Improved Reversible Data Hiding in Encrypted Image Using Block Histogram Shifting with RBHSM

Pallavi Singh

M.E Scholar, Department of Electronics and Communication Engineering,
University Institute of Technology, RGPV, MP, India.

Abstract : Histogram shifting method based image data hiding is advanced technique to secure image. The information or data transfer from one end to another end using internet is very easy, quick and correct. But security issue is a major challenge for confidential data transfer. In this paper, an efficient reversible data hiding method for encrypted image based on block histogram shifting is proposed, which includes image encryption, reversible data hiding in encrypted domain, and hidden data extraction. The cover image is first partitioned into non-overlapping blocks, and then the pixel values of each block are encrypted by modulo operation. A bit shifting histogram is the generalized ways for image data hiding and improves robustness of encrypted image. Proposed method enhances the quality of the encrypted image and data or information hiding. Mean square error and peak signal to noise ratio is also calculated and find better than existing BHS method.

IndexTerms –Encryption, Decryption, Data Hiding, PSNR, Reversible, Block Histogram Shifting, Watermarking.

I. INTRODUCTION

In the past few years, a considerable number of data hiding schemes for encrypted images or videos have been reported in the literature [2–10]. However, in these schemes, the original cover cannot be recovered completely without distortion due to data embedding. Strictly speaking, cloud service providers are not entitled to introduce permanent distortion, especially medical and military images. Consequently, many researchers show their interests in developing reversible data hiding in encrypted images (RDH-EI). Due to reversibility, the original image can be fully recovered after extracting the secret information.

However, the privacy and security of the digital media that resides on the cloud server may be questionable, since cloud data center is managed by a third party cloud server. One of the best ways to ensure the security and confidentiality is to encrypt the media. The user first converts the sensitive content into unintelligible form before uploading it to the cloud such that no information is revealed at all. All the processing and calculation in the cloud are performed in the cipher-text domain, and the processing result is provided to the user [1]. The authorized terminal user who has the decryption key can obtain the plaintext data after decrypting. Under this specific circumstance, the cloud service provider is not authorized to access the plaintext content. However, the effective management and reliability protection of massive cipher-text data in the cloud has become an urgent problem to be solved. Data hiding in encrypted domain is a new research field, which can directly embed some additional messages such as owner identity or authentication data, directly into an encrypted data for effective management or tamper detection purposes.

Reversible data hiding process are secure image data that hides information in cover images and data hiding system also needs secret communication. It is a method to hide extra message into cover media with a reversible approach accordingly that the original image and data cover content can be absolutely restored after extraction data or information of the hidden message. Traditionally, image data hiding is used for secret communication. Some Important applications, the embedded carriers or images are further encrypted to prevent the carrier or image from being analyzed to disclose the attendance of the embedment. Other applications could be for when the owner of the carrier or image might not want the other someone, including image data hider, to be familiar with the content of the image carrier before data hiding is actually performed, such as military images or secret medical images. This Condition, the content or data owner has to encrypt the content or data before passing to the data hider for information or data embedment. The receiver side can extract the embedded message and recover the innovative image. Many reversible data hiding have been proposed newly.

II. NEED OF DATA HIDING

Due to various applications of digital image data hiding, therefore data security is needed in image transmission. Some of the application is discussed below-

A. Copy Control Watermark may contain information required by the content owner that decided the policy of copying the digital content. The information contained by the watermark may specify “content may not be copied” or “only one copy” etc. subsequently, the devices used for copying the content may be required by law to contain watermark detector, which follows directives given by the content owner.

B. Authentication Watermark is hiding information used to provide authentication. Anyone provide wrong watermarked image or data then destroy entire image the watermark or leads to wrong watermark image after extraction.

C. Broadcast Monitoring Automatic identification of owners of data may be required to be done and used in systems responsible for monitoring the broadcasts. This may help in deciding the royalty payments. It also helps in ensuring that commercials of a particular advertiser are played at right time and for a right duration.

III. PROPOSED METHOD

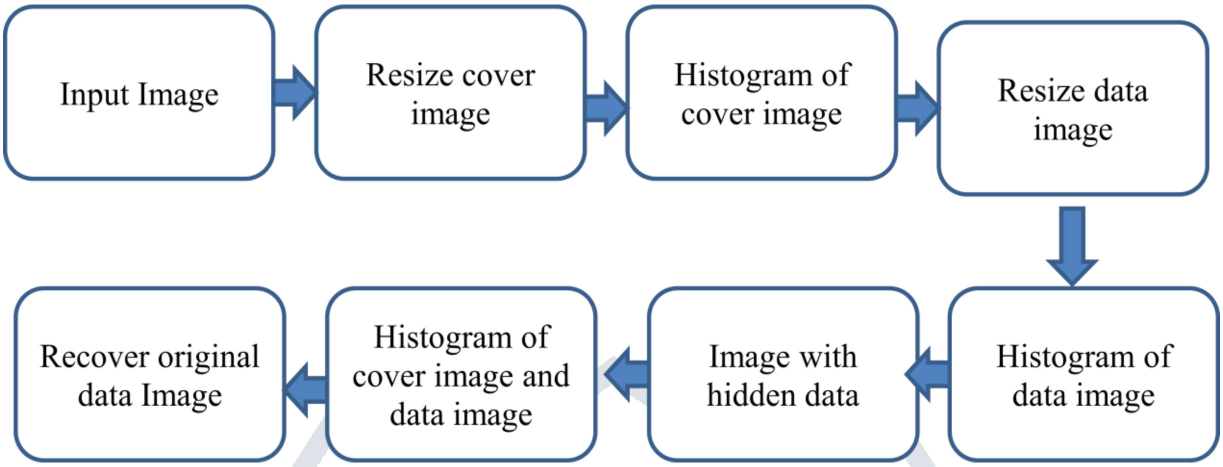


Figure 1: Flow Chart

Proposed method is a reversible bit histogram shifting method (RBHSM)based on bit shifting using data hiding in encrypted image based on bit shifting histogram and proposed method a is robustness is good as compare existing method block histogram shifting (BHS).our proposed method base on bit shifting through in histogram shifting method. The proposed scheme consists of 3 steps.

(i) The ownership of the host image encrypts the image by using a suitable encryption in bit change by histogram shifting.

(ii) The data image hides the data by host image by using another data image hiding through into host image.

(iii) Host image and data image both are embedding well-built and generated the watermarked image.

(iv) Extract data image into watermarked image. The receiver can access the data image as well as reconstruct the data image by using the respective decryption.

(v) Generate output.

The proposed framework aims to perform following three main operations-

(i) Encrypted image generation.

(ii) Data embedding in encrypted image.

(iii) Data extraction and image recovery.

First two operations will be performed at transmitter side and third will be at receiver side. For achieving this secrete data embedding algorithm is applied in the reverse order so as to separate the secrete data from watermarked image. And improve robustness of watermarking image and it is data of the host image can be recovered and reliable and it is providing strong robustness, data hiding ability, data authentication. This technology have advanced and almost of the people like using the internet because the primary medium to transfer information from one end to another end overall the world. The information or data transfer one end to another end using internet very easy, quick and correct. But different issues with sending information or data over the internet are that the security threat. In this process non-public or confidential information will be hacked are modified original information or data. Existing method block shifting histogram (BSH) based on block shifting so image are visible and low robustness. It is a very important requirement information security and it is also important requirement transfer information through internet and safety. There are several analysis process techniques related with internet security likes image data hiding, watermarking, cryptography, and steganography. Proposed method a bit shifting histogram is the generalized ways for image data hiding and improves robustness of encrypted image. Our proposed method enhances the standard of the encrypted image and data or information hiding. It is good security & privacy and data image recovery. In information hiding in encrypted image and highest robustness, so security of encrypted image also as maintaining the standard of original image during transfer and exchange of original image or image data

ALGORITHM:

Step1: Read a grayscale image as cover image (I). Begin load host image Hi (i,j) , here i is Colum ,j row and image as pixel values (0,1) .

Step 2. Host image Hi (i,j) is covert into gray scale image Gi (i,j) and resize.

Step3. Apply on Proposed Method on Gray scale image Gi (i,j) then generate image encrypt Ei (i,j).

Step4. Image encrypt Ei (i,j).and data image Di (i,j) both are Embedding and generate watermarked image Wi(i,j).

Step5. Extract data image Di (i,j) into Watermarked image Wi(i,j).

Step6. Generate output base on PSNR and MSE. Peak-Signal to Noise Ratio (PSNR)

1. The PSNR is most commonly used as a measure of quality of reconstruction of lossy compression codec's (e.g., for image compression).
2. The signal in this case is the original data, and the noise is the error introduced by compression.
3. When comparing compression codec's it is used as an approximation to human perception of reconstruction quality, therefore in some cases one reconstruction may appear to be closer to the original than another, even though it has a lower PSNR (a higher PSNR would normally indicate that the reconstruction is of higher quality)

$$PSNR = 10log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

MAX_I=Maximum value of pixel in Original image

m=No. of Row in Original image
n= No. of Column in Original image

STEPS:

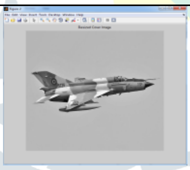
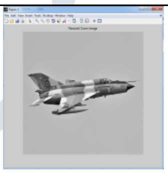
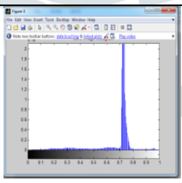
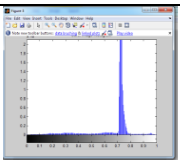
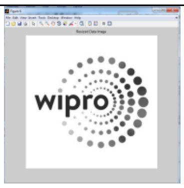
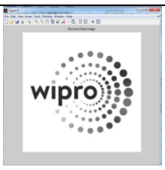
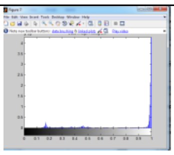
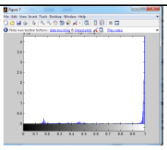
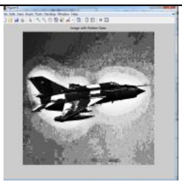
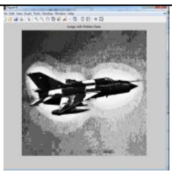
1. Read Original Image from current directory.
2. Read Noisy Image from current directory.
3. If Original Image is equal to Noisy Image then PSNR is 100%.
4. Find out difference between Original Image & Noisy Image.
5. Find out Mean Square Error by using above formula.
6. Find out maximum value of Pixel in Original Image.
7. Find out Peak Signal to Noise Ratio.

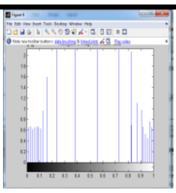
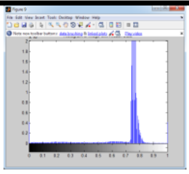
IV. SIMULATION RESULT

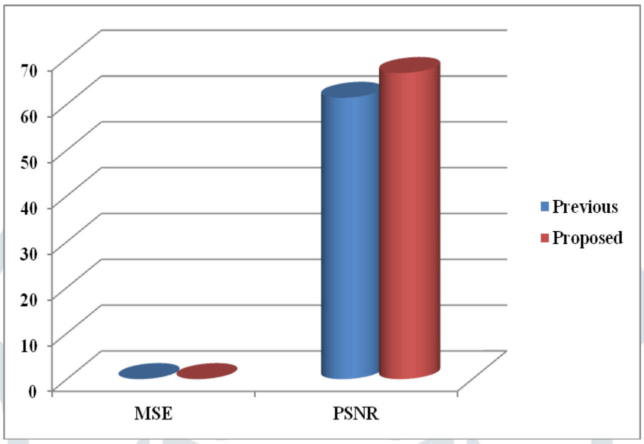
Reversible Data Hiding in Encrypted Image Using Block Histogram Shifting approach is simulating by using MATLAB 8.3.0.532 version. Image processing tool box are taken to script writing according to working procedure.

Now, first collect samples images from internet source. In re-size MiG-21_aircraft cover_image1 and re-size Wipro-logo data_image2 both are convert into histogram and embedding process using proposed method. It generates minimum error as compare to the existing block histogram shifting method. Proposed approach also gives better PSNR values than existing BHS.

Table 1: Simulation Result between BHS and RBHSM

Process	Previous Method (BHS)	Proposed Method (RBHSM)
Resize cover image		
Histogram of cover image		
Resize data image		
Histogram of data image		
Image with hidden data		

Histogram of cover image and data image		
Recover original data Image		
MSE	0.0930	0.0018
PSNR	25.4372	64.7696



Graph 1: Performance comparison

Graph 1 presents comparison chart of previous and proposed work in terms of MSE and PSNR. It is clear that proposed method gives significant better result than previous.

Table 2: Simulation Results

Sr. No	Image Name	BHS Method		RBHSM Method	
		MSE	PSNR	MSE	PSNR
1	Lena	0.0158	40.0155	0.0062	49.3313
2	Flower	0.282	26.0155	0.182	35.3313
3	Airplane	0.0930	25.4372	0.0018	64.7696

V. CONCLUSION

In this paper, an efficient approach is presented for data hiding. A specific RBHSM operation is utilized to hide the image, which can preserve less MSE and high PSNR. Since the embedding process is done on encrypted data, our scheme preserves the confidentiality of content. Data extraction is separable from image decryption; i.e., the additional data can be extracted either in the encrypted domain or in the decrypted domain. Experimental results show that the visual quality of marked decrypted image is very high and that the achieved PSNR is enough to embed some additional data. On the other hand, real reversibility can be achieved, which means that the secret data and original image can be restored without any error. Future works will focus on determining the optimal modification on the histogram to achieve the best rate-distortion performance.

REFERENCES

1. Zhaoxia Yin, Andrew Abel, Xinpeng Zhang,Bin Luo, Reversible Data Hiding In Encrypted Image Based On Block Histogram Shifting " IEEE ,2016.
2. Chauhan Usha, Singh Rajeev Kumar, "Digital Image Watermarking Techniques and Applications: A Survey", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 3, March 2016.
3. J. Zhou, W. Sun, L. Dong, et al., "Secure reversible image data hiding over encrypted domain via key modulation," IEEE Trans. on Circuits and Systems for Video Technology, vol. 26, no. 3, pp. 441-452, Mar. 2016.
4. Jiantao Zhou, Weiwei Sun, Li Dong,Xianming Liu, Oscar C. Au,and Yuan Yan Tang, "Secure Reversible Image Data Hiding over Encrypted Domain via Key Modulation", IEEE transactions on circuits and systems for video technology,2015.
5. B.Lei, E.L.Tan, S.Chen, D.Ni, T.Wang, H.Lei, Reversible watermarking scheme for medical image based on differential evolution", Expert Systems with Applications, Vol. 41, (7), pp. 3178–3188, 2014.

6. M.S Hwanga , L.Y. Tsengb ,LC Huang, “A reversible data hiding method by histogram shifting in high quality medical images”, Journal of Systems and Software, Vol. 86, (3), pp. 716–727, 2013.
7. Ashwind S , Ganesh K , Gokul R and Ranjeeth Kumar C, Secure Data Transmission Using Reversible Data Hiding”, International Journal of Computer Science and Information Technologies, Vol. 5 Issue 2 pp. 861-1863 , 2014.
8. Nutan Palshikar, Prof. Sanjay Jadhav, “ Lossless Data Hiding using Histogram Modification and Hash Encryption Scheme”,International Journal of Emerging Technology and Advanced Engineering,ISSN 2250-2459, Volume 4, Issue 1, 2014.
9. Mithu Varghese,Teenu S Jhon, “ A Survey on Separable Reversible Data Hiding in Encrypted Images”, International Journal of Computer Applications Advanced Computing and Communication Techniques for High Performance Applications ,0975 – 8887,2014.
10. L. R. Mathew, A. C. Haran V., “Histogram Shifting based reversible data hiding”, IJETT, pp. 482-485, 2014.
11. X. Zhang, “Separable reversible data hiding in encrypted image,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.
12. Siva Janakiraman, Suriya.N, Nithiya.V, Badrinath Radhakrishnan, Janani Ramanathan and Rengarajan Amirtharajan, " Reflective Code for Gray Block Embedding," Proceedings of the International Conference on Pattern Recognition, Informatics and Medical Engineering,IEEE, pp: 215-220, 2012.
13. I. J. Cox, M. L. Miller, and J. A. Bloom, Digital Watermarking and Steganography, Morgan Kaufmann, 2nd edition, 2007.
14. Z. Ni, Y. Shi, N. Ansari, and W. Su, “Reversible data hiding,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 16, no. 3, pp. 354–362, 2006
15. Rini.J, 4th Semester M.Tech, Dept. of Computer Science and Information Systems FISATAngamaly, Kerala, India “Study on Separable Reversible Data Hiding in Encrypted Images” International Journal of Advancements in Research & Technology, Volume 2, Issue 12, December-2013 Copyright SciResPub. IJOART, 2013.
16. K. A. Navas, M. C. Ajay, M. Lekshmi, T. S. Archana, and M. Sasikumar, “DWT-DCT-SVD based watermarking,” in Communication Systems Software and Middleware and Workshops, COMSWARE 2008. 3rd International Conference on, 2008, pp. 271–274, 2008.