International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 4, April 2014)

"RDH(Reversible Data Hiding) in Encrypted Images by Reserving Room Before Encryption"

Wagh Mahesh J.[1], Manish Koul[2], Murtadak Sona U.[3], Shinde Kavita S.[4], Prof. Bhandare M.G.[5]
[1,2,3,4]*B.E Comp S.N.D COE & RC, YEOLA)*

***Abstract*- Now a day, more attention is to reversible data hiding (RDH) in encrypted images as well as in audio and video, by using RDH method excellent property that the original image (cover) can be receive as it is recovered after embedded data is extracted also protecting the image content's confidentiality. All previous methods embedding data into image by reversibly vacating room in the encrypted images, which may be result as some errors on data extraction and/or image restoration. That mean some secrete information is loss in data extraction also degraded quality of image.In this paper, we propose a newmethod by reserving room before encryption .By using the new RHD method improvers efficiency of image. The proposed method improve efficiency & quality encrypted image usually used in medical area, aromatic etc.The new AlgorithmUsed in novel RDH are reduce noise Effect.**

***Keywords*- Reversible Data Hiding, image encryption, Novel method of RDH, encryption techniques, difference expansion, histogram shift.**

I. INTRODUCTION

Reversible data hiding (RDH) is a technique in image processing area for encryption, by which the original cover can be losslessly recovered after the embedded message is extracted. The RDH approach is widely used in medical science, defense field and forensic lab, where there is no degradation of the original content is allowed. Since more research RDH method in recently. In theoretical aspect rate-distortion model for RDH Kalker and Willems[1], through which they proved the rate-distortion bounds of RDH for memoryless covers and proposed a recursive code construction which, however, does not approach the bound. The recursive code construction for binary 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.

Many RDH techniques have emerged in recent years. Fridrich *et al*[2] constructed a general framework for RDH for method . By first extracting compressible features of original cover and then compressing them lossless, spare space can be saved for embedding auxiliary data.

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.

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 are few 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.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 4, April 2014)

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 errorcorrecting codes, the pure payloads will be further consumed.

In all methods of [5]–[7], the encrypted 8-bit gray-scale images are generated by encrypting every bit-planes with a stream cipher. The method in [5] segments the encrypted image into a number of nonoverlapping blocks size x*x each block is used to carry one additional bit. To do this, pixels in each block are pseudo-randomly divided into two sets A*B and according to a data hiding key. If the additional bit to be embedded is 0, flip the 3 LSBs of each encrypted pixel in A otherwise flip the 3 encrypted LSBs of pixels in B. For data extraction and image recovery, the receiver flips all the three LSBs of pixels in B to form a new decrypted block, and flips all the three LSBs of pixels in 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.

Hong *et al.* [6] reduced the error rate of Zhang's method [5] by fully exploiting the pixels in calculating the smoothness of each block and using side match.

The extraction and recovery of blocks are performed according to the descending order of the absolute smoothness difference between two candidate blocks and recovered blocks can further be used to evaluate the smoothness of unrecovered blocks, which is referred to as side match. Zhang's method in [7] pseudo-randomly permuted and divided encrypted image into a number of groups with size of M. The N LSB-planes of each group are compressed with a parity-check matrix and the vacated room is used to embed data. For instance, denote the pixels of one group by ,Ai…….Am and its encrypted N LSB-planes by c that consists of M*N bits. The data hider generates a parity-check matrix G sized (M*N-S)*M.N and compresses c as its syndrome such that s=G.C. Because the length of s is(M *N-S). S bits are available for data accommodation. At the receiver side, the 8-N most significant bits (MSB) of pixels are obtained by decryption directly. The receiver then estimates A1(1<=i<=M) by the MSBs of neighboring pixels, and gets an estimated version of c denoted by c` . On the other hand, the receiver tests each vector belonging to the coset of syndrome , where From each vector of , the receiver can get a restored version of , and select the one most similar to the estimated version as the restored LSBs.

III. System Architecture

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.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 4, April 2014)

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.

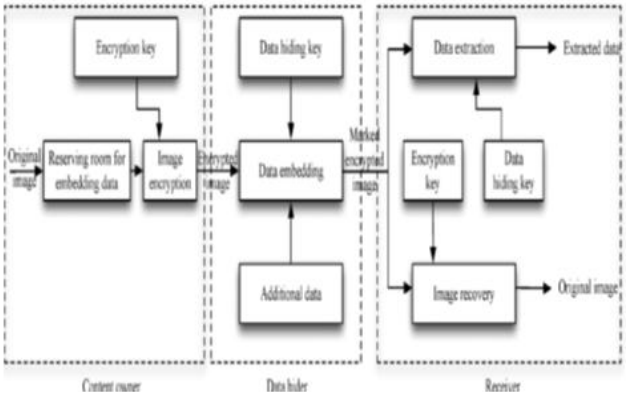

Figure 3.1 Framework of system of RRBE (Existing System).

IV. CONCLUSION

RDH in encrypted images is a new technology which is Drawing enormous attention because of its ability to uphold the content owners privacy and maintain integrity of data also real reversibility of data is realized, that is data extraction and image recovery are free from any error because of these requirements from cloud data management. Proposed methods implement RDH in encrypted images by vacating room before encryption, which is exactly opposed to the existing method of RDH in which we were vacating room after encryption.

Thus the data hider get advantage from the extra space which is created by vacating the room in previous stage to make data hiding process effortless because of proposed method. Thus the proposed method can take benefit of all previous RDH techniques for plain image and attain extremely good performance without loss of privacy and quality of data. At last we can say, this proposed method can achieve real reversibility, separate data from encrypted version of image and highly improve the quality of marked decrypted images.

REFERENCES

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

[2] J. Tian, "Reversible data embedding using a difference expansion,"IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896,Aug. 2003.2010.Process., vol. 19, no. 4,pp. 1097–1102, Apr. 2010.

[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] 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.

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

[6] 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.

[7] X. Zhang, "Separable reversible data hiding in encrypted image," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012. 0000000000000000000000000000000000000*