A Survey on Reversible Data Hiding

Ms. Sunita V. Pawar , Prof. N. G. Pardeshi

Abstract— **Reversible data hiding technique are techniques are used to hide secrete information inside cover image, as well as to recover the cover image after extraction of secrete message. Such techniques are used in medical, military, forensic applications etc. Because when information is shared by many people , privacy preservation becomes important for such data while transmission. To provide security for secrete information data hiding techniques are used . To recover the original image after extraction of the secrete message reversible data hiding techniques are used. RDH also gives better image quality as well as embedding capacity.**

Index Terms—**Reversible data hiding, privacy preservation, embedding capcity.**

I. Introduction

As Internet is growing rapidly, multimedia transmission becomes popular on Internet users. Now a days many services are also provided by cloud, So instead of Desktop applications people are interested in cloud services. Cloud services provides many application services as well as storage to the Internet users. Large amount of multimedia information stored as well as sheared by the user. For such services privacy preservation and authentication becomes important issue. So to achieve privacy some secrete message is sent inside the cover media for example in case of medical application sometimes we need to hide annotations related to image, then these annotations are considered as secrete message hidden inside the image. At the receiver side after extraction of secrete data image should be recovered. In such case reversible data hiding techniques are used, which recover original image after extraction of secrete message. There are many reversible data hiding techniques used are based on difference expansion, histogram shift. Generally these techniques are based on spatial relationship between the pixels. When RDH is applied on image algorithm can be measured by following criteria:

- Visual quality of image : This visual quality is measured by PSNR ratio in dB.
- Embedding capacity of image : EC is depend on secrete bits B hidden inside the image of size M X N.

Motivation behind Reversible data hiding is to achieve better embedding capacity as well as gives real reversibility for the cover image.

II. Different RDH Techniques

Tian [3] Introduce Reversible Data Hiding using Difference expansion in 2003 gives high capacity, high visual quality, reversible data embedding method for digital images. This method can be applied to digital audio and video. In this method difference of neighboring values are calculated and select some difference values for the difference expansion(DE). In the original image data related to authentication is will be embedded into difference values . This gives PSNR upto 44.20 at 0.1bpp.

In 2006 Zhicheng Ni et. al.[4] use histogram shifting for the first time. Which can embed a large amount of data (5–80 kb for a 512 X 512 X 8 grayscale image) while keeping a very high visual quality for all natural images, specifically, the PSNR of the marked image versus the original image is guaranteed to be higher than 48 dB. It utilizes the zero or the minimum point of the histogram and slightly modifies the pixel grayscale values to embed data. Basic idea is to shift each pixel only one grayscale value after data embedding so that visual quality of stago image can be retained. This provides PSNR higher than Tian's method. But limits the embedding capacity .

In 2010 Lixin Luo. Et. al.[5] proposed reversible watermarking scheme based on additive interpolation-error expansion, which features very low distortion and relatively large capacity. Different from previous watermarking schemes, we utilize an interpolation technique to generate residual values named interpolation-errors and expand them by addition to embed bits. The strategy is efficient since interpolation-errors are good at de correlating pixels and additive expansion is free of expensive overhead information. But this method increase in size of image.

In 2011 Xiaolong Li[6] proposed Reversible Watermarking Based on Adaptive Prediction-Error Expansion and Pixel Selection, to increase payload and low distortion.

Adaptive embedding: Prediction error which embeds data uniformly, first divide image pixels into two parts to get "flat regions" and "rough regions" according to local complexity; then adaptively embed 2 bits into each expandable pixel of flat regions and 1 bit into that of rough regions. When the capacity is high, this avoids expanding pixels with large prediction-errors and reduces embedding impact by decreasing the maximum modification to pixel values. Moreover, adaptive embedding can greatly increase the capacity in a single embedding pass. The maximum embedding rate (ER) of conventional PEE cannot exceed 1.0 bit per pixel (BPP).

Manuscript received June , 2015.

*Ms. **Sunita V. Pawar**, PG Computer Science Student , Savitribai Phule Pune University.*

***Prof. N. G. Pardeshi,**, Project Guide Computer Engineering Department, SRES COE Kopargaon, Savitribai Phule Pune University .*

- Pixel selection: As an intermediate step of PEE, to select relatively smooth pixels (i.e., pixels located in smooth area) and ignore the rough ones. Which means the rough pixels may remain unchanged, and only smooth pixels are expanded or shifted. In this way, compared with conventional PEE, a more sharply distributed prediction-error histogram is obtained, and a larger proportion of prediction-errors in the histogram are expanded to carry hidden data. So the amount of shifted pixels is diminished, which leads to a better image quality. It can embed larger payloads with less distortion.

Kim et. al. proposed Watermarking Algorithm Using Sorting and Prediction in 2009.This algorithm employs prediction errors to embed data into an image. A sorting technique is used to record the prediction errors based on magnitude of its local variance. Using sorted prediction errors and, if needed, though rarely, a reduced size location map allows us to embed more data into the image with less distortion.

In 2011 Zhang[8] proposed reversible data hiding in encrypted images, in this method content owner encrypts the original uncompressed image using an encryption key to produce an encrypted image, and then a data hider embeds additional data into the encrypted image using a data-hiding key though he does not know the original content. With an encrypted image containing additional data, a receiver may first decrypt it using the encryption key, and the decrypted version is similar to the original image. According to the data-hiding key, he can further extract the embedded data and recover the original image from the decrypted version. So security is provided to data as well as cover image while transmission.

In some methods RDH is applied on encrypted images, but this cause error while recover cover image. These methods does not achieve real reversibility. To achieve real reversibility Zhang et. al.[1] proposed Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption in march 2013. In this method novel reversible data hiding methods are applied on original images, this creates room for secrete message, then image is encrypted with data hiding key. This provides security for cover image, so that authorized user can only recover the original image. Then data hider hide secrete message. Receiver can extract message with data hiding key as well as he/she can recover original image with image encryption key or both. The RRBE method can achieve real reversibility, that is, data extraction and image recovery are free of any error. This also gives better quality of image and better embedding capacity than previous method.

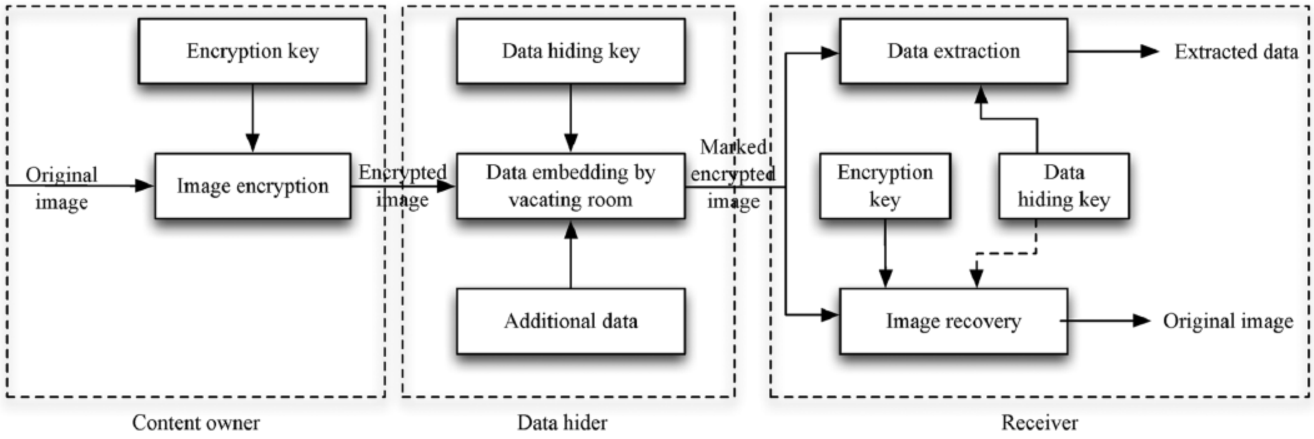

Fig1. Vacating Room After Encryption (VRAE).

III. RDH IN ENCRYPTED IMAGES

To provide security Reversible Data Hiding methods are applied on Encrypted Images proposed by Zhang [8][9]. RDH in Encrypted images can be applied in two ways:

1. Vacating Room After Encryption (VRAE).
2. Reserving Room Before Encryption (RRBE).

As shown in fig.1 First original image is encrypted at the content owner side. Then RDH is applied at the data hider side, to create vacant room for secrete message. Receiver can extract data with data hiding key and recover original image. To achieve reversibility vacating room from encrypted images is difficult.

To achieve real reversibility method proposed by Zhang et.al. [1],Reserving Room Before Encryption(RRBE).In this method RDH is applied on original image at the content owner side as shown in Fig.2 . Then image is encrypted and send to data hider to hide secrete data. By reserving room prior to image encryption at content owner side, data hider can hide secrete information easily as well as the receiver can recover original image. Data extraction and image recovery is identical in both techniques. User can apply any standard RDH technique to RRBE to create room for secrete message. As to provide security for image and secrete data different keys are used, So that user can either extract data or recover image by providing data hiding key and image encryption key. As RDH is applied on original image content owner can find the region to embed the data, to improve the quality of image.

This gives the better performance also achieve better embedding rate as well as improves image quality in terms of PSNR ratio.

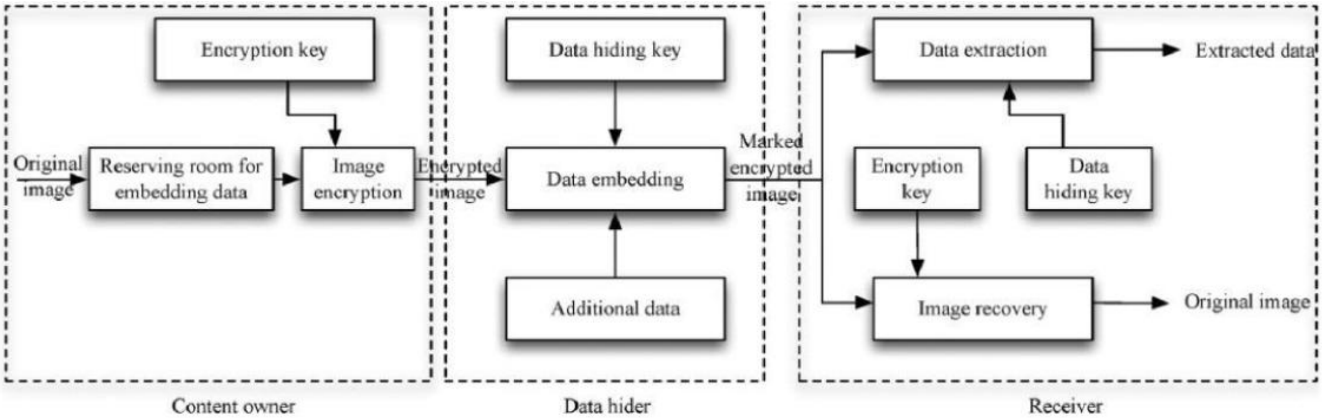

Fig.2 Reserving Room Before Encryption (RRBE).

IV. Conclusion

Reversible Data Hiding techniques provides the reversibility for cover image. Internet user can send data securely inside cover media with the help of data hiding techniques. RHD can be applied on encrypted image so that data hider does not know the original content. Major issues for RDH technique are Image quality and embedding capacity. User can apply RDH to achieve better embedding capacity as well as good image quality in acceptable range 30 dB to 60 dB for 8 bit pixel data.

Acknowledgment

I would like to express my sentiments of gratitude to all who rendered their valuable help for the successful completion of the paper. I am thankful to my guide Prof. N. G. Pardeshi, for his guidance and encouragement in this work. I am also thankful to Prof. D. B. Kshirsagar , Head of Department, Computer Engineering, S. R. E. S. COE, Kopargaon.

I also express my appreciation and thanks to all my colleagues and family members who knowingly or unknowingly have assisted and encouraged me for the completion of the paper.

References

[1] Kede Ma, Weiming Zhang, Xianfeng Zhao, Member, IEEE, Nenghai Yu, and Fenghua Li.,‖ Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption‖ IEEE Transactions On Information Forensics And Security, Vol. 8, No. 3, March 2013.

[2] Chin-Chen Chang, Thai-Son Nguyen, and Chia-Chen Lin, International Journal of Network Security, Vol.16, No.3, PP.201-213, May 2014,‖ Reversible Image Hiding for High Image Quality based on Histogram Shifting and Local Complexity‖

[3] J. Tian, ―Reversible data embedding using a difference expansion,‖ IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.

[4] Z. Ni, Y. Shi, N. Ansari, and S. Wei, ―Reversible data hiding,‖ IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.

[5] Lixin Luo, Zhenyong Chen, Ming Chen, Xiao Zeng, and Zhang Xiong-Reversible Image Watermarking Using Interpolation Technique,IEEE transactions on Information Forensics and Security,Vol. 5,no. 1, March 2010

[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, Dec. 2011.

[7] Vasiliy Sachnev, Hyoung Joong Kim, Jeho Nam, Sundaram Suresh, and Yun Qing Shi, -Reversible Watermarking Algorithm Using Sorting and Prediction, IEEE transactions on Circuits and Systems for Video Technology, Vol. 19, No. 7, JULY 2009

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

[9] X. Zhang, ―Separable reversible data hiding in encrypted image,‖ IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.