International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2016): 79.57 | Impact Factor (2017): 7.296

Reversible Data Hiding in Encrypted Images by Vacating Space in Advance

Prerna N. Deshmukh[1], Praveen Sathya[2]

[1] Dr.Babasaheb Ambedkar Marathwada University, Aurangabad, SY.College of Engineering and Technology, Aurangabad., India

[2] Assistant Professor at of SY.College of Engineering and Technology, Aurangabad. Dr.Babasaheb Ambedkar Marathwada University, Aurangabad, India

Abstract: ***Recently, more and more attention is paid to reversible data hiding (RDH) in encrypted images, since it maintains the excellent property that the original cover can be losslessly recovered after embedded data is extracted while protecting the image content's confidentiality. All previous methods embed data by reversibly vacating room from the encrypted images, which may be subject to some errors on data extract ion 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 achieve real reversibility, that is, data extraction and image recovery are free of any error. Experiments show that this novel method can embed more than 10 times as large payloads for the same image quality as the previous methods, such as for PSNR dB.***

Keywords: Reversible data hiding, image encryption, privacy protection, histogram shift

1. Introduction

In the current trends of the world, the technologies have advanced so much that most of the individuals prefer using the internet as the primary medium to transfer data from one end to another across the world. There are many possible ways to transmit data using the internet: via emails, chats, etc.

The data transition is made very simple, fast and accurate using the internet. However, one of the main problems with sending data over the internet is the security threat it poses i.e. the personal or confidential data can be stolen or hacked in many ways. Therefore it becomes very important to take data security into consideration, as it is one of the most essential factors that need attention during the process of data transferring.

Data security basically means protection of data from unauthorized users or hackers and providing high security to prevent data modification. This area of data security has gained more attention over the recent period of time due to the massive increase in data transfer rate over the internet. In order to improve the security features in data transfers over the internet, many techniques have been developed like: Cryptography, Steganography. While Cryptography is a method to conceal information by encrypting it to „cipher texts" and transmitting it to the intended receiver using an unknown key, Steganography provides further security by hiding the cipher text into a seemingly invisible image or other formats.

There are also a number of works on data hiding in the encrypted domain. The reversible data hiding in encrypted image is investigated in. Most of the work on reversible data hiding focuses on the data embedding/extracting on the plain spatial domain. This 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 achieve real reversibility, that is, data extraction and image recovery are free of any error. Thus the data hider can benefit from the extra space Emptied out in previous stage to make data hiding process effortless. The proposed method can take advantage of all traditional RDH techniques for plain images and achieve excellent performance without loss of perfect secrecy.

2. Existing System

In this Existing System, 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? The method in 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 generate 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.

3. Proposed System

In proposed method can achieve real reversibility, that is, data extraction and image recovery are free of any error. 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)".

4. Techniques Used

The idea is all about gaining an understanding on the fundamentals and state of the art of the area. The main objective of this survey is to approach latest methods and theories related to following aspect.

The Literature Survey for this project is divided into 2 parts:
1) Basic reversible data hiding techniques for plain spatial domain.
2) Reversible data hiding techniques for encrypted image
3) Basic reversible data hiding techniques for plain spatial domain

Proposed method of reversible data embedding based on difference expansion.

Author:Tian

Due to redundancy between the values of neighboring pixel in natural images, differences between pixels are used to embed data. In method of difference expansion method, the differences between two adjacent neighboring pixels are calculated and expanded or doubled i. e. multiplied by 2 and new least significant bits are generated. New least significant bits are used to hide additional data. A.M. Alattar proposed Generalized DE based method ,in which Tian's pixel-pair difference expansion was extended using difference expansion of vectors.

The advantages are – (i) no loss of data due to compression and decompression, (ii) it can be applicable to audio and video data. The disadvantages include – (i) there may be some round off errors , though very little, (ii) mainly depends on the smoothness of natural image; so cannot be applied to textured image where the capacity will be zero or very low, and (iii) there is significant degradation of visual quality due to bit-replacements of gray scale pixels.

Histogram-based reversible data hiding technique.
Author :Ni *et al.*

The data is embedded into the bins of histogram. This method utilizes pairs of peak points and zero points to achieve low embedding distortion. The advantages of this method are – (i) it is simple to use, (ii) it always gives a constant PSNR 48.0dB, (iii) distortions are quite invisible, and (iv) capacity is high. The disadvantages are – (i) capacity is limited by the frequency of peak-pixel value in the histogram, and (ii) it searches the image more times, so the algorithm is more time consuming. Ni et al. increased the hiding capacity by extending the histogram modification technique for integer wavelet transform.

Reversible data hiding method based on Interpolation Technique (IT)
Author: L. Luo

In which concealed data into interpolation errors. Instead of using the nearest neighbour interpolation technique, an image interpolation algorithm was used to obtain the interpolation errors. The reference pixels are adaptively selected in the original cover image and pixels other than the reference pixels are interpolated. Interpolation errors are calculated by subtracting the interpolated pixels from the original image. Data bits were concealed by modifying the interpolation errors. Because reference pixel values were not changed in the embedding process, the same set of interpolated pixels could be obtained in the decoding process and thus, the embedded data bits could be extracted and the original image was restored. In this technique, they reduced the number of reference pixels in smooth regions and increased the number of reference pixels in complex regions. But the distortions in the output image were much higher in histogram shifting method . However, in most cases, the number of reference pixels affects the payload and the stego image quality. Interpolation Technique is less secure against image manipulations and steganalysis due to the presence of LSB replacement style asymmetry.

Data hiding behind corners: using edges in images
Author :K. Hempstalk

In certain techniques do not take into account the cover's original information thereby they leave certain marks on the stego image. In Hiding behind Corners (HBC), this was avoided by taking the original information of cover. Two algorithms are used in HBC based on using image filters to determine the effective hiding places in an image. They were Filter First and BattleSteg. The main strength of FilterFirst was that it eliminates the need to provide any additional information such as original image. It was also very effective in hiding or embedding information. Whereas the disadvantage of Filter First was that it was not secure, because an attacker can repeat the filtering process. It could be also much easier to retrieve the hidden information once the stegoimage is identified. The strength of BattleSteg was that it requires a password to retrieve the message. Its weakness includes the absence of a random seed so it was impossible to know where to place the shots and also it was possible for BattleSteg to never have a hit. Hiding Behind Corners approach effectively utilizes edge areas but embedding capacity is less.

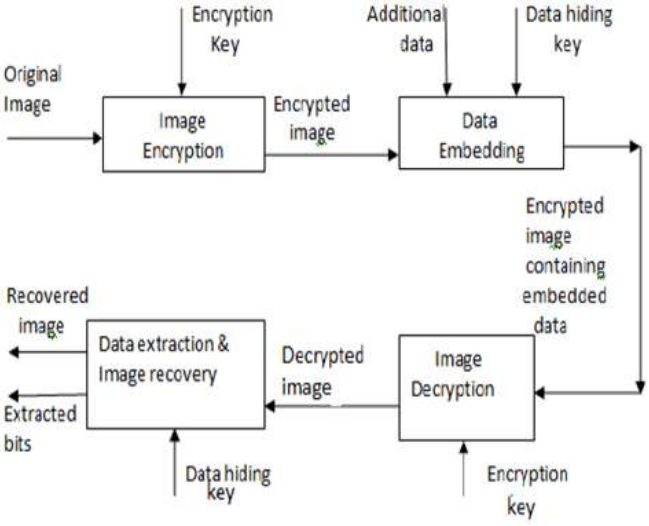
Hiding Secret Message in Edges of the image in , introduced a new least significant bit embedding algorithm for hiding secret messages in non-adjacent pixel locations at the edges of images. Here the messages were hidden in regions which were least like their neighboring pixels i.e. regions that contain corners, edges, thin lines etc., so that an attacker will have no or less suspicion of the presence of message bits in edges, because pixels in edges of an image appears to be much brighter or dimmer than their neighbors.

Capacity-approaching codes for reversible data hiding
Author : W. Zhang

By improved the recursive construction by using not only conditional compression but also conditional embedding, which enables to design an efficient embedding algorithm and a perfect compressing method to approach the rate distortion bound. In that, the receiver could extract messages from the marked cover with the help of the reconstructed

cover because of reversibility. However, there are still limitations in two aspects in. First, they construct embedding codes by improving the decompression algorithm of run-length coding, by which the recursive code construction is close to but cannot reach the rate–distortion bound. Second, the codes are restricted to some discrete embedding rates and cannot approach the maximum embedding rate at the least admissible distortion.

2) Reversible data hiding techniques for encrypted image
There are two different types of reversible data hiding for an encrypted image; non separable and separable reversible data hiding. A method of non separable reversible data hiding in encrypted image is as shown in Fig.1. Non separable data hiding technique is consisting of image encryption, data embedding, and image decryption and image recovery/data extraction phases.



Non separable reversible data hiding in encrypted image

First content owner encrypt the original uncompressed image by using encryption key to produce encrypted image and then data hider embeds additional data into encrypted image using data hiding key though he does not know the content of original image. With encrypted image containing additional data, the receiver may first decrypt it using encryption key and then extract the embedded data and recover the original image using data hiding. That is in this technique, the data extraction is not separate from image recovery.

Reversible data hiding scheme for encrypted image consisting of image encryption
Author:Xinpeng Zhang

First content owner encrypts the original image by a stream cipher. Then segments the encrypted image into number of non overlapping blocks of size a× a; each block is used to carry one additional bit. For this, pixels in each block are pseudo-randomly divided into two different sets S1 and S2 according to a data hiding key. If the bit to be embedded is 0, flip the 3 LSBs of every encrypted pixel in S1 otherwise flip the 3 encrypted LSBs of pixels in S2. For extraction of data and image recovery, the receiver flips all three LSBs of pixels in S1 to form a new decrypted block, and flips all three LSBs of pixels in S2 to form another new block; one of them will be decrypted to the original block. Because of spatial correlation in natural images, original block is presumed to be smoother than interfered block and embedded bit can be extracted correspondingly.

Proposed improved version of reversible data hiding in encrypted images using side match technique.

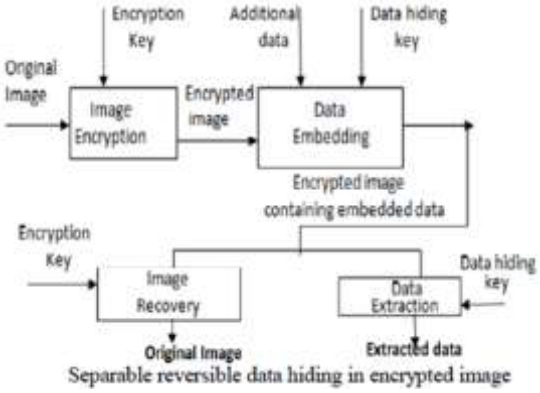
Author: Hong et al.

It is non separable reversible data hiding technique. In Hong et al. reduced the error rate of Zhang's method by fully exploiting the pixels in calculating the smoothness of each block and using side match technique. The recovery of blocks and extraction 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. The side match technique is employed to further reduce the error rate. The experimental results show that the propose method effectively improves Zhang's method, especially when the block size is small.

In, Xinpeng Zhang suggested technique for separable reversible data hiding in encrypted image. Separable reversible data hiding technique is as shown in Fig.:

Zhang creates space for data embedding by following the idea of compressing encrypted images First the content owner encrypts the original image using an encryption key. Once image is encrypted, data hider compresses the least significant bits of the encrypted image using a data-hiding key and creates a sparse space to accommodate the additional data. On other end, from an encrypted image containing additional data, using only the data-hiding key, the receiver may extract the additional data, or obtain an image as the original one using only the encryption key. When the receiver has both data hiding and encryption keys, he can extract the additional data and recover the original content without any error by exploiting the spatial correlation in natural image if the amount of additional data is not too large.

The method in based on framework reserving room after encryption. Lossless vacating room from encrypted images is relatively difficult and sometimes inefficient and generate marked image with poor quality for large payloads.



Separable reversible data hiding in encrypted image

5. 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 effortless. 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] D. M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for eversible watermarking,"IEEE Trans. Image Process.,vol.16,no.3, pp. 721–730, Mar. 2007.
[2] 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.
[3] 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.
[4] L. Luoet al., "Reversible image watermarking using interpolation tech-nique,"IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 187–193, Mar. 2010
[5] K. Hwang and D. Li, "Trusted cloud computing withsecure resources and data coloring,"IEEE Internet Comput., vol. 14, no. 5, pp. 14–22,Sep./Oct. 2010
[6] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL, USA: CRC, 1996 .
[7] C.-C. Chang, C.-C. Lin, and Y.-H. Chen, "Reversible data-embedding scheme using differences between original and predicted pixel values," IET Inform. Security, vol. 2, no. 2, pp. 35–46, 2008.
[8] M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. G. B. Natale, and A. Neri, "A commutative sdigital image watermarking and encryption method in the tree structured Haar transform domain,"Signal Pro-cessing: Image Commun., vol. 26, no. 1, pp. 1–12, 2011.
[9] T. Bianchi, A. Piva, and M. Barni, "Composite signal representation for fast and storage-efficient processing of encrypted signals,"IEEE Trans.Inform. Forensics Security, vol. 5, no. 1, pp.180–187,Feb.2010.

Author Profile

Prerna N. Deshmukh Student of SY.College of Engineering and Technology, Aurangabad.

Praveen Sathya Assistant Professor at SY.College of Engineering and Technology, Aurangabad.