International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 5 44 - 47

An Enhanced Reversible Data Hiding Technique for Coloured Images

Ms. Nilam N. Shaikh[a], Prof. Amit B. Chougule[b]

[a]Asst. Prof. ,S.S.P.M.'s College of Engineering, Mumbai University, Mumbai, India

nil4386@gmail.com

[b]Asst. Prof., Bharti Vidyapeeth College of Engineering, Shivaji University, Kolhapur, India

amit.bvcoek@gmail.com

Abstract: To maintain image contents confidentiality and to recover original image, there is a need of Reversible Data Hiding scheme. This paper proposes an enhanced reversible data hiding technique for the coloured image. All previous methods embed data by reversibly vacating room from the encrypted images, which may be subject to some errors on data extraction or image restoration. The proposed method embeds data by reserving room before encryption with a traditional RDH algorithm. It is easy for the data hider to reversibly embed data in the encrypted image. This paper also concerns with a method that embeds the data invisibly into an image. The transmission and exchange of image also needs a high security. To achieve a security, Visual Cryptography is used. Visual cryptography maintains security of a cover media and also it will not make a use of encryption key. Hence, it is less prone to attack. The proposed method can achieve real reversibility, that is, data extraction and image recovery are free of any error.

Keywords: *Reversible data hiding, image encryption, privacy protection, Data extraction*

*****

I. INTRODUCTION

Data Hiding is the process of hiding the data (representing some information) into cover media. The cover media can be image, audio or video file. 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. This method widely used in medical imagery, military imagery and law forensics. Such places do not suffer any distortion of the original cover media. In this paper, the cover media is taken as coloured image. The data is being hidden into the coloured image. There is no any correlation between the cover media and the embedded data. Encryption is an effective and popular means of privacy protection. In order to securely share a secret image with other person, a content owner may encrypt the image before transmission. To achieve a security, Visual Cryptography is used. Visual cryptography maintains security of a cover media and also it will not make a use of encryption key. Hence, it is less prone to attack. As long as image is concerned the technique could be useful in the area of protection and transmission of secret sensitive military and medical images.

II. LITERATURE SURVEY

Z. Ni, Y. Shi, N. Ansari, and S. Wei, has proposed a reversible data hiding algorithm[2].This algorithm can recover the original image without any distortion from the marked image after the hidden data have been extracted. It utilizes the zero or the minimum points of the histogram of an image and slightly modifies the pixels grayscale values to embed data into the image. It can embed more data than many of the existing reversible data hiding algorithms.

A non separable reversible data hiding method[3] proposed by Xinpeng Zhang ,is shown in Fig. 1.In this method, the data extraction is not separable from the content decryption. The additional data must be extracted from the decrypted image, so that the principal content of the original image is revealed before data extraction. If some has a data hiding key but not the encryption key, he cannot extract the information from the decrypted image containing additional data.

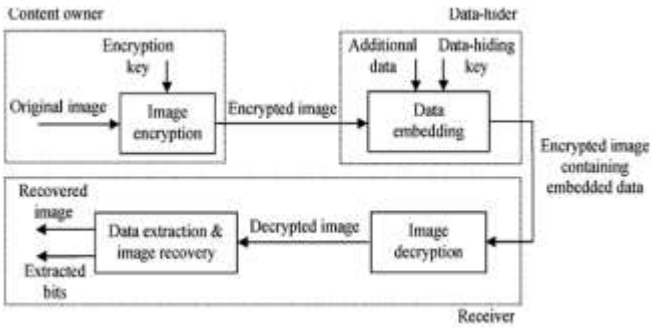

Fig. 1. A Non Separable Reversible Data Hiding method

Xinpeng Zhang has suggested, Separable Reversible Data Hiding in encrypted images [4]. As shown in Fig. 2, if the receiver has the data hiding key, he can

extract the additional data though he does not know the image content. If the receiver has the encryption key, he can decrypt the received data to obtain an image similar to the original one, but cannot extract the original data. If the receiver has the both the data hiding key and the encryption key, he can extract the additional data and recover the original content.

W. Hong, T. Chen, and H.Wu have proposed, an improved Reversible Data Hiding in Encrypted Images using Side Match[5].The authors work exploit the pixels in calculating the smoothness of each block and consider the pixel correlations in the border of neighboring blocks. These two issues could reduce the correctness of data extraction. This method 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.

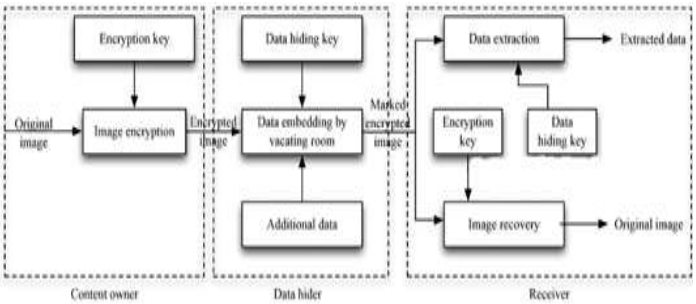

Fig. 2. A Separable Reversible Data Hiding method

Reversible Data Hiding in encrypted images by Reserving Room Before Encryption [1] suggested by Kede Ma, Weiming Zhang, Xianfeng Zhao is shown in Fig.3.The method reserves room before encryption with a traditional RDH algorithm. Hence it is easy for the data hider to reversibly embed data in the encrypted image. This method can achieve real reversibility, that is, data extraction and image recovery are free of any error.

III. PROPOSED WORK

Losslessly vacating room from the encrypted image is relatively difficult and sometimes inefficient. These methods may subject to some errors on data extraction and/or image. Hacker can recover embedding data because data is placed at particular bit position. Hence there is a need to reserve a room before encryption at content owner side using keyless encryption technique. Reversible data hiding is technique to embed the additional message in the some distortion unacceptable cover media. This is the technique that is mainly used for the authentication of data like images, videos, electronic documents. This paper proposes designing of reversible data hiding mechanism that can losslessly recover original image and can extract embedded data. It will protect the image content's confidentiality.

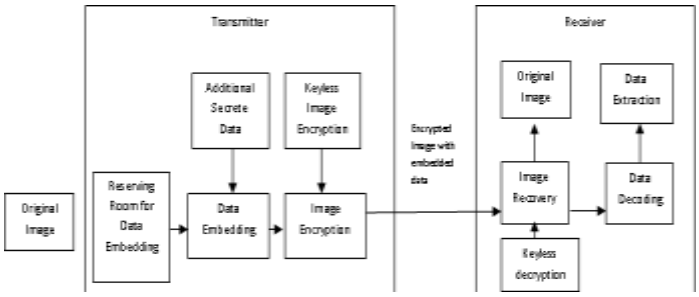

Fig.3 Reversible Data Hiding by Reserving Room before Encryption with keyless encryption

The proposed method combines the benefits of two different approaches together. Those are Reversible Data Hiding and keyless encryption of an image. Reversible Data Hiding, by Reserving Room before Encryption (RRBE) using keyless approach is shown in Fig.3.

The proposed system has designed and implemented with the following modules:

- Reserving Room for Data Embedding
- Data Hiding
- Keyless Image Encryption
  - i. Filtering
  - ii. Division
  - iii. Shuffling
- Image Decryption
- Data Extraction

The content owner selects the cover media as an image. From an original image space for embedding the secret data is found out. Then the image is encrypted with keyless image encryption methodology. Upon receiving receiver decrypts image using the keyless approach and extracts the data and recovers original image.

Figure 3 shows block diagram of proposed approach. Reserving room for data hiding is discussed in section 3.1. Section 3.2 describes Data hiding scheme. The keyless approach for image encryption is illustrated in section 3.3. Section 3.4 describes image decryption method and in section 3.5 data extraction process is mentioned.

3.1 Reserving Room for Data Embedding

The common approach for high capacity data embedding is to find the room for embedding data. The scheme involves partitioning the image logically. The goal of image partition is to construct a smoother area, on which RDH algorithm can achieve better performance.

Let us consider there is original color image with sized $M \times N$ and pixel $C_{i,j} \in [0,255], 1 \leq i \leq M, 1 \leq j \leq N$.First, the content owner finds several blocks from the original image, along the rows, several blocks whose number is determined by the size of to-be embedded messages, denoted by l. Image will be divided into number of blocks every block will be consisting of m rows, where $m = l/N$, and the

number of blocks can be computed from $No\_Of\_Blocks = M/m$.
For every block first order smoothness is measured with the help of following f function.
First order smoothness function can be defined as,

$$f = \sum_{u=2}^{m} \sum_{v=2}^{N-1} \left| C_{u,v} - \frac{C_{u-1,v} + C_{u+1,v} + C_{u,v-1} + C_{u,v+1}}{4} \right|$$

Higher f relates to blocks which contain relatively more complex textures. The content owner thus selects the blocks with relatively lower f value to be B which is logical smoother area to hide the data. For deciding over the smoother area the average value of f-value of all the blocks is considered and the blocks with f-value below average is considered to be relatively smoother.

$if(f - value_{i-block} < f - value_{avg})$
then
$block_{index}[i] = 1$
else
$block_{index}[i] = 0$

Thus blocks with index value 1 will be used for data hiding in the data embedding phase.

3.2 Data Hiding

The data hiding module separates Red, Green and Blue component of the image. Then each component of the colour is considered separately. By considering each separate colour component, the data is added into it. This increases the data embedding capacity of an image.

The data hiding algorithm:
1. Find separate Red, Green and Blue components of an image. We will have three different matrices of three different colour components like R-Matrix, G-Matrix, B-matrix.
2. Then apply the process of difference expansion for hiding data bits. Here pixel from blocks, which are having *f-value* lies below *f-avg* are used for embedding process. These blocks are smoother than others. After using all possible pixels of R-component of a block, G-component is considered then B-component is used. In this way data is being added into the different colour components.
3. Convert the message text into binary form. Then consider bits from the binary data one by one and hide it.
4. If certain block is completely used then the other block is taken under consideration. Likewise complete data file is hidden in the image blocks.

3.3 Keyless Image Encryption

The keyless approach of image encryption can be implemented with following steps:

3.3.1 Splitting

The splitting step includes distributing the combined RGB components into individual R, G and B components. The granularity of the sieve depends on the range of values that R/G/B component may take individually.

3.3.2 Division

After converting the original image into the Red, Green and Blue components, the next step is to divide the Red, Green and Blue components into z parts or shares each.

R -> (RA, RB, RC, ----------, RZ)
G -> (GA, GB, GC, ----------, GZ)
B -> (BA, BB, BC, ----------, BZ)

While performing division, it should be get confirmed that each element in RA-Z, GA-Z and BA-Z is assigned values randomly, such that the entire domain is available for randomized selection. For example, if x = 8, then individual elements should be randomly assigned a value varying from 0- 255. The shares so generated should be such that (RA, RB, RC, ---------- RZ) should regenerate R and similarly for G and B components.

3.3.3 Shuffling

, RA-Z, GA-Z and BA-Z shares are generated after performing division. Next is to perform the shuffle operation. This involves shuffling the elements in the individual shares. The sequence in which the elements within the shares are shuffled depends on the value of one of the other shares generated from the same primary colour. RB decides how RA is shuffled, RC decides how RB is shuffled, ---------- RZ decides RZ-1 is shuffled and RA decides how RZ is shuffled. After performing above three operations, the final generated share is combined and final Z-random shares are generated. The final z random shares are (RS).

RSA - > (RA- shuffle, GA- shuffle and BA- shuffle)
RSB -> (RB- shuffle, GB- shuffle and BB- shuffle)
- - - -
RSZ -> (RZ- shuffle GZ- shuffle and BZ- shuffle)

If we consider individual shares, then these individual shares does not predict any valid information. So to have original image, all shares are required.

3.4 Image Decryption

The process of retrieving the original image involves following process:

1. Filtering the random shares and retrieving R/G/B (A-shuffle) and R/G/B (B-shuffle)
2. Then, from the individual shuffled shares generate the original RA, GA, BA and RB, GB.
3. Using these, original image is then generated. The retrieved image is same as original and there is no loss of picture quality occurs.

3.5. Data Extraction

For performing the data extraction, the new pixel values of the image are considered. The difference of the

neighbouring pixels is calculated. The LSB of the difference is the bit which was hidden. For this, the data retrieval method require the index position of those blocks which were considered in hiding process and the pixel pairs position where the data is hidden as the input.

Data Extraction Algorithm:
1. Separate the Red, Green and Blue components matrices of the image blocks.
2. First, calculate the average and the difference of the Pixels(a',b').
3. The embedded data is least significant bit of y', and the original difference y is calculated.
4. The original pixels can be restored.
5. With the help of above process, one by one each bit will be extracted from the pixel pairs.
3. To find the hidden data, use and apply proper decoding technique. And extract binary data.

IV. CONCLUSION

An enhanced Reversible data hiding schemes for encrypted colored image is proposed, which consists of image encryption, data hiding, data extraction and image recovery phases. The original images are encrypted by a keyless image encryption strategy. A data hider does not need to know the original content. He can embed the secret data into the image by using difference expansion method. And at the receiver side, he can extract the data and also image can be decrypted using keyless image decryption method. If we consider individual shares, then these individual shares does not predict any valid information. So to have original image, all shares are required. Hence, security is maintained through keyless image encryption.

REFERENCES

[1] J. Fridrich and M. Goljan, "Lossless data embedding for all image formats," in Proc. SPIE Proc. Photonics West, Electronic Imaging, Security and Watermarking of Multimedia Contents, San Jose, CA, USA, Jan. 2002, vol. 4675, pp. 572–583

[2] W. Zhang, B. Chen, and N. Yu, "Improving various reversible data hiding schemes via optimal codes for binary covers," IEEE Trans. Image Process., vol. 21, no. 6, pp. 2991–3003, Jun. 2012.

[3] Nosrati Ronak Karimi Mehdi Hariri," Reversible Data Hiding: Principles, Techniques, and Recent Studies". World Applied Programming, Vol (2), Issue (5), May 2012. 349-353ISSN: 2222- 2510©2011 WAP journal. www.waprogramming.com

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

[5] 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.

[6] K.Shankar, Dr.C.Yaashuwanth, " Data Hiding and Retrieval in Encrypted Images". © 2014 IJEDR | Volume 2, Issue 1 | ISSN:2321-9939

[7] Dr. T. Bhaskara Reddy, Miss. Hema Suresh Yaragunti , Mr.T. Sri Harish Reddy, Dr. S. Kiran " An Effective Algorithm of Encryption and Decryption of Images Using Random Number Generation Technique and Huffman coding" Hema Suresh Yaragunti et al, Int.J.Computer Technology & Applications, Vol 4 ,883-891

[8] Xinpeng Zhang, Member, IEEE "Reversible Data Hiding With Optimal Value Transfer" IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 15, NO. 2, FEBRUARY 2013

[9] Subhanya R.J , Anjani Dayanandh N , " Difference Expansion Reversible Image Watermarking Schemes Using Integer Wavelet Transform Based Approach". International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 International Conference on Humming Bird (01st March 2014)

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

[11] C. Anuradha and S. Lavanya "A secure and authenticated reversible Data hiding in encrypted images" © 2013, IJARCSSE

[12] Che-Wei Lee1 and Wen-Hsiang Tsai1 "A Lossless Data Hiding Method by Histogram Shifting Based on an Adaptive Block Division Scheme" c 2010 River Publishers.

[13] Kede Ma, Weiming Zhang, Xianfeng Zhao, *Member, IEEE, Nenghai Yu, and Fenghua Li,* "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption", *IEEE Transactions on Information Forensics and Security,* vol. 8, no. 3, Mar. 2013

[14] 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.

[15] X. Zhang, "Reversible data hiding in encrypted image", *IEEE Signal Process. Lett.,* vol.18, no.4, pp. 255-258, Apr.2011

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

[17] 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.

[18] Weiming Zhang, Kede Ma, Nenghai Yu, "Reversibility improved data hiding in encrypted Images", *ELSEVIER Signal Process.,* 94 (2014) 118-127