International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Separable Reversible Data Hiding – A Review

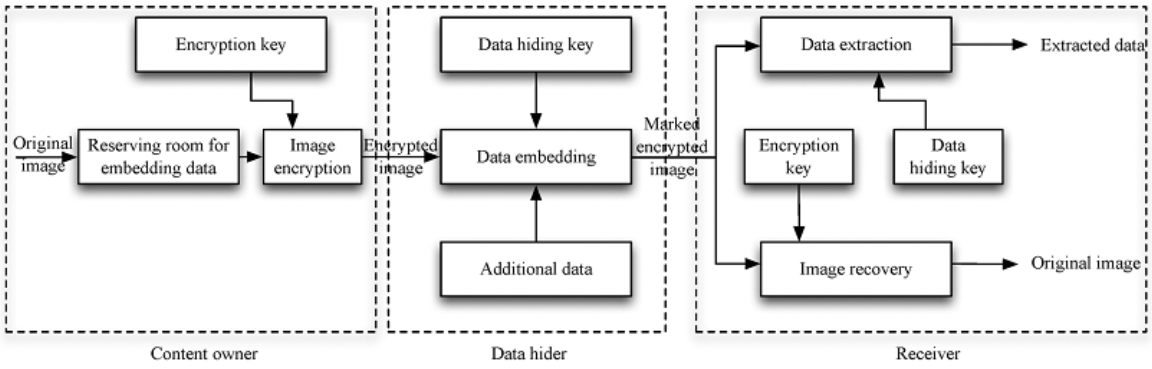
Suyash Sharma, Jaipal Bisht

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 some errors on data extraction and/or image restoration. In this paper we propose a different scheme which attains real reversibility by reserving room before encryption with a traditional RDH algorithm, and then encrypting the data and embedding the data in the encrypted image, which is encrypted using a new proposed algorithm. The proposed method can achieve real reversibility that is data extraction and image recoveries are free.***

Keywords: RDH, Image partition, AES, PSNR, data embedding,

1. Introduction

The amount of digital images has increased rapidly on the Internet. Image security becomes increasingly important for many applications, e.g., confidential transmission, video surveillance, military and medical applications. For example, the necessity of fast and secure diagnosis is vital in the medical world. Nowadays, the transmission of images is a daily routine and it is necessary to find an efficient way to transmit them over networks. To decrease the transmission time, the data compression is necessary. The protection of this multimedia data can be done with encryption or data hiding algorithms. Since few years, a problem is to try to combine compression, encryption and data hiding in a single step. For example, some solutions were proposed in to combine image encryption and compression. Two main groups of technologies have been developed for this purpose. The first one is based on content protection through encryption. There are several methods to encrypt binary images or gray level images. The second group bases the protection on data hiding, aimed at secretly embedding a message into the data. Nowadays, a new challenge consists to embed data in encrypted images. Previous work proposed to embed data in an encrypted image by using an irreversible approach of data hiding or data hiding, aimed at secretly embedding a message into the data. A new idea is to apply reversible data hiding algorithms on encrypted images by wishing to remove the embedded data before the image decryption. Recent reversible data hiding methods have been proposed with high capacity, but these methods are not applicable on encrypted images.



Figure

Separable Reversible Data hiding

As name itself indicates that it is the reversible data technique but which is separable. The separable means which is able to separate .In other words, we can separate the some things, activities using suitable criteria. Here in separable reversible data hiding concept. The separation of activities i.e. extraction of original cover image and extraction of payload (data which was embedded).This separation requires some basic cause to occur. In separable data hiding key explained by Xin peng Zhang the separation exists according to keys. Here at the receiver side, there are three different cases are encountered. The separation of extracting the data and getting the cover media come to be exists. That's why it is called as Separable Reversible Data hiding..

Why Reversible Data Hiding

As the technology has increased day by day the usage of multimedia, web documents and images has also increases on the network. Large amount of images are transferred on the internet every day, so it's necessary to provide security to these images from the hackers. It may happen that the hackers may capture the images, view the important contents and after viewing the contents they can modify the images and send it to destination. So the original image contents will be modified and the receiver can be totally unaware from this fact. Due to this, a small amount of distortion has occurred. Such distortion is not acceptable in some applications, such as medical imaging or in military images etc., because it may lead to risks of incorrect decision making. From this point of view a data hiding technique, which is referred to as reversible, invertible, lossless, or distortion-free, has been

developed in recent years [2]. In this review, a reversible data hiding methods which produces stego images with good qualities and high data hiding capacities are proposed. Reversible data hiding techniques [5] can be implemented to restore original images after the hidden data has been extracted out

2. Different Data Hiding Algorithms

The reversible data hiding was carried out using reversible data hiding algorithms. These algorithms are classified as following.

Separable Reversible Data Hiding in Encrypted Image
This technique proposes a novel scheme for separable reversible data hiding in encrypted images [6]. In the proposed method, a content owner (sender) encrypts the original uncompressed image using an encryption key. Then, a data hider may compresses the least significant bits (LSB) of the encrypted image using a key known as a data-hiding key to create a sparse space to accommodate some additional data. Now with an image i.e. the encrypted image containing the additional data, if the receiver has a data-hiding key, then he can extract the additional data though he does not have an idea about the original image content [7]. If the receiver at the destination has an encryption key, then the receiver can decrypt the received data to obtain the image similar to the original image that is to be transferred, but receiver cannot extract the additional data. If the receiver has both the keys i.e. data-hiding key and the encryption key, then receiver can extract the additional data which can also be called as watermark and recover the image i.e. the original content of the image without any bugs or any error by exploiting the spatial correlation, spatial space in original or natural image when the amount of additional data or the watermark is not too large. The scheme proposed in this paper is made up of image encryption, data embedding and data-extraction/image-recovery phases [7]. The sender also known as the content owner encrypts the original uncompressed image using the image encryption algorithms and using a key known as the encryption key to produce an encrypted image. Then, the data hider compresses the least significant bits (LSB) of the encrypted image using a data-hiding key for creating a sparse space to store the additional data or the watermark information. At the destination side, the data embedded in the image can be retrieved easily from the encrypted image containing additional data according to the data-hiding key. Since the embedding of data only affects the LSB, a decryption of the image with an encryption key can result in an image that is similar to the original version of the image. When both keys are used by receiver i.e. the encryption and data-hiding keys, the additional data embedded can be extracted successfully and the original image can be recovered perfectly by exploiting the spatial correlation in natural image. The disadvantage of this technique was eliminated by proposing a new scheme known as the separable reversible data hiding scheme [7]. This technique proposes the scheme of separable reversible data hiding by removing the disadvantages of non separable scheme.

Reversible Data Hiding With Optimal Value Transfer
In reversible data hiding techniques, the values of sender image are modified. According to some constraints the original content of the image can be correctly restored after extracting the watermark data on the receiver side [8]. According to this technique, the optimal constraint of value modification using a payload-distortion criterion is founded by using the iterative procedure, and a reversible practical data hiding scheme was proposed [7]. The secret data, as well as the auxiliary information used for recovering the content, were carried out by the differences between the original pixel-values and the corresponding values estimated from the neighbors [8]. In this, the errors estimated [9] were modified according to the optimal value transfer rule. Also, the original image was divided into a number of subsets of the pixel and the additional information of the subset were always embedded into the errors estimated in the next subset. The receiver could successfully extract the content i.e. the embedded secret data and recover the original content of the image in the subsets with an inverse order [7]. According to this technique, a good performance is achieved for the reversible data hiding. In this scheme, the secret watermark data, as well as the auxiliary information used for content recovery, were carried out by the differences between the original pixel-values and the corresponding values estimated from the neighbors, and the estimation errors are modified according to the optimal value transfer matrix [8]. The optimal value transfer matrix is produced for maximizing the amount of secret data, i.e., the pure payload, by the iterative procedure as described in the section. It also stated that the size of auxiliary information can not affected the optimality of the transfer matrix. By pixel division in the original image into two different sets and a number of different subsets, the embedding of the data is orderly performed in the subsets, and then the auxiliary information of a subset is always generated and embedded into the estimation errors in the next subset [7]. Similarly, the receiver could successfully extract the embedded secret data and could recover the original content in the subsets with an inverse order

3. Types of Encryption

A. Hashing Encryption
This is known as the first encryption method, creates a unique fixed-length signature for a message or data set. These are created with hash function, and we commonly use them to compare data set. Since a hash is unique to a specific message, even minor changes to that message result in an exponentionaly different hash, there user alerting to potential tampering by some resource.

B. Symmetric Encryption
Symmetric cryptography, also called private-key cryptography, this is one of the oldest and most Secure encryption methods. The term "private key" comes from the fact that the key used to encrypt and decrypt data must remain secure because anyone with access to it can read the coded messages. A sender encodes a message into cipher text using a key, and the receiver uses the same key to decode the information from the image which is very important for the robustness of the image and this key is generated by a function.

4. Reversible Data Hiding Techniques

Reversible data hiding techniques can be employed to restore stego-images to their pristine states after the hidden data are extracted. Such techniques can be classified into three groups: 1. Based on data compression 2. Based on pixel-value difference expansion 3. Based on histogram shifting . The strategy used in the techniques of the first group is to compress message data as well as related information and embed the result directly into the cover image. A method in this group is Barton which compresses the secret message before embedding them into the bit stream of digital data. a high-capacity lossless data hiding method which quantizes each image pixel by into L-level scales, compresses the quantization residues, and embeds the secret bits as well as the compressed data into the quantified image by the least-significant-bit (LSB) substitution technique. The second group of reversible data hiding methods aims to explore the redundancy of pixel values in images. A technique of pixel-value difference expansion by performing fundamental arithmetic operations on pairs of pixels to discover hide able space. A location map is used to indicate whether pairs are expanded or not. An enhanced pixel-value difference expansion method proposed here which used a refined location map and a new concept of expandability to achieve higher data hiding capacities while keeping the resulting image distortion as low as that yielded . The last group of reversible data hiding methods, to which the proposed method belongs, is based on the concept of histogram shifting. Here a reversible data hiding method which shifts slightly the part of the histogram between the maximum point (also called the peak point) and the minimum point to the right side by one pixel value to create an empty bin besides the maximum point for hiding an input message. Advantages of this method include yielding superior hiding capacities and providing higher qualities in stego-images. The knowledge of the maximum point and the minimum point of the histogram is necessary for retrieving the hidden data and restoring the stego-image lossless to the original state. In addition, the coordinates of the pixels whose gray values equal to the gray value of the minimum point b need be recorded as overhead information when the value of b is not zero. Consideration of multiple pairs of maximum and minimum points was also included in the method in order to raise the data hiding capacity, at the sacrifice of the resulting stegoimage quality. A problem occurs here when too many of such pairs are selected for data hiding. In such a case, a rapid increase of the size of the overhead information, which cannot be embedded completely in the cover image, might occur. So the idea of decomposing the entire cover image into blocks and using the peak point of the histogram of each block to hide data. The technique of block division successfully improves the data hiding capacity and keeps the stego-image quality at the same level, later the concept of slightly adjusting the pixel values located at both sides of a histogram peak to embed message data.. The Peak Signal-to-Noise Ratio (PSNR) of the stego-image needs a modification in some cases. A modification of the method using several pairs of peak points and minimum points instead of just one was also proposed. However, the more of such pairs are selected, the larger the decrease in the data hiding capacity becomes, because more information of the selected minimum points and the reversible points need be kept in the location map. Later used the block division technique to increase the data hiding capacity.

5. Theory of Separable Reversible Data Hiding

REVERSIBLE data hiding (RDH) in images is a technique, by which the original cover can be lossless recovered after the embedded message is extracted. This important technique is widely used in medical imagery, military imagery and law forensics, where no distortion of the original cover is allowed. Since first introduced, RDH has attracted considerable research interest. With the advance of computer networks and signal processing, digital multimedia are spread widely through the Internet nowadays. This causes the security problem of exposing transmitted digital data on the network with the risk of being copied or intercepted illegally. In order to protect the privacy of private data, various cryptographic techniques have been proposed to encrypt these data before conducting data transmission. However, with considerable increasing of the computing powers of modern computers, the security of the data yielded by these techniques is threatened. In addition, though cryptographic techniques encrypt secret messages into unrecognizable forms before transmission, the undisguised appearances of the encrypted message would easily arouse suspicion and bring on unexpected attacks from hackers. The development of information hiding techniques provides another solution to protecting digital media. Such techniques may be employed to embed private or secret information into cover media in such a way that the existence of the hidden information is imperceptible but known only to a preconcerted recipient. Information like private annotations, business logos, and critical intelligence can be embedded into a cover image in an invisible form so that many applications, like ownership claim of digital contents, copyright protection of media, covert communication between parties, etc., can be fulfilled. Information hiding techniques used for covert communication are often called steganography, and those for ownership or copyright protection are often called watermarking. In the early phase, conventional steganography emphasizes exploring higher hiding capacities and pursuing lower quality degradations in watermarked images (also referred to as stego-images in the sequel). In general, a small amount of content loss will occur in the stego-image, though often imperceptible. However, such a loss is not desirable in some applications, such as legal documentation, military reconnaissance, high-precision scientific investigation, etc., because it may lead to risks of incorrect decision making. In view of this, a type of novel data hiding technique, which is referred to as reversible, invertible, lossless, or distortion-free, has been developed in recent years. In this study, a reversible data hiding method which yields stego-images with good qualities and high data hiding capacities is proposed.

6. 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] X. Zhang, "Lossy compression and iterative reconstruction for encrypted image," IEEE Trans. Inform. Forensics Security, vol. 6, no. 1, pp. 53–58, Feb. 2011. [2]W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of

[2] Encrypted grayscale images," IEEE Trans. Image Process., vol. 19 no. 4, pp. 1097–1102, Apr. 2010.

[3] 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.

[4] W. Hong, T. Chen, and H .Wu, "An improved reversible data hiding in encrypted images using side match," *IEEE Signal Process. Let*, vol. 19, no. 4, pp. 199–202, Apr. 2012

[5] Y. C. Lin, "Reversible data hiding for progressive image transmission," Signal Processing: Image Communication, vol. 26, no. 10, pp. 628–645, Nov. 2011.

[6] C. Candan. A Transcoding Robust Data Hiding Method for Image Communication Applications. IEEE International Conference on Image Processing, 2005, vo!.3: 660-663.

[7] M. Ashourian, P. Moallem, Y. S. Ho. A Robust Method for Data Hiding in Color Images. Lecture Notes in Computer Science, 2005, vo!.3768: 258-269.

[8] A. Parisis, P. Carre, M. C. Fernandez, N. Laurent. Color Image Watermarking with Adaptive Strength of Insertion. IEEE International Conference on Acoutstics, Speech, and Signal Processing, 2004, vol.3: 85-88.

[9] Z. Ni, Y. Q. Shi, N. Ansari, W. Su, Q. Sun, X. Lin. Robust Lossless Image Data Hiding. IEEE International Conference on Multimedia and Expo., 2004: 2199-2202.

[10] 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]

[11] Miscellaneous Gray Level Images [Online]. Available: http://decsai. ugr.es/cvg/dbimagenes/g512.php