Survey on Reversible Data Hiding in Encrypted Images by Reversible Image Transformation (RIT)

Silpa Rajan, Minu Lalitha Madhavu

Abstract: To increase the security of the data, an image is in taken in an encrypted format. This process is followed in earlier techniques like RRBE, VRAE etc. In RIT, instead of converting it into an encrypted format, it is converted into another image. Hence this image appears simply an anotherimage which is difficult for other users to decrypt. Using contrast – enhancement RDH method, data is then hidden in to the image. The advantage of using RDH is that there occurs no loss of data and contrast of the image is highly enhanced. Hence visual quality of the image is increased. The embedded data is extracted after which it is decrypted to recover the original data.

Keywords: prediction error expansion, reversible data hiding, RRBE (reserving room before encryption), RIT (reversible image transformation), VRAE (vacating room after encryption).

I. INTRODUCTION

In Reversible Data Hiding, data can be embedded at the sender and the receiver it can be recovered without any loss of data. The data can be redeemed without any loss of data which makes it suitable for sensitive fields like medicine and military. The different modes used in RDH are Difference Expansion, whereby visual noticeability and hiding capacity is highly exalted. Also contrast enhancement is another method for RDH, in which the distortion is kept low keeping embedding capacity to a higher value[i]. Also RDH uses methods likeRRBE, VRAE proposing that in RRBE and VRAE the recovery of images and its extraction pauses no error. In RIT, the image is converted to another image difficult for a intrigued party to decrypt thereby increasing the security multiple folds compared to other RDH techniques. Inthe prediction-error method, the difference between pixel and the predicted value,is used to embed a bit '1' or '0' by expanding it additively or leaving it unaltered.The various methods of RDH discussed above can recover the data without any loss which gives a greater security to the data embedded into the cloud server.

II. RELATED WORKS

W. Hong, T. Chen, and H. Wu[ii], dictates about a method DCT for RDH in an encrypted images. In RDH ,the restoration of the original cover content in a reversible manner occurs after the extraction of the hidden message. Block smoothness is used for the extraction of the data. In this letter, smoothness of the data is measured which uses the closest match scheme thereby decreasing the error rate of the extracted W. Zhang, X. Hu, X. Li, and N. Yu[iii], Stated Reversible Data Hiding (RDH) on the basis of pixel-value ordering (PVO) and prediction error expansion. Here the minimum and maximum pixel block is explained and is modified such that PVO of each block is kept unalterable. Here either minimum or the maximum valued pixels are predicted first which is modified together in a way that its either unchanged or decremented or incremented by one.in value at the same time. More blocks are utilized to exploit image redundancy in a better way. Also, other mechanisms like advisable payload partition and pixel block selection is utilized to optimize payload partition and embedding performance is optimized in terms of capacity distortion behavior.

W. Zhang, X. Hu, X. Li, and N. Yu's[iv] paper states that secret messages which restores the original image without distortion can be extracted. Its used in many applications like medical image applications and multimedia archive management. Mostly, histogram applications is used in most of RDH literatures. Difference pair mapping (DPM) is incorporated into two- dimensional histogram and prediction – error expansion. This improves the image quality by 3 db with same quality of images. At the same quality of images , The embedding quality of images can be enhance even to 30, 000 bits.

X. Zhang discuss about[v] a separable reversible data hiding in encrypted images. Using an encryption key a content owner can encrypt the original image which is uncompressed in the first phase. The LSBs of the encrypted image is then compressed by a data hider to create a sparse space using a data hiding key to accommodate some additional space. If the receiver too knows the key for data hiding for an encrypted image containing additional data , he /she can extract the additional data even without knowing the image content. At the receiver end , with the aid of the encryption key , the received data can be decrypted an image similar to the original one can be obtained , but without the additional data. If the receiver has both the encryption and data hiding key, both the additional data and the original content can be obtained without any error. Here the property of spatial correlation in natural images is used when the additional data content in not too large.

I.-C.Dragoi and D. Coltuc[vi], predicts about Prediction – error expansion (PEE) which is composed of two steps:-In the first step, by utilizing pixel prediction strategies, a sharp prediction- error (PE) is generated. In the second step, through expanding and shifting the PE histogram, secret messages are embedded. In the previous PEE methods, two of the above steps are treated independently by focusing on pixel prediction thereby obtaining a sharp PE histogram by aiming at histogram modification aiming at embedding performance such that a given PE histogram.

Revised Version Manuscript Received on February 13, 2017.

Silpa Rajan, M. Tech. Scholar, Department of Computer Science and Engineering, Kerala University, (Kerala) India.

Minu Lalitha Madhavu, Assistant Professor, Sree Buddha College of Engineering, Kerala University, (Kerala) India.

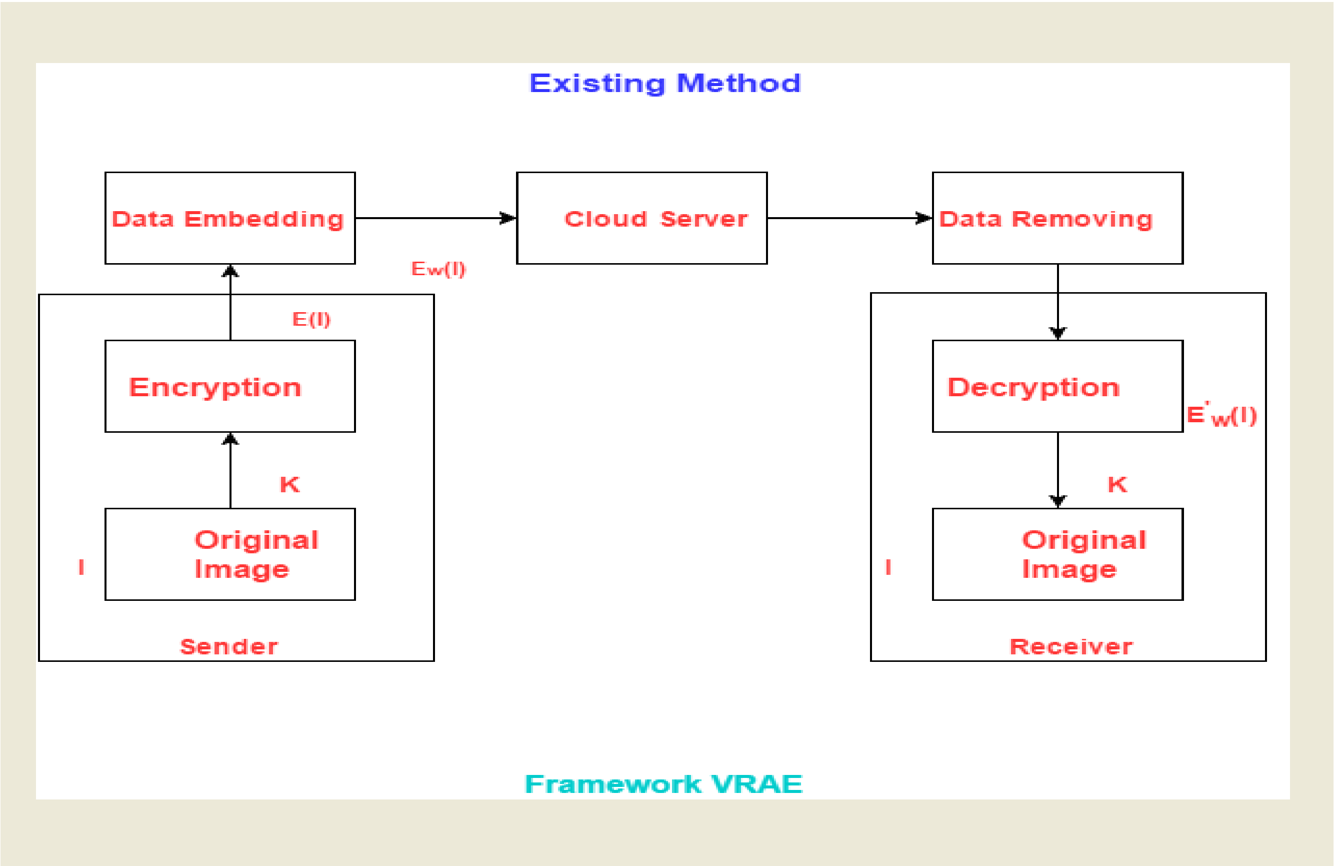
A pixel prediction method based on minimum rate criterion on the basis of minimum rate criterion for reversible data hiding establishing consistency in two steps where a novel histogram modification scheme presented is approximated to get the optimal embedding performance on the generated PE sequence. Through the experiments, it is proposed that the previous state- of- art is outperformed by the proposed method in terms of both prediction accuracy and final embedding performance.

X. Hu, W. Zhang, X. Li, and N. Yu [vii]explains about a two-step clustering thereby clustering thereby optimizing pixel prediction method for Reversible Data Hiding (RDH) exploiting self –similarities and group structural information of non-local images. Based on RDH schemes , prediction-error expansion (PEE) play an important role. Here based on the structural similarities of patches of image, the authors use a pixel clustering method. For each pixel associated with a pixel an optimized pixel predictor from the group context is predicted. From the experimental results, the proposed method is proven to be better than the state- of- art counterparts like median edge predictor, gradient- adjusted predictor, or simple rhombus neighbourhood etc. W.Zhang ,X. Hu, and N. Yu [vii] advances about rate- distortion method for RDH based on recursive code construction (RCC). The optimal transition probability matrix (OTPM) has to be determined for finding out the rate-distortion or for executing RCC. Some methods like square- error- distortion or Li Norm. A unified framework to explore OTPM was used to calculate rate- distortion bound thereby extending it to any distortion metrics.

This paper [viii] explains about online images. The online images obtained from Apple’s iCloud platform which offers automatic backup in iPhone. Though phishing and brute- force-attack guessing , the information stored in the iCloud was obtained ,where the information includes user names ,passwords, and security questions. From 2014, it was indicated that someone created “appleprivacysecurity” , a fake id for extracting secret information from celebrities. But by August 31st, the photos which was passed privately for at least a minimum of weeks were released privately. Even it was claimed that unreleased photos and videos do exist. “Collector”, the hacker responsible for the leak distributed leaked images on 4chan image boards and An-on in exchange for Bitcoin. By the end, all these leaked images and videos were made available online in Imgur and Tumblr. Reddit ,a link sharing centre was the major source of this activity where these photos were shared publicly by about 10, 000 people in a single day. Even though criticization were raised against the Reddit administrators. This allegation was banned by “The Fappening ”subreddit copyright issues on September 7th .They also stated that their workload was heavy.

This paper [ix] proposes two methods which are discussed below:

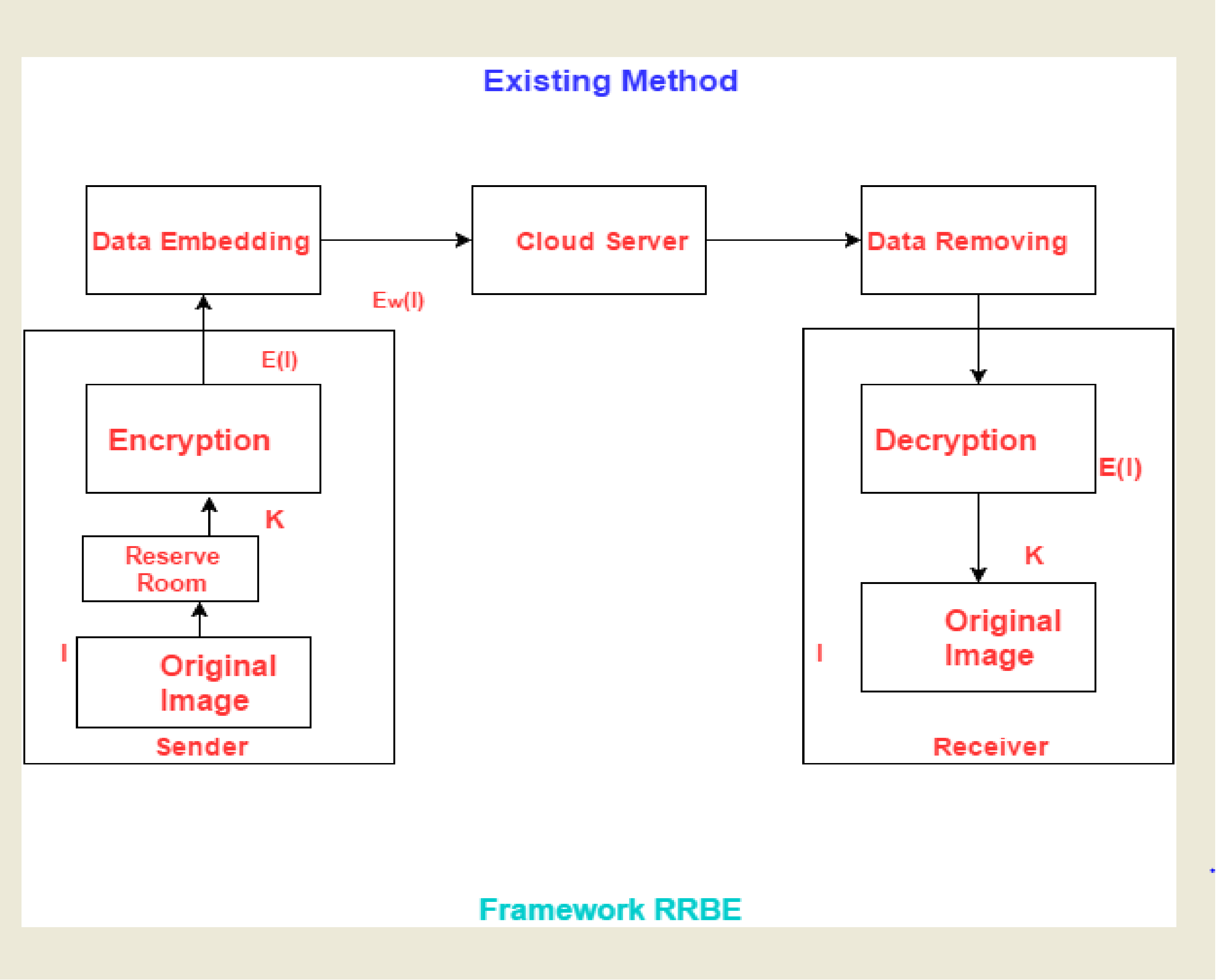
III. VACATING ROOM BEFORE ENCRYPTION (VRAE):



(i) **Framework VRAE**

This paper proposes that the image I is encrypted into E(I) with the aid of a key by the image owner. The encrypted image E(I) is compressed by embedding data into the cloud server which receiver by the cloud server which may be an authorized third party generating I through joint decompression and decryption with a key K. Hence E'w (I) may be just E(I) or a modified version obtained by removing the data embedded into it. The compression based RDH method used by cloud server should be specified by the receiver as the cloud server cannot restore E(I) from E'w(I).This in turn proves that RDH method is receiver relatedgeneratesEw(I) which is stored into the cloud. On a retrieval request, E'w (I) is returned to the

IV. RESERVING ROOM BEFORE ENCRYPTION (RRBE):



(ii) Framework RRBE

Here first a room is reserved for the image I by the image owner who embed data into the reserved room and generates E(I) with a key k and then sends it to cloud server which embeds it to the reserved room generating Ew(I) .This is then stored into the cloud from which data can be extracted by the server for further purposes. When the image I is to be retrieved by the receiver (authorised user) , Ew(I) is restored from E(I) by the cloud server which can be send to the user to decrypt the image using the key K. Here the complexity is occurred by the sender who reserves room for RDH by exploiting redundancy within the image ie, RDH used by the cloud should be specified within the sender. Therefore, RDH is sender related. Z. Qian and X. Zhang[x] points out a method called distributed source coding (DSC) for reversible data hiding in encrypted images. Using a stream cipher, the content owner encrypts the original data and the data hider can compress a series of selected bits from the encrypted image thereby creating room for secret data. Slepian –Wolf coding is done on the selected data bit series using low density parity check (LDPC) codes. Using the embedding key, the image receiver can extract only the secret bits at the receiver side. With the help of en encryption key only, he/she can recover the original image with high quality using an encryption algorithm. But by having both embedding and encryption keys, someone can extract the secret data while recovering the original image using distributed source coding thereby outperforming the previous methods.

W. Zhang, K. Ma, and N. Yu[xi] talks about a novel reversible data hiding in encrypted images. To embed additional data for finding errors, pixels are estimated before encryption.

For the rest of the pixels, a benchmark encryption scheme (AES) is used and for estimating errors a special encryption scheme is used. One can extract from the encrypt images or embed in the additional data with no knowledge from the original image. For all the images, error free extraction of errors and recovery of images occurs. In the aspect of embedding errors versus PSNR (Peak to Signal Ratio) the feasibility and efficiency of the proposed method increases.

This paper[xii] , authors like W. Zhang , K. Ma, and N. Yu talks about a new image transformation which is reversible enhancing the quality of the encrypted image, also restoring the secret image in lossless manner. The data is delegated to the cloud. Using any RDH methods, additional data can be embedded into the encrypted image into the cloud. For the security of the data, authors incorporated RIT or Reversible Image Transformation in encrypted images. In RIT, we transmute original image data into same sized target images. The transmuted data in the image appears like the same sized encrypted image. In this the transmutation takes place in the form of micro blocks of same size thereby increasing security. This in turn also makes the quality of the image to many folds. Authors like Y. Lee and W. Tsai’[xiii] are talking about an advanced computer art image called secret-fragment- visible mosaic image. Here small fragments of a given image is converted into a target image in a mosaic form thereby embedding the image visibly and secretly in a mosaic form. The above property is used in secure keeping of secret images. For the creation of a mosaic image from a secret colour image,1-D colorscale is obtained by transforming 3 –D colour space. Finding a similar tile image to fit into each block of the target image, a fast greedy search algorithm is used. Randomly – selected pixels are used for fitting the information of the tile image fitting sequence using a secret key by a lossless LSB scheme. The secret image can’t be retrieved back without the secret key. The above method can also be extended for grey scale mosaic images proven using experimental results thereby enhancing the feasibility of the method.

V. CONCLUSION

Sending data over the cloud server requires high security to prevent a third party from accessing the secret information hidden in it. Reversible Data Hiding acts as an efficient method for this purpose. This paper mainly explains RDH based on prediction error expansion. As the data is hidden in the form of images, it does not attract the attention of the curious cloud. It appears as an image to the person who is trying to access it. Once the data is embedded in to the image, it is encrypted at the sender, while at the receiver side, is decrypted to obtain the original image. The RDH process is irrelevant to both sender and receiver as it is considered to be semi- honest.

ACKNOWLEDGEMENT

I am grateful to my project guide and PG cordinator Prof.Anil A.R,HOD for his interminable support and for providinbg the indispensible adjuncts like Internet,Books etc. Also, I am appreciative to the staff members of Dept: of Computer Science and Engineering, Sree Buddha College of Engineering, Alappuzha.

REFERENCES

1. SilpaRajan, MinuLalithaMadhavu, “Reversible Data Hiding by Histogram Modification for Image Contrast Enhancement ” , International Research Journal of Engineering and Technology, vol .3 Issue 11 pp.761-766 November 2016
2. W. Hong, T. Chen, and H. Wu, “An improved reversible data hiding in encrypted images using side match,” IEEE Signal Process. Lett., vol. 19, no. 4, pp. 199–202, Apr. 2012
3. W. Zhang, X. Hu, X. Li, and N. Yu, “Recursive histogram modification: Establishing equivalency between reversible data hiding and lossless data compression,”IEEETrans.ImageProcess.,vol.22,no.7,pp.2775–2785, Jul. 2013.
4. B.ou, X. Li, Y. Zhao, R. Ni, and Y. Shi, “Pairwise prediction-error expansionforefficientreversibledatahiding,”IEEETrans.ImageProcess., vol. 22, no. 12, pp. 5010–5021, Dec. 2013.
5. X. Zhang, “Reversible data hiding in encrypted images,” IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.
6. Ioan – CatalinDragoi, DinuClotuc ,”Local – prediction – based difference expansion reversible watermarking ”, “IEEE Trans. On Image Processing, vol.23, no.4, pp 1779- 1790, April 2014 ”
7. X. Hu, W. Zhang, X. Li, and N. Yu, “Minimum rate prediction and optimized histograms modification for reversible data hiding,” IEEE Trans. Inf. Forensics Security, vol. 10, no. 3, 653–664, Mar. 2015.
8. 2014 celebrity photo hack [Online].Available:http://en.wikipedia.org/wiki/2014_celebrity_photo_hack
9. K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, “Reversible data hiding in encrypted images by reserving room before encryption,” IEEE Trans. Inf. Forensics Security, vol. 8, no. 3, pp. 553–562, Mar. 2013.
10. Z. Qian and X. Zhang, “Reversible data hiding in encrypted image with distributed source encoding,” IEEE Trans. Circuits Syst. Video Technol., vol. 26, no. 4, pp. 636–646, Apr. 2016.
11. W. Zhang, K. Ma, and N. Yu, “Reversibility improved data hiding in encrypted images,” Signal Process., vol. 94, pp. 118–127, Jan. 2014.
12. W. Zhang, K. Ma, and N. Yu, “Reversibility improved data hiding in encrypted images,” Signal Process., vol. 94, pp. 118–127, Jan. 2014.
13. X. Zhang, “Reversible data hiding in encrypted images,” IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011
14. Y. Lee and W. Tsai, “A new secure image transmission technique via secret-fragmentvisible mosaic images by nearly reversible colour transformation,” IEEE Trans. Circuits Syst. Video Technol., vol. 24, no. 4, pp. 695–703, Apr. 2014.

AUTHORS PROFILE

SilpaRajan, received B.Tech degree in Computer Science and Engineering from Mahatma Gandhi University, India. Now pursing M Tech degree in Computer Science and Engineering from Kerala University, India.

Minu Lalitha Madhavu, received B.Tech degree in Computer Science and Engineering from Rajeev Gandhi Institute of Technology, MG University, India received M .Tech degree in Technology and Management from Kerala university, India. Currently she is the Assistant Professor at Sree Buddha College of Engineering, Kerala University, India.