International Journal of scientific research and management
(IJSRM) ||Volume||2||Issue||5 ||Pages|| 802-808 ||2014||
Website: www.ijsrm.in ISSN (e): 2321-3418

Retrieving Information using Reversible Data Hiding

Lalitha.P[1], Vidhushavarshini.S[2]

[1]Gnanamani College of Technology, Department of Computer Science and Engineering,
Namakkal 637018, India
lalitnp@gmail.com

[2]Gnanamani College of Technology, Department of Computer Science and Engineering,
Namakkal 637018, India
vidhugctcs@gmail.com

Abstract: Nowadays huge 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. Recent Methods such as reserving room before encryption with a traditional RDH algorithm sometimes results in error and complicated usage at the time of data extraction and/or image restoration .Hence to overcome this problem, this project propose an efficient method which uses by combining cryptographic primitives based encryption with Histogram Shifting-based RDH algorithm, a high capacity and low distortion can be achieved efficiently, and thus it is easy for the data hider to reversibly embed data in the encrypted image. The proposed method can achieve real multi level reversibility, that is, data extraction and image recovery are free of any error. Experiments show that this method can embed more than 10 times as large payloads for the same image quality.

Keywords: Steganography, Reversible Data Hiding, Histogram shifting, watermarking.

1. INTRODUCTION

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. 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 pre-concerted 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*.

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 ; and (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 hidable 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 losslessly 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 stego-image quality. A problem occurs here when too many of such pairs are selected for data hiding.

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. The word Steganography is of Greek origin and means "concealed writing" meaning "covered or protected", Generally, messages will appear to be something else: images, articles, shopping lists, or some other cover text and, classically, the hidden message may be in invisible ink between the visible lines of a private letter. It is high security technique for long data transmission. Steganography is the process of hiding the one information into other sources of information like text, image so that it is not visible to the natural view. There are varieties of stenographic techniques available to hide the data depending upon the carriers we use.

2. RELATED WORKS

Histogram shifting (HS) is a useful technique of reversible data hiding (RDH). With HS-based RDH, high capacity and low distortion can be achieved efficiently. In this paper, we revisit the HS technique and present a general framework to construct HS-based RDH. By the proposed framework, one can get a RDH algorithm by simply designing the so-called shifting and embedding functions. Moreover, by taking specific shifting and embedding functions, we show that several RDH algorithms reported in the literature are special cases of this general construction. In addition, two novel and efficient RDH algorithms are also introduced to further demonstrate the universality and applicability of our framework. It is expected that more efficient RDH algorithms can be devised according to the proposed

framework by carefully designing the shifting and embedding functions.

Steganography, derived from Greek, literally means "covered writing". It includes a vast array of secret communications methods that conceal the message's very existence. These methods include invisible inks, microdots, character arrangement, digital signatures, covert channels, and spread spectrum communications. This paper proposes a new improved version of Least Significant Bit (LSB) method. The approach proposed is simple for implementation when compared to Pixel value Differencing (PVD) method and yet achieves a High embedding capacity and imperceptibility. The proposed method can also be applied to 24 bit color images and achieve embedding capacity much higher than PVD. The cover images used in the PVD method are supposed to be 256 gray-valued ones. In the embedding phase a difference value d is computed from every non-overlapping block of two consecutive pixels, say pi and pi+1 of a given cover image. The way of partitioning the cover image into two-pixel blocks runs through all the rows of each image in a zigzag manner. In the extracting phase, the original range table is necessary. It is used to partition the stego-image by the same method used for the cover image.

A reversible data hiding method to authenticate 3D meshes by modulating the distances from the mesh faces to the mesh centroid to embed a fragile watermark. It keeps the modulation information in the watermarked mesh so that the reversibility of the embedding process is achieved. Since the embedded watermark is sensitive to geometrical and topological processing, unauthorized modifications on the watermarked mesh can be therefore detected by retrieving and comparing the embedded watermark with the original one. Furthermore, as long as the watermarked mesh is intact, the original mesh can be recovered using some priori knowledge.

A novel lossless data hiding scheme is presented to exhibit high data-hiding capacity for color palette images. In the proposed method, each index value is predicted by using the average of its four precedent neighbors. If the difference between the index value and its predictive value is larger than a threshold, the pixel will be skipped. Otherwise the four precedent neighbors are used to predict the current index during data embedding and retrieving. Moreover, the difference expansion algorithm issued for lossless hiding secret data into prediction error. The prediction error of the indexed image will also be reduced. The algorithm allows the data embedding process to be reversed and recovers the exact original indexed image without any distortion at all. The experimental results show that the proposed method not only can improve the payload capacity but also can maintain good image quality.

A novel reversible data hiding algorithm, which can recover the original image without any distortion from the marked image after the hidden data have been extracted, is presented in this paper. This algorithm utilizes the zero or the minimum points of the histogram of an image and slightly modifies the pixel grayscale values to embed data into the image. It can embed more data than many of the existing reversible data hiding algorithms. It is proved analytically and shown experimentally that the peak signal-to-noise ratio (PSNR) of the marked image generated by this method versus the original image is guaranteed to be above 48 dB. This lower bound of PSNR is much higher than that of all reversible data hiding techniques reported in the literature. The computational complexity of our proposed technique is low and the execution time is short. The algorithm has been successfully applied to a wide range of images, including commonly used images, medical images, texture images, aerial images and all of the 1096 images in CorelDraw database. Experimental results and performance comparison with other reversible data hiding schemes are presented to demonstrate the validity of the proposed algorithm.

3. SYSTEM DESIGN & ARCHITECTURE

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)".As shown in Fig. , the content owner first reserves enough space on original image and then converts the image into its encrypted version with the encryption key. Now, the data embedding process in encrypted images is inherently reversible for the data hider only needs to accommodate data into the spare space previous emptied out. The data extraction and image recovery are identical to that of Framework VRAE. Obviously, standard RDH algorithms are the ideal operator for reserving room before encryption and can be easily applied to Framework RRBE to achieve better performance compared with techniques from Framework VRAE. This is because in this new framework, we follow the customary idea that first losslessly compresses the redundant image content (e.g., using excellent RDH techniques) and then encrypts it with respect to protecting privacy.

Logging Mail by Content Sender: This helps to log in to a mail in which this mail is configured and designed especially for sending confidential data with the Encrypted Image to another mail recipient.

Encrypted Image Generation: image partition step divides 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 final version

Cryptographic Primitives: A content owner encrypts the original image using multiple cryptographic primitives with standard cipher with an encryption key. After producing 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 auxiliary data into the encrypted image by losslessly vacating some room according to a data hiding key. Then a receiver, maybe the content owner himself or an authorized third party can extract the embedded data with the data hiding key and further recover the original image from the encrypted version according to the encryption key.

Data Extraction and Image Recovery:

Extracting Data from Encrypted Images to manage and update personal information of images which are encrypted for protecting clients' privacy, an inferior database manager may only get access to the data hiding key and have to manipulate data in encrypted domain. When the database manager gets the data hiding key, he can decrypt using the same cryptographic primitives and extract the additional data by directly reading the decrypted version.. As the whole process is entirely operated on encrypted domain, it avoids the leakage of original content.

Image Restoration

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

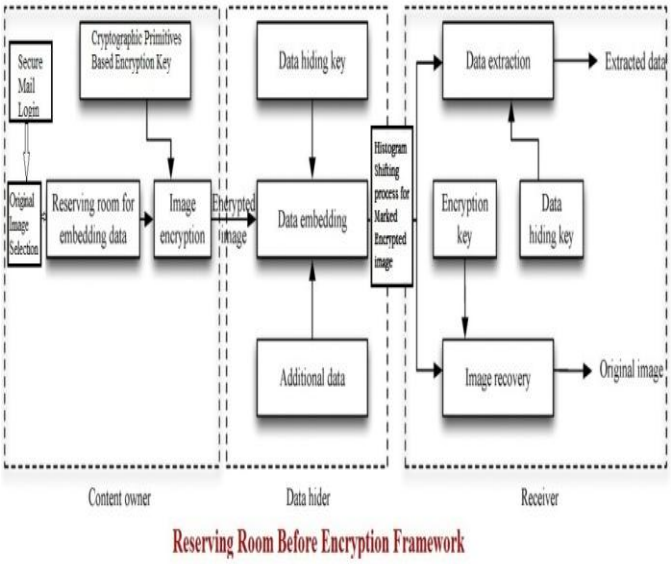

Figure 1 System Architecture

4. SYSTEM IMPLEMENTATION

A series of experiments have been conducted to test the proposed algorithms on images, some of which are shown in Fig. 8.. Each test image shown in the figure is a grayscale one of size 512 512 with the gray values

ranging from 0 through 255. For the purpose of comparing our results with those of other methods, we have implemented the algorithms of Histogram shifting, Pixel Value Difference Expansion and Data Compression. The step by step process of these algorithm usage for the reversible data hiding is shown.It shows first the statistics of some experimental results of our implementation. Each test image was divided into blocks of sizes from 256×256 down to 2×2. As can be observed, as the number of blocks in each test image increases, both the PSNR of the resulting stego-image and the data hiding capacity increase until a bottleneck at the block size of 8 8 is encountered.

The proposed method uses the combination of different block divisions C1 through C4 to break this bottleneck. First, the non-recursive Algorithms 1 and 2 were utilized, and the results are listed in the middle-left part of Table 2 which indeed shows the breakthrough effect. Specifically, the initial block size of 8 8 was used first in the experiments. As can be seen, both the data hiding capacity and the PSNR value resulting from each of the five test images are raised, compared with those yielded. For example, for the image of Lena, the bottleneck of the data hiding capacity is 33931 bits with the PSNR 48.73 dB, and the resulting capacity of the proposed algorithms is 41257 bits with the PSNR 48.90 dB. To see further the effectiveness of Algorithms 1 and 2, we tried the use of a smaller initial block size of 4 4 and the results are again good enough to break the bottleneck for all the five test images, as can be seen from the middle-right part of Table 2.

An image with more smooth regions usually includes more pixels with similar grayscale values, and so yields highly possibly a large peak value in the histogram. This means that the "bin" at the peak has a large volume of pixels, resulting in a large capacity for data hiding.

(a) Lena

(b) Airplane

512 512 (No. Of blocks)	256 256 (4)	128 128 (16)	64 64 (64)	32 32 (256)	16 16 (1024)	8 8 (4096)	4 4 (16384)	2 2 (65536)
Lena (PSNR of stego-image)	8996 (48.21)	12645 (48.25)	18422 (48.31)	24182 (48.39)	29537 (48.52)	33931 (48.73)	33349 (49.13)	23196 (50.13)
Airplane (PSNR of stego-image)	25555 (48.38)	30296 (48.45)	35109 (48.54)	41780 (48.68)	46945 (48.86)	50920 (49.13)	49690 (49.71)	38718 (50.94)

Table 1. Statistics of experimental results of the method of Kuo et al. [13] showing a bottleneck of data-hiding-rate increasing at block size 8 8.

Method		Kuo et al.'s		Proposed Non recursive method.(8x8)		Proposed Non recursive method.(4x4)		Proposed recursive method.(8x8)	
Hiding Capacity	Quality of Stego-Image	Bits	PSNR	Bits	PSNR	Bits	PSNR	Bits	PSNR
Lena (512 512)		33931	48.73	41257	48.90	42166	49.36	45342	49.13
Airplane(512 512)		50920	49.15	59397	49.37	58375	49.96	63787	49.64

Table 2. Comparison of results of proposed method and related lossless histogram-shifting data hiding methods.

It was found in this study that a lower bound for the PSNR value of the stego-image yielded by the proposed non-recursive Algorithms 1 and 2 can be estimated deterministically, and the estimation is conducted here. As an example, consider one block of the 4096 ones of size 8×8 in a cover image of size 512 512. In the extreme case, the block is not divided further, that is, the way of C1 is applied to the block. Denote the histogram of the given block as h and the location of its

peak as x0. In the worst case, the value of h(x0) is 1, and except the gray value x0 at the peak, the other 63 pixels' gray values in the block will be incremented or decremented by 1 after the process of data embedding is performed. In other words, at least one pixel's gray value is kept unchanged in each block. Therefore, the gray values of at least 4096 pixels will be kept the same in the stego-image.

CONCLUSION

A Reversible data hiding method based on histogram shifting has been proposed, which not only embeds large-volume data into cover images, but also produces stego-images with high qualities by using a strategy of hierarchical block division. The bottleneck of data-hiding-rate increasing at the block size of 8×8 found in existing methods is broken by the proposed non-recursive algorithms. And the proposed recursive versions of the algorithms enhance the performance further both in the data hiding capacity and the PSNR value, which result from the proposed scheme of recursive looking-ahead estimation of the data hiding capacity. The estimation process is a kind of optimal tree search under the quad-tree structure constructed by the hierarchical block division scheme, and so yields an optimal data hiding result under the tree structure. The experimental results show the effectiveness of the proposed method. Future researches may be directed to investigating more block division types for further improvement on the data hiding capacity, applying the histogram shifting technique to other information hiding applications, reducing the key size, eliminating the use to the location map, etc.

REFERENCES

1] Bender, W., Gruhl, D., Morimoto, N., Lu, A., 1996. Techniques for data hiding. IBM Systems Journal 35 (3–4), 313–336.

[2] Alattar, A.M., 2004. Reversible watermark using the difference expansion of a generalized integer transform. IEEE Transactions on Image Processing 13 (8), 1147–1156.

[3] Barton, J.M., 1997. Method and apparatus for embedding authentication information within digital data. US Patent 5 646 997.

[4] Carpenter, B., 2002. Compression via Arithmetic Coding <http://www.colloquial.com/ArithmeticCoding/>

[5] Chang, C.C., Lu, T.C., 2006. A difference expansion oriented data hiding scheme for restoring the original host images. Journal of Systems and Software 79 (12), 1754–1766.

[6] Cox, I.J., Miller, M.L., Bloom, J.A., Fridrich, J., Kalker, T., 2007.Digital Watermarking and Steganography. Morgan Kauffman, ISBN 978-0-12-372585-1.

[7] Davis, R.M., 1978. The data encryption standard in perspective. IEEE Communications Magazine 16 (6), 5–9.

[8] De Vleeschouwer, C., Delaigle, J.F., Macq, B., 2003. Circular interpretation of bijective transformations in lossless watermarking for media asset management. IEEE Transactions on Multimedia 5 (1), 97–105.

[9] Fridrich, J., Goljan, M., Du, R., 2001. Invertible authentication. In: Proceedings of the SPIE Security Watermarking Multimedia Contents, San Jose, CA, pp. 197–208 (January).

[10] Honsinger, C.W., Jones, P.W., Rabbani, M., Stoffel, J.C., 2001. Lossless recovery of an original image containing embedded data. US Patent 6 278 791 (August).

11] Howard, P.G., Kossentini, F., Martins, B., Forchhammer, S., Rucklidge, W.J., 1998. The emerging JBIG2 standard. IEE Transactions on Circuits and Systems for Video Technology 8 (7), 838–848.

[12] Kamstra, L., Heijmans, H.J.A.M., 2005. Reversible data embedding into images using wavelet techniques and sorting. IEEE Transactions on Image Processing 14 (12), 2082–2090.

[13] Kim, H.J., Sachnev, V., Shi, Y.Q., Nam, J., Choo, H.G., 2008. A novel difference expansion transform for reversible data embedding.

[14] Xiaolong Li Inst. of Comput. Sci. & Technol., Peking Univ., Beijing, China Bin Li ; Bin Yang ; Tieyong Zeng "General Framework to Histogram-Shifting-Based

Reversible Data Hiding"

[15] H.B.Kekre, Archana Athawale, and Pallavi N.Halarnkar "Increased Capacity of Information Hiding in LSB's Method for Text and Image " 2008.

[16] Alejandro Proan˜o and Loukas Lazos "Packet-Hiding Methods for Preventing Selective Jamming Attacks" IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 1, JANUARY/FEBRUARY 2012.

AUTHOR PROFILE

Lalitha.P received the B.Sc. degree in Computer science from Nehru Memorial College in 2005, MCA from Muthayammal Engineering College in 2008. She is pursuing towards the M.E degree in Computer Science and Engineering from Gnanamani College of Technology, Affiliated to Anna University, and Chennai since September 2012.Her research area is Data Mining and Database Management Systems.

Vidhushavarshini.S received the M.E degree in Computer Science and Engineering from Vinayaka Missions University in 2012, now working as Assistant Professor in Gnanamani College of Technology. Her research area includes Computer Networks and Database Management Systems.