www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-5, Issue-3, June 2017
Research Paper

Int. J. Sc. Res. in
Network Security
and Communication

ISSN: 2321-3256

# A Novel RDH Scheme for Real Time Applications

**Uma Shivalli**[1*], **B.K. Sujatha**[2]

[1*]Dept. of Telecommunication Engineering, M S Ramaiah Institute of Technology, Banglore, India
[2]Dept. of Telecommunication Engineering, M S Ramaiah Institute of Technology, Banglore, India

*Corresponding Author: umashivalli9@gmail.com*

Received 16th Mar 2017, Revised 25th Mar 2017, Accepted 24th May 2017, Online 30th Jun 2017

***Abstract***— Significance of Multimedia security is ever increasing due to threat of duplication, modification and manipulation of the multimedia data like photograph and documents. In the recent days reversible data hiding(RDH) in encrypted images is gaining widespread application in the digital world. Use of RDH for real time application helps in losslessly recovering the original image after the embedded data is extracted and image content's confidentiality is also protected. In this paper we propose a novel method of RDH for real time multimedia data by reserving room. Performance analysis is done for different embedding rates. Experimental results show that, this novel method ensures better security of the multimedia data and protects the original image from manipulation by the data hider.

***Keywords***— Image encryption, Reversible data hiding, Histogram, data extraction, PSNR

## I. INTRODUCTION

In this computerized era, security of the interactive media information is gaining more importance. An effective means of privacy protection is image encryption. During encryption the original image is converted to an unreadable form by the encryption key. Data hiding in encrypted images, allows the data hider to access the encrypted image and vacate room for embedding data. It is difficult to manipulate the encrypted image to embed data. Hence it is more efficient and easy to reserve room for the data before encryption. One of the efficient algorithms to hide data is Reversible data hiding (RDH), by which the original cover can be losslessly recovered after the embedded message is extracted.

The content owner encodes the first uncompressed picture utilizing an encryption key to deliver a scrambled picture, and later, the data hider embeds extra information into the encoded picture utilizing a data hiding key. With an encoded picture containing extra information, a recipient decrypts the image utilizing the encryption key. Using data hiding key, he can further extract the embedded data. Data hiding can be done for sending secured data in military applications, defense, for hiding details of patients, for authenticating documents, digital photographs etc.RDH scheme for real time application helps in privacy protection and authorizing the content owner, the copyright to his multimedia data.

In this paper we propose a novel RDH scheme, by automating the whole process of embedding a data string using a data key, generating encryption and decryption key, analyzing the histogram of original and decrypted image and extracting the embedded data. Performance analysis of real time data is done in terms of PSNR for different embedding rates. Variation in image quality is analyzed based on varying embed rates.

## II. RELATED WORK

As to provide secrecy to pictures, encryption is a viable and well known means as it changes converts original information to a scrambled form. Although few RDH methods in encrypted images have been proposed, there are some unexplored applications if RDH can be applied to real time encrypted images. In recent years, several RDH schemes have emerged. In [10] proposed a general system for RDH. By first extracting compressible components of original cover and later compressing them losslessly, the saved space can be used to embed additional information. A more prominent technique depends on difference expansion (DE) [9], in which the distinction of every pixel gathering is extended, e.g., multiplied by 2, and consequently the LSBs of the difference are all zero and can be utilized for embedding messages.

Another promising system for RDH is histogram shifting (HS) [8], in which space is set aside for information inserting by shifting the bins of histogram of gray values. A few endeavors on RDH in encrypted pictures have been made. Zhang isolated the encrypted images into blocks. By flipping 3 LSBs of the half of pixels in each block, room can be reserved for the embedded information. The data extraction and image recovery proceed by finding which part has been flipped in one block. This process can be realized with the help of spatial correlation in decrypted image.

To isolate the data extraction from image decryption, Zhang saved out space for embedding information following the idea of compressing encrypted images. The method compressed the encoded LSBs to clear space for extra information by discovering parity check matrix, and the side data utilized at the receiver side is likewise the spatial correlation of decrypted images.

All the strategies attempt to vacate room from the encrypted pictures directly. However, since the entropy of encoded pictures has been maximized, these procedures can just accomplish small payloads or produce marked picture with low quality for large payload and each one of them are liable to some error rates on information extraction and image restoration. In spite of the fact that it can eliminate errors by error correcting codes, the pure payloads will be further consumed. The method proposed by Kede Ma[3] reserves room before encryption with a traditional RDH algorithm for standard images, and thus it is easy for the data hider to reversibly embed data in the encrypted image. This method can achieve real reversibility, that is, data extraction and image recovery are free of any error.

## III. PROPOSED WORK

Making room in encrypted images for the additional data to be embedded is difficult and might distort the original image. To protect the original image a novel method is incorporated in this paper. In Proposed method, the content owner reserves room before encrypting the image using Reserving room before encryption (RRBE) technique. Then the image is encrypted using the encryption key. The data to be hidden is embedded to the encrypted image by the data hider. The encrypted image with hidden data is sent to the receiver. At the receiver side, the data is extracted from the received image and original image is restored using the decryption key.For given embedding rates, the PSNRs of decrypted image are significantly improved; and range of embedding rates is greatly enlarged. The proposed method allows us to use any format of the image in which we want to store data i.e jpeg,png, pgm etc [1,2,3,4,5,6,7,8,9,10].

The block diagram for the proposed system is as shown in Fig 1. There are basically three steps in this system. Part I at the content owner side, Part II at the data hider side and Part III at the receiver side.

### A. Generation of Encrypted Image

In this module, to build the encoded picture, the main stage can be separated into two stages. Image Partition and Self Reversible Embedding followed by image encryption. Toward the starting, image partition step partitions original image into two sections and afterward, the LSBs of the least dominant channels in the image are reversibly embedded into the dominant channel with a standard RDH algorithm so that vacant LSBs can be utilized to accommodate messages; finally, encrypt the rearranged image to create its final version.

Encryption of the rearranged image is done using the simple XOR encryption key. It is a simple yet secure encryption algorithm to convert the original image to a scrambled form. It is in a unreadable form. The encryption key must be a numerical value. Encryption key is generated by a simple XOR operation. The same key has to be used at the receiver side as decryption key to decrypt the original image and get the original image.

During image partition stage, the size of the image is not disturbed. Depending on the amount of data to be hidden in the original image, LSB planes are selected into which auxiliary data can be embedded. The more LSB planes selected, more data can be embedded.

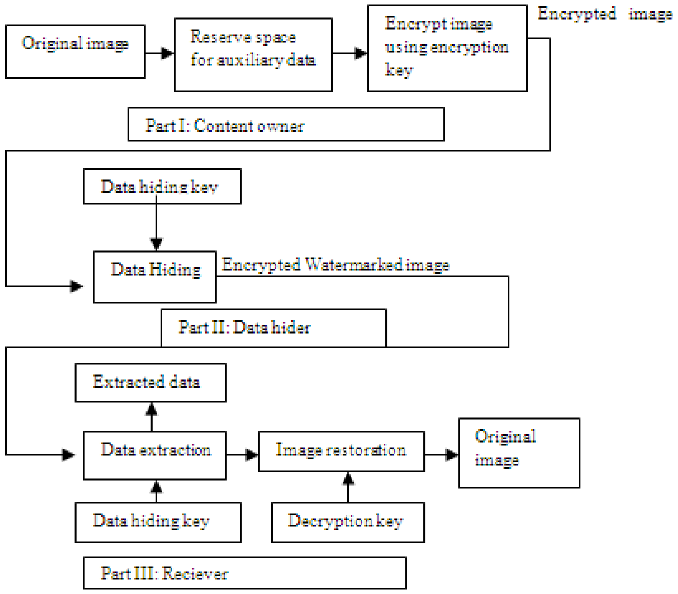


Fig 1: Framework for proposed system

### B. Data hiding in encrypted image

In this module,a content owner encrypts the original image using a standard cipher with an encryption key. After producing the encrypted image, the content owner hands over it to a data hider (e.g., a database manager) and the data hider can embed some auxiliary data into the encrypted image by lossless vacating some room according to a data hiding key.Then a receiver, maybe the content owner himself or an authorized third party can extract the embedded data with the data hiding key and further recover the original image from the encrypted version according to the encryption key.

### C. Data extraction and image recovery

In this module, Extracting Data from Encrypted Images to update individual data of pictures which are scrambled for securing customers' protection, a substandard database supervisor may just access the information concealing key and need to control information in encrypted domain. At the point when the database supervisor gets the information concealing key, he can unscramble and separate the extra information by directly reading the decrypted version. When requesting for updating information of encrypted images, the database manager, then, updates information through LSB replacement and encrypts up dated information according to the data hiding key all over again.

As the whole process is entirely operated on encrypted domain, it avoids the leakage of original content.

The secret data embedded by the data hider is extracted at the receiver side by using the same data hiding key which was used during hiding the data. The highly secure key ensures protection of the auxiliary data. The original image is also free from distortion after the embedded data is extracted from it.

### *D. Data extraction and image restoration*

In this module, after generating the marked decrypted image, the content owner can further extract the data and recover original image. Reversible hiding allows extraction of the original host signal and also the embedded message. There are two important requirements for reversible data hiding techniques: the embedding capacity should be large; and distortion should be low.These two requirements conflict with each other. In general, a higher embedding capacity results in a higher degree of distortion. An improved technique embeds the same capacity with lower distortion or vice versa. For the image restoration we have to follow the specified steps by which we can easily recover the original image. After the image encryption the image must be considered as an individual unit of work so we can fully concentrate on the watermarking technique and proceed further.

## IV. EXPERIMENTAL RESULTS

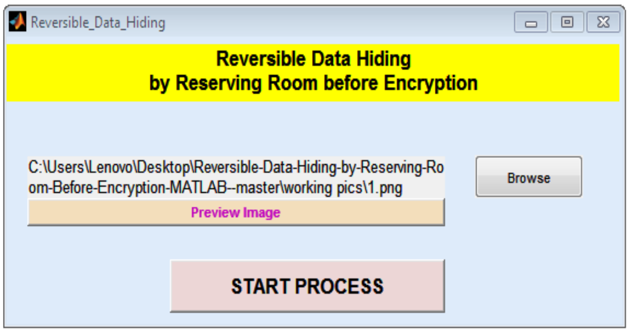
The performance analysis of this novel method for real time applications is done using the parameter of Peak signal to noise ratio (PSNR). PSNR of image hidden with data is calculated for varying embed data rates. The results are tabulated in Table 1 below.

Table I: PSNR Comparison for Various Embedding Rates

| PSNR Results(dB) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Embed Rate** | **0.005** | **0.01** | **0.05** | **0.1** | **0.2** | **0.3** | **0.4** | **0.5** |
| **Image 1** | **69.70** | **66.92** | **59.85** | **56.52** | **51.89** | **48.22** | **43.02** | **39.97** |
| **Image 2** | **72.23** | **69.05** | **62.26** | **59.48** | **56.40** | **54.27** | **52.94** | **51.94** |
| **Image 3** | **68.30** | **65.58** | **59.45** | **55.68** | **53.93** | **51.29** | **50.34** | **46.19** |
| **Image 4** | **68.65** | **65.95** | **59.60** | **57.14** | **54.61** | **52.55** | **51.67** | **48.83** |
| **Image 5** | **72.50** | **69.54** | **62.10** | **58.89** | **56.11** | **54.25** | **52.95** | **52.04** |

From the analysis Table above we can conclude that, PSNR varies along with the data embed rates. At lower embed rates, large data is not embedded into the original image, hence the original image is not corrupted much and PSNR remains high. Whereas at higher embed rates, large data is embedded into the original image and hence PSNR decreases. It can be observed that considerably better PSNR values are obtained even at higher data embed rates. All the images considered here are real time images of size 512x512 and are black and white images. Real time images could be either digital photographs or any documents.

In the proposed work we have automated the whole process of data embedding, encryption of the image, decryption of the image and data extraction using a Graphical user interface (GUI). Use of GUI makes it simpler and easier for the user to complete the whole process of data hiding for real time images. The results obtained are as follows.


Reversible_Data_Hiding

Reversible Data Hiding
by Reserving Room before Encryption

C:\Users\Lenovo\Desktop\Reversible-Data-Hiding-by-Reserving-Room-Before-Encryption-MATLAB--master\working pics\1.png

Fig 2: GUI of the entire process

Fig 3: Original image without hidden data

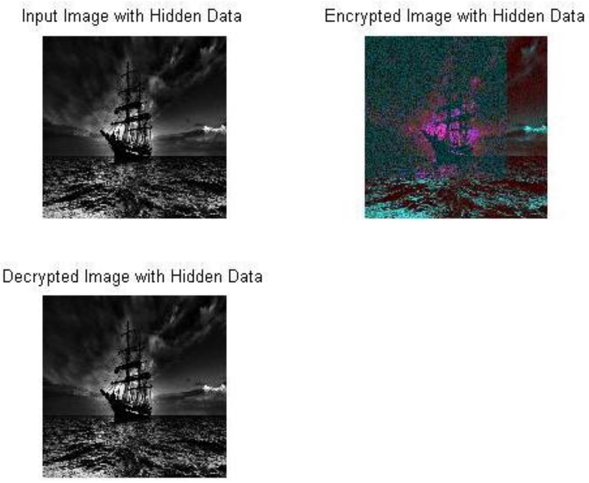

Input Image with Hidden Data
Encrypted Image with Hidden Data
Decrypted Image with Hidden Data

Fig 4: Original, encrypted and decrypted image with hidden data

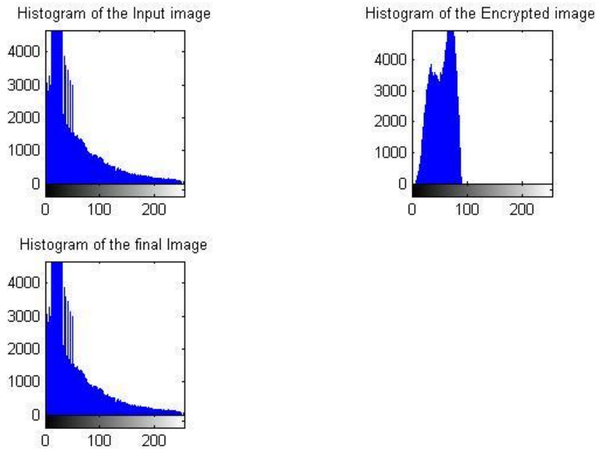


Fig 5: Histogram of the input, encrypted and final image.

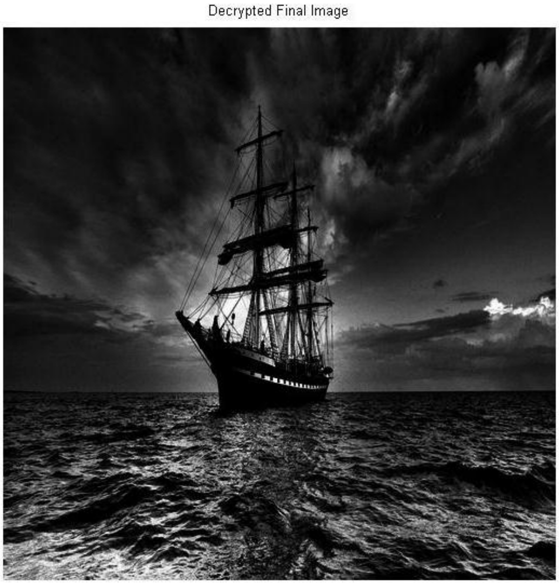
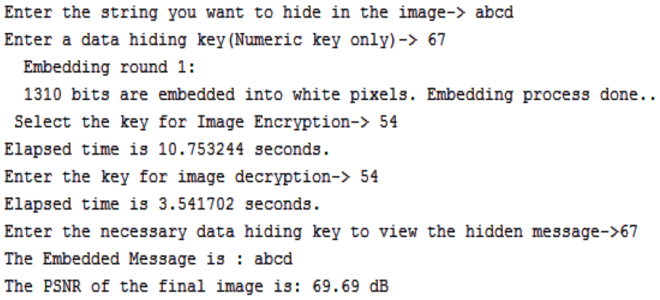


Fig 6: Final image after data extraction and decryption



```
Enter the string you want to hide in the image-> abcd
Enter a data hiding key(Numeric key only)-> 67
  Embedding round 1:
  1310 bits are embedded into white pixels. Embedding process done..
 Select the key for Image Encryption-> 54
Elapsed time is 10.753244 seconds.
Enter the key for image decryption-> 54
Elapsed time is 3.541702 seconds.
Enter the necessary data hiding key to view the hidden message->67
The Embedded Message is : abcd
The PSNR of the final image is: 69.69 dB
```

Fig 7: Interactive console to embed data string

## V. Conclusion

A novel RDH scheme by reserving room before encryption is designed and developed for real time applications like digital photography and documents. This scheme reduces the complexity in data embedding and achieves complete reversibility. Embed rates varying from 0.05 to 0.5 are considered. Various images are considered each of size 512x512. PSNR values for different embed rates are compared for various images. The GUI developed, automates the complete process and provides an interactive console to embed the data. Thus the proposed method is highly efficient and can be applied to several real time applications.

## References

[1] Xiaolong Li, Weiming Zhang, Xinlu Gui, Bin Yang, "*A Novel Reversible Data Hiding Scheme Based on Two-Dimensional Difference-Histogram Modification*", IEEE Transactions on Information forensics and security, Vol. 8, No. 7, pp.1-7, 2013.

[2] Shobha Elizabeth Rajan, Sreedevi P, "*Enhancing Visual Cryptography Using Digital Watermarking*", International Journal of Computer Sciences and Engineering, Vol.3, Issue.7, pp.152-156, 2015.

[3] Kede Ma, Weiming Zhang, Xianfeng Zhao, Nenghai Yu, Fenghua Li, "*Reversible Data hiding in Encrypted Images by Reserving Room before Encryption*", IEEE Trans. Inf. Forensics Security, Vol. 8, No. 3, pp. 826-832, 2013.

[4] W .Hong, T. Chen, H. Wu, "*An improved reversible data hiding in encrypted images using side match*", IEEE Signal Process. Lett., Vol.19, No. 4, pp. 199-202, 2012.

[5] X. Zhang, "*Separable reversible data hiding in encrypted image*", IEEE Trans. Inf. Forensics Security, Vol. 7, No. 2, pp. 826-832, 2012.

[6] 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, 2011.

[7] Zhi-Hui Wang, Chin-Chen Chang, Pei-Yu Tsai, "*Hiding Secret Data in an Image Using Codeword Imitation*", Journal of Information Processing Systems, Vol.6, No.4, pp.435-452, 2010.

[8] Akhila Sreenivas K. and Pretty Babu , "*An Approach for Data Hiding Technique Based on Reversible Texture Synthesis*", International Journal of Computer Sciences and Engineering, Vol.4, Issue.7, pp.81-85, 2016.

[9] Nitin Shelake and S. R. Durugkar , "*Extracting Hidden Data from Encrypted Images Using IWT*", International Journal of Computer Sciences and Engineering, Vol.3, Issue.5, pp.219-222, 2015.

[10] J. Fridrich and M. Goljan, "*Lossless data embedding for all image for-mats*", in Proc. SPIE Proc. Photonics West, Electronic Imaging, Secu-rity and Watermarking of Multimedia Contents, San Jose, CA, USA, pp. 572-583, 2002.