Reversible Data Hiding With Good Payload Distortion

Mathangi Srujan Kumar[1]

Saveetha School Of Engineering, Saveetha University

Abstract— In reversible data hiding techniques, the value of the data are modified using some rules and the original data can be restored after the extraction of hidden data on the receiver side. The optimal rule value modification under a payload distortion is done by using iterative algorithm .it calculates the estimated embedded image-original image .Here estimated errors are modified according to the optimal value transfer. The images are divided into the subsets. A receiver was successfully able to extract the secret data and recover the original content in the subsets in the inverse order hence the good payload distortion can be achieved.

Keywords: Data Hiding, Data Extraction and Content Recovery, Data Reversing

I. INTRODUCTION

Data Hiding is a software development technique used in object oriented programming to hide the data members. Data hiding protects objects integrity by preventing intended changes. A number of data hiding schemes has been proposed. They are classified into Loss less compression based methods, difference expansion (DE) methods, and histogram modification(HM)methods. The lossless compression based methods make use of statistical redundancy of the host media by performing lossless compression in order to create a spare space to accommodate additional secret data. 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. Here, the estimation errors are modified according to the optimal value transfer rule. Also, the host image is divided into a number of pixel subsets and the auxiliary Information of a subset is always 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. This way, a good reversible data hiding performance is achieved.We will find the optimal rule of value modification under a payload-distortion criterion. By maximizing a target function using iterative algorithm, an optimal value transfer matrix can be obtained. Furthermore, we design a practical reversible data hiding scheme, in which the estimation errors of host pixels are used to accommodate the secret data and their values are modified according to the optimal value transfer matrix. This way, a good payload-distortion performance cans be achieved. In reversible data hiding methods using DE or HM mechanisms, the particular data available for accommodating the secret data, such as pixel differences or prediction errors, are first generated from host image, and then their values are changed according to some given rules, such as difference expansion or histogram modification, to perform the reversible data hiding. Here, we use transfer matrix to model the reversible data hiding in available data.

A. 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 wills b generated automatically in a separate file. The receiver has to open the file and will get the required password to open the message and images. Hence the security can be maintained.

II. RELATED WORKS

A. Existing approach

On the receiving side, the original block can be recovered from a marked image in an inverse process. Payload of this method is low since each block can only carry one bit. Based on this method, a robust lossless data hiding scheme is proposed, which can be used for semi-fragile image authentication. A typical HM method presented for utilizes the zero and peak points of the histogram of an image and slightly modifies the pixel grayscale values to embed data into the image. In binary tree structure is used to eliminate the requirement to communicate pairs of peak and zero points to the recipient, and a histogram shifting technique is adopted to prevent overflow and underflow. The histogram modification mechanism can also be implemented in the difference between sub-sampled images and the prediction error of host pixels and several good prediction approaches have been introduced to improve the performance of reversible data hiding.

B. Proposed approach

The optimal rule of value modification under a payload-distortion criterion. By maximizing a target function using iterative algorithm, an optimal value transfer matrix can be obtained. Furthermore, we design a practical reversible data hiding scheme, in which the estimation errors of host pixels are used to accommodate the secret data and their values are modified according to the optimal value transfer matrix. This way, a good payload-distortion performance can be achieved.

III. SYSTEM ARCHITECTURE

A. Architecture Diagram

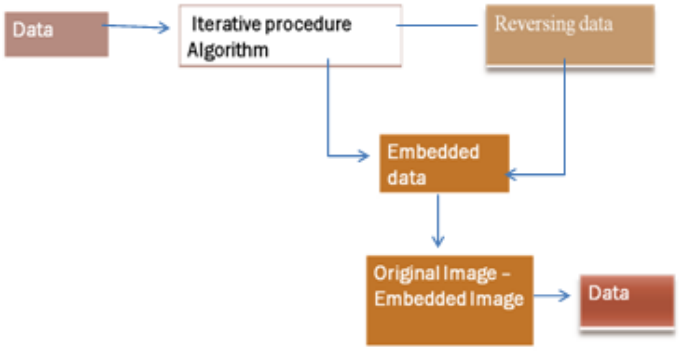

Fig. 1: System Architecture

IV. SYSTEM IMPLEMENTATION

A. Module Explanation

1) Data hiding

A data-hider can also employ histogram modification mechanism to realize reversible data hiding. In the host image is divided into blocks sized 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 a marked image in an inverse process. Payload of this method is low since each block can only carry one bit. Based on this method, a robust lossless data hiding scheme is proposed in which can be used for semi-fragile image authentication.

2) Optimal Value Transfer Matrix

This will introduce a value transfer matrix for illustrating the modification of cover values in reversible data hiding. Then, an iterative procedure is proposed to calculate the optimal value transfer matrix , which will be used to realize reversible data hiding with good payload-distortion performance .

3) Data Reversing

The secret data, as well as the auxiliary information used for content recovery, are carried by the differences between the original pixel-values and thecorresponding values estimated from the neighbors, and the estimation errors are modified according to the optimal value transfer matrix. The optimal value transfer matrix is produced for maximizing the amount of secret data, i.e., the pure payload, b y the iterative procedure described in the previous section. That implies the size of auxiliary information does not affect the optimality of the transfer matrix.

4) Data Extraction and Content Recovery

When having an image containing embedded data, the receiver firstly divides the image into Set Sets A and B, and divides Sets A and B into a number of subsets using the same manner. By dividing the pixels in host image into two sets and a number of subsets, the data embedding is orderly performed in the subsets, and then the auxiliary information of a subset is always gen rated and embedded into the estimation errors in the next subset. This way, a receiver can successfully extract the embedded secret data and recover the original content in the subsets with an inverse order.

V. EXPERIMENTAL ANALYSIS

A. Sender sends the secret data

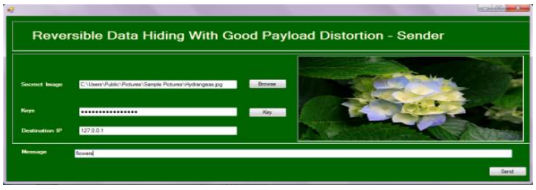

Fig. 2: Sender sends the secret data

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.

B. Generated key of the receiver

Fig. 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.

C. Utilization of the generated key

Fig. 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.

D. Secret data received

Fig. 5: Secret data received

In this figure 5.4, the actual data is extracted and viewed by the receiver without any distortion. hence the secret data is received with good payload distortion.

VI. CONCLUSION

In order to achieve a good payload-distortion performance of reversible data hiding, this work first finds 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. The differences between the original pixel-values and the corresponding values 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 information for original content recovery. According to the optimal value transfer matrix, the auxiliary information is generated andthe estimation errors are modified. Also, the host image is divided into a number of subsets and the auxiliary information of a subset is always embedded into the estimation errors in the next subset. This way, one can successfully extract the embedded secret data and recover the original content in the subsets with an inverse order. The payload-distortion performance of the proposed scheme is excellent. For the smooth host

images, the proposed scheme significantly outperforms the previous reversible data hiding methods. The optimal transfer mechanism proposed in this work is independent from the generation of available cover values. In other words, the optimal transfer mechanism gives a new rule of value modification and can be used on various cover values. If a smarter prediction method is exploited tomake the estimation errors closer to zero, a better performance can be achieved, but the computation complexity due to the prediction will be higher.

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.

