International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 6 –NOVEMBER 2014.

Reversible Data Hiding In Encrypted Images by Reserving Room before Encryption

T.Preetham[*1] and PollankiKusuma[#2]

[*]*M.Tech, CSE, Chalapathi Institute of Technology, A.R.Nagar,Mothadaka, Guntur dist*

[#]*Assistant professor, M.Tech, CSE, Chalapathi Institute of Technology, A.R.Nagar,Mothadaka, Guntur dist*

Abstract— A novel reversible data hiding technique in encrypted images is presented in this paper. Instead of embedding data in encrypted images directly, some pixels are estimated before encryption so that additional data can be embedded in the estimating errors. A benchmark encryption algorithm (e.g. AES) is applied to the rest pixels of the image and a special encryption scheme is designed to encrypt the estimating errors. Without the encryption key, one cannot get access to the original image. However, provided with the data hiding key only, he can embed in or extract from the encrypted image additional data without knowledge about the original image. Moreover, the data extraction and image recovery are free of errors for all images. Experiments demonstrate the feasibility and efficiency of the proposed method, especially in aspect of embedding rate versus Peak Signal-to-Noise Ratio (PSNR).

Index terms: Reversible data hiding, image encryption, privacy protection, histogram shift

I. INTRODUCTION

Reversible data hiding (RDH) in images is a technique, by which the original cover can be losslessly recovered after the embedded message is extracted. This important technique is widely used in medical imagery, military imagery and law forensics, where no distortion of the original cover is allowed. Since first introduced, RDH has attracted considerable research interest. In theoretical aspect, Kalker and Willems [1] established a rate-distortion model for RDH, through which they proved the rate-distortion bounds of RDH for memory less covers and proposed are cursive code construction which, however, does not approach the bound. Zhang etal.[2],[3]improved the recursive code construction forbinary covers and proved that this construction can achieve the rate-distortion bound as long as the compression algorithm reaches entropy, which establishes the equivalence between data compression and RDH for binary covers.

A various RDH method is more popular is based on difference expansion (DE)[3], in which the difference of each pixel group is expanded by various method or technique. Example, multiplied by 2, and thus the least significant bits (LSBs) of the difference are all-zero and can be used for embedding messages. Another reliable strategy for RDH is histogram shift (HS), in which space is saved for data embedding by shifting the bins of histogram of gray values. With respective to providing confidentiality for images, encryption is an effective and popular means as it converts the original and meaningful content to non-readable one. Although there are few RDH techniques in encrypted images have been published yet, there are some promising applications if RDH can be applied to encrypted images. Hwang et al. advocated a 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.[6]In our system we provide the high quality image to the users. It also provides the more security of the data. The proposed system is reduces the time as well as cost as compared to previous system.

With respect to providing confidentiality for images, encryption [12] is a strong and popular means as it converts the germinal and meaningful content to incomprehensible one. Although few RDH techniques in encrypted images acquire been published yet, there are some auspicious applications if RDH can be applied to encrypted images. In [9], Zhang et al. advocated a reputation-based trust-management representation enhanced with data coloring (a way of embedding data into covers) and software watermarking, in which information encryption and coloring offer possibilities for upholding the content owner's privacy and data state. Manifestly, the cloud service provider has no rightist to introduce permanent distortion during data coloring into encrypted data. Thus, a reversible data coloring technique based on encrypted data is preferred. Presume a medical image data- base is stored in a data center, and a server in the aggregation center can embed notations into an encrypted version of a medical image through a RDH technique. With the notations, the server can command the image or verify its integrity without having the knowledge of the germinal activity, and thus the patient's privacy is protected. On the additional accumulation, a doctor, having the cryptographic key, can decrypt and restore the image in a reversible behaviour for the purpose of further identification? In all methods of [10]-[12], the encrypted 8-bit

gray scale images are generated by encrypting every bit-planes with a occurrence cipher. The method in [10] segments the encrypted someone into a attribute of non-overlapping blocks sorted by a. a; each conceal is used to disseminate one more bit. To do this, pixels in each conceal are pseudo randomly segmented into two sets S1 and S2 according to increase hiding key. If many bit to be embedded is 0, riffle the 3 LSBs of each encrypted pixel in S1, otherwise sheet the 3 encrypted LSBs of pixels in S2. For system extraction and representation deed, the sound flips all the creator LSBs of pixels in S1 to modify a new decrypted block, and flips all the constraint in S2 to supplemental new block; one of them will be decrypted to the model block. Due to generalisation reciprocity in simple images, alternative impediment is presumed to be untold smoother than interfered preclude and embedded bit can be extracted correspondingly. Still, there is a chance of separation of bit extraction and finite recovery when allocated conceal is small eg. (a=8) or has described fine detailed textures.

To separate the data extraction from image decryption, Zhang [18] emptied out space for data embedding following the idea of compressing encrypted images [14], [15]. Compression of encrypted data can be formulated as source coding with side information at the decoder [14], 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. The method in [18] 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 the three methods try to vacate room from the encrypted images directly. However, since the entropy of encrypted images has been maximized, these techniques can only achieve small payloads [16], [17] or generate marked image with poor quality for large payload [18] and all of them are subject to some error rates on data extraction and/or image restoration. Al- though the methods in [16], [17] can eliminate errors by error- correcting codes, the pure payloads will be further consumed.

In the present paper, we propose a novel method for RDH in encrypted images, for which we do not "vacate room after encryption" as done in [16]–[18], but "reserve room before encryption". In the proposed method, we first empty out room by embedding LSBs of some pixels into other pixels with a traditional RDH method and then encrypt the image, so the positions of these LSBs in the encrypted image can be used to embed data. Not only does the proposed method separate data extraction from image decryption but also achieves excellent performance in two different prospects:

- Real reversibility is realized, that is, data extraction and image recovery are free of any error.
- 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.

This paper is organized in the following manner. Section II briefly introduces previous methods proposed in [16]–[18]. The novel method is elaborated in Section III followed by some implementation issues in Section IV. Experiments with analysis and comparison are given in Section V. The paper is concluded in Section VI.

II. LITERATURE REVIEW

The previous method can be summarized as the framework in which we are vacating room after encryption (VRAE) .In this content owner encrypts the original image using standard cipher with encryption key.

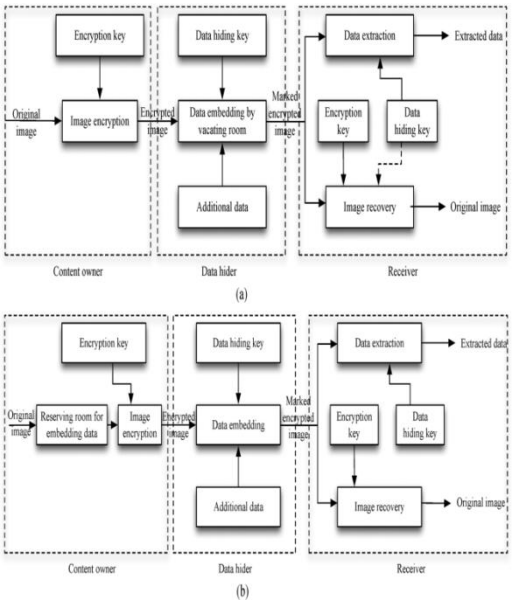
There is little technique by which we are vacating the room after encryption. 1. Fridich et al [4] constructed a general framework for RDH for vacating room in encrypted image. By first extracting compressible features of original image and then compressing them losslessly. In this way space can be created for embedding data. 2. Another method is based on difference expansion (DE) [3], for vacating room in encrypted image in which the difference of each pixel group is expanded, e.g., multiplied by 2, and thus the least significant bits (LSBs) of the difference are all-zero and the space created can be used for embedding data. 3. Another method is histogram shift (HS) [4], for vacating room in encrypted image in which space is saved for data embedding by shifting the bins of histogram of gray values. and the space created can be used for embedding data. The methods explained above are used for vacating the space from encrypted image for embedding data. After vacating room by creating space in the image the content owner encrypts the original image using a standard cipher with an encryption key. After producing the encrypted image, the content owner hands over. This version of image to a data hider i.e. database manager and the data hider can embed some data into the encrypted image by losslessly vacating some room according to a data hiding key. Then the content owner or an authorized third party can extract the embedded data from image with the help of data hiding key. All the three methods discussed above to vacate room from the encrypted version of images directly. Because the entropy of encrypted images has been maximized, these techniques can achieve only a small payloads [5], [6] or generate marked image with poor quality for large payload [7] and all of them are subject to some error rates on data extraction and/or image restoration. Although the methods in [5], [6] can eliminate errors by error correcting codes, the pure payloads will be further consumed.

III. PROPOSED METHOD

Since losslessly vacating room from the encrypted images is relatively difficult and sometimes inefficient, why are we

still so obsessed to find novel RDH techniques working directly for encrypted images? 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)" As shown in Fig. 1(b), the content owner first reserves enough space on original image and then converts the image into its encrypted version with the encryption key. Now, the data embed-ding process in encrypted images is inherently reversible for the data hider only needs to accommodate data into the spare space previous emptied out.

The data extraction and image recovery are identical to that of Framework VRAE. Obviously, standard RDH algorithms are the ideal operator for reserving room before encryption and can be easily applied to Framework RRBE to achieve better performance compared with techniques from Framework VRAE. This is because in this new framework, we follow the customary idea that first losslessly compresses the redundant image content (e.g., using excellent RDH techniques) and then encrypts it with respect to protecting privacy.



The new idea about reversible data hiding in encrypted image without loss can be achieved by proposed system. Reserving room before encryption in this we first losslessly compress the redundant image and then encrypts it with respect to maintain privacy the implementation is carried in following ways

A. Reserving Room

In this we first empty out room i.e. creating space in the image before encryption of image the RDH task in encrypted image would be more natural and much easier and real reversibility is realized this can be achieved by first losslessly compress the redundant data of image in this way space is created for embedding data and then encrypts the image by different encryption technique.

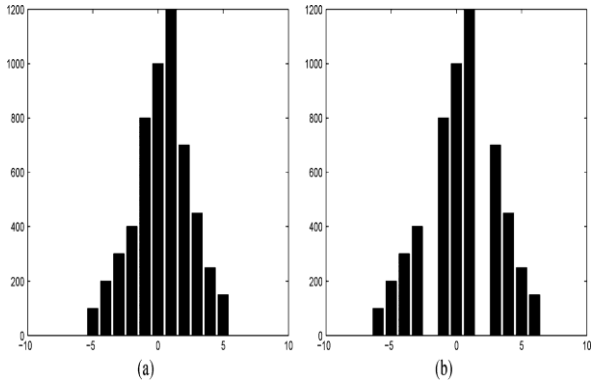
B. Encryption Key

This key is present at the content owner side the content owner first reserves enough space on original image and then encrypts the original image using standard cipher with an encryption key and then after producing the encrypted image the content owner hands over to database manager or any third party.

C. Data Hiding Key

This key is present at the data hiding center as well as receiver side the data hider can embed some auxiliary data into the encrypted image according to the data hiding key.

The receiver maybe the content owner himself or can be an authorized party can extract the embedded data with the data hiding key and further recover the original image from the encrypted version according to encryption key.



Data Hiding in Encrypted Image

Once the data hider acquires the encrypted image , he can embed some data into it, although he does not get access to the original image. The embedding process starts with locating the encrypted version of , denoted by Since has been rearranged to the top of , it is effortless for the data hider to read 10 bits information in LSBs of first 10 encrypted pixels. After knowing how many bit-planes and rows of pixels he can modify, the data hider simply adopts LSB replacement to substitute the available bit-planes with additional data . Finally, the data hider sets a label following to point out the end position of embedding process and further encrypts according to the data hiding key to formulate marked encrypted image denoted by . Anyone who does not possess the data hiding key could not extract the additional data.

Data Extraction and Image Recovery

Since data extraction is completely independent from image decryption, the order of them implies two different practical applications.

1) Case 1: Extracting Data from Encrypted Images:

To manage and update personal information of images which are encrypted for protecting clients' privacy, an inferior database manager may only get access to the data hiding key and have to manipulate data in encrypted domain. The order of data extrac- tion before image decryption guarantees the feasibility of our work in this case. When the database manager gets the data hiding key, he can decrypt the LSB-planes of and extract the additional data by directly reading the decrypted version. When requesting for updating information of encrypted images, the database man- ager, then, updates information through LSB replacement and encrypts updated information according to the data hiding key all over again. As the whole process is entirely operated on en- crypted domain, it avoids the leakage of original content.

2) Case 2: Extracting Data From DecryptedImages:

In Case 1, both embedding and extraction of the data are manipulated in encrypted domain. On the other hand, there is a different situa- tion that the user wants to decrypt the image first and extracts the data from the decrypted image when it is needed. The following example is an application for such scenario. Assume Alice out- sourced her images to a cloud server, and the images are en- crypted to protect their contents. Into the encrypted images, the cloud server marks the images by embedding some notation, including the identity of the images' owner, the identity of the cloud server and time stamps, to manage the encrypted images. Note that the cloud server has no right to do any permanent damage to the images. Now an authorized user, Bob who has been shared the encryption key and the data hiding key, down- loaded and decrypted the images. Bob hoped to get marked de- crypted images, i.e., decrypted images still including the nota- tion, which can be used to trace the source and history of the data. The order of image decryption before/without data extrac- tion is perfectly suitable for this case. Next, we describe how to generate a marked decrypted image.

IV. IMPLEMENTATION ISSUES

The proposed approach will be tested on public available standard images, which include "Lena", "Airplane", "Barbara", "Baboon", "Peppers" and "Boat" [19]. The size of all images is 512 512 8. The objective criteria PSNR is employed to evaluate the quality of marked decrypted image quantitatively. To achieve high PSNRs, several implement details for the pro- posed method are discussed first.

A. Choice of LSB-Plane Number

When original image is divided into and , the size of is determined not only by the length of to-be-embedded messages but also by the number of LSB-planes embedded reversibly in the use of multiple LSB-planes takes into ac- count the fact that the size of can be enlarged with an increase in embedding capability. Therefore, it is more likely that only need to implement embedding scheme once to accommodate LSB-planes of , thus leading to distortion reduction. In other words, shares part of distortion happens. Table I shows the comparison results measured by PSNR for three dif- ferent choices of LSB-planes (LSB-planes of are embedded into peak points of estimating error sequences in), where the embedding rate is measured by bits per pixel (bpp). The choice of single LSB-plane outperforms the other two at low embed- ding rate levels (less than 0.2 bpp). It is consistent with our intuitive understanding: when embedding rate is small, has the capacity to embed LSBs of in a single round without size enlargement. Utilizing multiple LSB-planes can only introduce average distortion from 0.5 to 1.75 (case of two LSB-planes) in, calculated by mean squared error (MSE). With a growing embedding rate, the gain by choosing two LSB-planes is especially.

V. EXPERIMENTS AND COMPARISONS

We take standard image Lena, shown in Fig. 5(a), to demonstrate the feasibility of proposed method. Fig. 5(b) is the encrypted image containing embedded messages and the decrypted version with messages is illustrated depicts the recovery version which is identical to original image. We have compared the proposed method with the state-of-the-art works [16]–[18]. As mentioned in Section I, all methods in [16]–[18] maybe introduce some errors on data extraction and/or image restoration, while the proposed method is free of any error for all kinds of images. The quality of marked decrypted images is compared in the term of PSNR. Fig. 6 plots the PSNR results of different marked decrypted images under given embedding rates. Out of fairness, we modify the methods in [16], [17] with error-correcting codes to eliminate errors. By introducing error-correcting codes, the pure payload of [16], [17] is reduced from Cap to , where is the binary entropy function with error rate . Take test image Baboon for instance. If each embedding block is sized of 8 8 with error rate 15.55% [16], then the pure payload is 1543 bits rather than 4096 bits. As for the method in [18], we only choose those results with a significantly high probability of successful data extraction and perfect image re- covery to draw the curves. From the Fig. 6, it can be observed that over all range of embedding rate, for all cases, our approach outperforms state-of-the-art RDH algorithms in encrypted im- ages. The gain in terms of PSNR is significantly high at embed- ding rate range that the methods in [16]–[18] can achieve. In addition, another advantage of our approach is the much wider range of embedding rate for acceptable PSNRs. In fact, the pro- posed method can embed more than 10 times as large payloads for the same acceptable PSNR (e.g.,dB) as the methods in [16]–[18], which implies a very good potential for practical applications.

VI. CONCLUSION

Reversible data hiding in encrypted images is a new topic drawing attention because of the privacy-preserving requirements from cloud data management. Previous methods implement RDH in encrypted images by vacating room after encryption, as opposed to which we proposed by reserving room before encryption. Thus the data hider can benefit from the extra space emptied out in previous stage to make data hiding process effort- less. The proposed method can take advantage of all traditional RDH techniques for plain images and achieve excellent performance without loss of perfect secrecy. Furthermore, this novel method can achieve real reversibility, separate data extraction and greatly improvement on the quality of marked decrypted images.

REFERENCES

[1] 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.

[2] W. Zhang, B. Chen, and N. Yu, "Capacity-approaching codes for reversible data hiding," in Proc 13th Information Hiding (IH'2011), LNCS 6958, 2011, pp. 255–269, Springer-Verlag.

[3] 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.

[4] J. Fridrich and M. Goljan, "Lossless data embedding for all image formats," in Proc. SPIE Proc. Photonics West, Electronic Imaging, Security and Watermarking of Multimedia Contents, San Jose, CA, USA, Jan. 2002, vol. 4675, pp. 572–583.

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

[6] 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.

[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] 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.

[9] P. Tsai, Y. C. Hu, and H. L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting," Signal Process., vol. 89, pp. 1129–1143, 2009.

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

[11] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y.-Q. Shi, "Reversible watermarking algorithm using sorting and prediction," IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 7, pp. 989–999, Jul. 2009.

[12] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL, USA: CRC, 1996.

AUTHOR'S DETAILS

Ms.T.preetham pursuing her M.Tech degree in Computer science & Engineering from Chalapathi Institute of Technology, A.R.Nagar,Mothadaka,Guntur dist.

Mrs. PollankiKusuma M.Tech CSE Presently she is working as Assistant professor at Chalapathi Institute of Technology, A.R.Nagar,Mothadaka, Guntur dist.