Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 7, Issue, 08, pp.19502-19506, August, 2015

INTERNATIONAL JOURNAL
OF CURRENT RESEARCH

ISSN: 0975-833X

RESEARCH ARTICLE

A COMPARATIVE STUDY OF REVERSIBLE DATA HIDING TECHNIQUES

*Aparna Gopinath, P. K. and Grace John, M.

Department of ECE, VJEC, Chemperi

ARTICLE INFO

Article History:
Received 17th May, 2015
Received in revised form
15th June, 2015
Accepted 20th July, 2015
Published online 31st August, 2015

Key words:

Reversible data hiding, Histogram,
Image encryption.

ABSTRACT

Reversible data hiding can restore the image after the hidden data is extracted. Security and integrity of data are two challenging areas for research. Recently more attention is paid to reversible data hiding in encrypted images as original cover image can be losslessly recovered after embedded data is extracted while protecting the image contents confidentiality. Its applications are in medical imagery, military imagery and law forensics. Data hiding helps in protecting the data against malicious attacks such as information stealing, copyright piracy. This paper compares two techniques used for reversible data hiding. The PSNR value of the recovered image of both techniques are compared.

Citation: Aparna Gopinath, P. K. and Grace John, M. 2015. "A comparative study of reversible data hiding techniques", *International Journal of Current Research*, 7, (8), 19502-19506.

INTRODUCTION

Data hiding is a process in which data is embedded into a cover media. Invisibility of hidden data is an important requirement. In most cases of data hiding, the cover media will experience some distortion due to data hiding and cannot be inverted back to the original media. In some applications, like medical diagnosis and law enforcement, it is critical to reverse the marked media back to the original cover media after the hidden data are retrieved for some legal considerations. In reversible data hiding the cover media can be losslessly recovered after the hidden data have been extracted out, thus providing an additional avenue of handling two different sets of data.Most of the existing data hiding techniques are not reversible. For example the widely utilized spread-spectrum based data hiding methods are not invertible because of truncation error and round-off error. The well-known least significant bit plane (LSB) based schemes are not lossless owing to bit replacement without memory. Another category of data hiding techniques, quantization-index modulation based schemes are not distortion-free owing to quantization error.

Reversible data hiding techniques are roughly classified into three types:lossless compression based methods, difference expansion (DE) methods, and histogram modification (HM) methods.

The lossless compression based methods uses statistical redundancy of the host media by performing lossless compression in order to create a spare space to accommodate additional secret data. The least significant digits of pixel values in an L-ary system (Alkaraki and Kamal, 2004) or the least significant bits of quantized DCT coefficients in a JPEG image (Karkvandi *et al*., 2011) can also be used to provide the required data space. In these reversible data hiding methods, a spare space is made available to accommodate hidden data as long as the chosen item is compressible, but the capacities are not very high. In the difference expansion method (Akkaya and Younis, 2005), differences between two adjacent pixels are doubled so that a new LSB plane without carrying any information of the original can be generated. The difference expansion method can embed a fairly large amount of secret data into a host image.

A data-hider can use histogram modification method to realize reversible data hiding. In (Junlin li and Ghassan Alkegib, 2009), the host image is divided into different blocks and gray values are mapped to a circle. After pseudo-randomly segmenting each block into two sub-regions, rotation of the histograms of the two sub-regions on this circle is used to embed one bit in each block. On the receiving side, the original block can be recovered from the marked image by the inverse process. Payload of this method is low as each block can carry only one bit. A typical HM method presented in (Jongseok Park and Sartaj Sahni, 2006) where the zero and peak points of

**Corresponding author: Aparna Gopinath, P. K.*
Department of ECE, VJEC, Chemperi

the histogram of an image slightly modifies the pixel grayscale values to embed data into the image. Section II discusses about the reversible data hiding technique by vacating room after encryprion. Section III describes about reversible data hiding by reserving space before encryption. Section IV discusses about the PSNR values of the restored image of the two reversible data hiding techniques. Paper is concluded in section V.

II. Reversible data hiding by vacating room after encryption

The methods proposed in (Hua and Yum, 2008; Alkaraki and Kamal, 2004; Karkvandi *et al.*, 2011) can be summarized as the framework, “vacating room after encryption (VRAE)”, as illustrated in Figure 1 (a). In this framework, 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, may be the content owner himself or an authorized third party can extract the embedded data with the data hiding encrypted version according to the encryption key.

The encrypted 8-bit gray scale images are generated by encrypting every bit planes with a stream cipher. The method segments the encrypted image into a number of non-overlapping blocks sized by a×a, each block is used to carry one additional bit. To do this, pixels in each block are pseudo-randomly divided into two sets S1 and S2 according to a data hiding key. If the additional bit to be embedded is 0, flip the 3 LSBs of each encrypted pixel in S1, otherwise flip the 3 encrypted LSBs of pixels in S2. For data extraction and image recovery, the receiver flips all the three LSBs of pixels in S1 to form a new decrypted block, and flips all the three LSBs of pixels in S2 to form another new Block. One of them will be decrypted to the original block. Due to spatial correlation in natural images, original block is presumed to be much smoother than interfered block and embedded bit can be extracted correspondingly. However, there is a risk of defeat of bit extraction and image recovery when divided block is relatively small or has much fine-detailed textures.

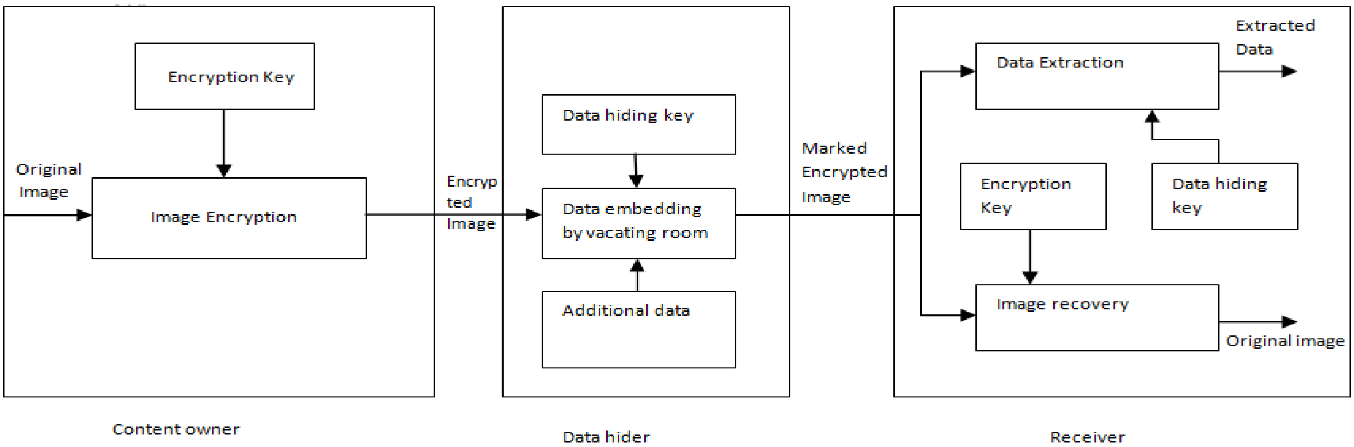

Fig.1. Vacating room after encryption framework

III. Reversible data hiding in encrypted images by reserving room before encryption

Most reversible data hiding techniques embed data by vacating room from the encrypted images. But this cause errors on data extraction. In this method room is reserved before encryption using a traditional RDH algorithm.

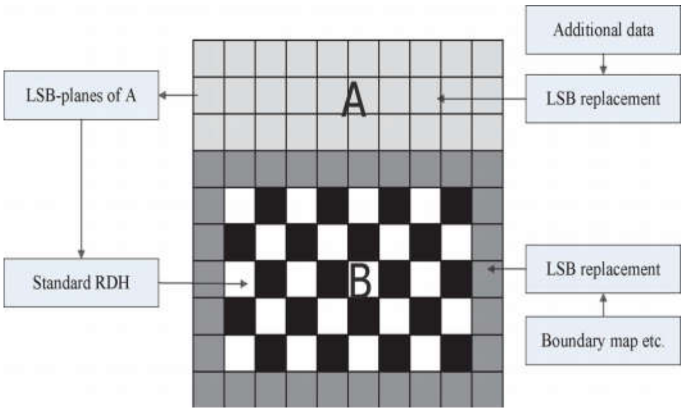

Fig.2. Illustration of image partition and embedding process

This method has four stages:generation of encrypted image, data hiding in encrypted image, data extraction and image recovery. Encrypted image generation includes image partition, self reversible embedding followed by image encryption. In image partition original image is divided into two parts A and B. Least significant bits of A are embedded reversibly into B with a standard RDH algorithm so that least significant bits of A can be used for accommodating the data.

Encrypted image is rearranged to generate its final version. After the encrypted image is obtained data hider can embed data into it. Data can be extracted from encrypted or decrypted images. In data extraction from encrypted image both embedding and extraction of data are done in encrypted domain. This reversible data hiding technique achieves real reversibility. There is good improvement in the quality of marked decrypted images.

A. Generation of encrypted image

Image partition is the first step in the generation of encrypted image. In image partition the original image is divided into two parts A and B.The LSB's of A are reversibly embedded into the LSB's of B using a reversible data hiding algorithm. Thus LSB's of A are used for embedding the additional data. Then the rearranged image is encrypted. Image partition is done to obtain a smoother area B on which the data hiding algorithm can achieve better performance. Consider an original image C as an 8 bit gray scale image with size M x N and pixel $C_{i,j} \epsilon$ (0,255), 1 ≤ I ≤ M,1 ≤ j ≤ N. The content owner first extracts several blocks along rows whose number is determined by the size of the message to be embedded denoted by l. Every block consist of m rows ,where m=l/N.The number of blocks can be computed by n=M-m+1.Each block is overlapped by the previous or sub sequential block along the rows. First order smoothness function of each block is calculated using the equation

$$f = \sum_{u=2}^{m} \sum_{v=2}^{N-1} |C_{u,v} - \frac{C_{u-1,v}+C_{u+1,v}+C_{u,v-1}+C_{u,v+1}}{4}| \ldots\ldots\ldots\ldots(1)$$

Block with higher f contains relatively more complex textures. The content owner selects the block with higher f as A. The content owner puts it in the front, concatenated by the rest part B which has fewer textured areas. Pixels in the rest of the image B are first categorized into two sets white and black pixels. Pixels whose indices satisfies the condition (i+j)mod2=0 are considered as white pixels and pixels whose indices satisfies the condition (i+j) mod2=1 are considered as black pixels. Each white pixel $B_{i,j}$is interpreted by the interpolation value obtained by the four black pixels surrounding it using the equation

$$B'_{i,j}=w_1B_{i-1,j}+w_2B_{i+1,j}+w_3B_{i,j-1}+w_4B_{i,j+1} \quad \ldots\ldots..(2)$$

The estimating error is calculated using the equation

$$e_{i,j}=B'_{i,j}-B_{i,j} \quad \ldots\ldots. (3)$$

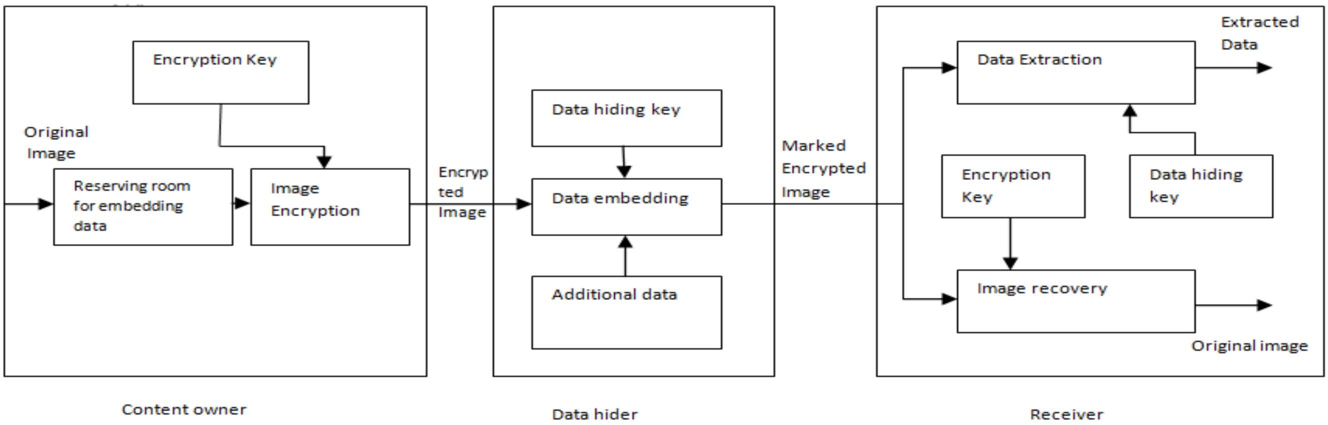

Fig.3. Reversible data hiding by reserving room before encryption (RRBE) framework

Data can be embedded into the estimating error sequence using histogram shift. The histogram of error sequence is first divided into two parts left part and right part and search for the highest point in each part denoted by LM and RM respectively. Then search for the zero point in each part denoted by LN and RN. To embed messages into an estimating error that is equal to RM shift all the error values between RM+1 and RN-1 with one step toward right and 0 bit is represented by RM and 1 bit by RM+1.The embedding process in the left part is similar to that of the right except that the shifting direction is left and the shift is realized by subtracting 1 from the corresponding pixel values. Overflow or underflow problems occur when natural boundary pixels change from 255 to 256 or from 0 to -1.To avoid this data is embedded into the corresponding pixels valued from 1 to 254.When no boundary pixels change from 1 to 0 or from 254 to 255 during the embedding process are referred to as pseudo boundary pixels. A boundary map is used to indicate whether a pixel in the marked image is natural or pseudo boundary pixel. A binary bit sequence with bit 0 indicates natural boundary pixel and bit 1 indicates pseudo boundary pixel. The marginal area of B part is used to accommodate the boundary map. A gray value $X_{i,j}$ ranging from 0 to 255 can be represented as

$$X_{i,j}(k) = \left\lfloor\frac{X_{i,j}}{2^\wedge k}\right\rfloor \text{mod2,k=0,1,2,}\ldots7 \quad \ldots\ldots\ldots.(4)$$

The encrypted bits $E_{i,j}(k)$ can be calculated using

$$E_{i,j}(k)=X_{i,j}(k)\oplus r_{i,j}(k) \quad \ldots\ldots\ldots..(5)$$

where $r_{i,j}(k)$ is determined by a stream cipher determined by the encryption key. After image encryption a data hider or a third party cannot access the content of the original image without using the encryption key. Thus the privacy of content owner is protected.10 bits of information is embedded into the LSB's of first 10 pixels of the encrypted version to tell the data hider about the number of rows where he can embed information.

After getting the encrypted image the data hider adopts LSB replacement method to substitute the available bit planes with additional data m. The data hider sets a label following m to indicate the end of embedding process. The data hider encrypts the data using the data hiding key. Using the encryption key the content owner decrypts the image. Let E' represent the encrypted image containing embedded data. The decrypted image can be calculated by the equation

$$X''_{I,j}(k)=E'_{i,j}(k)\oplus r_{i,j}(k) \quad \ldots\ldots\ldots\ldots\ldots..\ (6)$$

$$X''_{i,j}=\sum_{k=0}^{7} X''_{i,j}(k) \text{ x } 2^{k} \quad \ldots\ldots\ldots\ldots\ldots\ldots(7)$$

To extract the embedded data from the encrypted image, use the data hiding key to decrypt the data. Record the LSB planes from the encrypted image.

IV. RESULTS

The reversible data hiding by reserving room before encryption (RRBE) method is compared with the reversible data hiding by vacating room after encryption (VRAE) method. Both methods are tested on standard images like 'Lena', 'Peppers', 'Baboon', 'Boat'. All images are of size 512 x 512 x 8.

Table 1. PSNR comparison of two methods

Image	PSNR value of RRBE technique (dB)	PSNR value of VRAE technique (dB)
Lena	52.87	44.16
Barbara	53.98	45.94
Baboon	54.87	43.49
Boat	54.97	42.22
Airplane	53.67	45.94

This indicates that data hiding using RRBE method is better than VRAE technique. In vacating room after encryption space for embedding data is found out after encrypting the image. Therefore exact recovery of original image cannot be guaranteed.

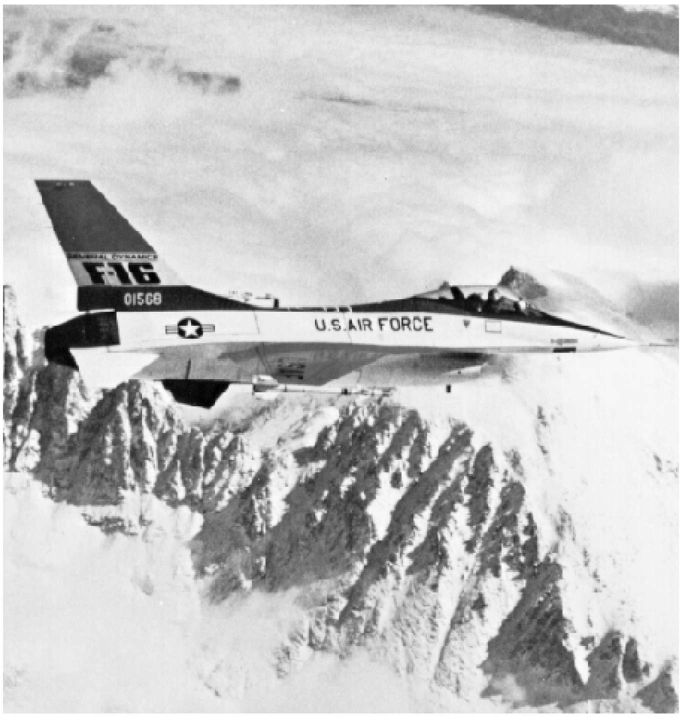

Fig.4. Original image

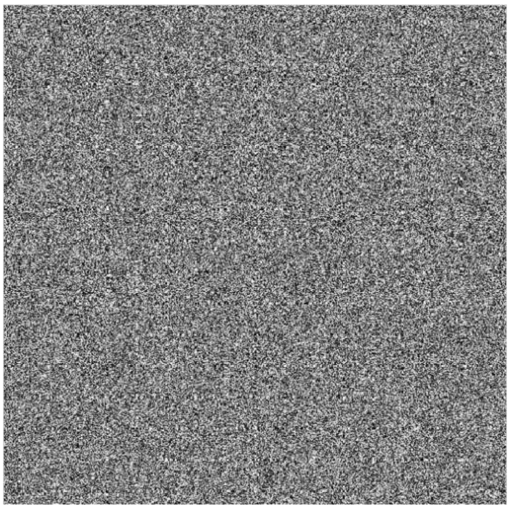

Fig.5. Encrypted image

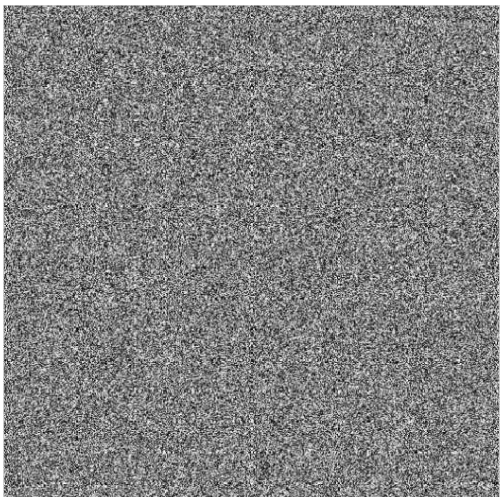

Fig.6. Encrypted image with embedded data

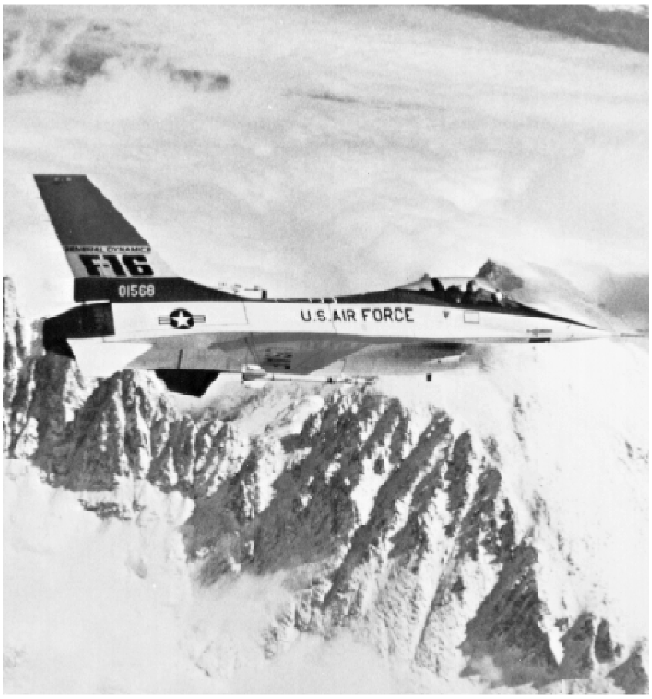

Fig.7. Recovered image

V. Conclusion

In reversible data hiding the original cover can be recovered after the embedded data is extracted from the image.Reversible data hiding in encrypted images by reserving room before encryption technique is easier for the data hider to reversibly embed data in encrypted image. It saves the time needed for creating space after encryption. Image recovery is free of any error. So it can achieve real reversibility. So RRBE method is better than reversible data hiding by VRAE method.

REFERENCES

Akkaya K. and M. Younis, "A survey of routing protocols in wireless sensor networks", *Ad Hoc Networks,* Vol.3, no.3, pp 325-349, May 2005

Alkaraki J.N, A.E Kamal, "Routing techniques in Wireless sensor networks a survey", *IEEE wirelss Communication,* vol.11, no.6.pp.6-28, Dec 2004

Chiang S.Y. and J.L Wang,"Routing analysis Fuzzy logic systems in wireless sensor networks" *IEEE Transactions,* Vol.11, No.2. pp 2-26, Oct 2011

Dr Sami Halawani, Abdul Waheed Khan," Sensor enhancement techniques in wireless sensor networks" *Journal of Computing,* vol.2, may 2011

Hua, C. and T.P Yum, "Optimal routing and data aggregation for maximizing the lifetime of wireless sensor network", *IEEE ACM ,* vol 16 no.4, pp 892-903, Aug 2008.

Jongseok Park and Sartaj Sahni, "An online Heuristic for maximum lifetime routing in wireless Sensor network", *IEEE Transactions ,* Vol.55, No.8, Aug 2006

Junlin li, Ghassan Alkegib, "Network lifetime Maximization for estimation in mulhop wire less sensor network."*IEEE Transactions,* Vol. 57, No.7, July 2009

Karkvandi H. R., E. Pecht, and O.Yadid,"Effective Lifetime aware routing in wireless sensor netwo-rks ", *IEEE Sensors Journal,* Vol 11, No 12, pp. 3359-3367, Dec 2011.

Kobi Cohen and Amir Leshem, "A time varying Opportunistic approach to lifetime maximization Of wireless sensor networks", *IEEE Transactions* vol.58, no.10, October 2010.

Wu, C., R. Yuan, H. Zhou, "A novel load balanced And lifetime maximization routing protocol in wireless sensor network", *IEEE Transactions*, Vol 3 pp. 305-314

****