IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727,
PP 16-21
www.iosrjournals.org

A Review: Reversible Data Hiding Techniques

Sruthi L.[1], Manoj Ray D.[2]

[1] *(Department of Computer Science, College of Engineering Karunagappally, India)*
[2] *(Department of Computer Science, College of Engineering Karunagappally, India)*

ABSTRACT: *This paper describes several different algorithms for Reversible Data Hiding(RDH). Data hiding is a technique for embedding information into covers such as image, audio and video files. Reversible Data Hiding (RDH) or lossless data hiding, is a method by which the original cover can be lossless restored after the embedded message is extracted. Many RDH techniques have been developed. This paper summarizes and reviews these techniques. Previous literature has shown that difference expansion, interpolation technique, prediction and sorting, histogram modification are the most common methods for data hiding, but previously these methods are implemented in plain images. Recently these methods are used in encrypted images to improve security. Different RDH algorithms have their own merits and no single approach is optimal and applicable to all cases. RDH is still an active topic. This paper is a comprehensive exploration of all the major reversible data hiding approaches implemented as found in the literature. Also paper presents a new method RDH by reserving room before encryption.*

Keywords: *RDH(Reversible Data Hiding), interpolation, sorting and prediction, histogram modification*

I. INTRODUCTION

Data hiding is a technique for embedding information into covers such as image, audio, and video files, which can be used for media notation, copyright protection, integrity authentication, covert communication, etc. Most data hiding methods embed messages into the cover media to generate the marked media by only modifying the least significant part of the cover and, thus, ensure perceptual transparency. The embedding process will usually introduce permanent distortion to the cover, that is, the original cover can never be reconstructed from the marked cover. However, in some applications, such as medical imagery, military imagery, and law forensics, no degradation of the original cover is allowed. In these cases, we need a special kind of data hiding method, which is referred to as reversible data hiding (RDH) or lossless data hiding, by which the original cover can be lossless restored after the embedded message is extracted. The block diagram of RDH is shown in figure 1.1. Reversible steganography or watermarking can restore the original carrier without any distortion or with ignorable distortion after the extraction of hidden data. So reversible data hiding is now getting popular.

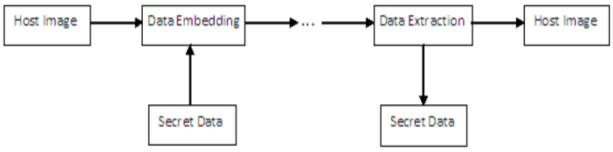


Fig 1.1 Reversible data hiding

As a basic requirement, the quality degradation on the image after data embedding should be low. An intriguing feature of reversible data embedding is the reversibility, that is, one can remove the embedded data to restore the original image. From the information hiding point of view, reversible data embedding hides some information in a digital image in such a way that an authorized party could decode the hidden information and also restore the image to its original, pristine state.The motivation of reversible data embedding is distortion-free data embedding. Though imperceptible, embedding some data will inevitably change the original content. Even a very slight change in pixel values may not be desirable, especially in sensitive imagery, such as military data and medical data. In such a scenario, every bit of information is important. Any change will affect the intelligence of the image, and the access to the original, raw data is always required. From the application point of view, reversible data embedding can be used as an information carrier. Since the difference between the embedded image and original image is almost imperceptible from human eyes, reversible data embedding could be thought as a covert communication channel. By embedding its message authentication code, reversible data embedding provides a true self authentication scheme, without the use of metadata.

II. REVERSIBLE DATA HIDING TECHNIQUES

2.1 Difference Expansion

Difference expansion explores the redundancy in digital images to achieve very high embedding capacity, and keep the distortion low. Jun Tian [1] selects an embedding area and embed both payload and original values. Reversible integer transform is applied. For an 8 bits grayscale-valued pair (x,y) x,y Є **Z** and $0 \leq x,y \leq 255$, define integer average l and difference h as :

$l=(x + y)/2$ and $h = x – y$ (1)

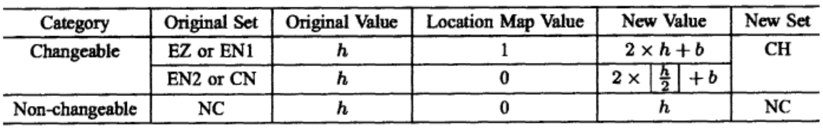
This difference value h is used for embedding bits b:

$h' = 2 \times h +b$ (2)

By inverse integer transform we can recover original values :

$x=l+[(h+1)]/2$ and $y=l-(h/2)$ (3)

Image is grouped into pair of pixels and apply integer transform.Difference value fall in four groups:expandable h=0, h=-1 (EZ), all expandable (EN), changeable (CN), non-changeable (NC).The subset of selected and non-selected difference values are denoted as EN1 and EN2.Location map is used to identify changeable difference value ,1 indicates selected expandable difference value.Location map is then compressed to bit stream L. Collect the original LSB values of difference values in EN2 and CN.Embed location map L , original LSBs C and payload P. After all bits are embedded to B, inverse integer transform is applied to obtain the embedded image.



Category	Original Set	Original Value	Location Map Value	New Value	New Set
Changeable	EZ or EN1	h	1	$2 \times h + b$	CH
	EN2 or CN	h	0	$2 \times \left\lfloor \frac{h}{2} \right\rfloor + b$	
Non-changeable	NC	h	0	h	NC

Fig 2.1 Embedding on difference values

In the retrieving process embedded bit stream B can be collected and thus can obtain the LSBs of all exchangeable difference values. Location map gives all the expandable difference values. thus the original image can be restored. For difference expansion based reversible data hiding, the embedded bit-stream mainly consists of two parts: one part that conveys the secret message and the other part that contains the binary (overflow) location map and the header file. The first part is the payload while the second part is the auxiliary information package for blind detection. To increase embedding capacity, we have to make the size of the second part as small as possible. The compressibility of location map has to be increased for different types of images.

2.2 Histogram Modification

In [2] Zhicheng Ni utilizes zero or maximum point of histograms of an image. The pixel gray scale values are slightly modified to embed data into image. In embedding process first a histogram is generated H(x). In the histogram , find the maximum point h(a) and the minimum point zero h(b) .If the minimum point h(b)>0, recode the coordinate (i,j) of those pixels and the pixel grayscale value b as overhead bookkeeping information (referred to as overhead information for short). Then set h(b)=0.Without loss of generality a<b, assume .Move the whole part of the histogram with to the right by 1 unit. This means that all the pixel gray scale values (satisfying) are added by 1. Scan the image, once meet the pixel (whose gray scale value is a), check the to-be-embedded bit. If the to-be embedded bit is “1”, the pixel gray scale value is changed to a + 1 . If the bit is “0”, the pixel value remains a. Decoding is just the reverse process. This method cannot be used for images with flat histogram.

To improve the embedding capacity A.S.Al-Fahoum[3] proposes another method. This method will be applied to the output of Zhicheng's method .Output from Zhicheng's method is divided into equally non-overlapping blocks.Contrast of histogram of each block is then stretched to create extra embedding space. The bits are embedded into the space created after contrast stretching Pixel values in embedding areas are modified by either adding or subtracting one bit :
$b''(i, j) = b'(i, j) - 1$ if $b'(i, j) >$ peak value (4)
$b''(i, j) = b'(i, j) + 1$ if $b'(i, j) <$ peak value (5)

V. Sachnev [4] proposes another method based on sorting and prediction. Data can be embedded by either cross embedding or dot embedding techniques. Pixel value is predicted based on surrounding pixels, then the prediction error is used for embedding data. The combination of histogram shifting and expansion is used in this method. Prediction error between two thresholds is used for data embedding. The histogram shift method embeds data with the thresholds. Cells are sorted in ascending order of the local variance values. Cells with smaller variance values are better for data hiding. Thus, the embedding process starts from the cell with the smallest variance value in the sorted row, and moves on to the next cells until the last bit of data is embedded.

In the decoding process recover the threshold value and payload form first 34LSBs of prediction errors. Original prediction errors can be recovered with the help of location map.

2.3 Interpolation Technique

L. Luo[5] estimate interpolated values and calculate interpolation error, e:
$e=x-x'$ (6)

Apply additive expansion to interpolation error and embedded watermarking information.Then e' becomes:

$$¿\begin{cases} e+sign(e)\times b, e=LM \vee RM \\ e+sign(e)\times 1\ e\in(\ln, LM)\cup(RM, RN) \\ e, otherwise \end{cases} \qquad (7)$$

where LM and RM denote the corresponding values of the two highest points of interpolation-errors histogram and LN and RN denote the corresponding values of the two lowest points of interpolation-errors histogram. The watermarked pixels x'' becomes:
$x''=x'+e'$ (8)

During the extracting process, the interpolation value x' is computed with the same interpolation algorithm and the corresponding interpolation-errors are obtained. Once the interpolation errors, LM, RM, LN and RN are known, the embedded secret data can be extracted. Then the inverse function of additive interpolation-error expansion is applied to recover the original interpolation-errors. Finally, we can restore the original pixels x by adding interpolation value x' and the interpolation error e.

After secret messages are embedded, some overhead information is needed to extract the covert information and restore the original image. The overhead information are the information to identify those pixels containing embedded bit(LM,LN,RM and RN) and the information to solve the overflow/underflow problem.

2.4 RDH in Encrypted Images

All the above methods are applied to plain images but it will not provide security to both the image and the embedded data. Many methods have been proposed later in which embedding is done in encrypted images also the embedded data is encrypted. Previous methods can be also applied to encrypted images. This section describes various hiding methods in encrypted images.

W. Puech [6] describes a method in which the image is encrypted by AES algorithm. Since AES is a block cipher, first divide the image into blocks X_i and apply AES to each block:
$Y_i = E_k(X_i)$ (9)

Data hiding step modifies only one bit of one encrypted pixel:
$Yw_i = DH_k(Y_i)$ (10)

Bit substitution data hiding is used ,secret key is used as seed to generate PSNR to substitute bit of pixel with the bit to hidden. During extraction read the bits of pixel marked by using secret key k and the same PRNG. Decryption removal is done by analyzing the local standard deviation For each marked cipher-text Yw_i apply the decryption function D_k () for the two possible values of the hidden bit (0 or 1) and analyse the local standard deviation of the two decrypted blocks $X0_i$ and $X1_i$. Standard deviation of encrypted images is higher than that of encrypted images. Select the bit value where standard deviation is smaller.

$$X_i \begin{cases} \text{¿}D_k(Y0_i) if\, \sigma(D_k(Y0_i)) < \sigma(D_k(Y1_i)) \\ \text{¿}D_k(Y1_i) else \end{cases} \qquad (11)$$

X. Zhang [7] proposes another method in which a stream cipher is used to encrypt the image. Each bit in the image is encrypted :

$$B_{i,j,k} = b_{i,j,k} \oplus r_{i,j,k} \qquad (12)$$

In the embedding step, segment the encrypted image into a number of non-overlapping blocks sized s x s. Each block is used to carry one additional bit. The pixels in each group are pseudo randomly divided into two sets S_0 and S_1. If additional bit to be embedded is zero flip the 3 LSBs of S_0 . Otherwise flip LSBs of S_1 . Other encrypted bits remains the same. Extraction is just the reverse process of embedding. The LSBs of S_0 and S_1 are flipped to form H_0 and H_1 , a fluctuating function is calculated for both the blocks and if $f_0 < f_1$ H_0 is original and extracted bit is 0,else H_1 is original and extracted bit is 1.The fluctuating function is :

$$f = \sum_{u=2}^{s-1} \sum_{v=2}^{s-1} \left| p_{u,v} - \frac{p_{u-1,v} + p_{u+1,v} + p_{u,v-1} + p_{u,v+1}}{4} \right| \qquad (13)$$

W. Hong [8] employs another method which proposes an improved version of Zhang's reversible data hiding method in encrypted images. The original work partitions an encrypted image into blocks, and each block carries one bit by flipping three LSBs of a set of pre-defined pixels. The data extraction and image recovery can be achieved by examining the block smoothness. Zhang's [7] work did not fully exploit the pixels in calculating the smoothness of each block and did not consider the pixel correlations in the border of neighboring blocks. These two issues could reduce the correctness of data extraction. This letter adopts a better scheme for measuring the smoothness of blocks, and uses the side-match scheme to further decrease the error rate of extracted-bits. A new smoothness function, f is used to better estimate the smoothness of image blocks :

$$f = \sum_{u=1}^{s_2} \sum_{v=1}^{s_1-1} \left| p_{u,v} - p_{u,v+1} \right| + \sum_{u=1}^{s_2-1} \sum_{v=1}^{s_1} \left| p_{u,v} - p_{u+1,v} \right| \qquad (14)$$

The extraction and recovery of blocks are performed according to the descending order of the absolute smoothness difference between two candidate blocks. The side match technique is employed to further reduce the error rate. In all these methods data extraction is not separable from the content decryption. In other words, the additional data must be extracted from the decrypted image, so that the principal content of original image is revealed before data extraction, and, if someone has the data-hiding key but not the encryption key, he cannot extract any information from the encrypted image containing additional data.

X. Zhang [9] proposed a novel scheme for separable reversible data hiding which is made up of image encryption, data embedding and data-extraction/image-recovery phases. The content owner encrypts the original uncompressed image using an 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 to create a sparse space to accommodate the additional data. At the receiver side, the data embedded in the created space can be easily retrieved from the encrypted image containing additional data according to the data-hiding key. Since the data embedding only affects the LSB, a decryption with the encryption key can result in an image similar to the original version. When using both of the encryption and data-hiding keys, the embedded additional data can be successfully extracted and the original image can be perfectly recovered by exploiting the spatial correlation in natural image. Following figure shows the three cases at the receiver side.

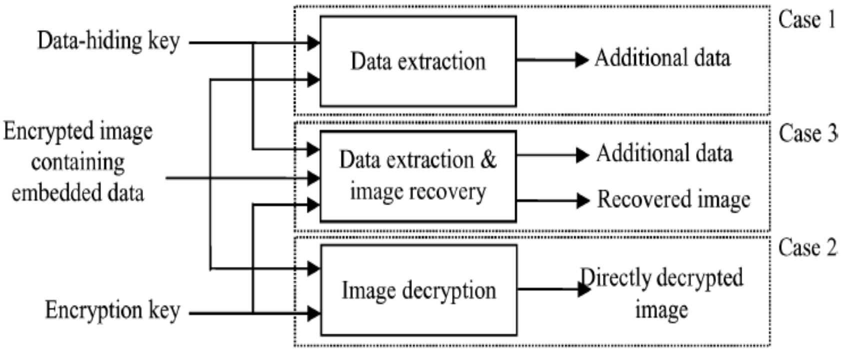


Fig 2.2: Seperable Reversible Data Hiding

III. NEW DEVELOPMENT

A.Reversible Data Hiding by Reserving Room Before Encryption(RRBE)

Losslessly vacating room from the encrypted images is relatively difficult and sometimes inefficient. If the order of encryption and reserving room is reversed it would be much easier also the entropy of encrypted image is maximized hence it result in only small payloads. The following figure describes the method.

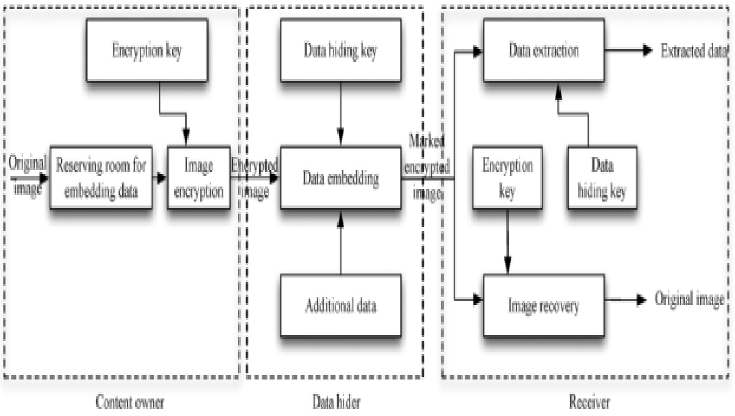


Fig 3.1: RDH by Reserving Room Before Encryption

The image is encrypted only after reserving room for additional data. For that first the image is divided into two parts, the LSB bits of complex textured areas are reversibly embedded into other part. Any of the previously mentioned method can be used for RDH. Image is then encrypted by using a stream cipher preferably rabbit stream cipher for better security. Then data is embedded into previously vacated space. During extraction either the data only can be retrieved or both data and image ie, separable reversible data hiding is achieved.

IV. CONCLUSION

This survey paper gives the detail analysis of data hiding in plain image and also encrypted image in which room for embedding data is find out from encrypted images which results in inefficiencies. Hence a new method for RDH, reserving room before encryption with rabbit stream cipher is presented. This method take advantage of all traditional RDH techniques for plain images and expects to achieve excellent performance without loss of perfect secrecy.

REFERENCES

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

[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]. A.S. Al-Fahoum, "Reversible data hiding using contrast enhancement approach", International Journal of Image Processing(IJIP),Vol (7):Issue (3):2013

[4]. 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.

[5]. L. Luo et al., “Reversible image watermarking using interpolation technique,” IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 187–193,Mar. 2010.

[6]. W.Puech,"A reversible data hiding method for encrypted images.", IS and T/SPIE Electronic Imaging,Version 1-3 July 2008

[7]. X. Zhang, “Reversible data hiding in encrypted images,” IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.

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

[9]. X. Zhang, “Separable reversible data hiding in encrypted image,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.