IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 9, Issue 3, Ver. V (May - Jun. 2014), PP 44-47
www.iosrjournals.org

A Review on Reversible Data Hiding Techniques

Aparna Gopinath P.K, Grace John
PG Scholar,Dept of ECE VJEC,Chemperi
Assistant Professor,Dept of ECE VJEC,Chemperi

Abstract: *Security and integrity of data are two challenging areas for research.Nowadays 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.It is used widely 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 discusses about the different reversible data hiding techniques.*
Index terms*: Reversible data hiding, histogram, image encryption*

I. Introduction

Data hiding is a process to embed data 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 other applications, like remote sensing and high-energy particle physical experimental investigation,it is also desired that the original cover media can be recovered because of the required high-precision nature. 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-indexmodulation 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. In the RS method [1] a regular-singular status is defined for each group of pixels according to a flipping operation and a discrimination function. It is then losslessly compressed to provide space for data hiding. The least significant digits of pixel values in an L-ary system [2] or the least significant bits of quantized DCT coefficients in a JPEG image [3] can also be used to provide the required data space. In these reversible data hiding methods, a spare place is made available to accommodate secret data as long as the chosen item is compressible, but the capacities are not very high.In the difference expansion method [4], differences between two adjacent pixels are doubled as a result 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 [9], 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 [7]uses the zero and peak points of the histogram of an image and slightly modifies the pixel grayscale values to embed data into the image. Section II,III and IV discusses about different reversible data hiding techniques.Paper is concluded in section V.

II. Separable reversible data hiding in encrypted image

The content owner encrypts the original uncompressed image using an encryption key. Then the data-hider compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space for accommodating the additional data. If the receiver has the data-hiding key, he can extract the additional data though he does not know the image content. If the receiver has the encryption key,then the received data can be decrypted to obtain an image similar to the original one, but cannot extract the additional data. If the receiver

has both the data-hiding key and the encryption key, he can extract the additional data and recover the original content without any error by exploiting the spatial correlation in natural image when the amount of additional data is not too large.This scheme is made up of image encryption, data embedding and data-extraction/image-recovery phases.

In the image encryption phase original image of size N_1XN_2 in uncompressed format is used.Each pixel with gray value falling into [0,255] is represented by 8 bits.The exclusive or operation of the original bits and pseudo random bits are performed.In the data embedding phase the least significant bits of the encrypted pixels are compressed to create space for accommodating the additional data.The data hider pseudo randomly selects N_p encrypted pixels which can be used to carry the parameters for data hiding.The other $(N-N_p)$ encrypted pixels are pseudo randomly permuted and divided into a number of groups,each of which contains L pixels.

In data extraction and image recovery phase there are three cases namely receiver with only data hiding key,receiver with only encryption key and both data hiding and encryption keys.If the receiver has only data hiding key then values of the parameters are first obtained from the least significant bits of the N_p selected encrypted pixels.The receiver then permutes and divides and divides the other $N-N_p$ pixels into $(N-N_p)/L$ groups and extracts the embedded bits from the least significant bit planes of each groups .Due to the pseudo random pixel selection and permutation, attacker without data hiding key cannot extract the embedded data.The receiver with data hiding key can successfully extract the embedded data but willnot get any information about the original image content.When the receiver has both of the keys, then additional data can be extracted and recovered from the original content without any error by exploiting the spatial correlation in natural image if the amount of additional data is not too large.

III. Reversible data hiding with optimal value transfer

In reversible data hiding techniques, the values of host data are modified based on particular rules and the original host content is perfectly restored after extraction of the hidden data on receiver side. Here the optimal rule of value modification under a payload-distortion criterion is found by using an iterative procedure, and a practical reversible data hiding scheme is proposed. The secret data, as well as the auxiliary information used for content recovery, are carried by the differences between the original pixel-values and the corresponding values estimated from the neighbors.The estimation errors are modified according to the optimal value transfer rule. The host image is divided into a number of pixel subsets and the auxiliary information of a subset is embedded into the estimation errors in the next subset. A receiver can successfully extract the embedded secret data and recover the original content in the subsets with an inverse order. Using this method a good reversible data hiding performance is achieved.

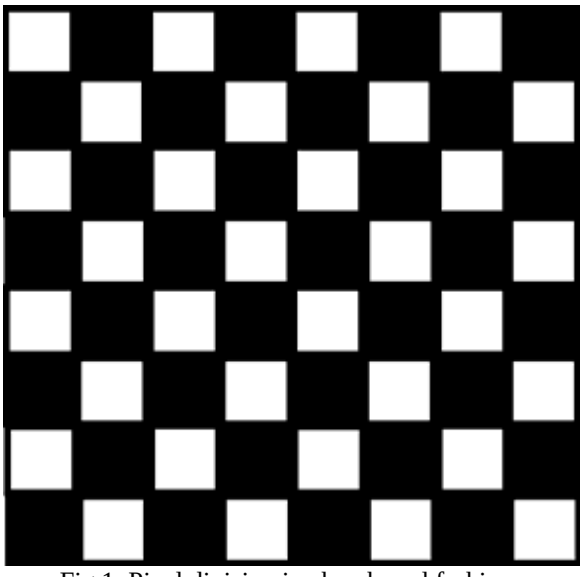

Fig.1. Pixel division in chessboard fashion.

The host pixel is denoted as P_{uv} ,where u and v are the indices of row and column.All pixels are divided into two sets.Set A contains pixels with even (u+v) and set B contains other pixels with odd (u+v).Figure 1 shows the division of pixels in chessboard like fashion.The white and black pixels belong to sets A and B respectively.The four neighbors of a pixel belong to different sets.For each pixel four neighbors are used to estimate its value.Pixels in set A/B are estimated using the pixels in B/A.The data embedding has two parts,data embedding

in estimation errors of set A and data embedding in estimation errors of set B.Before embedding data in estimation errors of set A optimal weights are found with least square error.

Data extraction and content recovery is the next phase.The receiver divides the image containing embedded data into two sets A and B and divides the sets A and B into a number of subsets.With the weight values the receiver can obtain the estimation error of each pixel in the subset.The histogram difference is used to retrieve the original scaled histogram.Optimal transfer matrix is then retrieved .The receiver recovers the original content and extracts the hidden data in the subsets.Secret data hidden in sets A and B are concatenated by the receiver to obtain the entire secret data.The payload distortion performance of this technique is good.Better performance can be achieved by making the estimation errors closer to zero.

IV. 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.

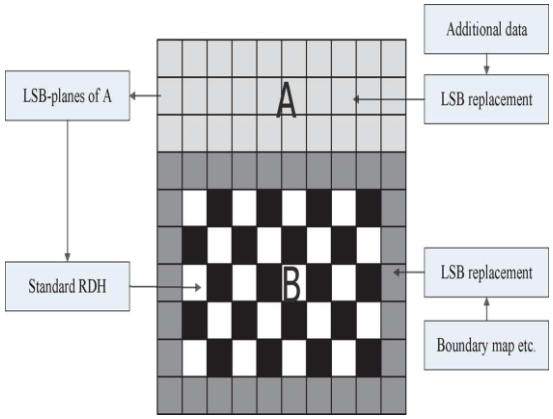

Fig.2.Illustration of image partition and embedding process

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.In extracting data from decrypted image the image is first decrypted and then data is extracted from it.This reversible data hiding technique achieves real reversibility.There is good improvement in the quality of marked decrypted images.

V. Conclusion

In reversible data hiding the original cover can be recovered losslessly after the embedded data is extracted from the image.In separable reversible data hiding in encrypted images when the receiver has both data hiding and encryption keys, then data can be extracted and recovered from the original image without any error by if the amount of data is not too large.In reversible data hiding with optimal value transfer technique better performance can be achieved,if a smarter prediction method is exploited to make the estimation errors closer to zero, but the computation complexity will be higher.Reversible data hiding in encrypted images by reserving room before encryption technique it is easier for the data hider to reversibly embed data in encrypted image.Data extraction and image recovery are free of any error.So it can achieve real reversibility.

Reference

[1] Y. Hu, H.-K. Lee, and J. Li, "DE-based reversible data hiding with improved overflow location map," *IEEE Transactions*, vol. 19, no. 2, pp. 250–260, Feb. 2009..

[2] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized-LSB data embedding," *IEEE Trans. Image Process.*, vol. 14, no. 2, pp. 253–266, Feb. 2005.

[3] J. Fridrich, M. Goljan, and R. Du, "Lossless data embedding for all image formats," in *Proc. Security and Watermarking of Multimedia Contents IV, Proc. SPIE*, 2002, vol. 4675, pp. 572–583.

[4] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 890–896, Aug. 2003.

[5] A. M. Alattar, "Reversible watermark using the difference expansion of a generalized integer transform," *IEEE Trans. Image Process.*, vol 13, no. 8, pp. 1147–1156, Aug. 2004.
[6] X. Wang, X. Li, B. Yang, and Z. Guo, "Efficient generalized integer transform for reversible watermarking," *IEEE Signal Process. Lett.*, vol. 17, no. 6, pp. 567–570, 2010.
[7] H.-C. Wu, C.-C. Lee, C.-S. Tsai, Y.-P. Chu, and H.-R. Chen, "A high capacity reversible data hiding scheme with edge prediction and difference expansion," *J. Syst. Softw.*, vol. 82, pp. 1966–1973, 2009.
[8] D.M. Thodi and J. J. Rodríguez, "Expansion embedding techniques for reversible watermarking," *IEEE Trans. Image Process.*, vol. 16, no. 3, pp. 721–730, Mar. 2007.
[9] L. Kamstra and H. J. A. M. Heijmans, "Reversible data embedding into images using wavelet techniques and sorting," *IEEE Trans. Image Process.*, vol. 14, no. 12, pp. 2082–2090, Dec. 2005.
[10] H. J. Kim, V. Sachnev, Y. Q. Shi, J. Nam, and H.-G. Choo, "A novel difference expansion transform for reversible data embedding," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 3, pp. 456–465, 2008.
[11] S. Weng, Y. Zhao, J.-S. Pan, and R. Ni, "Reversible watermarking based on invariability and adjustment on pixel pairs," *IEEE Signal Process. Lett.*, vol. 15, pp. 721–724, 2008.
[12] Kede Ma, Weiming Zhong, Xionfeng Zhao ," Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption ", *IEEE Transactions on information forensics and security,* vol. 8, No. 3, March 2013.
[13] Xinpeng Zhang , " Separable Reversible Data Hiding in Encrypted Image, "*IEEE Transactions on information forensics and security*, vol. 7, No. 2, April 2012.
[14] Xinpeng Zhang , "Reversible Data Hiding with optimal value transfer ",*IEEE Transactions on Multimedia*, Vol. 15, No. 2, February 2013.