RESULT ORIENTED APPROACH: RESERVING ROOM BEFORE ENCRYPTION IN REVERSIBLE DATA HIDING IN ENCRYPTED IMAGES

Mr.Pankaj Uttamrao Washimkar[1], S.T.Khandare[2]
[1]Department of CSE, Babasaheb Naik College of Engg, Pusad
Email: pankaj.washimkar1@gmail.com
[2]Department of CSE, Babasaheb Naik College of Engg, Pusad,

***Abstract*—** *Recently, reversible data hiding (RDH) in encrypted images is the most important property that the original cover can be lossless recovered after embedded data is extracted while protecting the image content's confidentiality. Due to use of embedding data by reversibly vacating room from the encrypted images, this method may be subject to some errors on data extraction and image restoration. In this paper, we propose method by reserving room before encryption with a traditional reversible data hiding algorithm, and thus it is easy for the data hider to reversibly embed data in the encrypted image. This method can achieve real reversibility,data extraction and image recovery are free of any error. according to this method, it can embed more times as large payloads for the same image quality as the previous methods, such as for PSNR dB.*

***Keywords*— Reversible data hiding (RDH), Histogram shift (HS), Difference expansion (DE).**

I. INTRODUCTION

Reversible data hiding in images is a method, by which the original cover can be losslessly recovered after the embedded message is extracted. This method is widely used in medical, military imagery and law forensics, where no distortion of the original cover is allowed [1] [7]. In recent studies, many new RDH techniques have emerged. General framework for Reversible data hiding (RDH) can first extract compressible features of original image cover and then compressing them losslessly, spare space can be saved for embedding auxiliary data. Another method is difference expansion (DE)[2], which expanded the difference of each pixel group e.g., multiplied by 2, and thus the least significant bits (LSBs) of the difference are all-zero and can be used for embedding messages. Another strategy for RDH is histogram shift (HS), in which space is saved for data embedding by shifting the bins of histogram of gray values [6][8]. The state-of-art methods usually combined difference expansion DE or histogram shift HS to residuals of the image, e.g., the predicted errors, to achieve better performance [8].

For providing confidentiality for images, encryption is another popular method as it converts the original and meaningful content to incomprehensible one. Another most popular reputation-based trust-management scheme enhanced with data coloring (a way of embedding data into covers) and software watermarking, in which data encryption and coloring offer possibilities for upholding the content owner's privacy and data integrity. Suppose a medical image database is stored in a data center, and a server in the data center can embed notations into an encrypted version of a medical image through a RDH technique. With the notations, the server can manage the image or verify its integrity without having the knowledge of the original content, and thus the person's privacy is protected. On the other hand, a doctor, having the cryptographic key, can decrypt and restore the image in a reversible manner for the purpose of further diagnosing. Some attempts on RDH in encrypted images have been made. 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. The method at the decoder side by further exploiting the spatial correlation using a different estimation equation and side match technique to achieve much lower error rate. These two Methods mentioned above rely on spatial correlation of original image to extract data. That is, the encrypted image should be decrypted first before data extraction. To separate the data extraction from image decryption, method can emptied out space for data embedding following the idea of compressing encrypted images. Compression of encrypted data can be formulated as source coding with side information at the decoder, in which the typical method is to generate the compressed data in lossless manner by exploiting the syndromes of parity-check matrix of channel codes [2]. The method in compressed the encrypted LSBs to vacate room for additional data by finding syndromes of a parity-check matrix, and the side information used at the receiver side is also the spatial correlation of decrypted images. All these methods try to vacate room from the encrypted images directly. However, since the entropy of encrypted images has

been maximize, these techniques can achieve small payloads and/or generate marked image with poor quality for large payload and all of them are subject to some error rates on data extraction and image restoration.

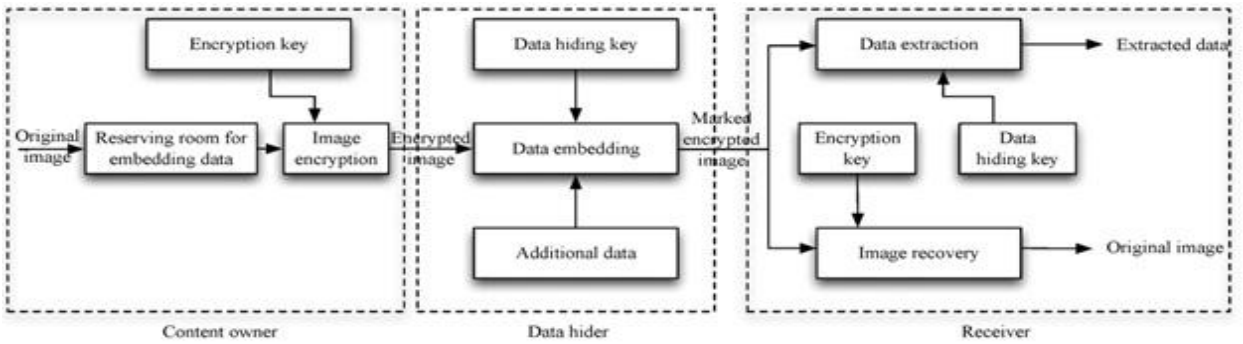

Fig 1. Framework RRBE.

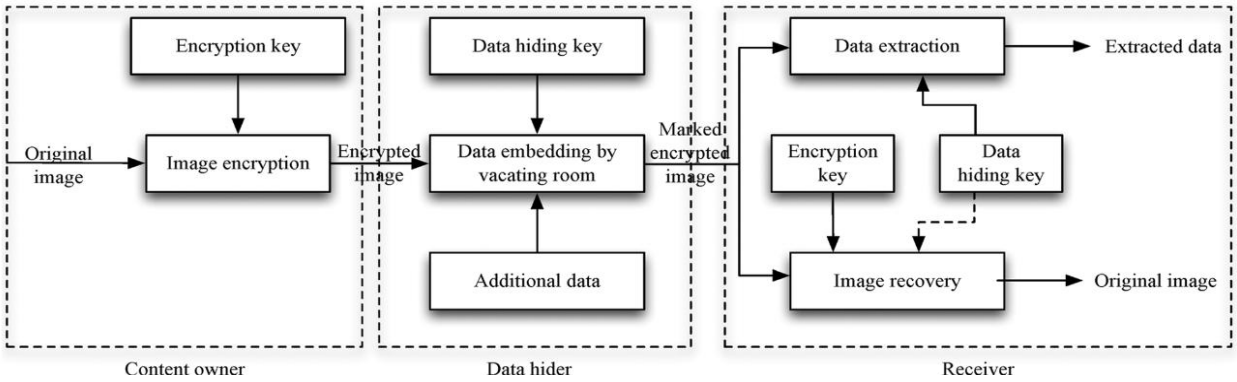

Fig 2. Framework VRAE

II. PROPOSED SYSTEM

In proposed method can achieve real reversibility, that is, data extraction and image recovery are free of any error. If we reverse the order of encryption and vacating room, i.e., reserving room prior to image encryption at content owner side, the RDH tasks in encrypted images would be more natural and much easier which leads us to the novel framework, "reserving room before encryption (RRBE)".

Advantage

Not only does the proposed method separate data extraction from image decryption but also achieves excellent performance in two different prospects:

1) Real reversibility is realized, that is, data extraction and image recovery are free of any error [11].

2) For given embedding rates, the PSNRs of decrypted image containing the embedded data are significantly improved; and for the acceptable PSNR, the range of embedding rates is greatly enlarged [11].

III. MODULES DESCRIPTION

A. Encrypted Image Generation: In this module, to construct the encrypted image, the first stage can be divided into three steps:

a. IMAGE PARTITION
b. SELF REVERSIBLE EMBEDDING followed by image encryption.

At the beginning, image partition step divides original image into two parts i.e in LSB And MSB then, the MSBs are are separated and also LSBs, then both are combined and are reversibly embedded into with a standard RDH algorithm so that both of can be used for accommodating messages; at last, encrypt the rearranged image to generate its final version [11].

FIG 1. ENCRYPTED IMAGE

a) IMAGE PARTITION: The operator here for reserving room before encryption is a standard RDH technique, so the goal of image partition [11].

b) SELF REVERSIBLE EMBEDDING: The goal of self-reversible embedding is to embed the LSB-planes of into by employing traditional RDH algorithms. We simplify the method in to demonstrate the process of self-embedding.

IV. 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 losslessly 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 [11].

FIG 2. ENCRYPTED IMAGES WITH DATA

V. DATA EXTRACTION AND IMAGE RECOVERY

In this module, Extracting Data from Encrypted Images to manage and update personal information of images which are encrypted for protecting clients' privacy, an inferior data base manager may only get access to the data hiding key and have to manipulate data in encrypted domain. When the database manager gets the data hiding key, he can decrypt and extract the additional data 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 [11].

VI. 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 [11].

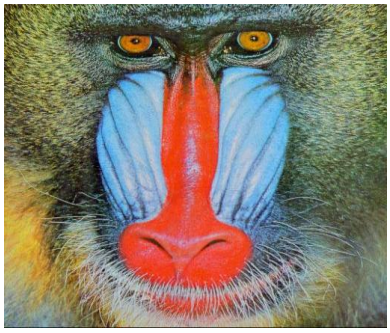

FIG 3.ORIGINAL IMAGE IS RESTORED

EXPERIMENTS:

We take standard two images, after that we take first image for separating its MSBs and LSBs After that the MSBs and LSBs are got separated and both are overwritten to demonstrate the feasibility of proposed method. Then we select second image for encrypting the first image into second image and both images are got encrypted, after that we encrypt data file into the encrypted image and the data file is encrypted and we get encrypted image with data file. That image file get decrypted and produced the original data file, finally, we get the original image from the encrypted images after decrypting it.

VII. CONCLUSION

Reversible data hiding in encrypted images is a new method which is popular due to the privacy-preserving requirements from cloud data management. Earlier methods implement RDH in encrypted images by vacating room after encryption, as opposed to which we proposed by reserving room before encryption. In this new technique data hider can benefit from the extra space emptied out in previous stage to make data hiding process effortless. The proposed method can achieve excellent performance without loss of perfect secrecy. and also real reversibility, separate data extraction and greatly improvement on the quality of marked decrypted images.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

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

[6] Jun Tian, "Reversible Data Embedding Using a Difference Expansion", IEEE transactions on circuits and systems for video technology, vol. 13, no. 8, august 2003.

[7] T. Kalker and F.M. Willems, "Capacity bounds and code constructions for reversible data-hiding", in Proc. 14th Int. Conf. Digital Signal Processing (DSP2002), 2002, pp. 71–76.

[8] Xiao Bo, Ying Lizhi, Huang Yongfeng," Reversible Data Hiding Using Histogram Shifting in Small Blocks", IEEE ICC 2010.

[9] Masoud Nosrati,Ronak Karimi,Mehdi Hariri, "Reversible Data Hiding:Principles, Techniques, and Recent Studies", World Applied Programming, Vol (2), Issue (5), May 2012. 349-353 ISSN: 2222-2510.

[10] V.Priya, "Reversible Information Hiding in Videos", International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014.

[11] Kede Ma, Weiming Zhang, Xianfeng Zhao, "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption". IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 3, MARCH 2013.