Reversible data hiding using Histogram Shifting Method: A Critical Review

Sarika Tomar[1], Punit Kumar Johari[2]

[1,2]*Department of CSE/IT, MITS Gwalior, MP, India*

Abstract: - *This paper is a critical review of the research work done in the recent past. The focus is on the reversible data-hiding scheme based on the histogram-shifting- imitated approach. Instead of utilizing the peak point of an image histogram, the scheme manipulates the peak points of segments based on image intensity. The secret data can be embedded into the cover image by changing the peak point pixel value into other pixel value in the same segment.*

The method uses a location map to guarantee the correct extraction of the secret data. Since the modification of the pixel value is limited within each segment, the quality of the stego image is only related to the size of the segmentation, which means after embedding data into the cover image, it can be reused to do the multi-layer data embedding while maintaining the high quality of the final stego- image.

Key words: reversible data hiding, histogram shifting, embedding, stego-image

INTRODUCTION:

The objective of transmitting secret data is to embed the secret message into some envelop. The main reason of hiding the data is copyright protection, annotation and defence applications. The controlling factors which affect the quantity of data hiding are the purpose of recovered image. In medical applications the quality of recovered image should be good. The three categories of data hiding are cryptography, steganography and watermarking.

The cryptography adversely affects the data. The digital methods which are currently being developed are more accurate, efficient and have a reliable quality. The negative part is the possibility of tampering the data and infringement of copy rights.

The chief motivation of the modern research in this field is Intellectual property protection, content manipulation indication, and annotation. Digital data hiding has groups like embedding copyright information in different digital media formats such as text, audio, image, or video with the least possible perceivable degradation effects on the host signals. For example, effects must be inaudible or invisible to its observers. Amount of payload and changes in the secret data before embedding uses many methods.

The techniques have evolved to solve the different problems. The requirements of payload and the quality of the recovered image. Main usages of digital media data hiding techniques are preserving copyright and assuring content integrity.

In order to achieve the purpose of embedding data the payload should be kept hidden. The quality of the original data is deteriorated due to digital processing like data compression, cropping, filtering or resampling. These are some of the challenges of the steganography.

Perceptual or statistical holes to be filled with data in host signals are likely to be removed by means of lossy signal compression. Important factor to achieve successful data hiding technique is to find holes which are not convenient to be exploited by compression algorithms. The main challenge is filling data in this kind of holes in a way that is not easy for compression algorithms to exploit it.

An enhanced challenge is filling the holes in a manner that remains invariant against signal transformation in big scale.

Following counted features and restrictions are the criteria which a data embedding algorithm must meet the following conditions:

• Quality of host signal should not be degraded objectionably and the perceptibility of embedded data must be kept minimal.

• The data must be embedded into whole body of the target media rather than wrapper or header. Therefore it would be kept intact in different formats.

• The data must be secure against intentional and intelligent removal attempts such as filtering, encoding, cropping, channel noise, lossy compressing, resampling, scanning and printing, digital to analog (D/A) conversion, analog to digital (A/D) conversion, and etc.

• Since data hiding goal is to keep the embedded data into host signal, embedded data asymmetrical encoding is desirable feature but not essential.

• To guaranty data integrity error correction coding is necessary. Degradation of embedded data at signal modification time is unavoidable.

• Arbitrary re-entrant and self-clocking are mandatory properties of the embedded data. These properties are to guaranty that embedded data will be retrievable even if only some fragments of the host be available. Today there are various applications of information hiding. Knowledge of data hiding might be used either in ethical or unethical ways. However, data hiding algorithms cannot easily be categorized either in steganography or watermarking categories as there is no transparent boundary between these two terms and mostly the classification relies on application of the algorithm. Therefore regardless classifying data hiding the most common data hiding applications are fingerprinting, secret communication, secure storage, covert communication, and copyright protection.

LITERATURE REVIEW

In this research paper, we go through recent researchers which hold the data related to histogram shifting technique and reversible data hiding[1,2,3,4,5,6,7,8,9], Modification of Prediction Error (MPE) and reversible data hiding[10,11,12], Histogram shifting technique and pixel value difference (PVD) [13,14,15],Histogram shifting technique and LSB matching [16,17,18,19], multiple scanning techniques and histogram technique[20], Difference Expansion algorithm, bilinear interpolation and Histogram shifting[21],Histogram shifting technique and non-recursive and recursive[22].

Histogram shifting technique and reversible data hiding.

[1] In this design, we have presented an efficient extension of the histogram modification technique by considering the differences between adjacent pixels rather than simple pixel value. One common drawback of virtually all histogram modification techniques is that they must provide a side communication channel for pairs of peak and minimum points. To solve binary tree is introduced that predetermines the multiple peak points used to embed messages thus, the only information the sender and recipient must share is the tree level L. In addition, since neighbour pixels are often highly correlated and have spatial redundancy, the differences have a Laplacian like distribution. This proposed method enables to achieve large hiding capacity while keeping embedding distortion low. Also the findings have been that hiding capacity increases many folds if color image is considered for carrying the message.

[2] Wien Hong et.al have developed a method which is an improvement over the histogram shifting method which is better known as Reversible data hiding method. The method is based on shifting pixel values between peak and zero points and thus space is created to hide secret bits. This method introduces distortions, which are uncontrolled. The proposed method yields better image quality. If the payload is small then smaller pixel shifting is required. The stego image quality is found to be better and reduces the computational time and cost. This has no negative impact on the embedding capacity.

[3] Li-chin Huang et.al have designed a method which can be applied very profitably in high quality medical imaging. The proposed method has higher resolution as it uses 16-bit depth. The classical data hiding algorithm are based on 8 bit depth. This is reversible data hiding technique which uses difference bit embedding method in high bit depth of three dimensional medical images. The medical images produced, the authors have explicitly used 6 different conditions for medical images, format of image which is characterized by sign and unsign 16 bit depth high quality medical image. The proposed method is based on blocks and shift histograms. This method distributes the secret bit to entire 3D medical images

and there is no need of salt-and-pepper. The common problem of underflow and overflow are solved by the use of histogram shifting utilization rate. Free location map criterion is used on only shift distance is recorded. The algorithm is applied to the slice of 3D medical objects. The smooth surfaces are kept as original by putting the entire slice together. Inter-slice PSNR is used to measure the distance between neighbouring pixels and adjust block size, threshold and member of embedding bits. This improves the surface appearance.

[4] The design is based on active steganalysis scheme for histogram-shifting based reversible data hiding methods. This is unique method. To accomplish this, we investigated histogram features that originate in the embedding procedure, and modelled them into four template categories by using a 1×4 sliding window. Discrimination between cover images and stego-images was performed by the combinational similarity measures and the trained SVM classifier. The hidden messages located at the histogram peak were further estimated by measuring the feature of adjacent histogram difference. Experimental results show that the proposed algorithm is highly effective on stego-images detection and embedding locations estimation at low bit rates.

[5] Wei-Jen Wang et.al have developed a data hiding methodology which results in high amount of data embedding. The scheme is based on neighbour mean interpolation. This improves the image quality without compromising with the data embedding capacity. The second step is to use histogram Shifting Methodology. This further improves the data hiding capacity. The secret data is hidden in two levels. The proposed schema is compared with Jung-Yoo scheme of the year 2009, PSNR values are used to compare the quality of stego images at two difference levels. The quality is improved in shifting the histogram due to the difference table. The better result are observed after the embedding stage as most of the pixel values of the middle stego-image are found between input and cover images. When the histogram is shifted both ways it results into those pixel values which are very to the original input image.

[6] Authors have developed a reversible data hiding method by using histogram-shifting limited approach. The peak point pixel value is changed into another pixel value in same segment then the secret information is embedded. This allows the multilevel data embedding. The stego image displays a very high quality. The proposed methods has low time complexity and provide ultimate security, the works well on the simple. The scheme is lossless in relation with the image is easy to decipher the embedded message and get back to the actual original appearance.

[7] Reversible data hiding recovers the original image from the stego-image without distortion after data extraction. In this paper, the authors have proposed a novel reversible data hiding method based on adaptive prediction techniques and histogram shifting. Because most natural images always contain edges, it is not suitable to predict these pixels using existing prediction methods. For more precise forecast, two prediction methods are adaptively used to calculate prediction error according to the characteristic of a pixel. As a result, two prediction error histograms are built. One is for pixels located at edges, and the other is for the rest pixels. Data are embedded in the image by using histogram-shifting method. In addition, a new sorting method is applied to histogram shifting, which considers the differences of all pixel pairs in the neighbourhood and better reflects the correlation among pixels. Through the sorting method, the prediction errors with small absolute values are arranged in the front and more embeddable pixels are preferentially processed. Therefore, the number of shifting pixels is decreased if the peaks in the histograms are all dealt with or the capacity is satisfied, which is beneficial to distortion reduction. Experimental results show that the proposed method acquires greater capacity and higher quality.

[8] In this paper, an efficient GA based multiple embedding scheme is proposed for HS-based RDH. By developing the rate and distortion model in terms of multiple pairs of peak and zero bins, the HS-based multiple embedding is formulated as the problem of rate and distortion optimization. GA is used to solve the optimization problem, which could not only adaptively determine the proper pair number of the peak and zero bins but also their corresponding nearly optimal values for HS- based multiple embedding. Two main propositions in distortion computation are also obtained to help the development of fast algorithm for distortion evaluation and the massive reduction of the solution space, which are preferable for practical application of GA. By partitioning the image into interleaved cross and round sets, the precise rhombus prediction and sorting are incorporated in the process of HS multiple embedding. The simulation demonstrates the superior rate and distortion performance of the proposed scheme. In this paper, based on the developed rate and distortion model, the problem of HS-based multiple embedding is formulated as the one of rate and distortion optimization. Two key propositions are then derived to facilitate the fast computation of distortion due to multiple shifting and narrow down the solution space respectively.

[9] The authors have presented an efficient data hiding method using histogram shifting is presented. The embedding is done using histogram shifting. This can embed high payloads. For image is over-enhanced which introduces annoying contrast, it can be controlled by controlled contrast enhancement. The cover images as well as the embedded bits are exactly recovered from the embedded image with better visual quality. Experimental results in terms of PSNR, SSIM and Embedding rate is significantly demonstrating the better performance of the proposed method. Proposed method can accurately recover the original image and extract the hidden data precisely. The highest two peak values of the host image's histogram are selected for data hiding. This embedding process is iterated, to attain larger embedding capacity. In addition, a Controlled Contrast Enhancement (CCE) is performed to get good visual perception. To verify the robustness of the proposed method various attacks on the host image such as impulse noise, shearing, rotation, and scaling are considered. The proposed algorithm efficiently removes the various attacks on the watermarked image and efficiently recovers the original and embedded data.

Modification of Prediction Error (MPE) and reversible data hiding:

[10] In this paper, a new reversible data hiding algorithm based on the efficient modification of prediction errors (MPE) algorithm. However, it integrates the two predictors are joined and uses only and one bin from the prediction errors histogram for embedding the data. The performance evaluation of the proposed algorithm showed its ability to increase the embedding capacity with competitive image quality. Additionally, no overhead information is added to cope with the increase in the number of predictors. Reversible data hiding (RDH) is a special class of steganography that can not only embed secret data into images, but also can restore the original images after secret data are extracted. Prediction-based techniques constitute an important class of reversible data hiding methods. However, most prediction-based RDH rely on the use of a single predictor to compute predictions that are used for data embedding. This may restrict the embedding capacity and image quality. In this paper the efficiency of prediction based reversible data hiding algorithms are used by proposing an algorithm that employs multiple predictors to take advantage of their varying characteristics and prediction accuracy in order to increase the embedding capacity. The proposed algorithm is based on the efficient modification of prediction errors (MPE) algorithm.

[11] This paper shows the improved method for the security of the multimedia files. It is based on Modified Prediction and chaotic encryption. Since prediction is enhanced, this hiding scheme yields more prediction errors concentrating around zero. Thus increases embedding capacity of the cover image. By validating this work with existing method, it is clear that this method yields a better performance. PSNR is maintained at higher level in the range of 40dB. In addition to this the secret data is also encrypted using chaotic method. The key used for encryption is based on both secret data and chaotic sequence which in turn provides high security. Modified prediction Reversible data hiding and Chaotic Encryption Method are combined to give more security for Multimedia Images. This method can be implemented for video files. The technique of reversible data hiding is capable of recovering the data embedded and the original image from a stego image without distortion. This is important for applications such as satellite and medical images, reversible data hiding is the valuable solution to render copyright or authentication. Reversible data hiding scheme is done based on Modification of Prediction Error (MPE). In this proposed MPE method, the histogram of prediction errors modified to prepare vacant positions for data embedding based on the secret data length. So data hiding capacity of an image is increased. The PSNR and embedding capacity of the stego image produced by MPE is more when compared to other techniques. To increase security, the secret data is encrypted using chaotic encryption algorithm. The encrypted secret message is then embedded into the image. It is very difficult to decrypt the data even though it is hacked.

[12] In this paper a method for embedding reversible dual-image data on pixel differences using histogram modification shifting and a cross magic matrix is proposed. It combines the best aspects of Chang et.al's and Lee et.al's methods. Our results prove that a good PSNR and high capacity though the capacity is the same as that achieved by Lee et al's method. Data hiding has been used to send sensitive information that is hidden in another signal/object, such as in audio or image data. The cover and marked signals are indistinguishable, so that they remain imperceptible to the human senses. Chang et al. proposed a dual-image data hiding method, which uses a magic matrix to embed secret data. Even though the peak signal-to-noise ratio (PSNR) of the image quality is 45 dB, the embedding capacity can only reach 1 bit per pixel. This study proposes a two-phase scheme for dual-image hiding with reversibility. Phase 1 embeds data on pixel differences, using a histogram-modification- shifting method and phase 2 uses a cross magic matrix to conceal secret digits on the plane with differences in its four quadrants. The proposed method can not only significantly improve the image quality measured by the PSNR but also can preserve the embedding capacity at a high level.

Histogram shifting technique and pixel value difference (PVD*):*

[13] Wang et al. have designed a histogram shifting imitation based reversible data hiding scheme in 203. They used the peak points of image intensity-based segments, instead of utilizing the peak point of a histogram. Their scheme has the limitation of the embedding capacity due to the embedding method. In this paper, we propose an improved data hiding scheme using median edge detection (MED) and hexadecimal exploiting modification direction (EMD). In embedding procedure, a predicted image is generated by using MED. The secret data is embedded into the peak points in segments by using hexadecimal EMD. In experimental results, the embedding capacity of the proposed scheme is superior to that of Wang et al. We have proposed a reversible data hiding scheme based on MED and the hexadecimal EMD to improve Wang et.al's scheme. The MED has been used to generate the predicted image. The hexadecimal EMD has been used to embed the secret data. On the basis of the experimental results it is shown that the embedding capacity is better than Wang et.al's scheme. Our scheme shown that the PSNR was ***B***47.52dB and embedding capacity was 176,757 bits on average. Compared to the proposed scheme and Wang et.al's schemes, the hiding capacity was increased, but the PNSR was reduced. However, the PSNR was sustained close to 47dB. The distortion of the image cannot be perceived by the human eye.

[14] Jeong-chun Joo et.al have developed a steganographic algorithm which is based on turnover method and adjustment technique. The present work is betterment over Pixel Value Difference (PVD) and modulus function as proposed by Wang et.al. It is found that numbers of artefact are introduced like increment and variation in the PVD histograms and this might reveal the hidden message. The authors have proposed a turnover policy to enhance the security. This method overcomes the shortcomings of PVD method. The RS stegnalysis, LSB matching and histogram based attacks are used to compare and check the proposed algorithm against the existing end.

[15] Author have designed a pixel value difference (PVD) method to hide the unequal amounts of secret information. This has been achieved by using pixel complexity secret data hiding methodology. The intruder can access the data by following the sequence. This method is the target for hackers. The difference histogram analyses employed in this method are vulnerable to the cyber-crimes. In this research the information of interest is embedded in 2*2embedding cell which are generated randomly. This method shows the improvement over IMF-PVD method. The difference histogram and chi-square test cannot detect the information easily.

Histogram shifting technique and LSB matching*:*

[16] In this paper, the ALE based steganalyzer has been designed in [12, 13], and gave an improved steganalytic method for detecting LSB matching steganography in gray-scale image. By considering the sum and difference image, summing the amplitude of each point of histogram (1-D, 2-D) and employing the calibration technique the novel steganalyzer thus obtained outperforms the old ones. Extensive experimental results have shown that LSB matching can be detected substantially with an embedding rate of 0.1 for compressed images and 0.5 for uncompressed images. The previous work can hardly reach such detection performance. Though LSB matching for compressed cover can be easily detected even for a low embedding Rate, the detection for uncompressed cover is still a challenge for steganalysts. For instance, the current steganalyzers cannot give an acceptable detection performance of LSB matching for the uncompressed USDA NRCS Photo Gallery even when the embedding rate is 1. Moreover, the proposed steganalyzer can be evidently applied to the additive noise based steganography, and then the further experimental results are expected to verify its universality.

[17] This paper proposes a novel steganalysis method for this issue by making use of the following two facts. One is the local maxima of an image histogram decrease and the local minima increase after LSB matching steganography. As a result, the area between upper envelope and lower envelope of the histogram of a stego image will be smaller than that of a cover image. The other is LSB matching embedding in the spatial domain of an image corresponds to low-pass filtering of the histogram. So, there are some differences in the high order statistical moments of high frequencies of the histogram. Based on these facts, this paper constructs a novel feature vector to distinguish between stego and cover images. The detection of LSB matching steganography remains unresolved, especially for the uncompressed grayscale images with high level of noise, such as scans of photographs. In this paper, we present a novel steganalysis scheme for this issue. By analyzing the embedding algorithm of LSB matching steganography, we prove the fact that the local maximum of histogram of a cover image decrease and local minimum increase after message bits are embedded. Moreover, due to the fact that the histogram of the stego image has less power in high frequencies than that of the histogram of the cover image, there are some differences in the high order statistical moments of high frequencies. Based on these facts, we construct a new feature vector and use

the FLD to distinguish between the cover and stego the experimental results show the proposed scheme is superior to the HCF and WAM methods in the dataset of scans of photographs.

[18] The authors have proposed a new a novel for detection of LSB matching steganography and evaluated its performance on two never compressed image databases. Extensive experimental results demonstrated the proposed steganalyzer performs a lot better even for RAW uncompressed images with low embedding rates. The main advantages of our steganalyzer are as follows. Difference operation enhances stego-noise so as to get better the discriminating ability between cover and stego images. The LVH-COMs take full advantage of image regions with different complexity, especially of the flat/smooth regions where the detection is easier. Calibration technique is introduced to weaken the influence of image content.

[19] The authors have smartly employed Histogram Base Steganalysis to detect the shortcomings in stego histogram. Two methods are evolved to save the cover image. One method is LSB and the other one is outguessing. The addition bit addition helps to maintain the originality of the cover picture. The LSB method shows the better results by isolating the sensitive pixels and shielding these pixels from the attack of extra bits. This result is minimum deviation in the co-occurrence matrices. The LSB++ method is further extended produces lesser traces. The histogram methods used by the hackers fail to detect the images containing secret information.

Multiple scanning techniques and histogram technique*:*

[20] The paper uses the improvised histogram data hiding by the use of multi-scanning methods. The embedding amount and scanning strategy is based payload and embedding sequence. The multiple scanning histogram modification has two phases. First the payload is encrypted to generate the stego image and then the cover image is decrypted to recover the payload and actual image the scanning methods can be horizontal, diagonal or vertical. The way the image is scanned can result in difference histogram payload of 1.12 bpp, 30db PSNR and maximum payload capacity achieved is 1.92 and shows the improvement of 120%.

Difference Expansion algorithm, bilinear interpolation and Histogram shifting:

[21] In this work the authors have used Difference Expansion (DE) algorithm, bilinear interpolation and histogram shifting to hide the secret message. The proposed method does not require to search for the peak points, nor does extra data need to be compressed. Therefore, the implementation costs are lower than Hong and Chen methods. The proposed method, the pixel (except for the reference pixel) in a smooth or complex region can embed secret data. After some secret data are embedded, the remaining secret data are embedded into the reference pixel. Finally, the proposed method can embed a large amount of payload.

[22] The new method is developed tested for the medical images. The classical histogram shifting model is modified for reversible medical image watering marking. The strategy is to break the cover image into several blocks using the histogram shifting method. This is downward division called as hierarchical division. The recursion yields the optimum data hiding capacity and security on the basis of block division scheme and histogram shifting algorithm it becomes easy to hide the medical images one can go for image segmentation to identity the ROI(Region of interest) before the block division. This not only increases the data hiding capacity but also improves the image quality

TABLE COMPARISON

S.No	Author	Year	Method Used	Embedding capacity/rate	PSNR	Objective
1	V.R.VijayKumar and V. Suresh Babu	2017	Histogram shifting technique and reversible data hiding	0.8	34	To achieve the embedded image with better visual quality. And better performance
2	Junxiang Wang, et.al	2016	Multiple Histogram Shifting and reversible data hiding	Not calculated	64	To provide high quality of stego-image and embedding capacity
3	P. Tamilselvi And M.Manikandan	2015	Modification of Prediction Error (MPE), reversible data hiding and Chaotic Encryption Method	76	47	This paper is to improve the security for multimedia files and to increase the volume of hidden data in an image
4	Enas N. Jaara and Iyad F. Jafar	2015	Modification of Prediction Error (MPE).and reversible data hiding	105	50	To increase the embedding capacity
5	Pyung-Han Kim et.al	2015	Media edge detection, hexadecimal exploiting modification direction and RDH	176	47	embedding capacity is better
6	Chin-Feng Lee*	2015	histogram-modification- shifting and Cross Magic Matrix	68	48	To achieve high embedding capacity and better stego image
7	Rui Liu et.al	2014	adaptive prediction techniques , histogram shifting and RDH	82	64	To provide greater capacity and higher quality
8	Jeanne Chen	2014	Histogram shifting technique and pixel value difference(PVD)	Not calculated	0.87	To provide good image quality and reduce the falling –off-boundary problem
9	Kazem Qazanfari et.al	2014	Histogram shifting technique	0.8	64	To optimize the LSB ++ technique and

			,LSB and LSB++			verification of robustness by using Chi-square attack
10	John Marin and Frank Y. Shih	2014	Multiple scanning techniques and histogram technique	1.92 bpp	30dB	To use multi scanning in improve histogram method RDH
11	Zhi-Hui Wang et.al	2013	Histogram shifting technique and reversible data hiding	6.5	54 db	To achieve high embedding capacity and low time complexity
12	Tzu-Chuen Lu et.al	2013	Difference Expansion algorithm ,bilinear interpolation and Histogram shifting	0.18	48	To provide high embedding capacity and improve the stego image quality
13	Wei-Jen Wang	2013	Histogram shifting technique and data hiding methodology	30(1.17bpp payload)	35.11	To achieve good image quality and high embedding capacity
14	C. Vinoth Kumar et.al	2013	Histogram shifting technique and non-recursive and recursive	Not calculated	59.05 non recursive	To provide high data hiding capacity and stego image quality good
15	Der-Chyuan Lou et.al	2012	Histogram shifting technique and RDH	0.03bpps	Not calculated	Embedding in template form to evaluate SVM clasifier
16	Li-Chin Huangc	2013	Histogram shifting technique and reversible data hiding	39.70	35.40	To find out novel reversible image data hiding by applying difference bit strategies in high bit-depth value structure on medical image
17	Jeong-Chun Joo et.al	2010	Histogram shifting technique and pixel value difference(PVD)	0.24	43.5	To provide high capacity and good image quality
18	Wien Hong et.al	2010	Histogram shifting technique and RDH	Not calculated	48.13db	To provide high embedding capacity and improve the stego image quality
19	Ergong Zheng et.al	2010	Histogram shifting technique and LSB matching	0.25	Not calculated	Detection of LSB matching using uncompressed image data base
20	S. L.V. Krishna et.al	2010	Histogram shifting technique and RDH technique	50	2.8	to achieve large hiding capacity
21	Jun Zhang et.al	2009	Histogram shifting technique and LSB matching	0.5bpp	Not calculated	To provide highly sensitive dataset from
						different sources
22	Yunkai Gao.etal	2009	Histogram shifting technique and LSB matching	0.5bpp	Not calculated	Authors have investigated the ALE based steganalyzers on the basis of the sum of difference image

The above table is the brief summary of the contribution made by the authors in reversible data hiding employing histogram shifting and other methods to optimize the embedding capacity, security and the recovery of the original image. This paper briefly describes the concept of reversible watermarking or data hiding for increasing the embedding capacity in medical images. It describes the need for increasing the embedding capacity, the care that needs to be taken followed by the utilization of a difference expansion based concept. This concept is used along with histogram shifting in a hybrid combination with the frequency domain transform to address all the three-optimization criteria namely, the robustness, the imperceptibility and the embedding capacity. Based on the study of the shortcomings of the reversible data hiding method.

CONCLUSION

In this paper, we have studied various techniques of data hiding in Image processing. The central idea of the research is reversible data hiding using histogram shifting. As discussed earlier, in image encryption due to random nature of resultant image there are chances of leakage of confidential data. This limitation is removed by using these data hiding techniques. The properties of digital image, which are high redundancy and strong spatial correlation, plays important role for implementation of these data hiding techniques. It can be concluded that the direct Histogram Shifting on pixels may be more powerful and of smaller difficulty than trying it on prediction- errors. The receiver will restore the same source image so that the watermark embedded and extractor remains in harmony. This process used to select the most locally proper watermarking modulation provides robustness the image is well protected. Better pixel prediction. Histogram shifting for embedding secret data provides security and authentication more payloads can be embedded with less distortion.

REFERENCES

[1] S. L.V. Krishna et.al "Lossless Embedding using Pixel Differences and Histogram Shifting Technique" Published by IEEE Conference, doi:10.1109/RSTSCC.2010.5712850,14 Feb 2010.

[2] Wien Hong et.al "A Modified Histogram shifting Based Reversible data Hiding Scheme for High quality Image" Published by Information Technology Journal,doi:10.3923/itj.2010.179.183, 2010.

[3] Li-Chin Huangc et.al "A reversible data hiding method by histogram shifting in high quality medical images" Published by Elsevier,doi.org/10.1016/j.jss.2012.11.024,3 march 2013.

[4] Der-Chyuan Lou "Active steganalysis for histogram-shifting based reversible data hiding" Published by Elsevier, doi.org / 10.1016 /j. optm. 2012.01.021, 15 May 2012.

[5] Wei-Jen Wang et.al "Steganography of Data Embedding in Multimedia Images Using Interpolation and Histogram Shifting" Published by International Conference,doi:10.1109/llH- MSP.2013.103,16-18 Oct 2013.

[6] Zhi-Hui Wanga et.al "Histogram-shifting- imitated reversible data hiding" Published by Elsevier,doi.org/10.1016/j.jss.2012.08.029,2 Feb 2013.

[7] Rui Liu et.al "A reversible data hiding based on adaptive prediction technique histogram shifting" Published by Institute of Information Science Beijing Jiaotong University, doi: 10. 1109 / APSIPA .2014.7041698, 16 Feb 2015.

[8] Junxiang Wang et.al "Rate and Distortion Optimization for Reversible Data Hiding Using Multiple Histogram Shifting" Published by IEEE transactions on cybernetics, doi: 10.1109 /TCYB. 2015.2514110,27 Jan 2016.

[9] V.R. Vijay Kumar and V. Suresh Babu "Histogram Shifting Based Reversible Data Hiding with Controlled Contrast Enhancement" Published by International Conference, doi:10.1109 /ICBSII.2017.8082277,26 October 2017.

[10] Enas N. Jaara and Iyad F. Jafar "Reversible Data Hiding Based on Histogram Shifting of Prediction Errors Using Two Predictors" Published by IEEE Jordan Conference, doi:10.1109/AEECT.2015.7360540,21 Dec 2015.

[11] P.Tamilselvi and M.Manikandan "Prediction Error and Histogram Shifting Based Reversible Data Hiding" Published by International Conference, doi:10.1109/ICSCN.7219918, 27 August 2015.

[12] Chin-Feng Lee et.al "Reversible Dual-image Data Embedding on Pixel Differences Using Histogram Modification Shifting and Cross Magic Matrix" Published by International Conference, doi:10.1109/IIH-MSP.2015.109,25 Feb 2016.

[13] Pyung-Han Kim et.al "Improved Histogram- Shifting-Imitated Reversible Data Hiding Scheme" Published by International Conference on Information Technology, doi:10.1109/ITNG. 2015.112,01 June 2015.

[14] Jeong-Chun Joo et.al "Improved Steganographic Method Preserving Pixel-Valuen Differencing Histogram with Modulus Function" Publishing by Corporation EURASIP Journal on Advances in Signal Processing, doi. Org/ 10.1155 /2010/24982, 29 April 2010.

[15] Jeanne Chen et.al "A PVD-based data hiding method with histogram preserving using pixel pair matching", Published by Elsevier, doi.org /10.1016/j.image.2014.01.003, March 2014.

[16] Yunkai Gao et.al "Detecting lsb matching by characterizing the amplitude of histogram" Published by Institute of Computer Science and Technology,doi:10.1109/ICASSP.2009.4959881,26 May 2009.

[17] Jun Zhang et.al "Detection of LSB Matching Steganography using the Envelope of Histogram" Published by journal of computers, doi: 10.4304/jcp.4.7.646-653, July 2009.

[18] Ergong Zheng et.al "Steganalysis of lsb matching based on local variance histogram" Published by International conference, doi:10.1109/ICIP.240.5652894,03 Dec 2010.

[19] Kazem Qazanfari and Reza Safabakhsh" A new steganography method which preserves histogram: Generalization of LSB++" Published by Elsevier, doi.org/10.1016/j.ins.2014.02.007,1 sept 2014.

[20] John Marin and Frank Y. Shih "Reversible Data Hiding Techniques Using Multiple Scanning Difference Value Histogram Modification" Published by Journal of Information Hiding and Multimedia Signal Processing, August 2014.

[21] Tzu-Chuen Lu et.al "High capacity reversible hiding scheme based on interpolation, difference expansion, and histogram shifting" Published by Springer,doi.org/10.1007/s11042-013-1369-0,07 Feb 2013.

[22] C. Vinoth Kumar et.al "High Capacity Reversible Data hiding based on histogram shifting for Medical Images" Published by International conference, doi: 10.1109 / iccsp. 2013.6577152,16 August 2013.