

# Reversible Image Data Hiding Using Encryption and Decryption with Contrast Enhancement

Asha S Raj

M.Tech student

Department of Computer Science and Engineering  
Mohandas College of Engineering  
Anad, Trivandrum

Mrs.Gayathri Nair P

Asst.Professor

Department of Information Technology  
Mohandas College of Engineering  
Anad, Trivandrum

**Abstract—** *The Reversible Data Hiding of image Using Encryption and Decryption with Contrast Enhancement is a widely used technique. Recoverance of host image is done. Using Encryption and Decryption with Contrast Enhancement. It is applied at medical and military applications. The data embedding continous loss is inevitable. In several areas such as medical, military, and law forensics degradation of cover image is not allowed. For the sake of Reversible Image Data Hiding Using Encryption and Decryption with Contrast Enhancement. The main applications are medical and military areas. The digital images that embeds data into image. For communication seceret maintenance alteration of pixel is much needed. Reversible Image Data Hiding Using Encryption and Decryption for high security and efficiency. It enables images to data in hidden format. Restoration process is focused. The Reversible Image Data Hiding Using Encryption and Decryption with Contrast Enhancement which uses the encryption and decryption for enhancing the security of the whole system.*

**Keywords—** Reversible Data Hiding, PSNR, RDH, HE, Difference expansion (DE), XOR Encryption, XOR Decryption

## I. INTRODUCTION

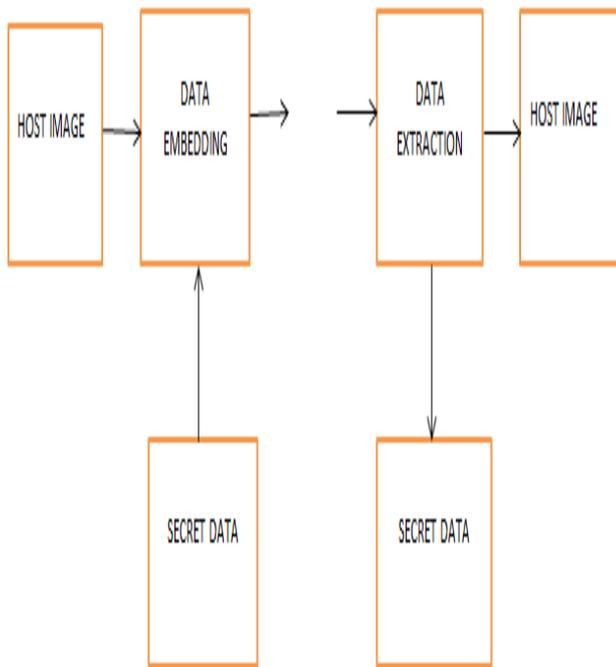
A reversible data hiding is used to recover the original image without any distortion. Reverse the data from the marked image. When the hidden data have been extracted [1]. The techniques utilizes the zero or the minimum points. The points of the histogram of an image can be used for reversing. It modifies the pixel values to embed data into the image. It is used to embed more data. One of the many existing reversible data hiding techniques are used. It is the peak signal to noise ratio (PSNR) of the marked image. The PSNR generated by the method for the easy calculation. The PSNR is higher value for all reversible data hiding techniques. It is used to embed a piece of information into the host images to generate the marked one. The techniques utilizes the zero or the minimum points are used.

original can be exactly recovered as such. Then after extraction, original image can be processed. It get the reversed image of the original one. One of the many existing reversible data hiding techniques are used. After the embedded information is extracted PSNR is followed up. The Reversible Data Hiding process eliminates the disadvantages of reverse process in watermarking. PSNR play much important role in reversing data hiding.

It is the most commonly used method. The measure of quality of reconstruction. Peak Signal Noise Ratio represent the distortion level between marked image and cover image. Reversible Data Hiding is used (DE) [2]. It is one of the. These techniques are used for reversible data hiding. With the help of PSNR value the recovered images can be checked.

The original image moved into the data hiding process. Then will get the reversed image. The modified part of the cover image is least significant part. The embedding process will usually introduce continuous distortion in original image. The original cover image is never be reconstructed image. From the marked cover image the original image can be retrieved. The main areas are medical imagery, military imagery, and law forensics. The original image is not undergoes any degradation allowed. It need a different type of data hiding method. Which is reversible data hiding (RDH) or lossless data hiding [3]. The original cover image can be reversibly restored after the embedded message is extracted.

Reversible data hiding that embeds more important data into images, audio, video, and so on. Sender side, the data is embedded by the reversible manner. The receiver side, the data is extracted by the converse manner. Once the secret data are embedded in the compression domain mode. The receiver store the cover image in a compression mode to save storage space. The output is used to extract the secret data to reconstruct the cover image. Then press the cover image again to generate compression codes.



**Fig 1.** Reversible data hiding

The PSNR [4] of a marked image generated with a predicted error. Based on the algorithm which is high. The visual quality can easily be improved. Because more degradation of data is introduced by the embedding operations. For the images acquired with poor illumination rate. The improving visual quality is more important than keeping the PSNR [4] value high. The contrast enhancement of medical or satellite images is used to present the features for visual observation method. The PSNR [4] value of the enhanced image is represented low. Once the secret data are embedded in the compression domain mode. The receiver store the cover image in a compression mode to save storage space. The output is used to extract the secret data to reconstruct the cover image. The visibility of image details has been improved. To the best idea there is no existing RDH algorithm to performs the function of contrast enhancement.

## II. RDH USING ENCRYPTION AND DECRYPTION WITH CONTRAST ENHANCEMENT

### A. Data Embedding by Histogram Modification

The Data embedding section is used for embedding the data or the image into the host image. The color images can be converted into the gray level images. The gray level images represented into the pixel format. The 8-bit gray level image denoted by  $I$ . The visual quality can easily be improved. Because more or less distortion has been introduced by the embedding operations. For the images

getting with less illumination rate. The histogram can be calculated by counting the pixel with a gray level value represented  $j$ . Use  $h_i$  to denote the image histogram so that  $h_i(j)$  denotes the number of pixels with value  $j$ . Then non empty bins in the histogram are denoted  $h_i$ . From the  $h_i$  the two peaks (i.e. the highest two bins) are selected. The denoted smaller and bigger values are denoted by  $I_S$  and  $I_R$  respectively.

### B. Pre-Process for Complete Recovery

In the RDH algorithm, it is used that all pixels counted in  $h_i$  are  $\{1,2,5,4\}$ . If the pixel having any bounding pixel value (0 or 255). The overflow or underflow problem will be caused by histogram shifting. The gray level images represented into the pixel format. The 8-bit gray level image denoted by  $I$ . The visual quality can easily be improved. Because more or less degradation has been generated by the embedding operations. To avoid this problem the histogram needs to be pre-processing. The histogram modification operations are pixel modifications. The pixel values of 0 and 255 are changed to 1 and 254. Because overflow or underflow will be caused because the possible change of all pixel is  $\pm 1$ . To remember the pre-processed pixels of the image. The location map with the same size as the original image is obtained. By giving 1 to the location of a modified pixel. And 0 to that of an unchanged one (including the 16 excluded pixels). The location map can be pre-computed. Then they given by the binary values to be hidden. In the extraction and recovery process can be done. It can be obtained from the data extracted. The marked image so that the pixels changed in the pre-process can be reported. By restoring the original values of those pixels. The original image can be completely recovered.

### C. Encryption

XOR encryption (or Exclusive-OR encryption) [5] is a common method. It encrypting text into a format that cannot be easily identified by the average person. XOR decryption (or Exclusive-OR encryption) is a common method of decrypting text into a format that cannot be easily identified by the average person. Secure or insecure XOR encryption is used in the RDH algorithm. It has no of valid use cases [7]. RDH is the best among others and is widely preferred too. XOR act as a supporting system towards it. Several notations are used and is highly protective, but tentative.

### D. Decryption

XOR decryption is tracked towards average person though for text decryption. XOR decryption is also used as a part of the decryption algorithms.

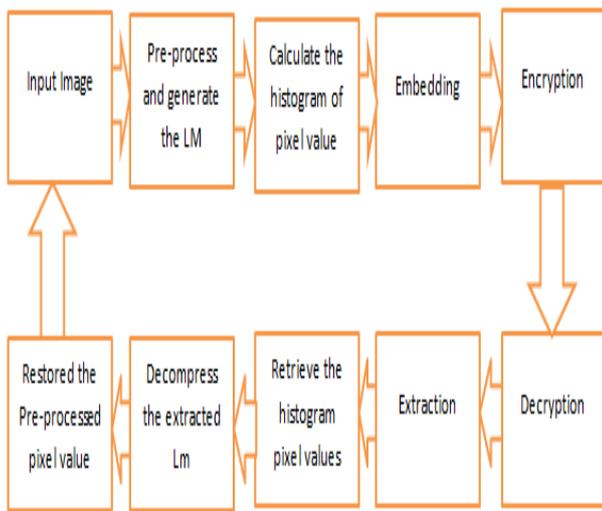
If special characters are presented then most importantly XOR functions to be crosschecked. XOR functioning is quite famous for web filtration and is used in

cipher too. Effective as well.

**E. Contrast Enhancement**

Bins are formed through splittation of Histogram For increasing the rate of hidden process 2 bins are splitted up. Histogram splitting and Equalization is focused. Peak values are chosen. ranges are from 0 to L-1 then from 256-L Changed pixel is offered with 1 and 0 otherwise.

The precalculation of the location map is done by compressing. Rate of the LM is defined as L and is stored in LSB's of the range of excluded pixel 16. Both splitting and embedding done and LM is extracted.



**Fig II.** The Reversible Data Hiding Using Encryption and Decryption with Contrast Enhancement

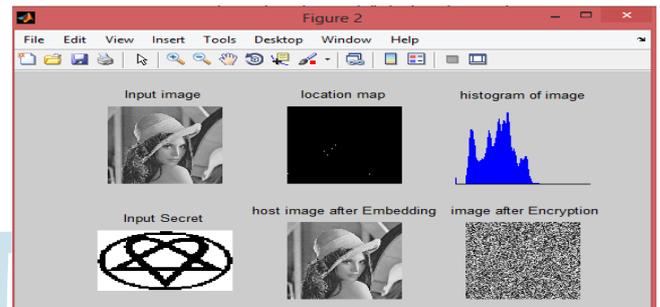
**III. SUMMARY**

RDH mannerism is followed up for the sake of cloud data. With Cryptographic techniques data hiding method [8]. The pixel reservation offers easier step for hidden mechanism For plain images and getting an excellent performance. The degradation of perfect data hiding data is used [9]. Extraction of data separately for the quality improvanse. The previous RDH techniques are used. For encrypted and decrypted the image are used for the processing. The previous step to make data hiding process very easy. The proposed method can take advantage of all previous RDH techniques. For plain images and getting an excellent performance.

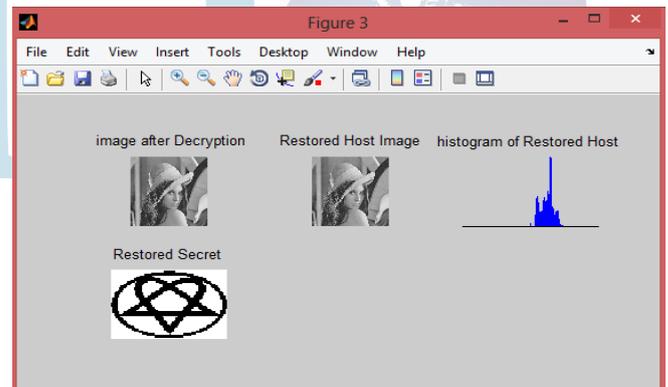
Algorithm emences with cipher technique followed with ceaser algorithmic approach [7]. The concept of shuffling the rows in the pixels of data. Huffman and

transposition is followed up. Both cryptographic techniques help from slipping into unauthorization with high security The data embedding process is used. By using the Integer Wavelet Transform for the process. It can reduce the mean square distortion between the original and watermarked image. And also to increase ratio [12]. experiments are done as per gray scale images.

The method also used in color images. Inovative algorithm paves the way for enhancement improvement histogram are being spitted as way of peak. The 2 peaks in the histogram can be calculated from the pixel values of the given images. The RDH which providing more security with the help of XOR-Encryption and XOR-Decryption techniques [6]. XOR-Encryption which encrypt the data with high security and the reverse process done in the side of XOR-Decryption [7].



**Fig III.** Output 1



**Fig IV.** Output 2

**IV. CONCLUSION**

The Reversible Data Hiding approach used in the proposed method with contrast enhancement using encryption and decryption. The 2 peaks values are selected for hidden purpose. Which is used to surely find out the 2 highest peak values. In the proposed approach is also used for the military and medical areas also. For the sake of histogram specification the image is used. The histogram values analogize to that image pixel value. The proposed approach is used in the color images. For the sake of increasing the enhancement to use the contrast enhancement

method. It is more important than storing the PSNR value high. The contrast enhancement put up the light on visual inspection through medical or satellite images and there by fulfilled the desires too. It is a known fact that lesser value is visible. Visibility of the image is improved and till now there is no other better technique which we can follow for the enhancement in contrast.

For providing high security for the whole system XOR-Encryption and XOR-Decryption techniques used. The Reversible Data Hiding techniques providing with high efficiency and high security.

### References

- [1] Nosrati \* Ronak Karimi Mehdi Hariri," Reversible Data Hiding:Principles, Techniques, and Recent Studies". World Applied Programming, Vol (2), Issue (5), May 2012. 349-353ISSN: 2222-2510©2011 WAP journal. www.waprogramming.com
- [2] Subhanya RJ (1), Anjani Dayanandh N (2)" Difference Expansion Reversible Image Watermarking Schemes Using Integer Wavelet Transform Based Approach". International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 International Conference on Humming Bird ( 01st March 2014)
- [3] X. Zhang, "Separable reversible data hiding in encrypted image," IEEETrans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.
- [4] O. Elbadawy, M. R. El-Sakka, and M. S. Kamel, "An information theoretic image-quality measure", Proceedings of the IEEE Canadian Conference on Electrical and Computer Engineering, vol. 1, pp. 169–172, 1998.
- [5] N. Taneja, B. Raman and I. Gupta, "Combinational domain encryption for still visual data", Journal of Multimedia Tools and Applications, DOI 10.1007/s11042-011-0775-4, (2011).
- [6] K. C. Ravishankar and M. G. Venkateshmurthy, "Region Based Selective Image Encryption", International Conference on Computing & Informatics, ICOCI 06, IEEE, Kuala Lumpur, (2006).
- [7] I. Ozturk and I. Sogukpınar, "Analysis and Comparison of Image Encryption Algorithms", Journal of transactions on engineering, computing and technology, vol. 3, (2004), pp. 38.
- [8] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.
- [9] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.
- [10] D. M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," IEEE Trans. Image Process., vol. 16, no. 3, pp. 721–730, Mar. 2007.
- [11] M.-Z. Gao, Z.-G. Wu, and L. Wang, "Comprehensive evaluation for HE based contrast enhancement techniques," Adv. Intell. Syst. Applicat., vol. 2, pp. 331–338, 2013.
- [12] Y. Yang, X. Sun, H. Yang, C.-T. Li, and R. Xiao, "A contrast-sensitive reversible visible image watermarking technique," IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 5, pp. 656–667, May 2009



# IJRDO