

Reversible Data Hiding in Encrypting Images - an System

V.V.Vinoth, E.Kanniga

Abstract : In today's technology data hiding has become an essential need due to the availability of the internet all over the world. Nowadays, it has become necessary task for the people to communicate through networks and share contents with each other. In the meanwhile, transferring the data in a secured manner has become a challenge and also a paradigm. Still there exists many ways for hiding the data in an encrypted images. Hiding information at the back end of the image should not affect the original data or image pixels. It is one type of steganographical method where the data can be hidden inside the images and original data can be losslessly retrieved after extracting the embedded text. The proposed work discusses encryption using reversible data hiding and produces an outline of various reversible data hiding techniques which includes quantization technique, histogram shifting, expansion technique, compression technique and dual image technique.

Keywords: Encrypted images, Reversible data hiding, Embedded image, histogram shifting, dispersion, interpolation, watermarking.

I. INTRODUCTION

Embedding original text or data within an image, retrieval of hidden data as needed and retaining the original copy of host image is defined as reversible data hiding technique. Generally encrypting techniques using reversible model mainly focuses towards simply encrypting the text in a simple unencoded images. [1,2]. It is one kind of art and science for communicating data in a secret manner using the multimedia carrier that includes text, image, audio and video files. It is one of the emerging techniques originated from the reversible data hiding in plaintext images [3,4]. In order to ensure transparency, many data hiding techniques enclose the messages inside media like covers that includes images, video that generate the specified media just by altering the least significant part of the cover. The embedded process generally produces perpetual deformation to the enclosure so that the original enclosure cannot rebuild in the already remarked cover [5]. Nowadays protecting the transmitted digital images against any unauthorized access, deleting or modifying play a vital role in image secure transmission across the vulnerable media [6]. Generally an information or data hiding technique is characterized by four factors such as security, capacity, robustness and perceptibility [7] Fig.1.

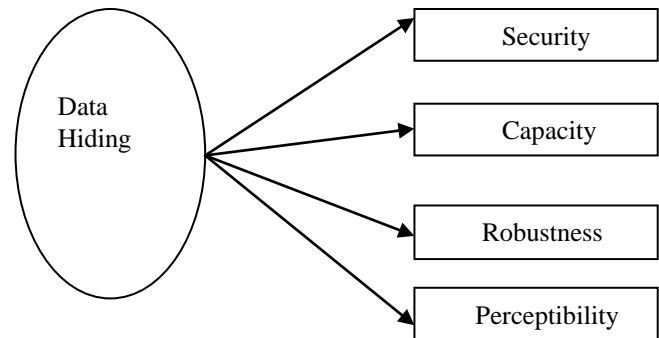


Figure 1. Characteristics of Data Hiding

The proposed work reviews various techniques of encryption in a reversed technology manner and distinct models being used for hiding the message within the embedded capacity and some invisible images are also discussed.

II. REVERSIBLE DATA HIDING

Reversible data hiding is defined as retrieval of original image promptly with lossless technique. This technique is mainly adapted in the field of medicine and defence department. It embeds data inside the image and the main trump card of this reversible technique is that the model retains exact copy of the original text shown in Fig 2. Some conventional reversible encrypting methods include mainly arithmetic additive using modulo format and spread-spectrum techniques [8, 9].

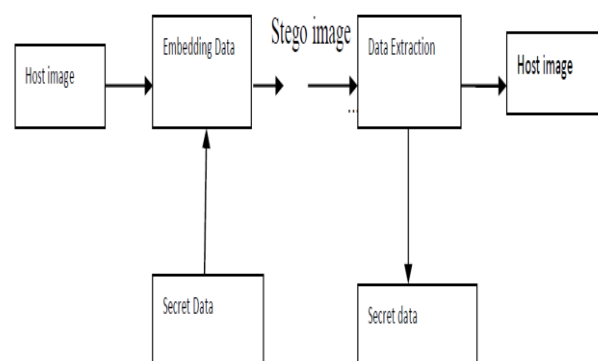


Figure 2. Reversible Data Hiding

Revised Manuscript Received on October 05, 2019

V.V.Vinoth, Research Scholar, Department of ECE, Bharath University, Chennai, India.

E.Kanniga, Professor Electronics and Engineering, Head Electronics & Instrumentation Engineering, Bharath University, Chennai, India.

III. REVERSIBLE DATA HIDING BASAED METHODS

Data hiding in an encrypted image is a huge task though there are some reversible data hiding techniques for encrypted images which provides a better usage in the field of medical applications [10, 11]. There exists five methods of reversible encrypting techniques (Fig 3) such as quantization method, histogram modification method, expansion method, compressed method and dual image based models. The proposed work furnishes few methods of reversible data hiding techniques.

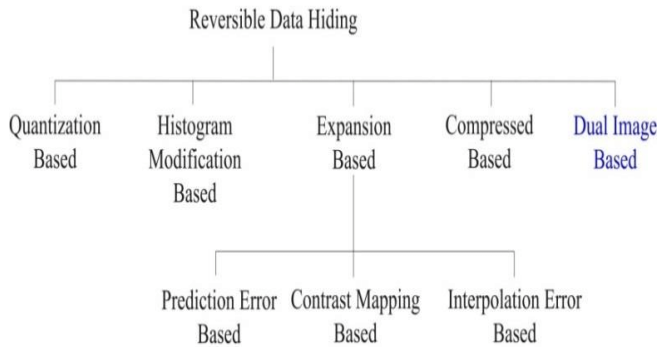


Figure 3 Reversible Data Hiding Techniques

A. Quantization Based Method

This method is one of the lossy efficient compression methods where it produces high efficiency. Some adjacent blocks are used for encoding the current block and this method obtains codebook that combines with specified vectors that is called by the code word. Operations such as generation, optimization, encoding and decoding are all included in the codebook. Compression depends upon the size and domain of codebook. The following steps show encryption method:

Step 1: Generate original codebook with the problem of local optimization.

Step 2: Linde-Buzo-Gray (LGB) is implemented in order to maximize codebook.

Step 3: Image is divided into equal size in non-overlapping block.

Step 4: The size of each block are same with coding dimension.

Step 5: During decoding, it considers the results of searching the sets of index.

Step 6: Corresponding code is found as in the original sort and image data is recovered.

B. Histogram Modification Based Method

In this histogram shifting method, a zero value or few dots of the histogram image are taken for encrypting. It modifies value of pixel gray scale mildly in order to enclose a huge quantity of data in to an original image [12]. Generally this method maintains better quality of the original images in nature and its Pixel signal to noise ration(PSNR) value for a specified image is assured approximately 48 dB. Steps to encryptan image:

Step 1: At first histogram image $H(a)$ is created and points (x,y) is taken as higher and lower limits respectively.

Step 2: If lower limit $H(y) > 0$, then coordinate values of specified pixels are recoded. Then set as $H(y) = 0$.

Step 3: And with lossless generality, entire part of histogram is moved towards right direction by 1 unit.

Step 4: Thus produces low processing complexity and very faster execution time.

C. Expansion Based Method

In the past one decade, reversible data hiding has lost its recognition of interest. Selecting the embedded area becomes a generalized concept for huge potential of encrypting technique. Differential expansion mainly finds the additional storage area by using the replication of the data image. Here, expandable distinct values of pixels are selected and one bit is embedded inside another bit in order to retrieve the enclosed data so as the difference values selected for DE can be known. In this model, location map contains relevant information for selected extendable distinct values which is suited for all audio and videos. This expansion based method again subdivided into prediction error based; interpolation error based and contrast mapping based expansion. In the first method, inherent correlation of a pixel is exploited in the neighbourhood image. The maximum embedded capacity is 1bpp in a single pass. It provides a significant improvement in the watermarked image. In the latter methods, a large quantity of covert message is embedded inside an image in wider modifications. This implies interpolation error. Following Table 1 shows the approximate interpolation (AI) in dB and improved approximate interpolation (IAI) for the given input images.

Table 1. Nearest Mean Interpolation

Input image	AI (dB)	IAI (dB)
Lena	31.79	33.47
Boat	29.51	30.83
Airplane	31.45	33.37
Peppers	33.39	35.29
Gold	31.8	33.06
Baboon	23.86	24.47

D. Compressed Based Method

In the described method, a resolution progressive compression is developed that has good encoding potential and minimum execution convolution. This method is mainly derived by Slepian-Wolf coding. This also improves the compression in an efficiently manner for encrypted real world images.

E. Dual Image Based Method

Dual image based techniques are widely used in recent years for reversible data hiding. Here [13], factor that affects the image quality is taken as the secret data and its values are evaluated. If the value is very large, then it is clear that it may show major distinction between the stego and original pixels. The described method used center folding strategy in order to minimize value of encrypted signs. These minimized signs are then taken for embedding into two stego images via an averaging method so that it maintains the quality of the image.



IV. RESULTS AND DISCUSSION

The paper describes the major four techniques. First the quantization based method is mainly based on the efficient compression method where adjacent blocks are encoded using the codebook with four main operations. The original data is recovered with the help of the code book. In the second method, histogram image are taken in to account with a zero or few points and with the slight modification of pixel scale values a huge amount of data is embedded into an original image producing good quality of natural images.[14] In the third method, some distinct values of pixels are selected and each one of the bit is embedded in other to find the distinct values taken for DE. Here other methods such as prediction error based, interpolation error based and contrast mapping based were discussed which provides significant improvement in the watermarked images. The fourth methods produces better coding efficiency and minimize computational complexity. The last method namely dual image based method used center folding strategy to minimize the value of secret symbols.[15] Among four methods interpolation based method derived from the expansion based method produces high peak signal to noise (PSNR) comparing to other methods shown in Fig.4.

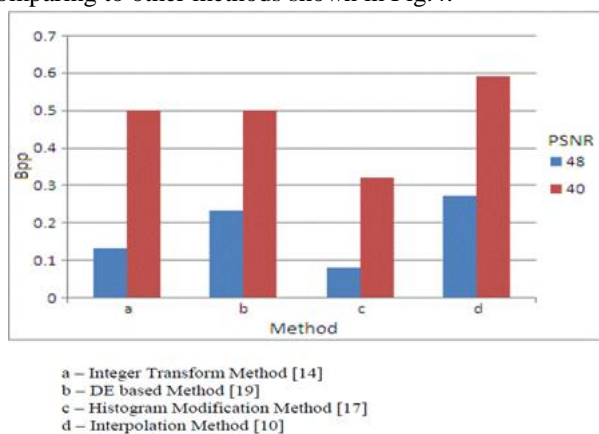


Figure 4. Capacity Graph of Reversible data hiding methods

V. CONCLUSION

This proposed system presents a detailed review of the several methods applied for reversible data hiding. Reversible data hiding models delivers the exact data promptly after separating from the secret encrypted message. The paper also depicts comparative analysis of the distinct techniques subject to hiding capacity. With the four techniques, it reveals the fact that interpolation technique provides highest hiding capacity comparing to other methods. Thus these techniques have its enormous applications in the field of medical analysis, imaging, forensics military for authentication, integrity purposes. Furthermore, it shows that many compression and data hiding methods are yet to come in future to provide secured encryption.

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. J. Fridrich and M. Goljan, "Lossless data embedding for all imageformats," in Proc. SPIE Proc. Photonics West, Electronic Imaging, Security and Watermarking of Multimedia Contents, San Jose, CA, USA, vol. 4675, pp. 572–583, Jan. 2002.
3. Z. Ni, Y. -Q. Shi, N. Ansari, and W. Su, Reversible Data Hiding, IEEE Transactions on Circuits and Systems for Video Technology, vol. 16, no. 3, pp. 354–362, 2006.
4. W. -L. Tai, C. -M. Yeh, and C. -C. Chang, Reversible data hiding based on histogram modification of pixel differences, IEEE Transactions on Circuits and Systems for Video Technology, vol. 19, no. 6, pp. 906–910, 2009.
5. Manisha G. Gedam, Shruti M. Rakhunde, Ushap P. Kosarkar, Reversible Data Hiding Technique and its Type, a survey, IOSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 2278-0661, pp. 43–48, National Conference on Recent Trends in Computer Science and Information Technology (NCRTCSIT), 2016.
6. Nour Kittawi, Ali Al-Haj, Reversible Data hiding in Encrypted Images, 8th International Conference on Information Technology (ICIT), IEEE, 2017.
7. Jun Tian, "Reversible Data Embedding Using a Difference Expansion", IEEE transactions on circuits and systems for videotechnology, vol. 13, no. 8, august 2003.
8. W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," IBM Systems Journal, vol. 35, pp. 313–336, 1996.
9. C. W. Honsinger, P. W. Jones, M. Rabbani, and J. C. Stoffel, "Lossless recovery of an original image containing embedded data," U. S. Patent, Ed., 2001.
10. H. M. Chao, C. M. Hsu, S. G. Miaou, "A Data-Hiding Technique with Authentication, Integration, and Confidentiality for Electronic Patient Records," IEEE Trans Inf Technol Biomed. Vol. 6, pp. 46–53, 2002.
11. D. Bouslimi, G. Coatrieux, and C. Roux, "A joint encryption/watermarking algorithm for verifying the reliability of medical images," Computer Methods and Programs in Biomedicine, 106(1), pp. 47–54, 2012.
12. Mehmet U. Celik, Gaurav Sharma, A. Murat Tekalp, and Eli Saber, 2002, "Reversible Data Hiding," in IEEE ICIP, pp. 157–160.
13. Tzu-Chen Lu, Jih-Huei Wu, Chun-Chih Huang, Dual-image-based reversible data hiding method using center folding strategy, Signal Processing, Elsevier, Vol. 115, pp. 195–213, 2015.
14. Nandagopal, V., Geeitha, S., Kumar, K. V., & Anbarasi, J. (2019). Feasible analysis of gene expression—a computational based classification for breast cancer. *Measurement*, 140, 120–125.
15. Nandagopal, V., Maheswari, V., & Anbarasi, J. (2019). Pyrolysis Electricity Generation and Biomass. *Journal of Computational and Theoretical Nanoscience*, 16(2), 428–429