International Journal of advancement in electronics and computer engineering (IJAECE)
Volume 7, Issue 3, March2018, pp.301-305, ISSN 2278 -1412
Copyright © 2012: IJAECE (www.ijaece.com)

Secure Reversible Image Data Hiding

Pooja Chourasia[1], Dr. Anubhuti Khare[2]

1P.G. Student, Electronic & Communication Department, U.I.T. RGPV College, Bhopal, India;
2Associate Professor, Electronic & Communication Department, U.I.T. RGPV College, Bhopal, India;

Abstract *– The world now gives opportunity to the computer and the related systems directly or indirectly for living. Information security is one of the major concerns in this System. Steganogrphy are the most popular or widely used information security scheme or techniques. It is the act of covert communications. The paper give a review on a novel framework for reversible data hiding in encrypted image (RDH-EI) based on reversible image transformation (RIT). Different from previous frameworks which encrypt a plaintext image into a cipher text form; RIT-based RDH-EI shifts the semantic of original image to the semantic of another image and thus protects the privacy of the original image. This paper is a survey which describes several different algorithms for Reversible Data Hiding (RDH). Previous literature has shown that histogram modification, histogram equalization (HE) and interpolation are the most common methods for data hiding.*

Keywords*: Difference expansion (DE), location map, reversible data embedding, reversible integer transform,*

I. Introduction

Now a days, Outsourcing photos to cloud and sharing photos through social media increasingly famous, which in the meantime make it challenging to ensure the protection of photos. Reversible image data hiding (RIDH) is a special category of data hiding technique, which ensures perfect reconstruction of the cover image upon the extraction of the embedded message. Data hiding is a technique for embedding information into covers such as image, audio, and video files, which can be used for media notation, copyright protection, integrity authentication, covert communication, etc. Most data hiding methods embed messages into the cover media to generate the marked media by only modifying the least significant part of the cover and, thus, ensure perceptual transparency. The embedding process will usually introduce permanent distortion to the cover, that is, the original cover can never be reconstructed from the marked cover. However, in some applications, such as medical imagery, military imagery, and law forensics, no degradation of the original cover is allowed. In these cases, we need a special kind of data hiding method, which is referred to as reversible data hiding (RDH) or lossless data hiding, by which the original cover can be lossless restored after the embedded message is extracted. This will received by image Decryption that will decrypt the received data and by this decrypt information the original information is extracted by performing the reverse operation by using the same Encrypt key. Recently, reversible data embedding techniques have drawn more and more interest. Existing methods can be classified according to the techniques associated with restoration. Some of the approaches rely on lossless compression to exploit the redundant space created by the compression operation The existing reversible data hiding algorithms, including some newest schemes, have been classified into three categories:

1) Those developed for fragile authentication.

2) Those developed for achieving high data embedding capacity.

3) Those developed for semi-fragile authentication.

The main motive of proposing the RIDH scheme is to develop a technique by which we can recover the embedded data without causing any harm to the cover media [1]-[3].

Data Hiding is the process to hide data (representing some information) into cover media. That is, the data hiding process links two sets, a set of the embedded data and another set of the cover media image. The relationship between these two sets characterizes different applications. A number of reversible data hiding techniques have been proposed, and they can be roughly classified into three types: lossless compression based methods, difference expansion (DE) methods, and histogram modification (HM) methods. In practical aspect, many RDH techniques have emerged in recent years [3]-[7]. Previously, the data RIDH mainly work in the non encrypted domain, that is, it embeds the plain text inside an image with the lossless compression technique. Since the lossless compression is useful indeed, embedding the plain text in the image is the lack of security. Some of the related terminologies are:

I.1. Watermarking

The term "Digital Watermark" was proposed by Andrew Tirkel and Charles Osborne in December 1992 [5]. The first successful embedding and extraction of a steganographic spread spectrum watermark was performed in 1993 by Andrew Tirkel, Charles Osborne and Gerard Rankin [5]. To provide a security, firstly the watermarking was used inside the carrier media which is the very basic model of security. Basically, the watermarking was developed to add the digital signature of the media product inside that media to make it authorized. It is used to verify the reality or integrity of the carrier signal or to show the personality of its owners. It is evidently used for tracing copyright violation and for banknote authentication. It does not change the size of the carrier signal.

I.2. Steganogrphy

The first reported use of the steganogrphy was coined by Johannes Trithemius in 1499 in his Steganographia [2]. A work on cryptography and steganography is a revolutionary change. The messages to be hide are generally embedded inside the image, video, audio, file, etc. For example, the hidden message may be in invisible ink between the visible lines of a private letter. Some practical works of steganography that fails to be described the secret of forms of security through ambiguity, where the scheme of key system follows to Kerckhoffs's principle. Steganography consists of the hiding of information inside the electronic media. Steganography includes electronic communications that may consist of steganographic coding within the transport layer, like a document, image, program or protocol. It is best to use the media files to hide data because it having a very large size to hide a big amount of data in it. Comparing with the other media, media files provide much flexibility to add data in it.

II. Literature Survey

Jiantao Zhou et. al. [1] “Secure Reversible Image Data Hiding over Encrypted Domain via Key Modulation” This work proposes a novel reversible image data hiding (RIDH) scheme over encrypted domain. At the decoder side, a powerful two-class SVM classifier is designed to distinguish encrypted and non-encrypted image patches, allowing us to jointly decode the embedded message and the original image signal. In this paper, author design a secure reversible image data hiding (RIDH) scheme operated over the encrypted domain. Author suggests a public key modulation mechanism, which allows us to embed the data via simple XOR operations, without the need of accessing the secret encryption key. The proposed technique embeds message through a public key modulation mechanism, and performs data extraction by exploiting the statistical distinguish ability of encrypted and non-encrypted image blocks.

J. Tian et. al. [2] “Reversible data embedding using a difference expansion” Reversible data embedding is also known as lossless data embedding, which is embeds invisible data (which is known as payload) into a digital image in a reversible pattern. The original digital content can be completely restored in reversible. In this method, reversible data-embedding method for digital images. Analyze the redundancy in digital images to achieve very high embedding capacity, as well as keep the distortion less. For digital images, this method presented a simple and efficient reversible date-embedding method. Search the repetition in the digital fulfilled to obtain reversibility.

Hao-Tian et. al. [3] “Reversible Image Data Hiding with Contrast Enhancement” The proposed algorithm was implemented on two sets of images to demonstrate its efficiency. To our best knowledge, it is the first algorithm that achieves image contrast enhancement by RDH. Furthermore, the evaluation results show that the visual quality can be preserved after a considerable amount of message bits have been embedded into the contrast-enhanced images, even better than three specific MATLAB functions used for image contrast enhancement. In this paper, a novel reversible data hiding (RDH) algorithm is proposed for digital images. Instead of trying to keep the PSNR value high, the proposed algorithm enhances the contrast of a host image to improve its visual quality. The proposed algorithm has made the image contrast enhancement reversible. Improving the algorithm robustness, and applying it to the medical and satellite images for the better visibility.

Hao Luo et. al. [4] “Reversible data hiding based on block median preservation” This paper proposes a reversible data hiding scheme for gray level images. It exploits the high correlation among image block pixels to produce a difference histogram. The image blocks are divided into four categories due to four corresponding embedding strategies, aiming at preserving the medians during data embedding. A reversible data hiding scheme for gray level images is proposed in this paper. It is based on a multi-level histogram shifting mechanism. The histogram is constructed by block differences with the reference of their integer medians. In order to preserve the block medians, the image blocks are divided into four categories with different embedding strategies used.

Guangyong Gao et. al. [5] “Reversible Data Hiding Using Controlled Contrast Enhancement and Integer Wavelet Transform” The conventional reversible data hiding (RDH) algorithms pursue high Peak-Signal-to-Noise-Ratio (PSNR) at the certain amount of embedding bits. A reversible data hiding scheme for gray level images is proposed in this paper. It is based on a multi-level histogram shifting mechanism. The histogram is constructed by block differences with the reference of their integer medians. In order to preserve the block medians, the image blocks are divided into four categories with different embedding strategies used.

Seung-Won Jung et. al. [6] “A New Histogram Modification Based Reversible Data Hiding Algorithm

Considering the Human Visual System" In the proposed algorithm, unlike the conventional reversible techniques, a data embedding level is adaptively adjusted for each pixel with a consideration of the human visual system (HVS) characteristics. The experimental results and performance comparison with other reversible data hiding algorithms are presented to demonstrate the validity of the proposed algorithm. In the proposed algorithm, unlike the conventional reversible techniques, the HVS characteristics are extensively exploited to alleviate the distortion caused by data embedding. The proposed technique effectively exploited the well-known HVS characteristics for reversible image data embedding.

III. Related Technology

The Steganography is defined as a technique to hide data into images in such a manner, which is unperceivable. Steganography and Cryptography, both are used for security purposes but with different implementation and approaches. In cryptography, the text file get converted to other form which provide confidentiality to sensitive data but in steganography we hide the actual data file in image form so that if leakage get occurred the third party fails to recognize the actual data. This provides confidentiality as well as security to the sensitive data. The idea is to hide text in image with the conditions that the image quality is retained along with the size of the image instead we can encrypt the data. So the need is, in cryptography output of an unreadable data files are being send over an internet is easily detectable that some important information is being conveyed. While in steganography hiding message in an image, along with the conditions, it make seem of just an exchange of picture between two user ends. The steps being followed in steganography are as under:-

1. Firstly the text message is being written, then encryption of the message is done.
2. Later, text is hidden in the selected media like image file and transmitted at the receiver side.
3. At receiver end, reverse method is done to implement and recover the original text message.

Various techniques are used in the field of steganography by arranging the different bits of the character of the text message in the image file and other media. In order to encrypt the data two files are needed:

(i) Image file and

(ii) The text file containing the data.

Our algorithm is simple and flexible using LSB (Least Significant Bit) technique. We have selected the formats that commonly use lossless compression that is BMP, PNG, TIFF and GIF. When data is streamed, it is captured after the header and chopped into 8 bits. In 24-bit BMP, Therefore comparing bit values byte by byte both of text and image. The technique we are using is LSB i.e. storing in LSB of a byte (pixel).

Some of the techniques used in steganography are domain tools or simple system such as least significant bit (LSB) insertion. In our security model, we divide the document / scanned images of document into parts. The parts will be reversibly transformed, encrypted and then encoded into target images which enhances the security of document and reduces possible attacks. At the time of file transfer we will check the access permission for the user as well as hash value of that document.

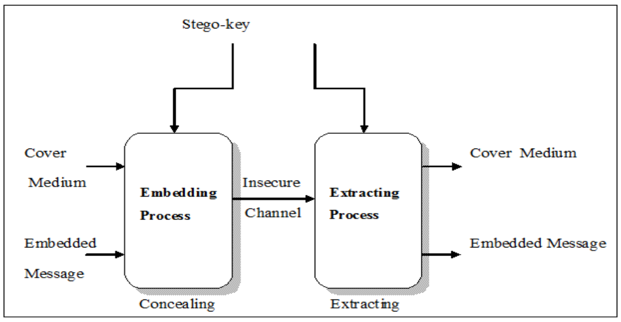

Fig.1. Steganographic Process

If the document is an official document and particular employee is trying to leak that particular document, system will automatically prevent it and send notifications to higher authority for further actions to be taken. In order to protect the data files being open source the data leakage must be detected in the early stage. Embedding data, which is to be hidden into an image, requires two files. The first is the image that will hold the hidden information, called the cover image. The second file is the message- the information to be hidden. When combined the cover image and the embedded message make a stegoimage or stego-file as shown in figure 1. Steganography system is designed for encoding and decoding a secret file embedded into an image file using random LSB insertion method in which the secret data is spread out among the image data in a seemingly random manner. This could be achieved using a secret key.

III .1. Steganographic Techniques

There have been many techniques for hiding information or messages in images.

A. Least significant bit insertion (LSB).

B. Masking and filtering.

C. Transform techniques.

Least significant bits (LSB) insertion is a simple approach to embedding information in image file. The simplest steganographic techniques embed the bits of the message directly into least significant bit plane of the cover-image in a deterministic sequence. Masking and filtering techniques, usually restricted to 24 bits and gray scale images, hide information by marking an image, in a manner similar to paper watermarks. The techniques performs analysis of the image, Transform techniques embed the message by modulating coefficients in a transform domain, such as the Discrete Cosine Transform

(DCT) used in JPEG compression, Discrete Fourier Transform, or Discrete Wavelet Transform. These methods hide messages in significant areas of the cover-image.

IV. Method

IV.1 Encryption Method

The Encryption is the process of converting a plaintext message into cipher text which can be decoded back into the original message. An encryption algorithm along with a key is used in the encryption and decryption of data. There are several types of data encryptions which form the basis of network security. Encryption schemes are based on block or stream ciphers.

The type and length of the keys utilized depend upon the encryption algorithm and the amount of security needed. In conventional symmetric encryption a single key is used. With this key, the sender can encrypt a message and a recipient can decrypt the message but the security of the key becomes problematic. In asymmetric encryption, the encryption key and the decryption key are different. One is a public key by which the sender can encrypt the message and the other is a private key by which a recipient can decrypt the message.

IV.2 Watermark Method

A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as an audio, video or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of hiding digital information in a carrier signal; the hidden information should, but does not need to, contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners.

It is prominently used for tracing copyright infringements and or banknote authentication. Like traditional physical watermarks, digital watermarks are often only perceptible under certain conditions, i.e. after using some algorithm. If a digital watermark distorts the carrier signal in a way that it becomes easily perceivable, it may be considered less effective depending on its purpose. Traditional watermarks may be applied to visible media (like images or video), whereas in digital watermarking, the signal may be audio, pictures, video, texts or 3D models. A signal may carry several different watermarks at the same time. Unlike metadata that is added to the carrier signal, a digital watermark does not change the size of the carrier signal.

IV.3 Embedded Method

An embedded system is a computer system with a dedicated function within a larger mechanical or electrical system, often with real-time computing constraints. It is embedded as part of a complete device often including hardware and mechanical parts. Embedded systems control many devices in common use today. When compared with general-purpose counterparts are low power consumption, small size, rugged operating ranges, and low per-unit cost. This comes at the price of limited processing resources, which make them significantly more difficult to program and to interact with. However, by building intelligence mechanisms on top of the hardware, taking advantage of possible existing sensors and the existence of a network of embedded units, one can both optimally manage available resources at the unit and network levels as well as provide augmented functions, well beyond those available. For example, intelligent techniques can be designed to manage power consumption of embedded systems.

The above discussed methods do not considered the image quality and image characteristics. The good method should must consider the image quality and attributes into consideration. Again, the security is the main concerned for the data to get hide inside the cover image which doesn't get focused into the above discussed approaches. In the sensitive areas like medical, military, research labs, it is important to recover the cover image without any loss of bits of cover image as well as the secret data. Our proposed system focuses mainly on these three points to provide security as well as to reconstruct the original image. The proposed system uses a powerful Burrows-Wheeler Transform (BWT) algorithm which provides higher security to data before embedding into the cover image. The BWT is the algorithm which is uses to encrypt the normal message to convert it into the cipher text so that the intruder even if finds the way to extract the data from the image, still he will fails to get the original message. Transforming the data before embedding will give you the much security than above discussed methods and even reconstruction of cover images are useful in the sensitive domains. At the decoder side, the hash function has been used instead of SVM classifier which distinguishes in between original image and the encrypted image. The key modulation concept will make the use of only the public key to encode and decode the data instead of private and public key mechanism which again reduces the computational complexities of the system.

V. Conclusion

In survey report of the work on Secure Reversible Image Data Hiding over Encrypted Domain via Key Modulation and related work should be taken in study and various result should be came after study and summarized as below. In [1] design a secure reversible image data hiding (RIDH) scheme operated over the encrypted domain. We suggest a public key modulation mechanism, which allows us to embed the data via simple XOR operations, without the need of accessing the secret encryption key. In [3] Compared with the special MATLAB functions, the visual quality of the contrast-enhanced images generated by our algorithm is better preserved. Moreover, the original image can be exactly recovered without any additional information. Hence the proposed algorithm has made the image contrast enhancement reversible. In [4] a reversible data hiding scheme for gray level images is proposed in this paper. It is based on a multi-level histogram shifting mechanism. The histogram is constructed by block differences with the reference of their integer medians. In order to preserve the block medians, the image blocks are divided into four categories with different embedding strategies used. In decoder, these medians are retrieved first, and accordingly the secret data is extracted and the host image is accurately reconstructed easily.

References

[1] Zhou, Jiantao, Weiwei Sun, Li Dong, Xianming Liu, Oscar C. Au, and Yuan Yan Tang. “Secure reversible image data hiding over encrypted domain via key modulation” IEEE Transactions on Circuits and Systems for Video Technology 26, no. 3 (2016): 441-452.

[2] Tian, Jun. "Reversible data embedding using a difference expansion." *IEEE transactions on circuits and systems for video technology* 13, no. 8 (2003): 890-896.

[3] Wu, Hao-Tian, Jean-Luc Dugelay, and Yun-Qing Shi. "Reversible image data hiding with contrast enhancement." *IEEE signal processing letters* 22, no. 1 (2015): 81-85.

[4] Luo, Hao, Fa-Xin Yu, Hua Chen, Zheng-Liang Huang, Hui Li, and Ping-Hui Wang. "Reversible data hiding based on block median preservation." *Information sciences* 181, no. 2 (2011): 308-328.

[5] Gao, Guangyong, and Yun-Qing Shi. "Reversible data hiding using controlled contrast enhancement and integer wavelet transform." *IEEE Signal Processing Letters* 22, no. 11 (2015): 2078-2082.

[6] Jung, Seung-Won, and Sung-Jea Ko. "A new histogram modification based reversible data hiding algorithm considering the human visual system." *IEEE Signal Processing Letters* 18, no. 2 (2011): 95-98.

[7] Z. Zhao,H.Luo,Z.-M. Lu, and J.-S. Pan, “Reversible data hiding basedon 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, “Adaptive 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 for HE based contrast enhancement techniques,” Adv. Intell. Syst. Applicat., vol. 2, pp. 331–338, 2013.

[15] C.C. Lin, W.L. Tai, C.C. Chang, Multilevel reversible data hiding based on histogram modification of difference images, Pattern Recognition 41 (12) (2008) 3582–3591.