International Journal of Science Engineering and Advance Technology

Evaluate The Quality Of Marked Decrypted Image Quantitatively To Encrypted Images Using Rdh

1**N.Bhaskar**, 2**VijayKumar Janga**
1,2Dept. of CSE, Balaji Institute of Technology & Science, Narsampet, w.g.dt,AP, India

Abstract:
Encryption is an effectual and popular means as it converts the original and significant content to incomprehensible one. Even though few RDH methods in encrypted images have been published yet there are some talented applications if RDH can be applied to encrypted images. Hwang *et al.* supported a reputation-based trust-management system enhanced with data colouring a way of embedding data into covers and software watermarking in which data encryption and colouring offer potential for upholding the content owner's privacy and data integrity. Apparently the cloud service provider has no right to commence everlasting distortion during data colouring into encrypted data. Therefore a reversible data colouring technique based on encrypted data is preferred. Suppose a medical image database is stored in a data centre and a server in the data centre can implant notations into an encrypted version of a medical image through a RDH technique. With the notations the server can handle the image or confirm its integrity without having the knowledge of the original content and thus the patient's privacy is protected. On the other hand a doctor having the cryptographic key can decrypt and reinstate the image in a reversible manner for the reason of additional diagnosing.

Keywords: Reversible data hiding (RDH), image encryption, privacy protection and histogram shift.

Introduction:
Reversible data hiding (RDH) in images is a method by which the original cover can be lossless improved after the embedded message is extracted. This significant technique is extensively used in medical imagery, military imagery and law forensics where no deformation of the original cover is allowed. Since first introduced RDH has concerned considerable research interest. Recently more and more concentration is paid to reversible data hiding (RDH) in encrypted images because it uphold the excellent property that the original cover can be lossless recovered after embedded data is extracted while protecting the image content's privacy. All previous methods embed data by reversibly check out of room from the encrypted images which may be subject to some mistakes on data extraction and/or image restoration. In this paper we propose a novel method by reserving room before encryption with a traditional RDH algorithm and thus it is easy for the data hider to reversibly embed data in the encrypted image. The proposed method can attain real reversibility that is data extraction and image recovery is free of any error.

Related Work:
Several RDH methods have appeared in recent years. Fridrich *et al.* built a common framework for RDH. By first extracting compressible features of original cover and then compressing them lossless extra space can be saved for embedding auxiliary data. A more popular method is based on difference expansion 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 can be used for embedding messages. An additional promising scheme for RDH is histogram shift (HS) in which space is set aside for data embedding by shifting the bins of histogram of gray values. The state-of-art methods frequently combined DE or HS to residuals of the image e.g. the predicted errors to accomplish better performance. Some attempts on RDH in encrypted images have been made. Zhang divided the encrypted image into several blocks. By flipping 3 LSBs of the half of pixels in each block room can be vacated for the embedded bit. The data extraction and image recovery go on by finding which part has been flipped in one block. This process can be understood with the assist of spatial correlation in decrypted image.

Existing System:
Since lossless vacating room from the encrypted images is comparatively hard and from time to time incompetent. The method in compacted the encrypted LSBs to vacate room for additional data by searching 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. Though since the entropy of encrypted images has been maximized

these techniques can only attain small payloads produce marked image with poor quality for large payload and all of them are subject to some error rates on data extraction and/or image restoration.

Disadvantages:

Low error rate. Data extraction and image restoration problem.

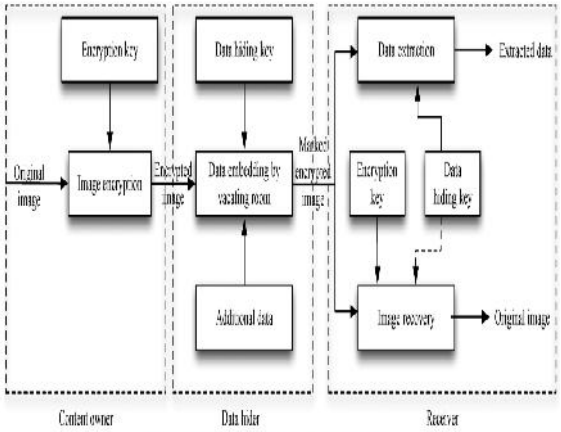
Proposed System:

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

Advantages:

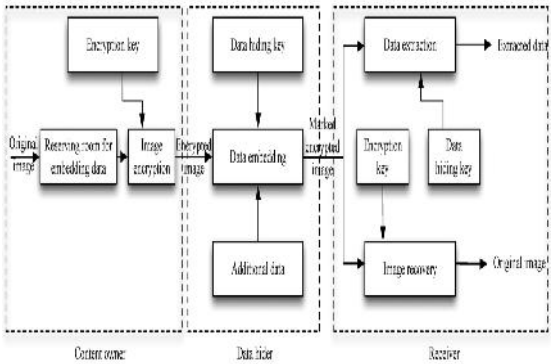
Real reversibility is realized that is data extraction and image recovery are free of any error. For given embedding rates the PSNRs of decrypted image containing the embedded data are significantly improved and for the acceptable PSNR the variety of embedding rates is greatly enlarged.

Vacating Room After Framework:



Vacating Room After Encryption Framework

Reserving Room Before Encryption Framework:



Reserving Room Before Encryption Framework

Encrypted Image Generation:

At the commencement image partition step separates original image into two parts and then the LSBs of are reversibly embedded into with a standard RDH algorithm so that LSBs of can be used for accommodating messages at last encrypt the rearranged image to generate its last version.

Image Partition:

The operator is here for reserving room before encryption is a standard RDH technique so the goal of image partition.

Self Reversible Embedding:

The objective of self-reversible embedding is to embed the LSB-planes of into by employing traditional RDH algorithms. We make simpler the method in to make obvious the process of self-embedding.

Data Hiding In Encrypted Image:

A content owner encrypts the original image using a standard cipher with an encryption key. After creating 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 supplementary data into the encrypted image by lossless vacating some room according to a data hiding key. Then a receiver perhaps the content owner himself or an authorized third party can take out the embedded data with the data hiding key and further recuperate the original image from the encrypted version according to the encryption key.

Data Extraction And Image Recovery:

Extracting Data from Encrypted Images to handle and update personal information of images which are encrypted for protecting client's privacy an inferior database manager may only get right to use the data hiding key and have to influence 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 completely operated on encrypted domain it keeps away from the escape of original content.

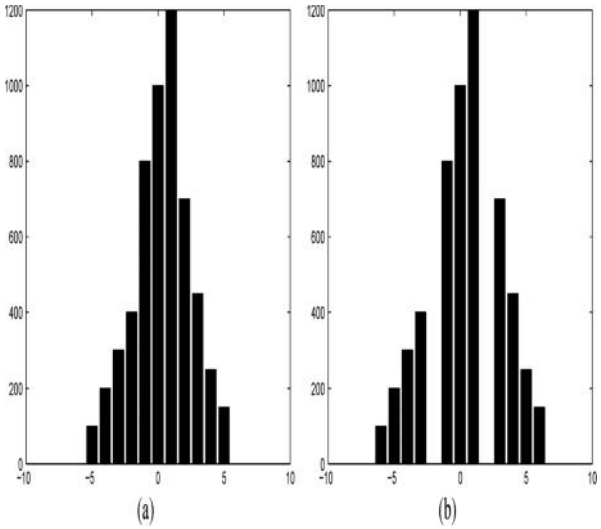
Data Extraction And Image Restoration:

After producing the marked decrypted image the content owner can further extract the data and recover original image.

Results:

In general two solutions can increase considerably improvement in terms of PSNR when the length of data is comparatively short. And the advantage of one solution over the other depends highly on statistics of natural image itself. The same with other RDH algorithms overflow/underflow problem occurs when natural border pixels change from 255

to 256 or from 0 to -1. To keep away from it we only embed data into approximation error with its corresponding pixel valued from 1 to 254. Though ambiguities still arise when no boundary pixels are misshapen from 1 to 0 or from 254 to 255 throughout the embedding process. These created boundary pixels in the embedding process are defined as pseudo-boundary pixels. Hence a boundary map is brought in to tell whether boundary pixels in marked image are natural or pseudo in extracting process.



(a) original histogram, (b) shifted histogram

CONCLUSION:

Previous methods put into practice 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 advantage from the extra space emptied out in previous stage to make data hiding process easy. The proposed method can take advantage of all traditional RDH techniques for plain images and accomplish excellent performance without loss of perfect secrecy. Besides this novel method can achieve real reversibility, separate data extraction and greatly improvement on the quality of marked decrypted images. Reversible data hiding in encrypted images is a novel topic drawing attention since the privacy-preserving requirements from cloud data management.

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 imagewatermarking 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.

[13] K. Hwang and D. Li, "Trusted cloud computing with secure resources and data coloring," *IEEE Internet Comput.*, vol. 14, no. 5, pp. 14–22, Sep./Oct. 2010.

[14] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing

encrypted data," *IEEE Trans. Signal Process.*, vol. 52, no. 10, pp. 2992–3006, Oct. 2004.

[15] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," *IEEE Trans. Image Process.*, vol. 19, no. 4, pp. 1097–1102, Apr. 2010.

Authors:

Mr.N.Bhaskar is a student of Balaji Institute of Technology & Science, Narsampet. Presently he is pursuing his M.Tech [Computer Science & Engineering] from this college and he received his B.Tech from Balaji Institute of Engineering and Sciences, affiliated to JNT University, Hyderabad in the year 2012. His area of interest includes Web Programming, Network Security and Object oriented Programming languages, all current trends and techniques in Computer Science.

Mr.Vijaykumar Janga, well known Author and excellent teacher Received M.Tech (CSE) from JNTU Hyderabad and Pursuing PhD from JNTU Hyderabad university is working as Assistant Professor in M.Tech Computer science engineering , Balaji Institute of Technology & Science. He has 8 years of teaching experience in various institutions affiliated to JNTU Hyderabad. His area of Interest includes Data mining, Information retrieval systems and Knowledge Engineering
.