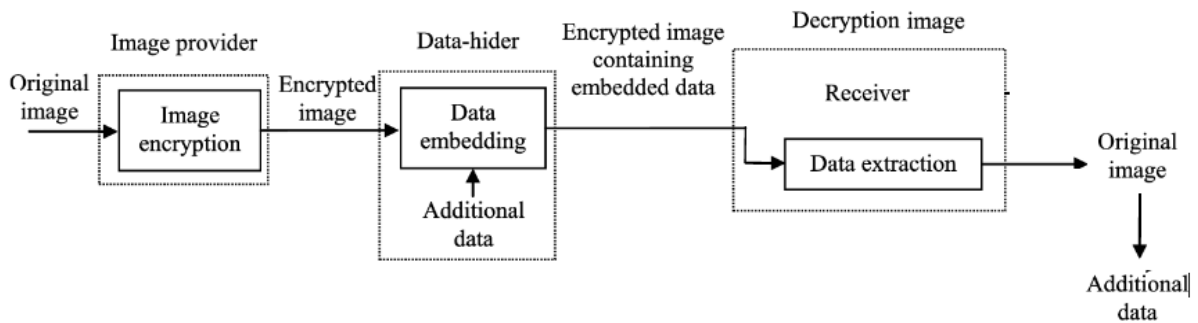

Fig 1: General Block Diagram of BHSEA

Types of information concealment techniques

1) Spatial domain technique: In spatial domain steganography bits within the pixels values are modified so as to cover the information. Spatial domain techniques will be classified into least vital Bit (LSB), picture element worth Differencing (PVD), Random constituent Embedding methodology, bar graph Shifting methodology, Texture based mostly methodology etc. LSB is that the wide used simplest methodology wherever there's less probability for degradation of original image [4].

2) transform domain technique: transform domain embeds data in transform area. During this domain, the image is transformed from spatial domain to frequency domain by exploitation any transforms and once a transformation method, the embedding methods are going to be tired correct transform coefficients. The method of embedding information within the frequency of a symbol is way stronger than embedding principles that operate within the time domain. Transform domain techniques embody DFT, DCT, DWT and that they are less exposed to compression, cropping etc [5].

Robust Reversible information hiding: process is obsessed to cover the information in a picture in many applications. Original image can't be recovered absolutely if the process isn't reversible. RDH want the essential property of hardiness to recover the hidden information fully from the processed image. Projected and evaluated a brand new severable RDHEI framework. Further information will be embedded into cipher image antecedently encrypted exploitation general traversal and a stream cipher. A Block bar graph shifting (BHS) approach exploitation self-hidden peak pixels is adopted to perform reversible information embedding. Looking on the keys command, legal receivers will extract solely the embedded information with the information hiding key or they will decode a picture terribly just like the initial image with the decoding key. They will extract each the embedded information and recover the initial image error-free if each keys area unit accessible. The results demonstrate of that higher information embedding capability, higher decrypted-marked-image quality, error-free information extraction and correct image reconstruction

II. LITERATURE SURVEY

In Xu et al. [6] Reversible information hiding is a vital topic of information hiding. This paper proposes a unique divisible and error-free reversible knowledge hiding in an encrypted image supported two-layer picture element errors. Specially, the projected scheme divides the initial image into a series of non-overlapped blocks and permutes these blocks. Then, a closed Hilbert curve is employed for scanning every block to get a one-dimensional picture element sequence. The pixels of the sequence are encrypted with key transmission. Throughout information hiding, every non-overlapped block of the encrypted image is scanned within the closed Hilbert order to come up with a one-dimensional encrypted picture element sequence. Finally, it exploits the bar graph of two-layer adjacent encrypted picture element errors to insert secret information by bar graph shifting and generate a marked encrypted image. Several experiments are distributed, and therefore the results demonstrate that the projected scheme reaches a high payload and outperforms some reversible information hiding schemes within the encrypted image.

In Qin et al.[7] A PDE-based image inpainting methodology victimization aeolotropic heat transfer model, which might at the same time propagate the structure and texture data. In structure inpainting, the propagating direction and intensity are associated with image contents, and the strength of propagation on gradient direction is created reciprocally proportional to the magnitude of gradient. In texture inpainting, the another texture term reflects cyclicity on the feel and its perpendicular direction. For numerical implementation, the step size of finite distinction is adaptively chosen in step with the curvature, resulting in fewer iteration steps and satisfactory in painting quality. Compared with alternative high order PDE ways and bedded ways, the projected approach is additional curt and doesn't want image decomposition. Image in painting, on the opposite hand, is to imitate human professionals in repairing photos mistreatment some mathematical models and pc algorithms to recreate the missing content within the image. The target is to supply visually satisfactory or acceptable results, instead of an honest estimate of the initial since there's merely no original. Inpainting of digital pictures has found applications in such areas as restoration of historical pictures, filling in or removing chosen areas in pictures, and wiping out visible watermarks.

In Rintu Jose et al.[8] The owner of the image 1st encrypts the image by permutation, creating use of AN encoding key. Since permutation only shuffles the pixels, the bar graph of the image remains a similar. The information hider, with none data regarding the first image content, hides information into the encrypted image by bar graph modification methodology. Before hiding the information, the information hider permutes image victimization information hiding key and once data hiding he performs inverse permutation. At the receiver facet, if the receiver has only information hiding key, he will extract the information, however cannot browse the content of the image. If he has solely encoding key, he will decipher the image to get a picture the same as the first one. If he has each keys, he could 1st extract the information victimization data hiding key and so decipher the image mistreatment encoding key. This decrypted image is strictly same because the original image.

In Zhao et al. [9] information hiding, additionally known as data hiding, plays a very important role in data security. It aims at embedding imperceptible hint in cover media like still pictures, videos, audios, 3D meshes, etc. It consists of many branches like steganography, watermarking, visual cryptography, etc. the information hiding scheme planned during this work are often classified into the class of steganography. Steganography is sometimes used for covert communications. so the high embedding capability is that the main concern during this quite technique. In distinction, watermarking is sometimes used for copyright protection and announcement. so researchers aim at up the strength of watermark content against intentional or unintentional attacks. Therefore, most offered information hiding strategies will give a better capability than that provided by watermarking schemes. This advantage broadens the appliance situations of information hiding. A reversible information hiding scheme supported bar graph modification. Its principle is to change the bar graph made supported the neighbor pixel variations rather than the host image's bar graph. Several peak points exist round the bin zero during this bar graph because of the similarity of adjacent picture element values. Besides, several zero points exist in either side of the bin zero. Here the height purpose refers to the peak of bar graph bin with the biggest applied math price (i.e., the count falling within the corresponding bin), and also the numerical quantity suggests that the bar graph bin with zero price. In our case, all the variations are classified into levels of [−255, 255] and every level corresponds to a bar graph bin. Hence it is reasonable to change the bar graph with a structure mechanism for hiding a lot of secret information. In decoder, the host image pixels are recovered one by one. That is, every pixel is recovered motor-assisted by its antecedently recovered neighbor. Meanwhile, the key information is extracted from the marked adjacent pixels' variations.

In Xinpeng Zhang et al.[10] used the Reversible information activity with optimum worth transfer. Within the secret information additionally because the valuable data used for content recovery. It carried by the variations between the first element values. The closest element values calculable from the neighbors. The estimation errors are changed in line with the optimum worth transfer rule. Another technique embeds image or text information invisibly into a video supported whole number wavelet transform. The mean sq. worth distinction between the first and watermarked image. it's additionally to extend Peak signal to noise quantitative relation. Divisible Reversible information activity in Encrypted Image may be used. A content owner encrypts the first uncompressed image exploitation AN encoding key. an information hider could compress the smallest amount vital bits of the encrypted image. It is using a information activity key to make a element distinction to accommodate some extra information.

In Shie et al.[11] a picture steganographic scheme enforced on block-truncation-coding (BTC) compressed image is planned. Within the planned theme, the primary stage hides secret information into the reconstructed XH and XL values of image block and therefore the second stage uses bar chart modification technique to cover the key information into the electronic image of block. Experimental results show that the planned scheme permits for activity massive amounts of secret information, and therefore the reconstituted image has sensible image quality. Moreover, the planned scheme may be a reversible image steganographic scheme. That's the first BT compressed image may be losslessly recovered from the stegoimage once extracting the key information.

In Chen et al. [12] This paper tries to supply a brand new perspective for the analysis of reversible watermarking supported bar chart shifting of prediction errors. rather than getting one prediction error for the present element, we calculate multiple prediction errors by coming up with a multi-prediction theme. AN uneven error bar chart is then made by choosing the appropriate one from these errors. Compared with traditional bilaterally symmetrical bar chart, the uneven error bar chart reduces the number of shifted pixels, therefore up the watermarked image quality. Moreover,

a complementary embedding strategy is planned by combining the utmost and minimum error histograms. Because the 2 error histograms shift within the opposite directions throughout the embedding, some watermarked pixels are restored to their original values; therefore the image quality is additional improved. Experimental findings additionally show that the planned technique re-creates watermarked pictures of upper quality that carry larger embedding capability compared to traditional symmetrical bar chart ways.

In Ni al. [13] This paper presents a unique reversible information hiding algorithmic program, which may recover the first image while not distortion from the marked image once the hidden information are extracted. This algorithmic program utilizes the zero or the minimum purpose of the bar graph and slightly modifies the picture element values to insert information. It will insert a lot of information as compared to most of the prevailing reversible information hiding algorithms. A theoretical proof and various experiments show that the PSNR of the marked image generated by this methodology is often higher than forty eight decibel that is way above different reversible information hiding algorithms. The algorithmic program has been applied to a good vary of various pictures with success. Some experimental results are given to demonstrate the validity of the algorithmic program.

In Mo et al.[14] Recently, reversible information hiding in encrypted image (RDHEI) has attracted intensive attention, which may be utilized in secure cloud computing and privacy protection effectively. During this paper, a unique RDHEI scheme supported block classification and permutation is planned. Content owner 1st divides original image into non-overlapping blocks then set a threshold to classify these blocks into swish and non-smooth blocks severally. Once block classification, content owner utilizes a particular secret writing methodology, together with stream cipher encoding and block permutation to guard image content securely. For the encrypted image, information hider embeds further secret data within the most important bits (MSB) of the encrypted pixels in swish blocks and therefore the final marked image may be obtained. At the receiver aspect, secret information are extracted properly with data-hiding key. Once receiver only has encoding key, once stream cipher decoding, block scrambling cryptography and MSB error prediction with threshold, decrypted image are achieved. once information concealing key and secret writing key are each obtained, receiver will notice the graceful and non-smooth blocks properly and MSB in smooth blocks are foretold properly, hence, receiver will recover marked image lossless. Experimental results demonstrate that our scheme can do higher rate-distortion performance than a number of progressive schemes

In Che-Wei Lee et al.[15]proposed a lossless information hiding methodology supported bar graph shifting, that employs a scheme of adaptation division of canopy pictures into blocks to yield giant information hiding capacities further as high stego-image qualities. The tactic is shown to interrupt a bottleneck of data-hiding-rate increasing at the image block size of eight × eight, that is found in existing histogram-shifting strategies. Four ways that of block divisions are designed, and therefore the one that provides the most important information hiding capability is chosen adaptively.

In Zhang et al. [16] used a unique methodology for divisible reversible information hiding .The content owner 1st encrypts the first uncompressed image victimization AN secret writing key. Then turn out AN encrypted image. the information hider compresses the LSB bits of the image employing a data concealing key. To make a distributed house to accommodate the extra information. At the receiver aspect the information embedded within the created house. It may be simply retrieved from the encrypted image. The information in line with the info concealing key for secret writing. The information embedding only affects the LSB. A decoding with the secret writing key may result in a picture. To the first version. Victimization each of the secret writing and knowledge hiding keys. The embedded further information may be with success extracted. The first image may be dead recovered by exploiting the special correlation in natural image. The information and therefore the image which will be recovered simply. The calculations are terribly simple.

III.   MATLAB TOOL

It is simulating on mat lab 2013a and for this work we use Intel 1.4 GHz processor Machine. Matlab setup may be a high-level language and technical calculate and interactive surroundings for algorithmic program development, information visualization, records analysis, and numeric computation Mat lab may be a software system program that permits you to try to information manipulation and visualization, calculations, mathematics and programming. It is wont to do terribly easy moreover as terribly subtle tasks. Image procedure function provides a comprehensive set of reference normal method end graphical tools for image process, analysis, visualization, and algorithmic program development. You'll be able to perform image improvement, image declaring, feature detection, noise decrease, image segmentation, abstraction transformations, and image registration. Several functions within the tool case are multithreaded to require good thing about multicore and digital computer computers. The Performance analysis of MATLAB version R2013a i.e. used for this thesis simulation results of image process provides processor optimized libraries for quick execution and image computation. It uses its JIT (just in time) compilation technology to produce execution speeds that rival ancient programming languages. It may also more advantage of multi core and digital computer computers, MATLAB give several multi rib algebra and numerical perform. These functions mechanically execute on multiple procedure thread during a single MATLAB session, enabling them to execute quicker on multicourse computers. During this thesis, all increased pictures results were performed in MATLAB R2013a to induce

AN increased results of compressed and decompressed image, and once colorization of decompressed image, image quality and numerical price once analysis. So as to check the planned technique, Simulation victimization MATLAB R2013a is performed on input pictures. Simulation tool is that the language and interactive environment utilized by many engineers and scientists worldwide.

IV. RESULT ANALYSIS

Reversible information hiding in encrypted image using histogram process in main objective image data or information secure and authentication.RDH method additionally improve PSNR and decrease MSE.

(a) Image1 result graph between RIEDHA and BHSEA: An image is a visual representation in form of digital signal or format jpg, the term has several usages case1 an image is a picture that has been created or copied and stored in electronic form. Digital image design as image data file or text image contains secrets information or data that relations to different images on a specified condition with standard images. The image parameters evaluation measure includes likes peak signal to noise ratio (PSNR) or robust. Standard size image used karen wetterha image and paytm image as data image. Paytm image as data image and KarenWetterhah as a cover image embedding then get encrypted images or watermarked image. BHSEA embedding capacity is good as compare to RIEDHA.Data image as a logo image types as an original image extract in paytm image into KarenWetterhah as a cover image. In this process PSNR value is high in BHSEA compare to RIEDHA.
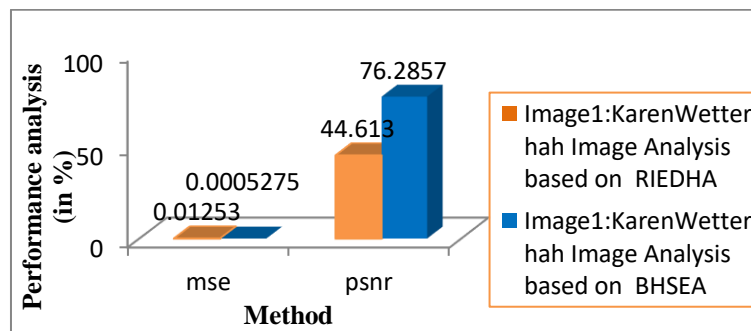

Fig.2 Robustness comparisons between RIEDHA and BHSEA based on Experimentation1

(b) Image2 result graph between RIEDHA and BHSEA: Toshiba-logo-slogan image as data image and IT_Park_Manipur Information Technology as a cover image embedding then get encrypted images or watermarked image. BHSEA embedding capacity is good as compare to RIEDHA.Data image as a logo image types as an original image extract in Toshiba-logo-slogan image into IT_Park_Manipur Information Technology as a cover image. In this process PSNR value is high in BHSEA compare to RIEDHA.
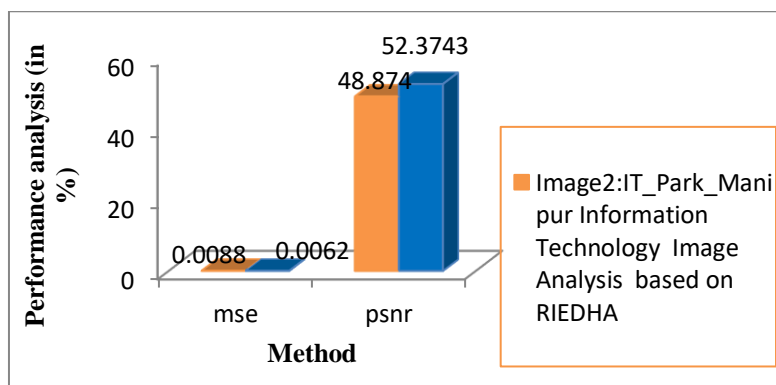

Fig3 Robustness comparisons between RIEDHA and BHSEA based on Experimentation 2

IV. CONCLUSION

Reversible data hiding in encrypted image is obtaining additional attention recently because of security maintaining requirements. Reversible data concealing in encrypted image is also a robust technique to enhance the protection of knowledge. Data concealing in encrypted pictures provides additional security for the data. Reversible data activity schemes for encrypted image with associate occasional computation complexity is analyzed, that consists of image

encryption, data concealing and data extraction/ image recovery phases each methodology has its own benefits and disadvantages. These models have little scope for economical security. It's quite essential to develop effective system for data embedding and data recovery in lossless manner whereas not scope for any distortion. In research of reversible data concealing (RDH) techniques. Among the special domain of RDH technique, the digital photos in JPEG domain, this rule contains the hierarchal methodology for the information embedding and additionally the key writing, among the projected methodology will to boot used for the military and medical field conjointly. The image is used to chart specification. The chart worth's compare thereto image element worth supported PSNR and MSE the data hider can insert secret data into the encrypted image victimization bar chart shifting of two-layer encrypted picture element errors whereas not knowing the primary image content. it is necessary to develop associate economical and effective system that has data embedding and recovery with none distortion and provides higher Security. In this method PSNR value is high in BHSEA compare to RIEDHA. Overall high PSNR in BHSEA compare to RIEDHA and additionally low MSE in BHSEA compare to RIEDHA.

REFERENCES

[1]. Zhicheng, Yun Q. Shi, Nirwan Ansari, Wei Su, Qibin Sun, and Xiao Lin. "Robust lossless image data hiding." In 2004 IEEE International Conference on Multimedia and Expo (ICME)(IEEE Cat. No. 04TH8763), vol. 3, pp. 2199-2202. IEEE, 2004.

[2]. Linb, Ching-Yu Yanga Chih-Hung, and Wu-Chih Hu. "Reversible data hiding for high-quality images based on integer wavelet transform." Journal of Information Hiding and Multimedia Signal Processing 3, no. 2 (2012).

[3]. Petitcolas, Fabien AP. "Watermarking schemes evaluation." IEEE signal processing magazine 17, no. 5 ,58-64, 2000.

[4]. Raja, K.B., C.R.Chowdary, K.R.Venugopal, & L.M. Patnaik. "A secure image steganography using LSB, DCT & compression techniques on raw images." In 2005 3rd international conference on intelligent sensing and information processing, pp. 170-176. IEEE, 2005.

[5]. Ali, Musrrat, Chang Wook Ahn, and Millie Pant. "A robust image watermarking technique using SVD and differential evolution in DCT domain." Optik-International Journal for Light and Electron Optics 125, no. 1: 428-434, 2014.

[6]. Xu, Dawen, Kai Chen, Rangding Wang, and Shubing Su. "Separable reversible data hiding in encrypted images based on two-dimensional histogram modification." Security and Communication Networks 2018 (2018).

[7]. Qin, Chuan, Shuozhong Wang, and Xinpeng Zhang. "Simultaneous inpainting for image structure and texture using anisotropic heat transfer model." Multimedia Tools and Applications 56, no. 3 (2012): 469-483.

[8]. Jose, Rintu, and Gincy Abraham. "A separable reversible data hiding in encrypted image with improved performance." In 2013 Annual International Conference on Emerging Research Areas and 2013 International Conference on Microelectronics, Communications and Renewable Energy, pp. 1-5. IEEE, 2013.

[9]. Zhao, Zhenfei, Hao Luo, Zhe-Ming Lu, and Jeng-Shyang Pan. "Reversible data hiding based on multilevel histogram modification and sequential recovery." AEU-International Journal of Electronics and Communications 65, no. 10 (2011): 814-826.

[10]. Xinpeng Zhang, "Reversible Data Hiding With Optimal Value Transfer" Ieee Transactions On Multimedia, Vol. 15, No. 2, Feb 2013.

[11]. Shie, Shih-Chieh. "A Steganographic Scheme Implemented on BTCCompressed Image by Histogram Modification." In Proceedings of the International Conference on Information and Knowledge Engineering (IKE), pp. 135-136. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2017.

[12]. Chen, Xianyi, Xingming Sun, Huiyu Sun, Zhili Zhou, and Jianjun Zhang. "Reversible watermarking method based on asymmetric-histogram shifting of prediction errors." Journal of Systems and Software 86, no. 10 (2013): 2620-2626.

[13]. Ni, Zhicheng, Yun-Qing Shi, Nirwan Ansari, and Wei Su. "Reversible data hiding." In Proceedings of the 2003 International Symposium on Circuits and Systems, 2003. ISCAS'03., vol. 2, pp. II-II. IEEE, 2003.

[14]. Mo, Qun, Heng Yao, Fang Cao, Zheng Chang, and Chuan Qin. "Reversible Data Hiding in Encrypted Image Based on Block Classification Permutation." Cmc-Computers Materials & Continua 59, no. 1 (2019): 119-133.

[15]. Che-Wei Lee and Wen-Hsiang Tsai "A Lossless Data Hiding Method by Histogram Shifting Based on an Adaptive Block Division Scheme" River Publishers, 2010.

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

[17]. Jafar, Iyad F., Khalid A. Darabkh, Raed T. Al-Zubi, and Ramzi R. Saifan. "An efficient reversible data hiding algorithm using two steganographic images." Signal Processing 128: 98-109, 2016.

[18]. Sumathi, C. P., T. Santanam, and G. Umamaheswari. "A study of various steganographic techniques used for information hiding." arXiv preprint arXiv: 1401.5561, 2014.

[19]. Pinkas, Benny. "Cryptographic techniques for privacy-preserving data mining." ACM Sigkdd Explorations Newsletter 4, no.2: 12-19, 2002.

[20]. Sullivan, Kenneth, Upamanyu Madhow, Shivkumar Chandrasekaran, and B. S. Manjunath. "Steganalysis for Markov cover data with applications to images." IEEE Transactions on Information Forensics and Security 1, no. 2 : 275-287, 2006.

[21]. Chandramouli, Rajarathnam, and Nasir Memon. "Analysis of LSB based image steganography techniques." In Proceedings 2001 International Conference on Image Processing (Cat. No. 01CH37205), vol. 3, pp. 1019-1022. IEEE, 2001.

[22]. Bierbrauer, Jürgen, and Jessica Fridrich. "Constructing good covering codes for applications in steganography." In Transactions on data hiding and multimedia security III, pp. 1-22. Springer, Berlin, Heidelberg, 2008.

[23]. Chao, Hui-Mei, Chin-Ming Hsu, and Shaou-Gang Miaou. "A data-hiding technique with authentication, integration, and confidentiality for electronic patient records." IEEE Transactions on Information Technology in Biomedicine 6, no. 1 : 46-53, 2002.

[24]. Gutub, Adnan, and Manal Fattani. "A novel Arabic text steganography method using letter points and extensions.": 28-31, 2007.

[25]. Cheddad, Abbas, Joan Condell, Kevin Curran, and Paul Mc Kevitt. "Digital image steganography: Survey and analysis of current methods." Signal processing 90, no. 3 : 727-752, 2010.

[26]. Rhoads, Geoffrey B. "Video steganography." U.S. Patent 6,026,193, issued February 15, 2000.

[27]. Gopalan, Kaliappan. "Audio steganography using bit modification." In 2003 International Conference on Multimedia and Expo. ICME'03. Proceedings (Cat. No. 03TH8698), vol. 1, pp. I-629. IEEE, 2003.

[28]. Cox, Ingemar J., Joe Kilian, F. Thomson Leighton, and Talal Shamoon. "Secure spread spectrum watermarking for multimedia." IEEE transactions on image processing 6, no. 12: 1673-1687, 1997.