Result Analysis of Reversible Data Hiding in Encrypted JPEG Bitstream

Pooja Dwivedi
M.Tech Scholar
Department of Electronics & Communication Engineering,
IES, Bhopal, India

Sonulal
Asst. Professor
Department of Electronics & Communication Engineering,
IES, Bhopal, India

Deepak Mishra
Asst. Professor
Department of Electronics & Communication Engineering,
IES, Bhopal, India

ABSTRACT

In this paper to identify usable bits suitable for data hiding so that the encrypted bit stream carrying secret data can be right decoded. The secret message bits area unit encoded with error correction codes to achieve a perfect data extraction and image improvement. the propose technique aims at encrypting a IMAGE bit stream into a appropriately prepared structure, and embed a secret message into the encrypted bit stream by slightly modifying the IMAGE stream. In this paper result analysis of reversible data hiding method.

Keywords

Encrypted image, image recovery, information hiding, JPEG, reversible data hiding

1. INTRODUCTION

Data hiding could be a method of hiding information behind the cover media. That is, the information hiding method has 2 sets of information, one set of the embedded information and another set of the cover media information.[2] the connection between these 2 sets of information characterizes completely different applications. For instances, in covert communications the hidden information could often be relevant to the cover media. In authentication but the embedded information are closely associated with the cover media. [3]In most cases data information hiding the cover media experiences some distortion because of data hiding and inverting back to the original media isn't possible. That's some permanent deformation has arise to cover media even later than the hidden data has been extracted out. It's employed in medical and law forensics where data secrecy should maintain.

RDH tasks in encrypted pictures would be more natural and much easier which leads us to the completely unique framework, “reserving room before encryption (RRBE)”. [1] The information extraction and image recovery are identical to specified Framework VRAE. Typical RDH algorithm rule are ideal for reserving room before encryption and may be simply applied to Framework RRBE to accomplish better presentation evaluate with techniques from Framework VRAE. [1] This is often because in this new framework, follow the customary concept that 1st lossless compresses the redundant image content (e.g., using excellent RDH techniques) then encrypts it with regard to protective privacy. Next elaborate a practical methodology maintain the Framework “RRBE”, that mainly consists of 4 point: generation of encrypted image, data hiding in encrypted image, information extraction and image recovery. [4] The reserving operation adopt within the proposed methodology may be a traditional RDH approach.

Reversible data hiding (RDH) is methods that embed secret information into a cover image in a reversible manner. On the receiving aspect, the hidden message is extracted and therefore the original image perfectly remodeled. This technique is very useful in applications such as medical and military imaging where the original image must not be altered once the embedded data are extracted.

Digital watermarking, typically stated as data hiding, has recently been planned as a promising technique for the data assurance. Because of information hiding, however, some permanent distortion could occur and thus the original cover medium might not be able to be reversed specifically even when the hidden information are extracted out. Following the classification of information compression algorithms, this sort of information hiding algorithms is stated as lossy data hiding.

Digital steganography and watermarking are the 2 sorts of data hiding technology to offer hidden communication and authentication. The word steganography is derived from the Greek words “stegos” that means “cover” and “grafia” that means “writing” defining it as “covered writing”. In contrast to Cryptography, wherever the enemy is allowed to observe, intercept and modify messages while not having the ability to violate certain security premises, the goal of steganography is to hide a secret message within harmless medium in such some way that it's impossible even to find that there's a secret message. The medium for data hiding is additionally known as as cover, host and carrier. To human eyes, information typically contains known forms, like pictures, videos, sounds and text. Most net data naturally includes unwarranted headers too. These are media exploited using steganograpy techniques. pictures are the most powerful medium for information hiding as a result of of the limitation of Human visual System(HVS). Basic plan of watermarking is to embed covert data into a digital signal, like digital audio, image, or video, to trace ownership or protect privacy. Information hiding is used in an oversized quantity of information formats within the digital world of nowadays. the most common information formats used are .bmp, .doc, .gif, .jpeg, .mp3, .txt and .wav in the main as a result of of their quality on the net.

2. THEORY

Reversible data hiding (RDH) could be a technique that embeds secret information into the cover, like military or medical images, by slightly modifying the info of the cover; and on the receiver side, the original image may be lossless recovered [1,2]. Several RDH ways are planned for digital pictures, like the general RDH framework by redundancy compression [3], the difference expansion (DE) technique [4], the histogram shifting (HS) technique [5], so on [6-8]. Historically, these ways are useful for embedding information into the images that are open to the data-hider. However, in some situations, the owner of the cover is unwilling to show the data of the original image to the data-hider. for instance, to protect the patient’s privacy, content of the medical image may be unavailable for the technician WHO embeds the data into the medical image. These applications need RDH embedding information into the encrypted version of the original image.

This work proposes a new separable RDH theme for encrypted pictures. we tend to make full use of the disordered histogram and also the encrypted image, And outline an n-nary information hiding theme for data hiding. The planned is separable, during which the secret bits may be extracted severally from the stego. the original image may be perfectly recovered using the embedding key and also the encoding key, and might be or so recovered if only the encryption key's obtainable. Compared to the existing RDH ways for encrypted images, the planned technique mostly im-proves the embedding capacity than the ways in [9] ~ [11], and needs no room-reserving operation like for the senders.

3. METHODOLOGY

3.1 Image Encryption

A new image encryption theme is usually recommended during this Letter. Since digital images are sometimes represented as 2 dimensional arrays, so as to disturb the high correlation among pixels, Arnold cat 2d map or chaotic 3D cap map is usually used to shuffle the positions of the pixels within the image [3]. different from the 2d or 3D chaotic map that's used to shuffle the pixel positions of the plain-image, the encryption planned here consists of 2 processes, firstly, we tend to shuffle the image supported total image shuffling matrix generated by using logistical map, then encrypt the shuffled image by using hyper chaos.

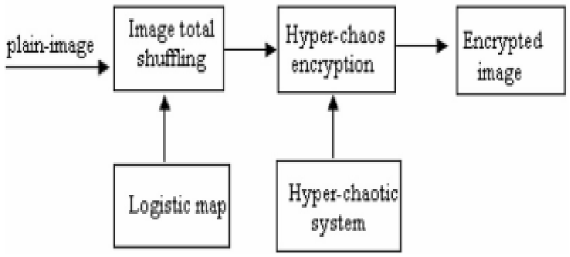


Fig.1 Block diagram of image encryption

Image encryption schemes are increasingly studied to satisfy the demand for real-time secure image transmission over the web and through wireless networks. Traditional image encryption algorithmic rule like data encryption standard (DES) has the weakness of low-level efficiency once the image is large [1] the chaos-based encryption has suggested a new and efficient way to deal with the intractable problem of fast and highly secure image encryption.

3.2 Embedding and Extraction Flow Charts

The proposed reversible data hiding and extraction algorithms can be illustrated by the flow charts shown in figs. 2 and 43, respectively.

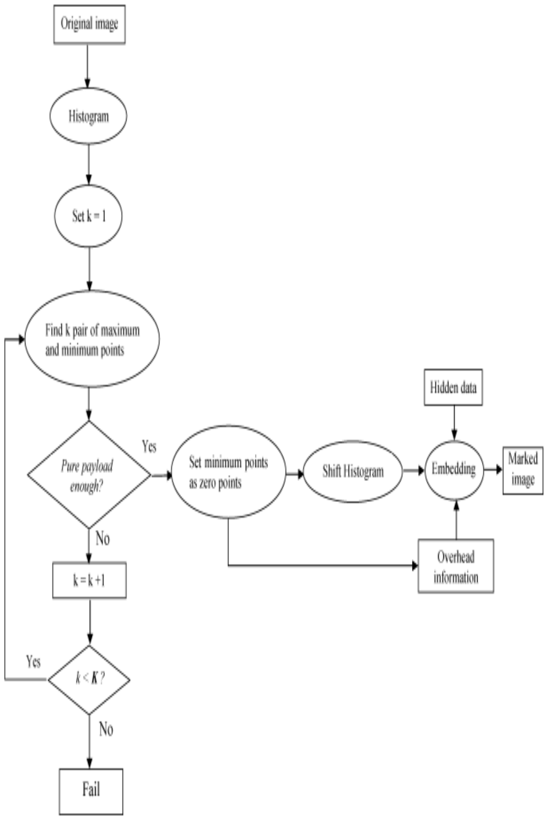


Fig 2 Data Embedding Algorithm

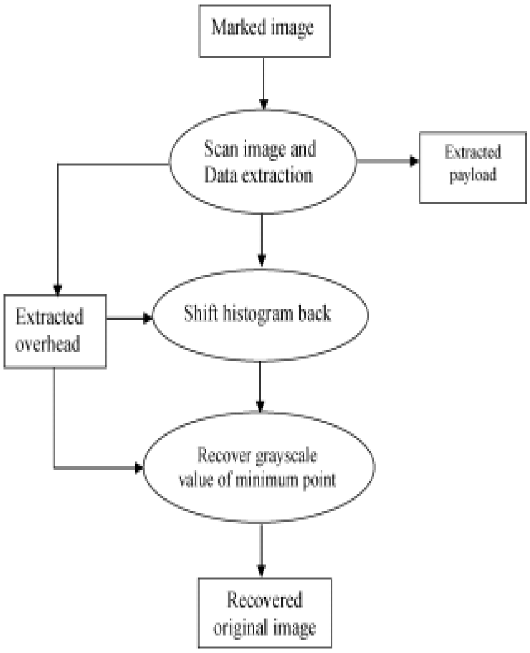


Fig. 3 Data extracting algorithm for one pair of maximum and minimum points

3.3 Image Recovery

In this part, we will think about the 3 cases that a receiver has only the data-hiding key, only the encryption key, and each the data-hiding and encryption keys, severally. Note that due to the pseudo-random pixel selection and permutation, any attacker while not the data-hiding key cannot get the parameter values and also the pixel-groups, so cannot extract the embedded information. Moreover, though the receiver having the information-hiding key will with success extract the embedded data, he cannot get any information concerning the original image content.

4. RESULT

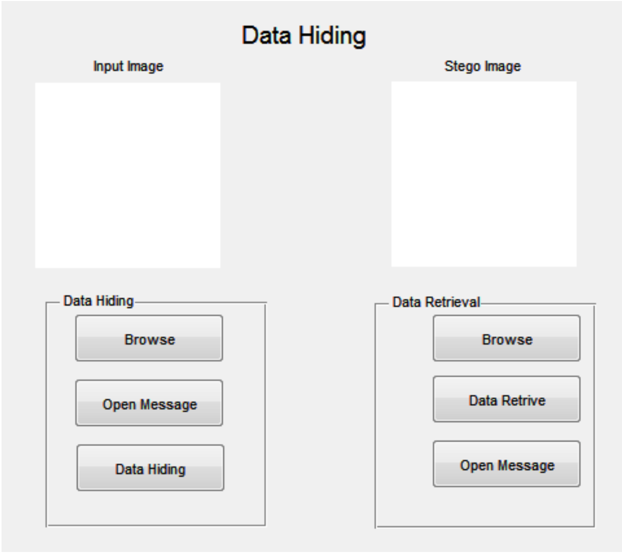


Fig.4 Data hiding figure window

When we run the main program file then open this data hiding fig.4 window.

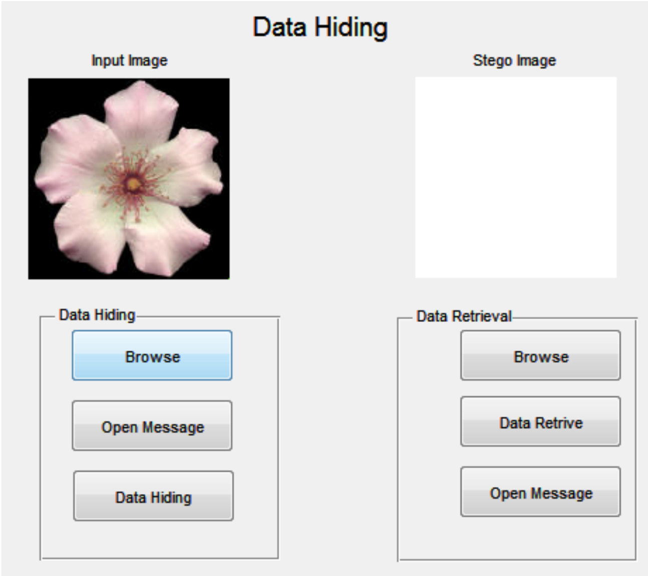
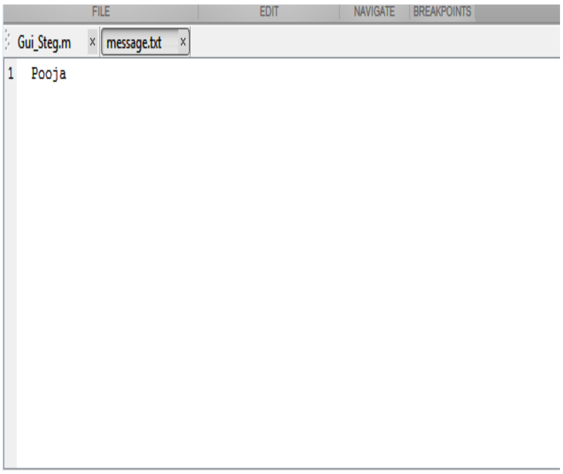


Fig.5. Data hiding input

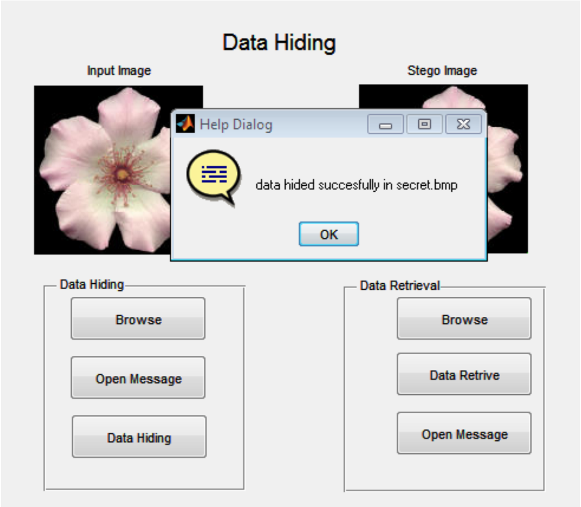
In this fig.5 we take the input image for data hiding. Firstly brows the bmp input image.



```
Pooja
```

Fig.6 Message text editor window

In this fig. 6 we write the text message which text message is hide.



data hided succesfully in secret.bmp

Fig.7 Data hiding

In this fig.7 we are hide the message then press the data hide button then open the dialog box that is our data is hided successfully in secret.bmp.

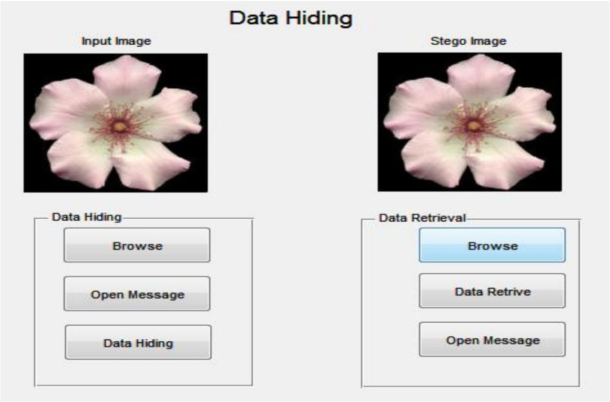
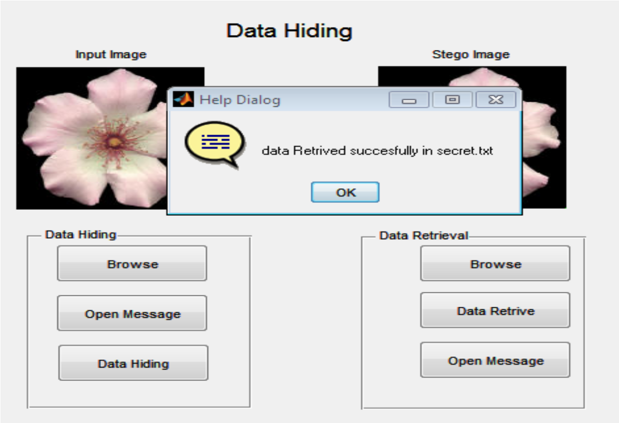


Fig.8 Stego image input

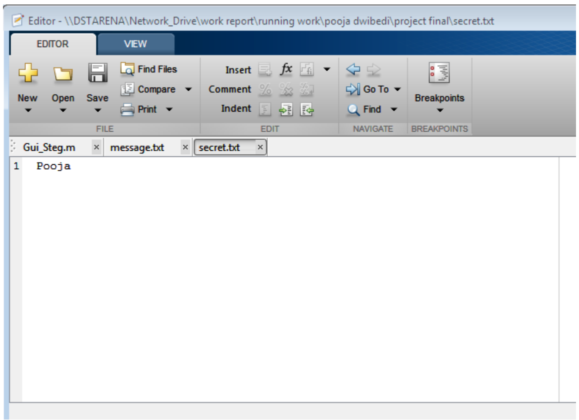
In this fig.8 again secrete bmp image are browse for data retrieval.



data Retrived succesfully in secret.txt

Fig.9 Data Retrieval Window

In this fig. 9 we are press the data retrieve button are press then open the dialog box in our window that is we know that our data is successfully retrieved.



Editor - \\DSTARENA\Network_Drive\work report\running work\pooja dwibedi\project final\secret.txt

```
Pooja
```

Fig.10 Output window

In this fig.10 we know that which data that is text message is hided in the input bmp image. Then we get the output in same data.

Table 1 Comparison Table

Algorithm	PSNR(dB)
Base Paper	38.00
Proposed	67.00

5. CONCLUSION

In this paper result analysis of reversible data hiding in encrypted JPEG bit stream. During which we will find the expected outcome including in results. During this paper image encryption and completely different techniques used for improve results. As compare to previous work. Then the performance parameters like Accuracy and PSNR for the image are calculated. By using the embedding and encryption keys, the receiver will dig out the included data and fully recover the image used initially.

6. REFERENCES

[1] Hao-Tian Wu, Jean-Luc Dugelay and Yun-Qing Shi, \“Reversible Image Data Hiding with Contrast Enhancement”, IEEE Signal Pro. Letters, vol. 22, no. 1, pp. 81-85 Jan. 2015

[2] Xinpeng Zhang, “Reversible Data Hiding in Encrypted Image”, IEEE Signal Pro. Letters, vol. 18, no. 4, pp. 255-258 April 2011.

[3] Wei-Liang Tai, Chia-Ming Yeh, and Chin-Chen Chang, “Reversible Data Hiding Based on Histogram Modification of Pixel Differences”, IEEE Trans. on Circuits and Systems for Video Techno., vol. 19, no. 6,pp. 906-910 June 2009.

[4] Mehmet U. Celik, Gaurav Sharma, A. Murat Tekalp and Eli Saber, “Reversible DATA Hiding” IEEE ICIP pp. 157-160. 2002.

[5] Chia-Chen Lina, Wei-Liang Tai and Chin-Chen Chang “Multilevel reversible data hiding based on histogram modification of difference images” Pattern Recognition 41 pp. 3582 -- 3591 2008.

[6] Z. Ni, Y. Shi, and N. Ansari et al., “Reversible data hiding,” IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar.2006.

[7] 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.

[8] L. Luo et al., “Reversible image watermarking using interpolation technique,” IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 187–193,Mar. 2010.

[9] X. L. Li, B. Yang, and T. Y. Zeng, “Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection,” IEEE Trans. Image Process., vol. 20, no. 12, pp. 3524–3533, Dec.2011.

[10] X. Zhang, “Reversible data hiding with optimal value transfer,” IEEE Trans. Multimedia, vol. 15, no. 2, pp. 316–325, 2013.

[11] W. Zhang, B. Chen, and N. Yu, “Improving various reversible data hiding schemes via optimal codes for binary covers,” IEEE Trans. Image Process., vol. 21, no. 6, pp. 2991–3003, Jun. 2012.

[12] N. Memon and P. W. Wong, “A buyer-seller watermarking protocol,” IEEE Trans. Image Process., vol. 10, no. 4, pp. 643–649, Apr. 2001.

[13] 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.

[14] 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.

[15] X. Zhang, “Reversible data hiding in encrypted images,” IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.