Reversible Data Hiding in Enrcypted Image by Vacating Room before Encryption

Sayli P. Raut
M.E. Student
Department of Computer Engineering
Thakur College of
Engineering And Technology

Kiran A. Bhandari
Associate Professor
Department of Computer Engineering
Thakur College of
Engineering and Technology

ABSTRACT
Steganography has emerged as a very popular topic in recent years. A lot of research is being done in order to enhance the confidentiality measures. RDH i.e. Reversible Data Hiding is a step in the same direction that has been taken recently. Data confidentiality and integrity have become most important aspect of this communication world. Where, cryptography involves both encryption and embedding of data, the main aspects to keep the data integrity and confidentiality intact. Encryption domain has more importance in data hiding. Data concealing can be done through any channels like audio, video, image etc. and send to receiver. Receiver will acquire data from the media where it embeds data. Data hiding can be done for sending highly classified data. For with Reversible Data Hiding is becoming more popular. Reversible data hiding is an approach by which the original image can be recovered without any loss when the data embed in it is extracted. This paper focuses on main approaches of RDH i.e. Vacating Room after Encryption and Vacating Room before Encryption and compares the performance of same on the basis of various RDH techniques.

General Terms
Data Hiding, Confidentiality, Integrity, Retrieving original image and Algorithms

Keywords
Cryptography, Encryption, Decryption, Reversible Data Hiding, Data Embedding

1. INTRODUCTION
Steganography's basic concept is to hide the presence of the data in the cover image or object by embedding the confidential message into it. To hide the confidential data in a media cover i.e. image in this case and retrieve that same cover media with as less as possible loss of it is the basic concept of Reversible Data Hiding, which tends to be helpful in the fields like military or medical images. After the extraction of the confidential data, image should be recovered perfectly in reversible manner [1].

Data hiding can be achieved even by separable reversible data hiding, in which the content owner encrypts the image with the help of an encryption key,[1][2][3] and then the data hider performs compression algorithms to compress the image and create spare space in order to embed data into it. However, if the content owner or the user does not have complete trust on the service provider then the secrete data can be encrypted while it is to be transmitted [4].

Theoretically, Kalker and Willems [5] introduced a rate-distortion technique for RDH, by which they proved the rate-distortion bounds of RDH for the covers without any memory

in it, also he suggested a recursive code construction which, however, does not approach the bound. In the paper of 2011, Zhang et al. [6], [7] was able to improvise the recursive code construction for binary covers and justified that the recursive code construction can obtain the rate-distortion bound considering the compression algorithm sustain the ability to reach the entropy, which establishes the equal balance between data compression and RDH for binary covers.

The aim of the proposed idea in this paper is to improve the payload to be embedded in encrypted images. This paper introduces a separable reversible data hiding method for encrypted images using Slepian-Wolf source encoding [8]. Inspiration of the proposed method is from the DSC [9-10], in which the selected bits takes from the stream-ciphered image using LDPC codes [11] are encoded into syndrome bits to vacant unoccupied room to embed the secret data. The proposed method becomes separable with the help of two different keys. The embedded secret data is completely extracted using the embedding or data hiding key, also by using the encryption key the original image can be approximately retrieved with high quality. Availability of both key ensures that the hidden data can be and the original image can be, completely extracted and recovered respectively with the backup of some estimated side information.

The proposed idea can achieve considerably high embedding payload along with good image retrieval quality, where the sender is out of context of room-reserving operations. The further research includes the topics as below. Section 2 contains with literature review done on the proposed method. Section 3 deals with the methodology. Section 4 conclude the work done and discuss the scope for future research.

2. LITERATURE REVIEW
In the literature survey section, the state-of-the-art i.e. the basic working of RDH techniques of embedding confidential messages in encrypted images are retrieved. RDH for encrypted image are usually designed for the applications in which the data-hider and the image owner are not the same individual. The data-hider cannot access the image content, and the secret message is held by the data-hider, encryption is done by the sender, hiding by the data-hider, and data extraction and/or image reconstruction by the receiver. RDH methods that exist are classified into two categories as below:

- Vacating Room After Encryption (VRAE)
- Vacating Room Before Encryption (VRBE) [12]

In the VRAE technique, the sender encrypts the original image where the date is to be embedded, while the data is embedded by the data-hider by modifying some bits of the encrypted image. Puech et al. [13], first proposed this idea, where in the image owner encrypts the original image by Advanced Encryption Standard (AES), and the data is embedded by the data-hider, one bit in each block containing *n* pixels, which achieves 1/*n* bit-per-pixel (*bpp*) embedding rate. Data extraction and image retrieval on the receiver side, are realized by evaluating the local standard deviation during decryption of the encrypted image. This method requires that image decryption and data extraction operations must be done jointly. In simple words, data extraction and image decryption are inseparable.

In order to overcome the disadvantages of inseparability in [13], a separable RDH scheme was introduced for encrypted images in [14]. Pseudo-randomly, the data-hider permutes and divides the encrypted image into sets of size *L*. The *P* LSB-planes of each set are compressed/tighten with a matrix **G** sized $(P \cdot L\text{-}S) \times P \cdot L$ to generate corresponding vectors. Thus, *S* bits of vacant space are available for data hiding. A total of (8-P) most significant bits (MSB) of pixels, on the receiver side, are retrieved by decryption. The receiver then estimates the P LSBs by the MSBs of neighboring pixels. By comparing the estimated bits with the vectors in the coset Ω corresponding to the extracted vectors, the receiver can retrieve the original bits of the P LSBs. Because the additional bits are embedded in LSBs of the encrypted images, which can be extracted directly before image recovery, data extraction and image retrieval are therefore separable. Besides, this method achieves a better embedding rate than [15] and [16]. Another separable method was proposed in [17], in which the data-hider embeds additional bits by a histogram shifting and n-nary data embedding technique, greatly improving the embedding payload as compared to [14]-[15]. However, as the encryption of the original image is done with pixel permutation and affine transformation, leakage of image histogram is inevitable under exhaustive attack.

In Vacating Room Before Encryption method, the original images, before encryption, are processed by the owner to create vacant area for data embedding, and the secret data are embedded into specified positions by the data-hider. For example, the method in [18] creates embedding room in the plaintext image by embedding LSBs of certain pixels into other pixels by applying a traditional RDH algorithm. To generate and encrypted image the pre-processed image is then encrypted by the owner of the original image. Thus, positions of these vacated LSBs in the encrypted image can be used by the data-hider, and a large payload i.e. embedding rate up to 0.5 bpp, can be achieved. Another technique with a similar idea, based on an estimation technique was proposed in [19], in which a large portion of pixels are used to estimate the rest before encryption, concatenating the encrypted estimating errors and a large group of encrypted pixels forms the final version of the encrypted image. By modifying the estimated errors, some additional bits can be embedded in the encrypted image. With this method, PSNR of the approximate image retrieved by the receiver is higher as compared to the previous technique.

Both [15] and [17] are separable RDH methods with good embedding rates and reconstruction capability, but require an additional RDH operation by the sender before image encryption. That means the issue of RDH in encrypted images is actually transformed into a traditional RDH in plaintext images.

Although higher payload can be achieved with VRBE, it requires that the sender must perform an extra RDH prior image gets encrypted. In case the sender has no idea of the forthcoming data to be embedded by the data-hider, or he/she has no computational capability of the traditional RDH, this seems impractical. On the other hand, in case the sender can reserve room for embedding by reversibly hiding redundant bits into the original plain image, all embedding tasks can also be done on the sender side and then the data-hider becomes redundant.

In view of these problems, we propose a method to achieve high embedding payload by combining the MSB estimation with DSC. As estimating MSB is much more accurate than estimating LSB planes, the original data of the MSB plane can be retrieved by DSC decoding with an acceptable decoding error probability. In other words, large data embedding rate can be achieved by this kind of combination.

3. METHODOLOGY

Real Reversibility can be achieved in the proposed method i.e. image can be recovered without any loss along with the extraction of the data from it free of any error, achieving separable reversible data hiding. There was need of only reversing the order of vacating room and encryption of the image. To be more precise, the proposed method creating space in the image prior to encrypting the image at the content owner's side. The RDH tasks in encrypted images perform more naturally and much easily which leads us to the framework, "vacating room before encryption (VRBE)". The proposed method not achieves separable reversible data hiding. That can separate data extraction from decryption of image and also achieve exceptional performance in different aspects. Data extraction and original image retrieval are free of any error. The PSNRs of image after decryption containing the embedded data are significantly improved; for given embedding rates, and for the acceptable PSNR, the range of embedding rates is greatly enlarged. The proposed method allows the content owner to use different formats of the image in which user wants to store data i.e. .jpeg, .png, .bmp etc.

The proposed techniques block diagram is presented in the Fig. 1, which contains three stages Image encryption, data embedding, and data extraction/image retrieval.

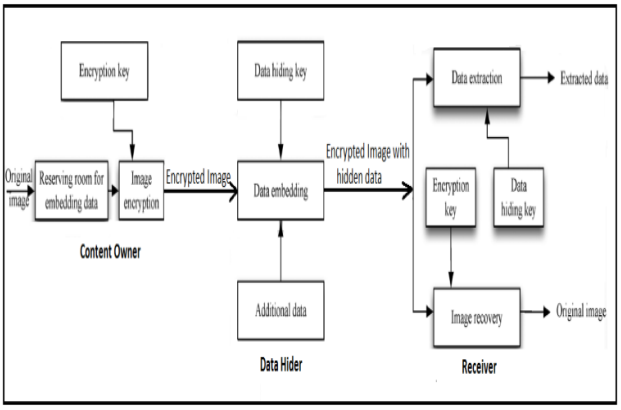

Figure 1: Vacating Room Before Encryption (VRBE)

- In stage I, the data-hider selects and compresses some MSB of the secret image using LDPC codes to generate a spare space, and embeds additional bits into the encrypted image using an embedding key.
- In stage II, using a stream cipher and an encryption key, the owner encrypts the original image into an encrypted image.
- In stage III, the receiver extracts the secret bits using the embedding key. If he/she has the encryption key, the original image can be approximately retrieved via image decryption and estimation. When both the encryption and data-hiding keys are available, the receiver can extract the compressed bits, and implement the distributed source decoding using the estimated image as side information in order to perfectly retrieve the original image.

3.1 Vacating Room in Original Image

Here, the first stage can be distributed into two parts, image partitioning and reversible embedding.

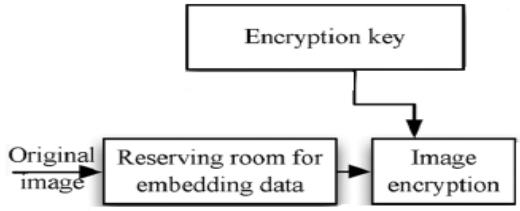

Figure 3: Creating spare space

1. **Image partitioning:** The LSB planes are used for the vacating room operation, so the goal of image partition is to construct a smoother area, so that standard RDH algorithms can achieve better performance. To do that, without loss of ordinarily, take the three cubes of original image as 8 bits gray-scale images with its size is M X N and pixels Ci,j belongs to [0,255]. 1<=i<=M, 1<=j<=N. so we have to perform every action to the three channels of the image. First, the content owner extracts bits along the rows, from the original image, Discrete overlapping blocks whose number is determined by the size of the data to be embedded, denoted by l. In detail, every block consists of m rows, where m = [l/N] and the number of blocks can be figured through n=M-m+1. An important thing is that each block along the rows, is overlapped by previous or sub sequential blocks. The content owner, selects the particular block with the highest smoothness to be A, and puts it in front of the image concatenated by the rest part B with fewer textured areas as shown below.

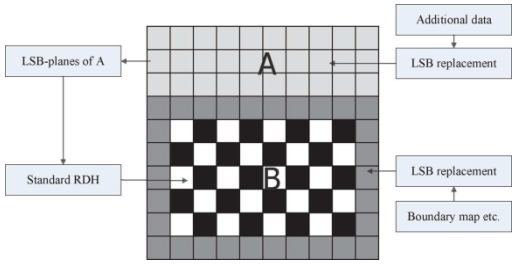

Figure 2: Image Partitioning and Embedding process

3.2 Image Encryption

The encrypted image E can be created by performing the encryption on rearranged self-embedded image, denoted by X. Encryption of X can easily obtained by the use of stream cipher. For a color image, we take the three channels as three grayscale images. For example, a gray value Xi,j whose range is from 0 to 255 can be represented by 8 bits, Xi,j(0), Xi,j(1),…… Xi,j(7), such that

Xi,j(k)=[Xi,j/2k] mod 2, k=0,1,….7

Exclusive- or i.e. XOR operation can be used for gain encrypted bits.

Where ri,j(k) is generated by a standard stream cipher algorithm determined by the encryption key. At last, 10 bits information is embedded into LSBs of first 10 pixels in encrypted version of original image i.e. A to let data hider know the number of rows and the number of bit-planes he can embed confidential data into After image encryption to provide the privacy.

3.3 Data Hiding in Encrypted Image

Encrypted version of the original is provided to the data hider. Data hider can embed data to the encrypted image. The embedding process of confidential data can start at AE which is encrypted version of A. The data hider read 10 bits data in LSBs of first 10 encrypted pixels, as it is aligned at the top of encrypted image. After knowing how many bit-planes and rows of pixels data hider can modify, he can simply select LSB replacement to substitute the available bit-planes with additional to-be-embedded data m. The data hider analyses additional data and the concealing of data process continues with that information. Every pixel values will be modified to binary form and binaries of data bits attached to last bit of pixel values. So a new image containing the embedded data will be generated. Anyone who does not have the data hiding key could not extract the additional data from the cover image.

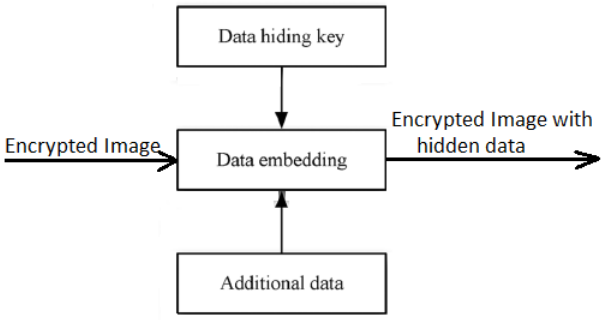

Figure 3: Embedding Data

3.4 Data extraction and Image recovery

Image decryption and data extraction can be completed independent of each other. So the order of them implies two different practical applications.

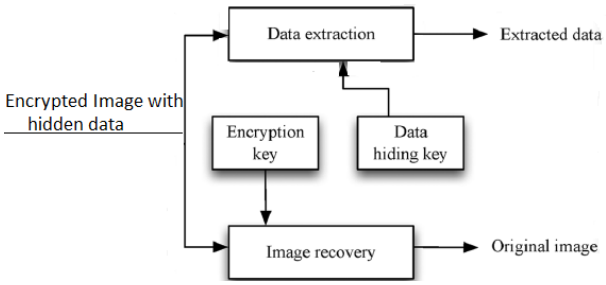

Figure 3: Data extraction and Image retrieval

3.4.1 Case 1: Extracting Data from Encrypted Images:

To manage and update personal information of images which are encrypted for securing clients' privacy, a poor database manager may only get access to the data hiding key and have to manage data in encrypted domain. The feasibility of work is when following the order of data extraction before decrypting image. The database manager gets the data hiding key for decrypting the LSB-planes of AE and retrieve the additional data m by directly reading the decrypted version. Leakage of original content avoids because the whole process is entirely conducted on encrypted domain.

3.4.2 Case 2: Extracting Data from Decrypted Images:

we can proceed with the following scenarios,

- **Generating the Marked Decrypted Image**: To form the marked decrypted image X'' which is made up of A'' and B'', the data owner should do following two steps.

  Step 1: With the encryption key, the data owner decrypts the encrypted image except the LSB-planes of AE. The decrypted version of E' containing the embedded data can be calculated by

  Step 2: Retrieve SR and ER in marginal area of B". By rearranging A'' and B'' to its original state, the plain image containing embedded data is obtained.

- **Data Extraction and Image Restoration**: After generating the marked decrypted image, the content owner can further retrieve the data and recover original image.

4. CONCLUSION

Reverse data hiding using Vacating room before encrypting image technique is drawing attention because of the privacy-preserving requirements of the confidential data from cloud data management. Previous methods implement RDH in encrypted images by vacating room after encrypting the original image, as reversed to which the proposed technique by reserving room before encryption. Thus the data hider can benefit from the spare space vacated in the very first stage to make data embedding process effortless. The proposed method takes advantage of traditional state-of-art RDH techniques for plain images and achieves excellent performance without loss of perfect confidentiality. Furthermore, by this method can achieve reversibility as well as separate data extraction and great improvement on the quality of marked retrieved decrypted images.

Reverse data hiding using Vacating room before encrypting image technique, for colored images are proposed here in this paper. Previous studies show that several techniques have been implemented, such as, reserving room after encryption of image for data hiding for images such as gray scale images only. For encrypted images, RDH is done by vacating room before encryption, by using LSB Plane technique as opposed to the one which have proposed Histogram Shifting. Thus the data hider can benefit from the spare space in each channel of the color image. Time delay may arise for color images when vacating room before encrypting it. By re sizing the image we can remedy it out but we have to compensate for the extra space utilization. Subsections

5. REFERENCES

[1] Reversible Data Hiding in Encrypted Images by ReservingRoom Before Encryption Kede Ma, Weiming Zhang, Xianfeng Zhao, Member, IEEE, Nenghai Yu, and Fenghua Li MARCH 2013

[2] 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.

[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] 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.

[5] 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.

[6] 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.

[7] 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.

[8] D. Slepian and J. K. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inform. Theory*, vol. IT-19, pp. 471–480, July 1973.

[9] T. M. Cover and J. A. Thomas, Elements of Information Theory. New York: Wiley, 1991

[10] W. Liu, W. Zeng, L. Dong, et al. "Efficient compression of encrypted grayscale images," *IEEE Trans. on Image Processing*, vol. 19, no. 4, pp. 1097-1102, 2010.

[11] W. E. Ryan, "An introduction to LDPC codes," in *CRC Handbook for Coding and Signal Processing for Recoding Systems (B. Vasic, ed.)*, CRC Press, 2004.

[12] K. Ma, W. Zhang, et al. "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 3, 553-562, 2013

[13] W. Puech, M. Chaumont and O. Strauss, "A reversible data hiding method for encrypted images," *Proc. SPIE 6819, Security, Forensics, Steganography, and Watermarking of Multimedia Contents X*, 68191E, Feb. 26, 2008, doi:10.1117/12.766754

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

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

[16] 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.

[17] Z. Qian, X. Han and X. Zhang, "Separable Reversible Data hiding in Encrypted Images by n-nary Histogram Modification," *3rd International Conference on Multimedia Technology (ICMT 2013)*, pp. 869-876, Guangzhou, China, 2013.

[18] K. Ma, W. Zhang, et al. "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 3, 553-562, 2013.

[19] W. Zhang, K. Ma and N. Yu, "Reversibility improved data hiding in encrypted images," *Signal Processing*, vol. 94, pp. 118–127, 2014.