Review of Distributed Robust and Reversible Watermarking Technique

Anamika Agrawal[#1], Dr. Ajay Kumar Bharti[*2], Dr. Santosh Kumar[$3]

[1]School of Computer Science, Maharishi University of Information Technology, Lucknow, India.
[2]Professor, School of Computer Science, Maharishi University of Information Technology, Lucknow, India
[3]Associate Professor, School of Computer Science, Maharishi University of Information Technology, Lucknow, India

Abstract: Steganography is the science of hiding the secret messages inside other medium files in a way that hides the existence of the secret message at all. Secure LSB Reversible image steganography can be applied to text, audio, image, and video file types. In this study, we propose a new reversible steganography approach for digital images in which the RGB coloring model was used, in that we are using max histogram technique. The efficiency of the proposed approach has been tested and evaluated. The experimental results show that our proposed reversible secure LSB steganography approach produce high-quality stegano images that resist against visual and statistical attacks.

Keywords: Steganography, digital images, RGB, LSB.

I. INTRODUCTION

Secure Reversible Data Hiding (SRDH) has been intensively studied in the community of signal processing. Also referred as invertible or lossless data hiding, SRDH is to embed a piece of information into a host signal to generate the marked one, from which the original signal can be exactly recovered after extracting the embedded data. The technique of RDH is useful in some sensitive applications where no permanent change is allowed on the host signal. In the literature, most of the proposed algorithms are for digital images to embed invisible data or a visible watermark.
Generally speaking, direct modification of image histogram provides less embedding capacity. In contrast, the more recent algorithms manipulate the more centrally distributed prediction errors by exploiting the correlations between neighboring pixels so that less distortion is caused by data hiding. Although the PSNR of a marked image generated with a prediction error based algorithm is kept high, the visual quality can hardly be improved because more or less distortion has been introduced by the embedding operations. For the images acquired with poor illumination, improving the visual quality is more important than keeping the PSNR value high. Moreover, contrast enhancement of medical or satellite images are desired to show the details for visual inspection. Although the PSNR value of the enhanced image is often low, the visibility of image details has been improved.
In existing system after hiding the information in images the quality of the image is not proper, means it produce a poor quality images. In the existing system information can be hidden only in B/W image.

II. MOTIVATIONS

In today's world, there are a number of people who claim some documents to be there when it actually does not belong to them. In order to authenticate the images, documents, videos and images, we need a method that ensures the authority belongs to that person. For example, many companies need to claim that their company logo or trademark belongs to them rather that some fraud who claims it as his/her works. For that the companies can use data hiding techniques in their logos in order to prove that the logo is theirs. Hence we can use data hiding techniques in images for authentication and safeguarding of documents from hackers, intruders or frauds. Data hiding can also be used special agents or government security agencies to send classified information to other security agencies or officers without being disrupted by hackers.

III. PROBLEM STATEMENTS

Now day's data hiding become a challenging task because lot of security threats and quality issues are there, many existing techniques are there but all are having some drawback based on quality, security, and data safety. There exists a problem between data and image that is if we increasing the hiding rate often causes more distortion in image content. To measure the distortion, the peak signal-to-noise ratio (PSNR) value of the marked image is often calculated. Generally speaking, direct modification of image histogram provides less embedding capacity. In contrast, the more recent algorithms manipulate the more centrally distributed prediction errors by exploiting the correlations between neighboring pixels so that less distortion is caused by data hiding. Based on our knowledge, there is no existing SRDH algorithm that performs the task of contrast enhancement so as to improve the visual quality of host images. So in this study, we aim at inventing a new SRDH algorithm to achieve the property of contrast enhancement instead of just keeping the PSNR value high. In principle, image contrast enhancement can be achieved by histogram equalization. To perform data embedding and contrast enhancement at the same time, the proposed algorithm is performed by modifying the histogram of pixel values. Firstly, we will select max histogram value from image.
Selected histogram values are used for data hiding, we are hiding data in last two bit so that it not going to affect quality of image quality. While hiding data first data get converted to binary after that we will break it to four part two bit each. These four part we will hide in four different image pixel values. To avoid the overflows and underflows due to histogram modification, the bounding pixel values are pre-processed and a location map is generated to memorize

their locations. For the recovery of the original image, the location map is embedded into the host image, together with the message bits and other side information.
The proposed algorithm was applied to two set of images to demonstrate its efficiency. To our best knowledge, it is the first algorithm that achieves image contrast enhancement by SRDH. Furthermore, the evaluation results show that the visual quality can be preserved after a considerable amount of message bits have been embedded into the contrast-enhanced images.
Here we are using Secure Reversible Data Hiding technique (SRDH) to hide information in images and after hiding secret information image quality is retained well. Image contrast enhancement can be achieved by histogram equalization. The original image can be exactly recovered without any additional information.

IV. LITERATURE REVIEW

A novel reversible data hiding algorithm, which can recover the original image without any distortion from the marked image after the hidden data have been extracted, is presented in this paper. This algorithm utilizes the zero or the minimum points of the histogram of an image and slightly modifies the pixel grayscale values to embed data into the image.

In this section contains many existing steganography techniques review. Some famous techniques like Reversible data hiding, PSNR, DCT and DWT [2], using these various techniques we can hide data in digital image. In these techniques some are good with respect to image quality, because after hiding data in images, stegano image quality is damaged, for that lot of improvement is going on in various techniques so that image quality should be good with respect to original images.

In PSNR technique the lower bound of PSNR is significantly higher than that of every single reversible datum concealing systems detailed in the writing. The computational unpredictability of our proposed procedure is low and the execution time is short. The calculation has been effectively connected to an extensive variety of pictures, including regularly utilized pictures, therapeutic pictures, surface pictures, airborne pictures and the greater part of the 1096 pictures in CorelDraw database. Trial results and execution correlation with other reversible information concealing plans are displayed to show the legitimacy of the proposed calculation [Z Ni, YQ Shi, N Ansari, W Su - Reversible information concealing, IEEE, 2006].

Watermarking using Reversible techniques is preferred now days, because people need privacy for their data [3]. In reversible watermarking techniques we can hide information and any time we can extract that information. People using this technique for image authentication also, while sharing image on social media, third party storage platform [1].

It can embed more data than many of the existing reversible data hiding algorithms. It is proved analytically and shown experimentally that the peak signal-to-noise ratio (PSNR) of the marked image generated by this method versus the original image is guaranteed to be above 48 dB. This lower bound of PSNR is much higher than that of all reversible data hiding techniques reported in the literature. The computational complexity of our proposed technique is low and the execution time is short. The algorithm has been successfully applied to a wide range of images, including commonly used images, medical images, texture images, aerial images and all of the 1096 images in CorelDraw database. Experimental results and performance comparison with other reversible data hiding schemes are presented to demonstrate the validity of the proposed algorithm [Z Ni, YQ Shi, N Ansari, W Su - Reversible data hiding, IEEE, 2006].
The experimental results for many standard test images show that prediction-error expansion doubles the maximum embedding capacity when compared to difference expansion. There is also a significant improvement in the quality of the watermarked image, especially at moderate embedding capacities [D.M. Thodi and J. J. Rodriguez- Expansion embedding techniques for reversible watermarking, IEEE, 2007].
The watermark information is normally embedded in the LSB of features of relational databases to minimize distortions. Whereas, in RRW, a GA based optimum value is embedded in the selected feature of the dataset with the objective of preserving the data quality while minimizing the data distortions as a result of watermark embedding. Another reversible watermarking technique proposed in [26] is based on difference expansion and support vector regression
(SVR) prediction to protect the database from being tampered. The intention behind the design of these techniques to provide ownership proof. Such techniques are vulnerable to modification attacks as any change in the expanded value will fail to detect watermark information and the original data. Genetic algorithm based on difference expansion watermarking (GADEW) technique is used in a proposed robust and reversible solution for relational databases [27]. GADEW improves upon the drawbacks mentioned above by minimizing distortions in the data, increasingwatermark capacity and lowering false positive rate. To this end, a GA is employed to increase watermark capacity and minimize introduced distortion. This is because the watermark capacity increases with the increase in number of features and the GA runs on more features to search the optimum one for watermarking, watermark capacity decreases with the increase in watermarked tuples. GADEW used the distortion measures
(AWD and TWD) to control distortions in the resultant data. In this context, the robustness of GADEW can be compromised whenAWDandTWDare given high values. Prediction-error expansion watermarking techniques (PEEW) like [28] incorporate a predictor as apposed to a difference operator to select candidate pixels or features for embedding of watermark information. The PEEW proposed technique by Farfoura and Horng is fragile against malicious attacks as the watermark information is embedded in the fractional part of numeric features only. In this particular scenario, the scheme works because the intention of the attacker is to preserve the usefulness of the data; otherwise, he can easily compromise the fractional part. RRW is robust, as the watermark information is embedded in the values of numeric features, to make the scheme resilient

against such attacks. In the authors proposed a robust, blind, resilient and reversible, image based watermarking scheme for large scale databases. The bit string of an image is used as a watermark where one bit from the bit string is embedded in all tuples of a single partition and the same process is repeated for the rest of the partitions. This technique demonstrates a remarkable decrease in watermark detection rate during various types of heavy attacks, and the database tuples get highly distorted. In RRW, a GA is used to generate a parameter that controls the data distortions to make sure that the data quality remains intact after watermarking. Moreover, the semi-blind nature of the technique allows robustness against heavy attacks and also for regeneration of the original dataset after watermark decoding. Gupta and Pieprzyks' [23], proposed reversible watermarking technique introduces distortions as a result of the embedding process. Changes in the data are controlled by placing certain bounds on LSB. On the contrary, to limit the distortions, the data outside the limited bounds is left un watermarked. As a result, the watermark robustness gets compromised. However, RRW has no such limitations. The reversible watermarking techniques DEW, GADEW PEEW, proposed in [23], [27], [28] respectively, are not robust and reversible against heavy attacks. Features are selected in these techniques for watermarking without considering their importance in knowledge discovery. RRW is robust and reversible and copes with the above mentioned problems and data quality is preserved by taking into account the importance of the features in knowledge discovery. In RRW, all the tuples of the selected feature can be marked thanks to the selection of a low distortion watermark; therefore, the attacker will have to attack all the tuples to corrupt the watermark to mitigate the effect of the majority voting scheme. Attacking all the tuples is not a viable option for the attacker because he has no knowledge of the original data or the usability constraints and that would completely compromise its usefulness. Moreover, since RRW can afford to embed watermark bits in all or a large fraction of the tuples of the selected feature; it achieves high robustness against heavy attacks. However, marking all tuples is not a requirement. RRW is configurable in that the data owner can choose a fraction for watermarking if it is required.

X. Li, B. Yang, and T. Zeng, Forecast mistake development (PEE) is a vital method of reversible watermarking which can install vast payloads into computerized pictures with low contortion. In this paper, the PEE method is additionally examined and an effective reversible watermarking plan is proposed, by joining in PEE two new procedures, to be specific, versatile inserting and pixel choice. Not at all like ordinary PEE which implants information consistently, we propose to adaptively insert 1 or 2 bits into expandable pixel as indicated by the neighborhood multifaceted nature.

This abstains from growing pixels with substantial expectation mistakes, and consequently, it diminishes installing sway by diminishing the most extreme adjustment to pixel esteems. In the interim, versatile PEE permits expansive payload in a solitary implanting pass, and it enhances the limit furthest reaches of customary PEE.

We additionally propose to choose pixels of smooth region for information inserting and leave unpleasant pixels unaltered. Thusly, contrasted and customary PEE, an all the more forcefully appropriated expectation blunder histogram is acquired and a superior visual nature of watermarked picture is watched. With these changes, our technique outflanks ordinary PEE. Its predominance over other best in class strategies is additionally exhibited tentatively.

Shunquan Tan, Bin Li, In this paper, the writers call attention to that the correcting period of edge versatile picture steganography in light of LSB coordinating returned to acquaints a heartbeat bending with the long exponential tail of the histogram of the supreme distinction of the pixel sets. Mentioning utilization of this objective fact, a focused on steganalytic strategy in light of B-Spline fitting is proposed. Test comes about demonstrate that the proposed technique acquires great outcomes for distinguishing stego pictures with low implanting rate. The predominant execution of our strategy contrasted and cutting edge daze steganalyzers, for example, SPAM and SRM is evident. Besides, our strategy can precisely assess the limit utilized as a part of the mystery information inserting method and can isolate the stego pictures with unit square size from those with square sizes more prominent than one.

Pallavi Khare, 2 Jaikaran Singh, 3 Mukesh Tiwari, Steganography is the workmanship and investigation of undetectable correspondence. This is proficient through concealing data in other data, accordingly concealing the presence of the conveyed data. The word steganography is gotten from the Greek words "stegos" signifying "cover" and "grafia" signifying "stating" characterizing it as "secured written work". In picture steganography the data is concealed only in pictures. Computerized Image Steganography framework enables a normal client to safely exchange instant messages by concealing them in an advanced picture record. A blend of Steganography and encryption calculations gives a solid spine to its security. Advanced Image Steganography framework highlights inventive systems for concealing content in a computerized picture document or notwithstanding utilizing it as a key to the encryption.

Wei Huang, Yao Zhao, and Rong-Rong Ni, As of late, an edge versatile picture stegano-realistic strategy in light of slightest critical piece (LSB) coordinating returned to (EA-LSBMR) has been proposed, which holds great visual quality and legitimate security under fitting inserting rates. In any case, from the broad investigations to EA-LSBMR, we find that the discrete Fourier change (DFT) range of pixel-sets contrasts histogram still uncovers the nearness of a mystery message even in a low inserting rate. To upgrade the security, a changed plan is proposed in this paper, which can crush the previously mentioned investigation and keep the visual quality superior to EA-LSBMR in higher installing rates. Trial comes about utilizing a most recent widespread steganalysis strategy have shown the proposed technique's great execution.

Jarno Mielikainen, LSB Matching Revisited, This letter proposes a change to the minimum critical piece (LSB) coordinating, a steganographic technique for installing message bits into a still picture. In the LSB coordinating, the decision of whether to include or subtract one from the

cover picture pixel is arbitrary. The new strategy utilizes the decision to set a twofold capacity of two cover pixels to the coveted esteem. The implanting is performed utilizing a couple of pixels as a unit, where the LSB of the main pixel conveys one piece of data, and an element of the two pixel esteems conveys another piece of data. Hence, the adjusted technique permits implanting an indistinguishable payload from LSB coordinating however with less changes to the cover picture. The test consequences of the proposed strategy indicate preferred execution over conventional LSB coordinating as far as twisting and obstruction against existing steganalysis.

V. Histogram comparing the cover and stego images

Differences between the original and stego images cannot be easily detected by vision; to evaluate the visual attacks more Accurately the RGB histogram for cover image and its 32k stego image was used to make the comparison more accurate, this shown in Figure 2. Based on the original and stego images histograms, it is obvious that both stego and original images RGB histogram seems to be identical.

VI. Stego-image modified LSB plan

The pixel selection model applied in this study selects the image pixels adaptively based on the message size; this provides the ability to use the cover image pixels starting from the pixels that are extremely different from their adjacent pixels (edge pixels) when the message is small to those that has small difference from their adjacent pixels until nearly all cover image pixels are used to embed large messages. This approach will cause the least distortion and will maximize the visual quality to the generated stego images relatively to message size. Figure 7 shows Airplane modified pixels LSB plan for different message sizes.

VII. Stego-Image quality

To evaluate the stego image quality we used two measures: Mean Square Error (MSE) and the peak signal-to-noise ratio (PSNR). MSE is the parameter that calculates the magnitude of average error between the original image and stego image. The difference between the observed values of the original and stego image are squared and then their average is calculated. The smaller value of the MSE the higher will be the quality of stego image. The formula for calculation of MSE is depicted below.

VIII. CONCLUSION

A new Secure reversible data hiding algorithm is proposed with the property of contrast enhancement. Basically, the max histogram are selected for data embedding so that histogram equalization can be simultaneously performed by repeating the process. The data is stored in the LSB of the pixels and each character is stored in four pixels .changing the LSB of the pixels does not affect much in the contrast or the quality of the images since a slight variation in the RGB value would not affect or be noticed by the user. In this review a secure way of transmission of a secret message is achieved in which no intruder can know about the information being exchanged. The experimental results have shown that the image contrast can be enhanced by changing last two bit of pixel values. Compared with the other existing techniques, the visual quality of the contrast-enhanced images generated by our algorithm is better preserved. Moreover, the original image can be exactly recovered without any additional information. Hence the proposed algorithm has made the image contrast enhancement secure reversible and there is maximum retrieval of data.

REFERENCES

[1] Tan, S. and B. Li, “Targeted steganalysis of edge adaptive imagesteganography based on LSB matching revisited using B-spline fitting” IEEE Signal Processing Letters,Vol. 19, pp. 336-339, 2012.

[2] Huang, F., Y. Zhong, and J. Huang, “Improved algorithm of edge adaptive image steganography based on LSB matching revisited algorithm” n Digital-Forensics and Watermarking.pp. 19-31,2014.

[3] B.C. Nguyen, S.M. Yoon et H.-K. Lee “Multi bit plane image steganography” Digital Watermarking, 5th International Workshop, IWDW, Vol. 4283, Novembre 2006.

[4] Ahmad T. Al-Taani. and Abdullah M. AL-Issa.” A novel steganographic method for gray-level images” International Journal of Computer, Information, and Systems Science, and Engineering,Vol. 3, 2009.

[5] Anu, rekha, Praveen “Digital image steganography” International Journal of Computer Science & Informatics, Vol. 1, 2011.

[6] Saurabh V. Joshi , Ajinkya A. Bokil, Nikhil A. Jain and Deepali Koshti “Image steganography combination of spatial and frequency domain” Intarnational journal of computer applications. Vol. 53, September 2012.

[7] Elham Ghasemi, Jamshid Shanbehzadeh and Nima Fassihi “High capacity image steganography using wavelet transform and genetic algorithm” International MultiConference of Engineers and Computer Scinetests. Vol. 1, 2011.

[8] Joshi, Kamaldeep, and Rajkumar Yadav. "A new LSB-S image steganography method blend with Cryptography for secret communication." In 2015 Third International Conference on Image Information Processing (ICIIP), pp. 86-90. IEEE, 2015.

[9] Charan, Gunda Sai, S. S. V. Nithin Kumar, B. Karthikeyan, V. Vaithiyanathan, and K. Divya Lakshmi. "A novel LSB based image steganography with multi-level encryption." In Innovations in Information, Embedded and Communication Systems (ICIIECS), 2015 International Conference on, pp. 1-5. IEEE, 2015.

[10] Jain, Mamta, and Saroj Kumar Lenka. "Secret data transmission using vital image steganography over transposition cipher." In Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on, pp. 1026-1029. IEEE, 2015.

[11] Niels Provos and Peter Honeyman “Hide and seek: An introduction to steganography” IEEE Security and Privacy, vol. 1, no.3, pp. 32-44, 2003.

[12] Anderson, Ross J., and Fabien AP Petitcolas. "On the limits of steganography." IEEE Journal on selected areas in communications 16, no. 4 (1998): 474-481.

[13] Hardik Patel, Preeti Dave “Steganography technique based on DCT coefficients” International Journal of Engineering Research and Applications, Vol. 2, pp.713-717, Jan-Feb 2012.

[14] Chen, W.-J., C.-C. Chang, and T. Le “High payload steganography mechanism using hybrid edge detector”

Expert Systems with applications, Vol. 37, pp. 3292-3301, 2010.

[15] Jain, N., S. Meshram, and S. Dube, "Image steganography using LSB and edge–detection technique" International Journal of Soft Computing and Engineering (IJSCE), 2012.

[16] Ioannidou, A., S.T. Halkidis, and G. Stephanides "A novel technique for image steganography based on a high payload method and edge detection" Expert Systems with Applications,Vol. 39, pp. 11517-11524, 2012.

[17] Shahzad Alam, Vipin Kumar, Waseem A Siddiqui and Musheer Ahmad "Key dependent image steganography using edge detection" Fourth International Conference on Advanced Computing & Communication Technologies (ACCT), 2014.

[18] Mielikainen, J., "LSB matching revisited" IEEE Signal Processing Letters, Vol. 13, pp. 285-287, 2006.

[19] Luo, W., F. Huang, and J. Huang "Edge adaptive image steganography based on LSB matching revisited" Information Forensics and Security, Vol. 5, pp. 201-214,2010.

[20] Huang, W., Y. Zhao, and R.-R. Ni "Block based adaptive image steganography using LSB matching revisited" J. Elec. Sci. Tech, Vol.9 , pp. 291-296,2011.

[21] Fridrich, Jessica, Miroslav Goljan, and Rui Du. "Reliable detection of LSB steganography in color and grayscale images." In Proceedings of the 2001 workshop on Multimedia and security: new challenges, pp. 27- 30. ACM, 2001.

[22] Pfitzmann, Birgit. "Information hiding terminology-results of an informal plenary meeting and additional proposals." In Proceedings of the First International Workshop on Information Hiding, pp. 347-350. Springer-Verlag, 1996.

[23] Gupta, Shilpa, Geeta Gujral, and Neha Aggarwal. "Enhanced least significant bit algorithm for image steganography." IJCEM International Journal of Computational Engineering & Management 15, no. 4 (2012): 40-42.