INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)

Reversible Data Hiding with Good Payload Distortion

Indhumathi M.
Undergraduate Student, Saveetha School of Engineering, Saveetha University
Regina B.
AssistantProfessor, Saveetha School of Engineering, Saveetha University

Abstract:
In reversible data hiding, the data value is modified by some rules and the exact data can be re-stored after the extraction of data on the receiver system. Here optimal rule value under payload criteria is done by using iterative algorithm .it calculates the estimated embedded image-original image. The estimated image is modified according to the optimal value transfer. The images are divided in to the subsets. A receiver was successfully able to extract and recover the original content in the subsets on inverse order. Hence good payload distortion can be achieved.

1. Introduction

Data hiding is software development technique used in object oriented programming to hide the data content. The data hiding has the capability of hiding the intended changes. A huge number of data hiding scheme has been proposed. They had been classified into difference expansion, loss less compression based method and the histogram methods. the lossless compression based technique made use of the statistical redundancy of the loss data by performing lossless compression in order to create a spare space to accommodate secret data in addition. The optimal rule of value under payload distortion criteria is found by using the iterative procedure, and by the data reversing scheme has been proposed. The secret data and the auxiliary information is used for content recovery, are carried out by the difference between the corresponding pixel value and the original pixel are estimated from the neighbours. The estimated errors were modified according to the optimal value transfer rule. The host images were divided in to a number of pixel subsets and the auxiliary information of a subset is always embedded in to the estimated errors in the proceeding subsets. A receiver can successfully extract the embedded secret data and recover the original data content in an reverse order. By this way a good payload distortion can be achieved.

Under a payload distortion criteria we ll find the optimal rule value by expanding a target function using the iterative algorithm, an optimal value matrix can be obtained , further we design a practical reversible data hiding scheme, in which values has been modified according to the optimal value transfer matrix. In reversing data hiding methods using DE or HM mechanisms, the particular data available for accommodating the secret data, such as pixel difference or prediction errors, they are first generated from the host image, and their values are modified according to the given rules. Such as the difference expansion or the histogram modification to perform the reversible data hiding. Here, we using optimal value transfer matrix to model the reversible data hiding in the available data.

1.1. Functional Overview

The server sends the secret data to the receiver. The receiver can extract the message or image only if he knows the key value. Here the key value will be generated automatically in a separate file. The receiver can open the file and will get the required password to open the image and message. Hence the high level of security can be maintained in the medical and the military applications.

2. Related Works

2.1. Exsisiting Approach

The original mark can be recovered from the marked image in an inverse order process. Payload of this method is low since the each block can carry one bit. Based on this, a robust lossless data hiding scheme has been proposed, which can be used for semi-fragile image authentication. a typical HM methods used for utilizes the zero and the peak point histogram of an image it slightly modifies the pixel grayscale values are embedded data in to the image. In binary tree structure is used to eliminate the requirement to communicate with pairs of peak and the zero points to the recipient and the histogram technique we used for preventing the underflow and the overflow. The histogram modification mechanisms can also be implemented in the difference between the sample images and the

prediction error of the host pixels and the several prediction approaches have been introduced to improve the performance of the reversible data hiding.

2.2. Proposed Approach

The optimal rule value modification under payload-distortion criteria. By maximizing a target using an iterative algorithm, an optimal rule value can be obtained. Further, we can design a practical data reversing scheme, in which the estimated errors of the host pixels have been used to accommodate the secret data and their values are modified according to the optimal value transfer matrix, hence by this way a good payload distortion can be achieved.

3. System Architecture

3.1. Architecture Diagram

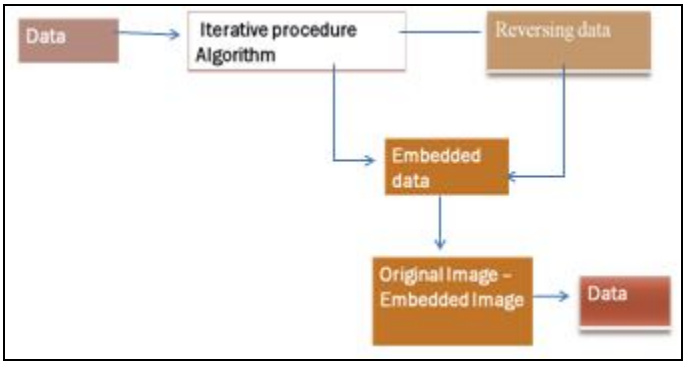

Figure 1

4. System Implementation

4.1. Module explanation

- 1. Data hiding: A data-hider can also terminate the histogram modification to realize reversible data hiding in the host image is divided in to blocks sized and the gray values are mapped in to a circle. Then pseudo randomly segmentation of each block in to sub-regions, rotation of the histogram of the two sub-regions are embedded as one bit in each block. On the receiver side, the original block can be extracted from a marked image in an reverse order. hence the payload of this particular method is low since each one carry one bit.
- 2. Optimal value transfer matrix: This again deals with the value transfer matrix for the modification of the cover value in the reversible data hiding. By using the iterative procedure is then calculated for the optimal value transfer matrix, which will be later used for reversing data hiding schemes with the good payload performance.
- 3. Data reversing: The auxiliary information and the secret data are used for the content recovery, are carried out by the differences between the original pixel values and the corresponding values are estimated from the neighbours. And according to the optimal value transfer matrix the estimated errors are modified. For maximizing the amount of secret data optimal value transfer is produced. That is by pure payload, by the iterative procedure described in the previous section. That implies the size of auxiliary information does not purely affect the optimality of the transfer matrix.
- 4. Data extraction and Content recovery: When an image containing embedded data, the receiver first divides the image in to the sets such as set A and set B and it divided the subsets using the same manner. By dividing the pixels in the host image in to two subsets, the data embedding is orderly performed in the subsets, and then the auxiliary information of a subset is always generated and embedded in to the next subsets as the estimated errors. This way, a receiver can extract their embedded image and message and recover the original content in the subsets in the reverse or an inverse order.

5. Experimental Analysis

Figure 2

- Sender sends the secret data : The sender sends the data to the receiver in the form of image and text sender sends the key to the receiver to receive the secret data. Optimal value transfer matrix and data hiding module are used.

Figure 3

- Generated key of the receiver: The key value is stored in the receiver side as a file. The receiver will generate the key to extract the secret data. The key is stored as a text file.

Figure 4

- Utilization of the generated key: The generated key in the text file from the sender is used by the receiver as the password. Then this key is used by the receiver for the extraction process so that the data is retrieved.

Figure 5

- Secret data received: In this figure 5 the actual data is extracted and viewed by the receiver without any distortion. Hence the secret data is received with good payload distortion.

6. Conclusion

In order to achieve a good payload distortion performance of reversible data hiding, this paper found the optimal value transfer matrix by maximizing a target function of pure payload with an iterative procedure, and then proposes a practical reversible data hiding scheme. This differences the original pixel values and the corresponding values are estimated from the neighbors are used to carry the payload that is made up of the actual secret data to be embedded and the auxiliary content recovery. Based on the optimal value transfer matrix, the auxiliary information is created and the estimation errors are modified. Then the host image is divided into several subsets. This way, one must successfully extract the embedded secret data and recovers the original content in the subset with an inverse order. The payload distortion evaluation of the proposed scheme is great. And for the smooth host images, the proposed scheme significantly performs the previous reversible data hiding methods. Then the optimal transfer mechanism proposed in this paper is independent from the generation of available cover values.

7. References

1. M. Goljan, J. Fridrich, and R. Du, “Distortion-free data embedding,” in Proc. 4th Int. Workshop on Information Hiding, Lecture Notes inComputer Science, 2001, vol. 2137, pp. 27–41.
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 MultimediaContents 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