ISSN: 2321-7782 (Online)
Volume 2, Issue 2, February 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Paper / Case Study
Available online at: www.ijarcsms.com

Confidential Protection of Data using Histogram Shifting based Reversible Data Hiding

Binita Roshni.M[1]
PG Scholar
Dept Of Applied Electronics
Christ the King College of Cngineering
Tamilnadu - India

S.Raja[2]
HOD/ECE
Christ the King College of Cngineering
Tamilnadu - India

Abstract: ***The concept of Reversible Data Hiding presents privacy protection of medical images with information using histogram shifting based reversible data hiding. A module that is implemented involves image encoding and histogram shifting based difference expansion. Embedding the secret data into the medical images would be one of the useful methods for protecting the privacies. Next, because external data are hidden into the original image, some alterations are supposed to be induced. After data embedding, the output image should be as similar as its original counterpart, and medical doctors may lead to proper treatment by using the images with hidden data when necessary. Reversible data hiding is a newly developed branch in data hiding or watermarking researches. Later on, the medical image containing data might be retrieved by medical doctors while necessary, and both the original image and the hidden data can be perfectly recovered with the algorithm corresponding to the embedding scheme. Finally the performance of an algorithm will be evaluated by mean square error, peak signal to noise ratio.***

Keywords: Reversible Data Hiding (RDH), Histogram Shifting, Pixel Difference, Parameters Validation.

I. INTRODUCTION

To use the local energy feature dispersions of high-pass and low-pass wavelet sub-bands for texture classification, the algorithm is with a special local energy histogram (LEH) to demonstrate the distribution of the coefficients in each wavelet sub-band. General definition shows how a new discrepancy measure between two images by adding up all the summarized divergences between two LEHs on the corresponding sub-bands. Regarding this, discrepancy measure, a classifier is then built for supervised classification based on texture and all the other techniques. It is manifested by the experiments that our novel algorithm has a satisfactory classification performance in comparison with many state-of-the-art texture classification techniques.

Data hiding is in a big demand in our day-to-day life. Wherever we go, it is now-a-days mandatory to hide some data which is to be kept secret in an image or in an audio file or even in a video file, we can hide any data. In medical research and all, the growing scenario specifically targets on the secret data communication and transmission only. Many algorithms including watermarking, data hiding, steganography and cryptography are used to hide the secret data or some information.

II. LITERATURE REVIEW

To make medical image sharing efficient in many resources such as remote diagnosis aid [1], to make the image more efficient by watermarking it with its associated knowledge. The ultimate application of data hiding is for authentication, a new trans-coding system with the help of the technique data hiding is proposed. Additional information is extracted before the image resizing. Another one approach [2] proposes a high capacity Reversible Data Hiding (RDH) scheme based on integer-to-integer wavelet transforms.

The scheme [3] divides an input image into non-overlapping blocks and embeds a watermark into the high-frequency wavelet coefficients of each block. The considerations to nullify both underflow and overflow are discussed for a wavelet and size of the pixels. An undesirable side effect of many watermarking and other secret data transmission scheme is that the image into which primary data is merged is distorted. Identifying an optimum balance between the amounts of information merged and the induced deviation is therefore a field of research. It's been a comparable work [4] in understanding the basic limits of the capacity versus distortion of secret data hiding techniques. A few applications, however, have no distortion resulting from auxiliary data can be permitted.

III. EXISTING SYSTEM

Integer Transformation Technique:

Basically many transformation techniques are been implemented. Integer Wavelet Transformation technique paves way in getting the wavelets or wavelet packets as features extracted from it.

We have much modification in identifying the wavelet packets of a normal signal, specifically an image and after going through the transformation technique, we can hide the data in the same.

Pixel Substitution and Difference:

Numerous secret bits are merged with every pixel using the change in LSB substitution method. Parameters that mentioned previously represent the same condition. A data hiding algorithm is taken into account, if the same can provide a greater PSNR values when embedding with a similar capacity. Thus, the distinguishing of SNR values based on capacity of data hiding that are slightly larger than those provided by all the existing algorithms. A potential possibility is that this method treats non-overlapping 2 x 2 pixel blocks in spite of two successive pixels, such that the features of edges may be treated enough and the pixels in edge areas can withheld much more alterations without making detectable distortion.

IV. PROPOSED SYSTEM

Reversible Data Hiding

The Reversible Data Hiding [2] & [5] is nothing but of the work that hides the data embedding/extracting [5] on the normal plotting of signals. But, some scenarios take reward of a deficient thing or a channel administrator treats to append some additional information such as authentication data, inside the encrypted signal. It is also hopeful that the original image should be recovered without any error after signal decryption and message extraction at receiver side. This demonstrates a practical scheme satisfying the mentioned requirements.

Encrypting the original image and a data-hider can embed additional data into the encrypted image using a data hiding key though the programmer does not know the input. Most of the data hiding algorithms are lossy. Distortion is brought into the host image during the embedding process. This targets the necessity of reversible data hiding which can be brought back as the original host signal perfectly after the watermark extraction.

The consignment of reversible watermarking is typically lower than that of lossy data hiding techniques. With an encrypted image containing excessive data, a receiver may first decrypt it accordingly and then extract the embedded data and recover the original image according to the data-hiding key. In the scheme, the data extraction is not separable from the content decryption. In regarding, the additional data must be extracted from the decrypted image, so that the primary content of original image is exposed before data extraction.

Histogram Shifting:

Histogram shifting is nothing but the algorithm that comes with pixel difference histogram, difference histogram with various levels, complexes with Reversible Data Hiding (RDH) algorithm. Histogram shifting is nothing but the complex or composite mixture of color representation in a graphical manner. If someone has the data-hiding key but not the encryption key, data extraction can never be done because of the layer levels of security. During image resizing, we quantize the image into M x M blocks (assume M is a positive integer larger in value). To contribute medical images with some consequent data, one technique involves summing, when allowed by the image file format, some extra information.

In other words, when compared to a dimensional histogram, difference pixel level-histogram is far good to do hiding. It is regular in shape and has a much higher peak point. A novel HS-based method is identified by modifying the anticipating-error histogram. This technique can exploit the image redundancy and reach better performance in comparison to the predefined DE-based methods. HS-based method where the histogram used for embedding is picked such that the noisy level in embedding is minimized.

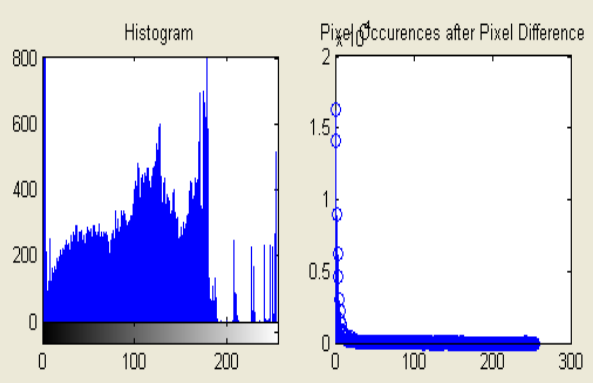

fig 1: Histogram shifting

Embedding Technique:

The embedding technique consists of various procedures. Initially, dividing the input image into non-overlapping scheme is done and then the blocks are divided into various parts to get in an image as *L1*, *L2* and *L*3. By shifting the pixel location using histogram shifting and embedding functions, the hidden data in embedded into *L*1 and L3. By using replacement technique (for instance, say LSB), embed the histogram mapping that records the pixels into L1. To be notified, before replacing LSBs, the original LSBs of L1 should be treated to a LSB sequence. At last, the LSB is embedded in a sequence into L2 using shifting and embedding functions.

Here, the partition of three parts is to figure out the problem by hiding the location map into the input image. The component L1 is doubled to embed first the hidden data (using histogram shifting and embedding functions) and then the location is mapped (using LSB replacement).

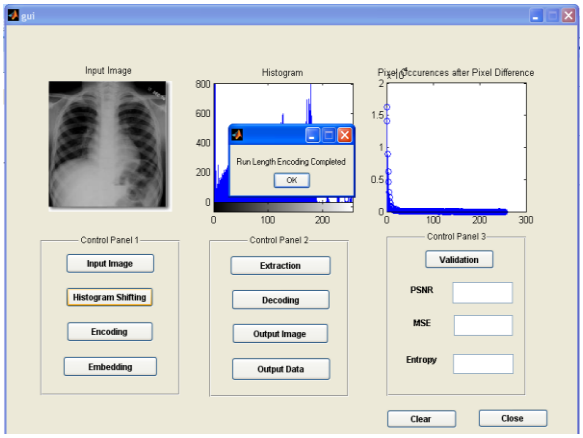

fig 2: Embedding Technique

Embedded Image:

An image that comprises of a secret data or a text file into it is termed to be the embedded or watermarked or data hidden image. Based upon the pixel values and the location of the images, the pixel classification and the difference histogram are followed. Embedded image will be presented by using the basic unique embedding technique.

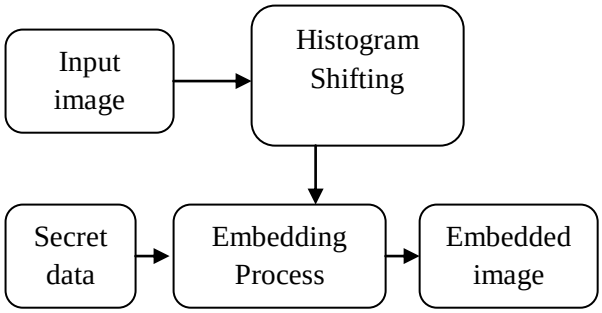

fig 3: Embedding Process – Flow Diagram

Data Extraction:

Data extraction comes as a reverse process. Data Extraction occurs with a concept of acquiring the embedded image simultaneously along with the reverse process of extracting the data from the host image separately as secret data and the host content.

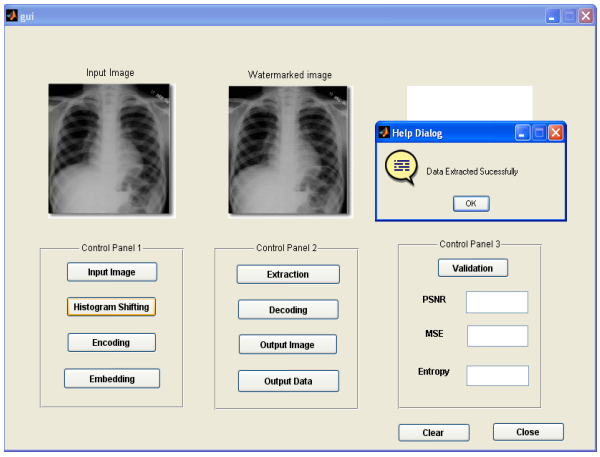

fig 4: Data Extraction Process

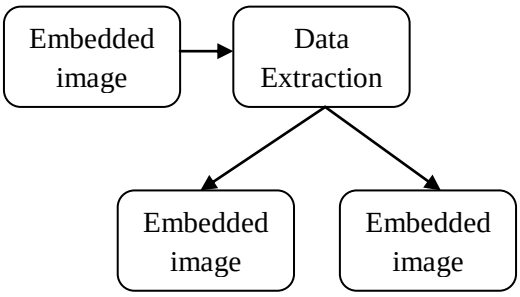

fig 5: Data Extraction Process

Data embedding and the extraction process come simultaneously, such that both the process is carried with the use of encoding and decoding procedures. Matrix encoding enhances the efficiency of embedding by decreasing the number of required changed bits. Wavelet Transform is done as a reversible process such that the image can be retrieved back from the input given.

Decoding process:

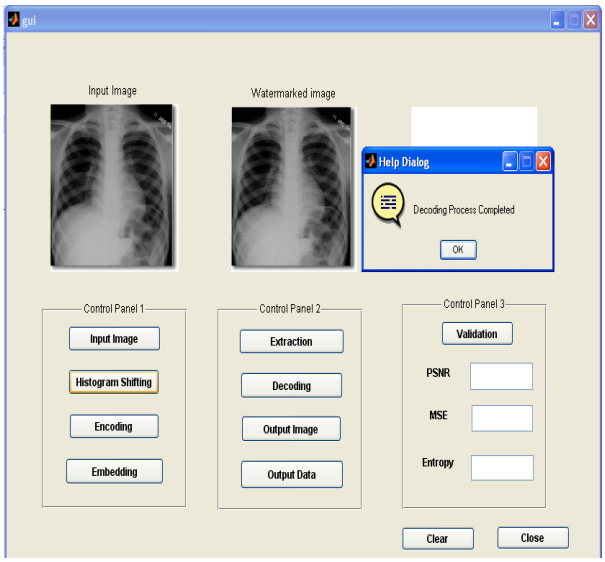

fig 6: Decoding Process

The image is decoded as an image such that after having the formal procedure of encoding and decoding procedure only, each and every image's embedding procedure can be followed. Without the proper execution of the image encoding and decoding process the pixel substitution method can't be fulfilled. Wherever the process of encoding is undergone, simultaneously decoding step is also to be followed.

V. RESULTS

The results are finally needed to be discussed about the application of the data hiding in the medical field and at the receiving output section; we can go for retrieving process termed to be the data extraction process. Data extraction flow comes with the output retrieval and the display of the same. Any medical data or our personal data can also be hidden in it.

VI. FUTURE WORK

Future work can be implemented with the additional technique of adding any hardware for the same process. Hardware implementation can be done for hiding the data using Reversible Data Hiding (RDH).

VII. CONCLUSION

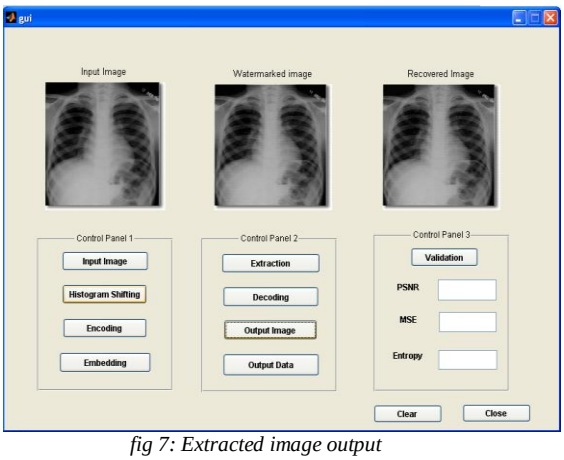

fig 7: Extracted image output

According to techniques imparted, to obtain Reversible Data Hiding (RDH) algorithm, one seeks to identify the shifting procedure and embedding functions. This process flow will help the pattern of RDH. Somehow, by insisting the Pixel Expansion algorithm and selection techniques, two new RDH algorithms are also developed. This can achieve a rapid

performance as compared. So this work has a potential to provide a good RDH algorithms. However, the proposed model may use different RDH algorithms, it has also a very few drawbacks. PSNR and MSE values are identified correspondingly for all the images and those values changes from image to image. However for an example image it is brought out and shown in fig 9.

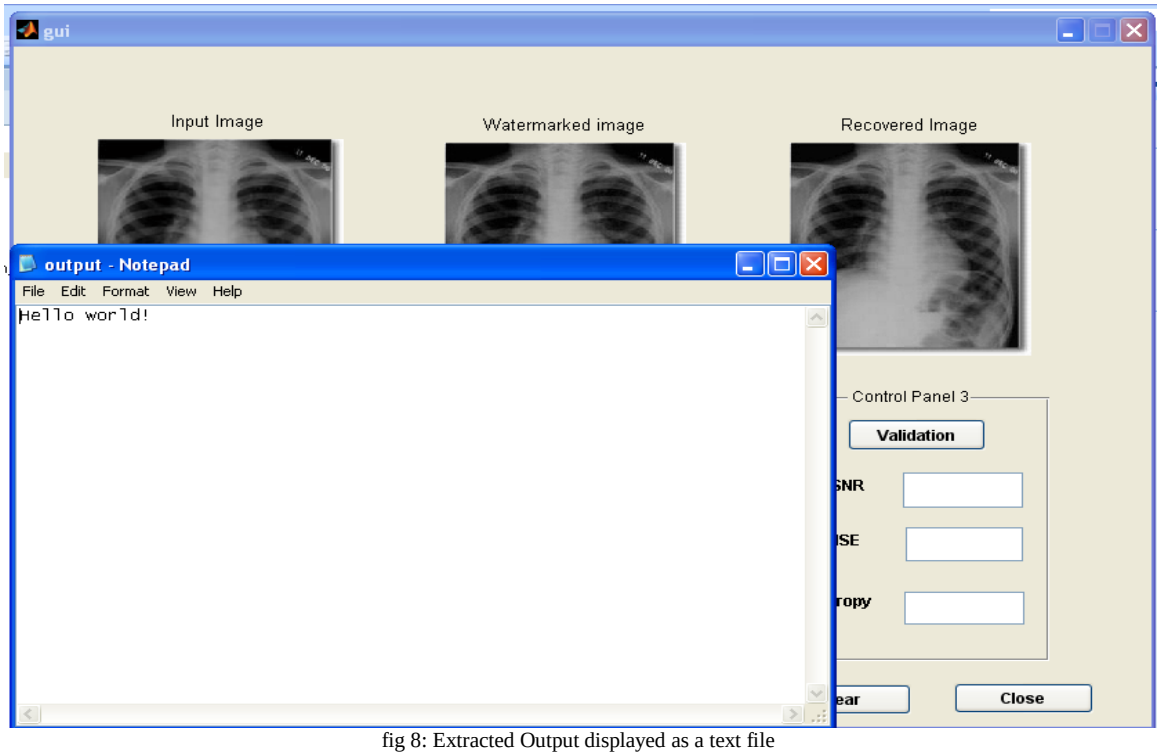

fig 8: Extracted Output displayed as a text file

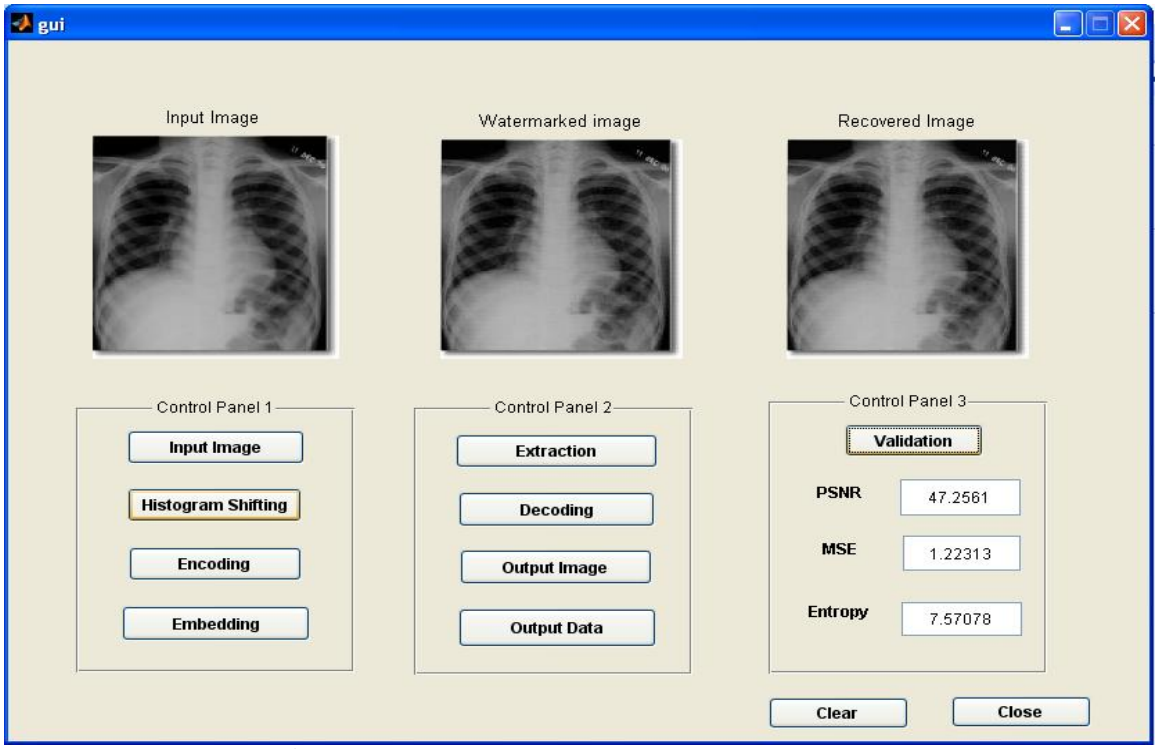

fig 9: Output Data Hiding and Retrieval with Parameters Validation

Acknowledgement

We wish to acknowledge the efforts of Pantech ProEd Pvt ltd., for guidance which helped us work hard towards producing this research work.

References

1. M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," IEEE Trans. Signal Process., vol. 52, no. 10, pp. 2992–3006, Oct. 2004.
2. W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," IEEE Trans. Image Process., vol. 19, no. 4, pp. 1097–1102, Apr. 2010
3. X. Zhang, "Lossy compression and iterative reconstruction for encrypted image," IEEE Trans. Inform. Forensics Security, vol. 6, no. 1, pp. 53–58, Feb. 2011.
4. T. Bianchi, A. Piva, and M. Barni, "On the implementation of the discrete Fourier transform in the encrypted domain," IEEE Trans. Inform. Forensics Security, vol. 4, no. 1, pp. 86–97, Feb. 2009.
5. T. Bianchi, A. Piva, and M. Barni, "Composite signal representation for fast and storage-efficient processing of encrypted signals," IEEE Trans. Inform. Forensics Security, vol. 5, no. 1, pp. 180–187, Feb. 2010.
6. N. Memon and P. W. Wong, "A buyer-seller watermarking protocol," IEEE Trans. Image Process., vol. 10, no. 4, pp. 643–649, Apr. 2001.
7. M. Kuribayashi and H. Tanaka, "Fingerprinting protocol for images based on additive homomorphic property," IEEE Trans. Image Process., vol. 14, no. 12, pp. 2129–2139, Dec. 2005.
8. M. Deng, T. Bianchi, A. Piva, and B. Preneel, "An efficient buyer-seller watermarking protocol based on composite signal representation," in Proc. 11th ACM Workshop Multimedia and Security, 2009, pp. 9–18.
9. S. Lian, Z. Liu, Z. Ren, and H. Wang, "Commutative encryption and Watermarking in video compression," IEEE Trans. Circuits Syst. Video Technol., vol. 17, no. 6, pp. 774–778, Jun. 2007.
10. M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. G. B. Natale, and A. Neri, "A commutative digital image watermarking and encryption method in the tree structured Haar transform domain," Signal Processing: Image Commun., vol. 26, no. 1, pp. 1–12, 2011

