ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

Reversible Image Data Hiding Using Contrast Data Enhancement

Sonia Bajaj

M.Tech Student, Department of Computer Science and Engineering, Jhulelal Institute of Technology, Nagpur, India

ABSTRACT: This paper aims at proposing a novel method by reserving groom before encryption with atraditionalRDH algorithm. 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 losslessley covered 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 extraction and/or image restoration however, the proposed method can achieve real reversibility, that is, data extraction and image recovery are free of any error. MD5 algorithm is used and implemented in order to enhance and provide double layer of data secure mechanisms.

KEYWORDS: Reversible Data Hiding, Contrast Enhancement, MD5, Data hiding techniques.

I. INTRODUCTION

Reversible Data Hiding aims at solving the problem related to data extraction and image restoration. This method aims at achieving real reversibility, Separate data extraction and great improvement on the quality of marked decrypted images. With the employment of key less approach for image encryption our goal is to retrieve the original image lossless with minimum computation required and also task related to key generation and key management will be minimized. In this method we hide the data and the cover file so that it can be recieved lossless at the receiver side. On the transmitter side, this system involves a cover image, additional data, encryption key and data hiding key. The original image will be encrypted, data will be hidden and then image will be transmitted. The receiver thus needs to decrypt the image and extract the data.

Contrast Enhancement is the process of changing the intensity of the pixels of the input image in order to utilize maximum possible bins. Histogram equalization is one of the method of achieving image contrast enhancement, it is performed by modifying the histogram of pixel values. The two highest bins of the histogram are found out and then the bins between the peaks are unchanged while the outer bins are shifted outwards thereby splitting the two peaks in two adjacent bins. This process is used to obtain data embedding with contrast enhancement simultaneously. The highest two bins in the histogram can be further splitted ans so on to achieve increased embedding capacity alongwith satisfactory contrast enhancement. To recover original image, the location map is fixed into the host image together with the bits of message and other side information.

The MD5 message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of cryptographic applications, and is also commonly used to verify data integrity.On Sender's side -Instead of directly adding the text into the image. We will perform md5 encryption on the data. Then we will convert the encrypted data into bits and embded the bits in the image using contrast enhancement algorithm.Then we will divide the image into 4 shares,Once this is done we will send the each share to receiver side.
On the Receiver's side, we will receive all the 4 shares of the image,then we will generate the original image from 4 shares, then we will extract the bits from the image using contrast enhancement technique. Then we will decrypt the bits using md5 decryption and get the original data.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

II. MD5 WORKING

The message digest called the "hash" or "fingerprint" of the input. A 128-bit output found security hazard in the algorithm. Moreover, a 128-bit hash output may not offer a sufficient amount of security protection in the near future. The content of Message-Digest is strongly related to the original data. Once the original data were altered, the content of Message-Digest integrity different to the old . The output from the original data is unalterable, which means it can not be reverted to original data or can not be accomplished through reverse-computing. So it usually can not only be used for data reliability validation but also for content encryption . Therefore the algorithm based on this principle can provide more robust protection about data. MD5 is used in many situations where a long message requires to be processed and compared rapidly i.e. mostly used in creation and verification of digital signatures. MD5 was developed from MD, MD2, MD3 and MD4 . It is a improved version in all MD"s algorithms. The input message is divided into chunks of 512-bit blocks. And the process of MD5 contains the following steps: Preparing the input (Padding bits, appending data length), initializing MD5 buffer, processing message in 16-word block and output.

MD5 is a widely used cryptographic function with a 128- bit hash value. MD5 has been employed in a wide variety of security applications, and is also commonly used to check the integrity of files. An MD5 hash is typically expressed as a 32digit hexadecimal number. MD5 algorithm is one of the most common Hash function. Its basic principle is to process the input information divided groups by 512 bits, and each group divided into 16 sub-groups with 32 bits. After a series of processing, the algorithm output composed by 4 groups with 32 bits, and cascade this 4 groups will generate a hash value with 128 bits. In the process of MD5 algorithm, fill information first to make its length 64 less than the multiple numbers of 512. The filling method is to attach a 1 and millions of 0, and add an information length before filling indicated by binary system with 64 bits. These two steps are to make the information length be the integer multiple of 512, and ensure the difference after different information filling.

III. LITERATURE SURVEY

Data hiding plays an important role in protecting sensitive data. Most of the hiding techniques perform data embedding by altering the contents of a host media. As a result the host image cannot be completely recovered afterthe bit extraction. These types of data hiding techniques are thus irreversible. However in a number of domains such as military, legal and medical imaging although some embedding distortion is admissible, permanent loss of signal fidelity is undesirable. This highlights the need for Reversible (Lossless) data embedding techniques.
One of the generalized data embedding methods is the LSB (Least significant Bit) modification. In this well known method the LSB of each signal sample is replaced by a payload data bit. During extraction, these bits are read in the same scanning order, and payload data is reconstructed.Various researchers have worked for devising various techniques for reversible data hiding into the digital mediaMany of them have come up with various promising approaches which enable the recovery of both the original host media and the secret message from the stegno-image. These methods can be classified into four main categories in These are as follows:

Difference Expansion Techniques:
This technique [3] was devise to achieve high capacity, low- distortion reversible data hiding. This technique divide the image into pairs of pixels and a secret messages was embedded into the difference between the pixel of each pair that was not expected to cause overflow/ underflow issues.

Histogram-Based Schemes:
Histogram shifting based reversible data hiding schemes embed data by shifting the histogram into fix direction. In this method two points which are important is peak point and zero point. Here pixel between the peak and zero pairs were modified in the embedding processing, the pixel and zero pairs were modified in the embedding processing, and the pixel in the peak point was used to carry a bit of the secret message.

Prediction-Based Methods:
Reversible data hidings based on prediction error use predicted system to embed data, there are many predictors which have been proposed. They are horizontal predictor, vertical predictor, Casual weighted average, Casual and SVF. Each pixel of the cover image, excluding the first row and the first column, is predicted by its top and left neighboring pixels

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

in the raster-scanning order. The relationship between the prediction error and the pre-determined threshold decides whether the current pixel is embeddable or not. Since the proposed prediction process provides small prediction error, our method can achieve high embedding rate and good visual quality of the stego image by the expansion of prediction error. During the procedure of extraction and recovery, the same prediction process is conducted, and then the embedded secret data and the cover image can be recovered correctly.

Vector Quantization Based Scheme: In this scheme in compression domain, which is called as reversible data hiding based on vector quantization (VQ). VQ is one of efficient compression technique, and it has widely used for its good character of easy implementation and high efficiency. This technique uses upper block and left blocks to predict the current block to embed data.

After embedding the data in the image the main focus is on protection of such image in transmission. Thus protecting the image in transmission involves encrypting the image. For maintaining the security of images two different approaches can be employed that is one encrypting the image using the encryption keys and second approach can be without using the keys, where the image is divided into different shares to maintain the image secrecy. This allows the visual information to be encrypted in such a way that their decryption can be performed by human visual system. Unfortunately heavy computation cost and key management limit the employment of the first approach and the poor quality of the recovered image from the random shares limit the application of the second approach. Thus various measures can be employed to retrieve the cover image losslessly in process.

IV. PROPOSED PLAN OF WORK

The proposed method gives an efficient technique to overcome the limitations of existing schemes in the area of reversible data hiding. Reversible data hiding using images is the technique by which the original cover image can be losslessly recovered.
It involves five main steps:

- Image Pre Processing
- Image Histogram
- Embedding data
- Original image recovery
- Data extraction.

At Transmitting end, we will get image to be transferred. At receiving end, we will get the hidden data as well as image without any loss of data.

EXPECTED OUTPUT
Input:
First, we will give one text file which will contain the data that is to be hidden in an image

Second, will be the image in which we are hiding the data.

EXPECTED OUTCOME
At Transmitting end, we will get image to be transferred. At receiving end, we will get the hidden data as well as image without any loss of data.

PARAMETERS FOR PERFORMANCE EVALUATION
PSNR ratio, Execution Time, Size of text to be hidden.

V. CONCLUSION AND FUTURE WORK

We are going to apply the technique of Reversible data hiding for maintaining the confidentiality of the data and to provide double layer of security, MD5 algorithm(message digest algorithm) is implemented on both the sender and the receiver side. Reversible data hiding in encrypted image is drawing lots of attention because of privacy preserving

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

requirements. Thus proposed scheme provides a completely new framework for reversible data hiding. In the proposed approach we take advantage of visual cryptography approach for encrypting the image. Thus the image is protected in transmission and secret data is also transmitted securely. As this approach does not involve any use of keys is keyless approach for image encryption with the complete lossless image recovery and data extraction.

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] Z. Ni, Y. Q. Shi, N. Ansari, andW. Su, "Reversible data hiding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354–362, Mar. 2006.
[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] D. Coltuc and J.-M. Chassery, "Very fast watermarking by reversible contrast mapping," *IEEE Signal Process. Lett.*, vol. 14, no. 4, pp. 255–258, Apr. 2007.
[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] X. Li, B. Yang, and T. Zeng, "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection," *IEEE Trans. Image Process.*, vol. 20, no. 12, pp. 3524–3533, Jan. 2011.
[7] Z. Zhao,H.Luo,Z.-M. Lu, and J.-S. Pan, "Reversible data hiding based on multilevel histogram modification and sequential recovery," *Int. J. Electron. Commun. (AEÜ)*, vol. 65, pp. 814–826, 2011.
[8] H. T.Wu and J. Huang, "Reversible image watermarking on prediction error by efficient histogram modification," *Signal Process.*, vol. 92, no. 12, pp. 3000–3009, Dec. 2012.
[9] Y. Yang, X. Sun, H. Yang, C.-T. Li, and R. Xiao, "A contrast-sensitive reversible visible image watermarking technique," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 19, no. 5, pp. 656–667, May 2009.
[10] J. A. Stark, "image contrast enhancement using generalizations of histogram equalization," *IEEE Trans. Image Process.*, vol. 9, no. 5, pp. 889–896, May 2000.
[11] P. G. Howard, F. Kossentini, B. Martins, S. Forchhammer, and W. J. Rucklidge, "The emerging JBIG2 standard," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 8, no. 7, pp. 838–848, Jul. 1998.
[12] The USC-SIPI Image Database [Online]. Available: http://sipi.usc.edu/ database/
[13] Kodak Lossless True Color Image Suite [Online]. Available: http:// www.r0k.us/graphics/kodak/
[14] M.-Z.Gao, Z.-G.Wu, and L.Wang, "Comprehensive evaluation forHE Based contrast enhancement techniques," *Adv. Intell. Syst. Applicat.*, vol. 2, pp. 331–338, 2013.