SEPARABLE DATA HIDING IN IMAGES BY RESERVING ROOM BEFORE ENCRYPTION

Mr. T.A. Muhammed Shafeek
PG Scholar,
Applied Electronics,
Maharaja Institute of Technology,
Coimbatore, Tamilnadu, India

Mr. S. Nagaraj
Assistant professor,
Applied Electronics,
Maharaja Institute of Technology,
Coimbatore, Tamilnadu, India

Abstract— ***Recently more and more attention is paid to reversible data hiding (RDH) in encrypted images, since it maintains the excellent property that the original cover can be lossless recovered after embedded data is extracted while protecting the image content's confidentiality. All previous methods embed data by reversibly vacating room from the encrypted images, which may be subject to some errors on data extract ion and/or image restoration. In this paper, we propose a novel method by reserving room before encryption with a traditional RDH algorithm, and thus it is easy for the data hider to reversibly embed data in the encrypted image. The proposed method can achieve real reversibility, that is, data extraction and image recovery are free of any error.***

Keywords— RDH, Prediction Error Expansion, Lossless Recovery

I. INTRODUCTION

Here we are investigating the data hiding technique which is reversible in nature. Thus it is termed as Reversible data hiding technique. Using the encrypted image as a cover data in which the data is embedded. In separable reversible data hiding technique firstly a content owner encrypts the original uncompressed image then a data hider compress the image to create space to accommodate some additional data. At the receiver side there are three possibilities to retrieve the embedded data and get covering data; this is the basic theme of this concept[1].

Reversible data hiding is a technique to embed additional message into some distortion-unacceptable cover media, such as military or medical images, with a reversible manner so that the original cover content can be perfectly restored after extraction of the hidden message. As an effective and popular means for privacy protection, encryption converts the ordinary signal into incomprehensible data, so that the general signal processing typically takes place before encryption or after decryption. However, in some circumstances that a content owner does not trust the service provider, the ability to manipulate the encrypted data when keeping the plain content secret is desired. When the secret data to be transmitted are encrypted, a channel provider without any knowledge of the cryptographic key may compress the encrypted data due to the limited channel resource[2].

Data hiding is referred to as a process to hide data (representing some information) into cover media. That is, the data hiding process links two sets of data, a set of the embedded data and another set of the cover media data. In most cases of data hiding, the cover media becomes distorted due to data hiding and cannot be inverted back to the original media. That is, cover media has permanent distortion even after the hidden data have been removed. In some applications, such as medical diagnosis and law enforcement it is desired that the original cover media can be recovered efficiently with no loss. The marking techniques satisfying this requirement are referred to as reversible, lossless, distortion-free or invertible data hiding techniques.

As name itself indicates that it is the reversible data technique but which is separable. The separable means which is able to separate .In other words, we can separate the some things, activities using suitable criteria. Here in separable reversible data hiding concept. The separation of activities i.e. extraction of original cover image and extraction of payload (data which was embedded).This separation requires some basic cause to occur. In separable data hiding key the separation exists according to keys.

Here at the receiver side, there are three different cases are encountered. The separation of extracting the data and getting the cover media come to be exists. That's why it is called as Separable Reversible Data hiding. Here I am investigating a hardware implementation of data hiding technique, which is reversible in nature.

There are several methods for data hiding in images available now. But most of them are not reversible in nature. Here in this paper we propose a method to achieve pure recovery of image and data. Thus here gives same importance for both image and data.

In the Existing System, Vacating Room after Encryption technique is following. Since lossless vacating room from the encrypted images is relatively difficult and sometimes inefficient, why are we still so obsessed to find novel RDH techniques working directly for Encrypted Images? The method in compressed the encrypted LSBs to vacate room for additional data by finding syndromes of a parity-check matrix, and the side information used at the receiver side is also the spatial correlation of decrypted images. All the three methods try to vacate room from the encrypted images directly[3].

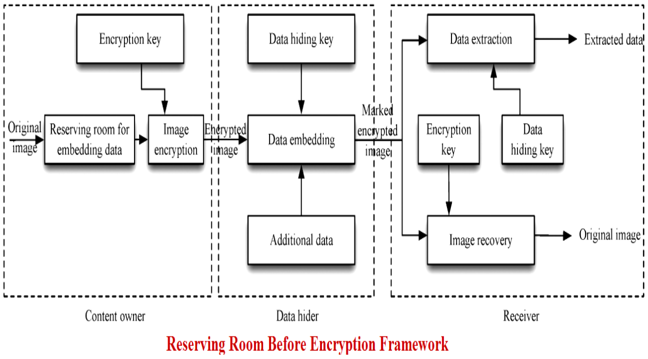


Fig 1 : Block Diagram

In proposed method can achieve real reversibility, that is, data extraction and image recovery are free of any error. If we reverse the order of encryption and vacating room, i.e., 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)".

Not only does the proposed method separate data extraction from image decryption but[5] also achieves excellent performance in two different prospects.

- Real reversibility is realized, that is, data extraction and image recovery are free of any error.
- For given embedding rates, the PSNRs of decrypted image containing the embedded data are significantly improved; and for the acceptable PSNR, the range of embedding rates is greatly enlarged.

1.1 Encrypted Image Generation

In this module, to construct the encrypted image, the first stage can be divided into two steps. Image Partition and Self Reversible Embedding followed by image encryption.

At the beginning, 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.

1.2 Data hiding in encrypted image

In this module, a content owner encrypts the original image using a 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 lossless vacating some room according[4] 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.

1.3 Data extraction and image recovery

In this module, 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 and extract the additional data by directly reading the decrypted version. When requesting for updating information of encrypted images, the database manager, then, updates information through LSB replacement and encrypts up dated information according to the data hiding key all over again. As the whole process is entirely operated on encrypted domain, it avoids the leakage of original content[5].

1.4 Data extraction and image restoration

In this module, after generating the marked decrypted image, the content owner can further extract the data and recover original image. Reversible hiding allows extraction of the original host signal and also the embedded message. There are two important requirements for reversible data hiding techniques: the embedding capacity should be large; and distortion should be low. These two requirements conflict with each other. In general, a higher embedding capacity results in a higher degree of distortion. An improved technique embeds the same capacity with lower distortion or vice versa.

II. ALGORITHM DESCRIPTION

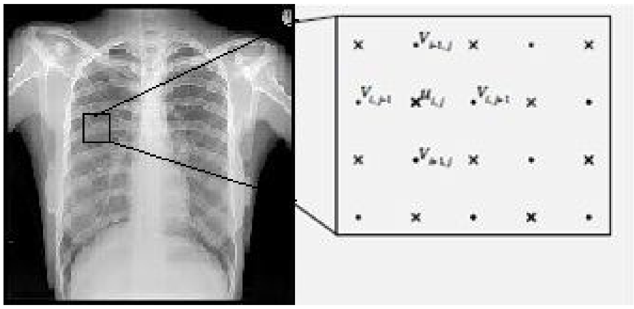


Fig 2 : Prediction Pattern

We are here modified the reversible data hiding algorithm. Here introduces a Prediction Error Expansion method using rhombus Prediction pattern. The pixel value *u* of the Cross set can be predicted by using the four neighboring pixel values of the Dot set and expanded to hide one bit of data[6].

In order to predict the pixel value of position *ui, j* in Fig. 1, four neighboring pixels (i.e., *vi, j*−1, *vi*+1, *j* , *vi, j*+1, and *vi*−1, *j*) are used. The five pixels including *ui, j* comprise a cell which is used to hide one bit of data. All pixels of the image are divided into two sets: the “Cross” set and “Dot” set (see Fig.1). The Cross set is used for embedding data and Dot set for computing predictors. Henceforth, this scheme will be called the Cross embedding scheme.

2.1 Encoding Scheme

The encoder of the Cross embedding scheme for a single cell is as follows. Center pixel *ui, j* of the cell can be predicted from the four neighboring pixels *vi, j*−1, *vi*+1, *j* , *vi, j*+1, and *vi*−1, *j*. The predicted value *ui, j* is computed as follows:

$$u'_{i,j} = \left\lfloor \frac{v_{i,j-1} + v_{i+1,j} + v_{i,j+1} + v_{i-1,j}}{4} \right\rfloor.$$

Based on the predicted value U’*i, j* and original value *ui, j* , the prediction error *di, j* is computed as

$$d_{i,j} = u_{i,j} - u'_{i,j}.$$

This prediction error can be expanded to hide information like the difference expansion algorithm proposed as follows:

$$D_{i,j} = 2d_{i,j} + b$$

Where *Di, j* is the prediction error after expansion called modified prediction error. The value *b* is one bit of the hidden message. Note that *Di, j* is modified. After data hiding, the original pixel value *ui, j* is changed to *Ui, j* as

$$U_{i,j} = D_{i,j} + u'_{i,j}.$$

2.2 Decoding Scheme

The decoding procedure for the Cross embedding scheme for a single cell is an inverse of the encoding scheme. During data hiding, pixels from the Dot set are not modified, so the predicted values *u i, j* are also not changed. Using the predicted value *u i,j* and the modified pixel value *Ui, j* , the decoder can exactly recover the embedded bit and original pixel value. The modified prediction error is computed as

$$D_{i,j} = U_{i,j} - u'_{i,j}.$$

The embedded bit value is computed as

$$b = D_{i,j} \bmod 2.$$

T

he original prediction error is computed as

$$d_{i,j} = \left\lfloor \frac{D_{i,j}}{2} \right\rfloor.$$

The original pixel’s value is computed as

$$u_{i,j} = u'_{i,j} + d_{i,j}.$$

Note that the two sets (the Cross set and Dot set) are independent of each other. Independence means changes in one set do not affect the other set[7], and vice versa. Pixels from the Dot set are used for computing predicted values *ui, j* , whereas pixels from the Cross set *ui, j* are used for embedding data. The order of hiding data in cells is not important and can be changed. Sorting reorders cells according to the magnitudes of local variance and enables hiding data in cells with small prediction errors. Thus, sorting can significantly improve the data embedding scheme.

2.3 Flowchart

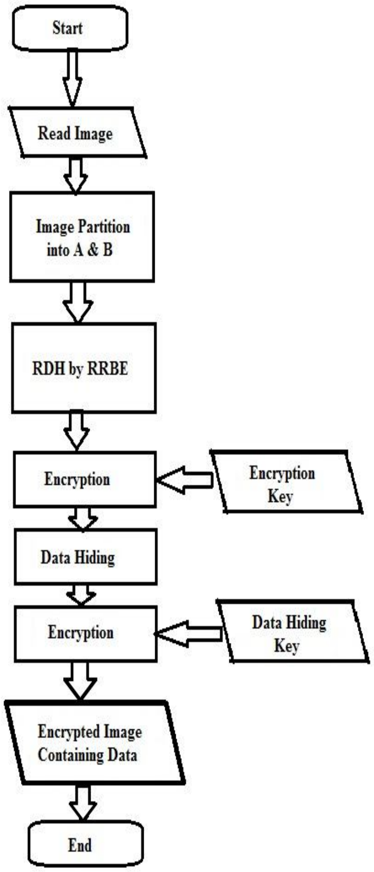


Fig 3 : Flowchart

III. RESULT AND DISCUSSION

The proposed reversible data hiding algorithm is a combination of efficient well-known existing techniques and new techniques which enables performance significantly. Using a new rhombus prediction scheme can enables the efficient exploitation of sorting. A set of sorted prediction errors can be efficiently used for low distortion data hiding. This method exploited over the sorted prediction errors produces excellent ratio between capacity and distortion. We can faster the computations using FPGA based design and thus providing a hardware platform for radiological medical image diagnosis.

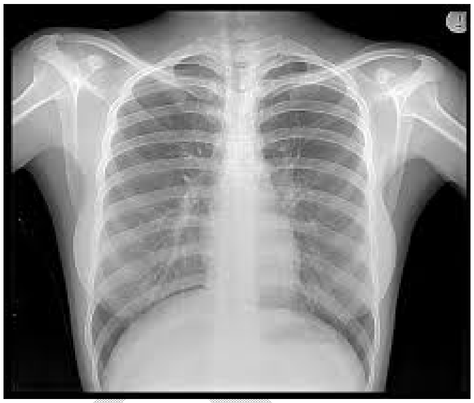


Fig 4 : Sample XRAY image before RDH

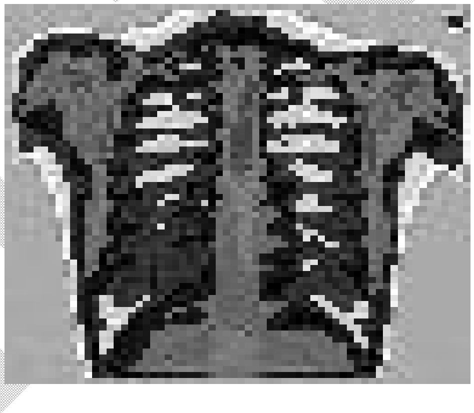
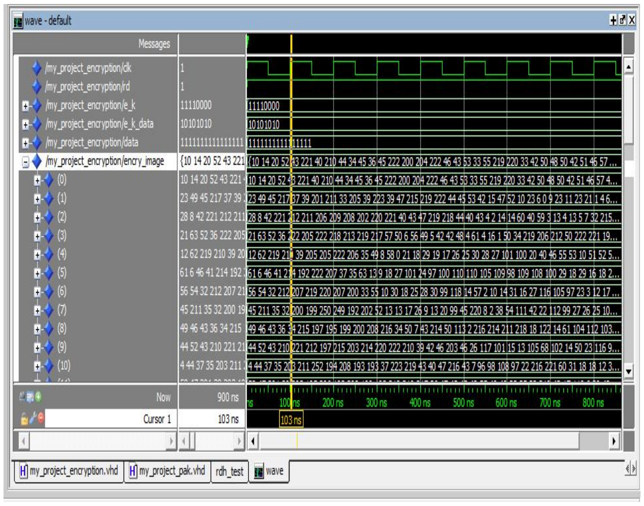


Fig. 5 : Sample XRAY image after RDH



```
/my_project_encryption/clk          1
/my_project_encryption/rd           1
/my_project_encryption/e_k          11110000           11110000
/my_project_encryption/e_k_data     10101010           10101010
/my_project_encryption/data         1111111111111111   11111111111 11111
/my_project_encryption/encry_image  {10 14 20 52 43 221 {10 14 20 52 43 221 40 210 44 34 45 36 45 222 200 204 222 46 43 53 33 55 219 220 33 42 50 48 50 42 51 46 57 ...
  (0)   10 14 20 52 43 221   10 14 20 52 43 221 40 210 44 34 45 36 45 222 200 204 222 46 43 53 33 55 219 220 33 42 50 48 50 42 51 46 57 4...
  (1)   23 49 45 217 37 39   23 49 45 217 37 39 201 211 33 205 39 223 39 47 215 219 222 44 45 53 42 15 47 52 10 23 6 0 9 23 11 23 21 1 4 6...
  (2)   28 8 42 221 212 211  28 8 42 221 212 211 206 209 208 202 220 221 40 43 47 219 218 44 40 43 4 2 14 14 60 40 59 3 13 4 13 5 7 32 215...
  (3)   21 63 52 36 222 205  21 63 52 36 222 205 222 218 213 219 217 57 50 6 56 49 5 42 42 48 4 61 4 16 1 50 34 219 206 212 50 222 221 19...
  (4)   12 62 219 210 39 20  12 62 219 210 39 205 205 222 206 35 49 8 58 0 21 18 29 19 17 26 25 30 28 27 101 100 20 40 46 55 53 10 51 52 5...
  (5)   61 6 46 41 214 192   61 6 46 41 214 192 222 207 37 35 63 13 9 18 27 101 24 97 100 110 110 105 109 98 109 108 100 29 18 29 16 18 2...
  (6)   56 54 32 212 207 21  56 54 32 212 207 219 220 207 200 33 55 10 30 18 25 28 30 99 118 14 57 2 10 14 31 16 27 116 105 97 23 3 12 17 ...
  (7)   45 211 35 32 200 19  45 211 35 32 200 199 250 249 192 202 52 13 13 17 26 9 13 20 99 45 220 8 2 38 54 111 42 22 112 99 27 26 25 10...
  (8)   49 46 43 36 34 215   49 46 43 36 34 215 197 195 199 200 208 216 34 50 7 43 214 50 113 2 216 214 211 218 18 122 14 61 104 112 103...
  (9)   44 52 43 210 221 21  44 52 43 210 221 212 197 215 203 214 220 222 210 39 42 46 203 46 26 117 101 15 13 105 68 102 14 50 23 116 9...
  (10)  4 44 37 35 203 211   4 44 37 35 203 211 252 194 208 193 193 37 223 219 43 40 47 216 43 7 96 98 108 97 22 216 221 60 31 18 18 12 3...
```

Fig 6 : Final Image cover after Performing Data Hiding

The proposed reversible data hiding algorithm is a combination of efficient well-known existing techniques and new techniques which enables performance significantly. Using a new rhombus prediction scheme can enables the efficient exploitation of sorting. A set of sorted prediction errors can be efficiently used for low distortion data hiding. This method exploited over the sorted prediction errors produces excellent ratio between capacity and distortion.

IV. CONCLUSION

Reversible data hiding in encrypted images is a new topic drawing attention because of the privacy-preserving requirements from cloud data management. Previous methods implement RDH in encrypted images by vacating room after encryption, as opposed to which we proposed by reserving room before encryption. Thus the data hider can benefit from the extra space emptied out in previous stage to make data hiding process effortless. The proposed method can take advantage of all traditional RDH techniques for plain images and achieve excellent performance without loss of perfect secrecy. Furthermore, this novel method can achieve real reversibility, separate data extraction and greatly improvement on the quality of marked decrypted images.

References

[1] Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption Kede Ma, Weiming Zhang, Xianfeng Zhao, Member, IEEE, Nenghai Yu, and Fenghua Li IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 3, MARCH 2013

[2] A J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL, USA: CRC, 1996.

[3] D.M. Thodi and J. J. Rodriguez, “Expansion embedding techniques for reversible watermarking,” IEEE Trans. Image Process., vol. 16, no. 3, pp. 721–730, Mar. 2007.

[4] K. Hwang and D. Li, “Trusted cloud computing with secure resources and data coloring,” IEEE Internet Comput., vol. 14, no. 5, pp. 14–22, Sep./Oct. 2010.

[5] Lixin Luo, Zhenyong Chen, Ming Chen, Xiao Zeng, and Zhang Xiong, Reversible Image Watermarking Using Interpolation Technique IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 5, NO. 1, MARCH 2010

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

[7] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, “On compressing encrypted data,” IEEE Trans. Signal Process., vol. 52, no. 10, pp. 2992–3006, Oct. 2004.