International Journal of Current Trends in Engineering & Technology
www.ijctet.org, ISSN: 2395-3152
Volume: 06, Issue: 03 (May-June, 2020)

A Survey on Enhanced of Image Authentication Based on Reversible Image Data Hiding Techniques

Chandra Gupta, Dr. Rajeev Gupta
Department of Computer Science and Engineering
SISTEC, RGPV Bhopal, India

Abstract— *Reversible data hiding can be defined as an approach where the data is hidden in the host media such as image, audio, and video files. Reversible Data Hiding (RDH) or lossless data hiding is a method by which the original cover can be lossless restored after the embedded information is extracted. Hiding information destroys the host image even though the distortion introduced by hiding is imperceptible to the human visual system. Reversible data hiding techniques are designed to solve the problem of lossless embedding of large messages in digital images so that after the embedded message is extracted, the image can be restored completely to its original state before embedding occurred. To protect this data from unauthorized access and tampering various methods for data hiding like cryptography, hashing, authentication have been developed and are in practice today. In this paper, they will be discussing one such data hiding technique called Steganography. Steganography is the process of concealing sensitive information in any media to transfer it securely over the underlying unreliable and unsecured communication network. Our paper presents a survey on various data hiding techniques in steganography that are in practice today along with the comparative analysis of these techniques.*

KEYWORDS:- Reversible Data Hiding, Image Encryption, Image Decryption, Data Hiding, Image Recovery, Image Protection, Block Histogram Shifting, Image Recovery, Error Rate, PSNR.

I. Introduction

Today, in the digital era, any sort of data such as images, text, audio, can be digitized and stored indefinitely and can be transmitted at high speeds. Therefore there is a need to hide secret identification inside certain types of digital data. This information can be used to identify attempts to tamper with sensitive data, to embed annotations, and to prove copyright ownership. Storing, hiding, or embedding secret information in all types of digital data is one of the tasks of the field of steganography. Secret data can be embedded in various types of cover. If the data are embedded in an image (cover image), the result is a stego-image (or stegoimage) object. The data can also be embedded in a text file, audio, video, etc. Embedding data in a cover is a technological challenge. The size of the embedded data should not increase the size of cover as it becomes noticeable to an attacker who is familiar with the original cover [1]. Therefore secret data should be embedded in "holes" in the cover (places where the cover data have redundancies). Data hiding is the art and science of communicating secret data in an appropriate multimedia carrier, e.g., image, audio, and video files. Digital Steganography and watermarking are the two kinds of data hiding. Reversible data hiding can be defined as an approach where the data is hidden in the host media that may be a cover image. A reversible data hiding is an algorithm, which can recover the original image losslessly after the data have been extracted. Reversible data embedding, which is also called lossless data embedding, embeds invisible data (which is called a payload) into a digital image in a reversible fashion. As a basic requirement, the quality degradation on the image after data embedding should below. An intriguing feature of reversible data embedding is the reversibility, that is, one can remove the embedded data to restore the original image [2].

Reversible Data Hiding Technique

Data hiding is a term encompassing a wide range of applications for embedding messages in the content. Usually, hiding information destroys the host image even though the distortion introduced by hiding is imperceptible to the human visual system. However, there are some sensitive images for which any embedding distortion of the image is intolerable, such as medical images, military images, or artwork preservation. For images like in the medical field, even slight changes are unacceptable because of the potential risk of a physician misinterpreting the image. In other applications, such as remote sensing it is also desired that the original cover media can be recovered because of the required high-precision nature. In these cases, a special kind of data hiding method called reversible data hiding or lossless data hiding is used. Reversible data hiding (RDH) techniques are designed to solve the problem of lossless embedding of large messages in digital images so that after the embedded message is extracted, the image can be restored completely to its original state before embedding occurred. Steps of RDH, data embedding, data extraction, and the data embedding process will usually introduce permanent loss to the cover medium. However in some applications such as military, medical, and law forensics where degradation of cover is not allowed [3]. In these cases, a special kind of data hiding method called reversible data hiding or lossless data hiding is used. Reversible Data Hiding (RDH) in digital images is a technique that embeds data in digital images by altering the pixel values of image for secret communication and the cover image can be recovered to its original form after the extraction of the secret data from it. The block diagram of RDH is shown in Fig.1. Watermarking & Reversible Steganography can restore the original carrier without any or with ignorable distortion after the extraction of hidden data. Thus reversible data hiding method is now getting popular. In this paper, some important reversible data hiding techniques for digital images are explained and the results are analyzed [4, 5].

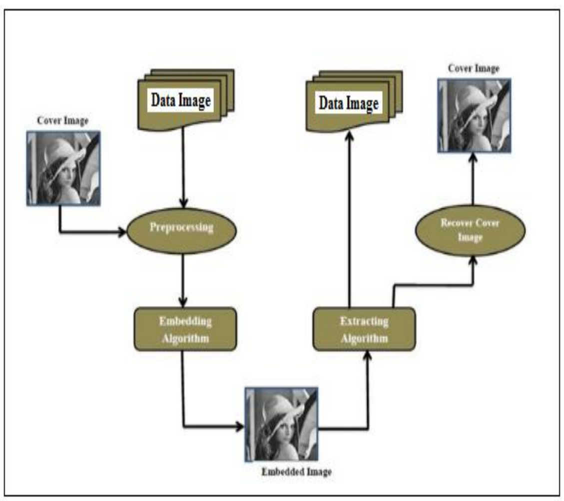

Figure 1 General Block diagram of Reversible Data Hiding

II. Related Work

Ni et al. [6] proposed a reversible data hiding method; their method uses the histogram of an original image to embed secret messages. In the histogram, they found multiple pairs of peak and zero points, where a peak point corresponds to the pixel value with a maximum number of pixels in the cover image assume and a zero point corresponds to the pixel value with no pixel in the cover image assumes. It uses a pair of peak and zero points to embed the secret messages.

Naseem et al. [7] presented an Optimized Bit Plane Splicing algorithm to hide the data in the images. This method incorporates a different approach than the traditional bit plane splicing technique. In this approach instead of just hiding the data pixel by pixel and plane by plane, the procedure involves hiding the data based on the intensity of the pixels. The intensity of the pixels in categorized into different ranges and depending on the intensity of the pixel, the number of bits is chosen that will be used to hide data in that particular plane. Also, the bits are hidden randomly in the plane instead of hiding them adjacent to each other and the planes are transmitted sporadically thus making it difficult to guess and intercept the transmitted data.

Zhaoxia Yin et al. [8] since there is good potential for practical applications such as encrypted image authentication, content owner identification, and privacy protection, reversible data hiding in the encrypted image (RDHEI) has attracted increasing attention in recent years. In this paper, we propose and evaluate a new separable RDHEI framework. Additional data can be embedded into a cipher image previously encrypted using Josephus traversal and a stream cipher. A block histogram shifting (BHS) approach using self-hidden peak pixels is adopted to perform reversible data embedding. Depending on the keys held, legal receivers can extract only the embedded data with the data hiding key, or, they can decrypt an image very similar to the original with the decryption key. They can extract both the embedded data and recover the original image error-free if both keys are available. The results demonstrate that higher embedding payload, the better quality of the decrypted-marked image, and error-free image recovery are achieved.

Kuo et al. [9] presented a reversible technique that is based on the block division to conceal the data in the image. In this approach, the cover image is divided into several equal blocks and then the histogram is generated for each of these blocks. Maximum and minimum points are computed for these histograms so that the embedding space can be generated to hide the data at the same time increasing the embedding capacity of the image. A one-bit change is used to record the change of the minimum points.

P. H. Pawar et al. [10] use the histogram-based RDH method. In this approach, the cover image is divided into several equal blocks/tiles and then the histogram is generated for each of these blocks. Maximum and minimum points are computed for these histograms so that the embedding space can be generated to hide the data at the same time increasing the embedding capacity of the image. A one-bit change is used to record the change of the minimum points. This improves the level of hiding places. This technique of block division successfully enhances the data hiding capacity because the total data that can be hidden in multiple blocks is generally larger than that can be hidden in a single cover image.

Dey et al. [11] have proposed a novel approach to hide data in stego-images which is an improvement over the Fibonacci decomposition method. In this method, the authors have exploited Prime Numbers to hide data in the images. The main agenda is to increase the number of bit planes of the image so that not only the LSB planes but even the higher bit planes can be used to hide to data. This is done by converting the original bit planes to some other binary number system using prime numbers as the weighted function so that the number of bits to represent each pixel increases which in turn can be used hide data in higher bit planes. The authors have also performed a comparison of the Fibonacci decomposition method with the traditional LSB data hiding technique showing that the former outperforms the latter method and comparing the Fibonacci Decomposition method with the proposed method which outclasses the former method. Also, the proposed method generates the stego-image which is virtually indistinguishable from the original image

Rajkumar et al. [12] Lossless data hiding is the technique of embedding data in an image and retrieval of the data with the lossless reconstruction of the original image. In this paper, we present a novel lossless data hiding scheme based on histogram modification. This technique is based on differences of adjacent pixels for embedding data and has more hiding capacity compared to existing methods. The number of message bits that can be embedded into an image equals the number of pixels associated with the peak point. Here, a histogram shifting. proposes the differences between adjacent pixels instead of the simple pixel value is considered, since image neighbor pixels are strongly correlated the difference is expected to be very close to zero, at the sending side, the image is scanned in an inverse s-order as shown in figure 2 and then calculate the pixel difference between pixels and peak points of the histogram are determined

Wen-Chung et al. [13] the authors have proposed a method that segments the image into blocks of equal sizes. Also, the process involved in this method is reversible hence there is no loss of hidden data. The approach followed in this scheme to conceal data is quite different. In this technique, the histograms of the blocks of images are taken and they are shifted to the minimum point of the histogram and then the data is hidden between these points. The improvement of this technique is that it provides a higher capacity to hide data than the previous method.

Jigsaw-based approach [14] is used to transfer data over the communication channel securely. In this scheme, the data is fragmented in the block of variable sizes and a message authentication code (MAC) is used to authenticate every piece of data. Also, every message is prefixed and suffixed with a binary 1 along with XOR-ing the data with the randomly generated one-time pad. By fragmenting the data the attacker is unable to make sense of the data at the same time he cannot access the data unless he possesses the authentication code for the data.

Soo-Chang et al. [15].A low computational complexity noise-balanced error diffusion (NBEDF) technique is proposed for embedding watermark into error-diffused images. The visual decoding pattern can be perceived when two or more similar NBEDF images are overlaid each other, even in a high activity region. Furthermore, with the modified improved version of NBEDF, the two halftone images can be made from two different gray-tone images and still provide a clear and sharp visual decoding pattern. With the self-decoding techniques, we can also decode the pattern by only one NBEDF image. However, the NBEDF method is not so robust to the damage due to printing or other distortions. Thus, a kernels-alternated error diffusion (KAEDF) technique is proposed. We find that the two well-known kernels proposed by Jarvis et al. and Stucki are very compatible by alternately using them in the halftone process. In the decoder, because the spectral distribution of Jarvis and Stucki kernels are different in the 2-D fast Fourier transform domain, we use the cumulative squared Euclidean distance criterion to determine each cell in a watermarked halftone image either belonging to Jarvis or Stucki, and then decode the watermark. Furthermore, because the detailed textures of Jarvis and Stucki patterns are somewhat different in the spatial domain; the lookup table (LUT) technique is also used for fast decoding. From the simulation results, the correct decoding rates using both techniques are high and extremely robust, even after printing and scanning processes. Finally, we extend the hybrid NBEDF and KAEDF algorithms to two color EDF halftone images, where eight independent KAEDF watermarks and 16 NBEDF.

III. CONCLUSION

Reversible data hiding in the encrypted image is getting more attention these days because of security maintaining requirements. Reversible data hiding techniques getting popular because of the reversibility of the carrier medium in the receiving end after extraction of secret data. In these paper different types of reversible data hiding techniques for digital images least significant Bit substitution (LSB), HSBT, Difference expansion, Histogram modification each are studied, analyzed, and compared. The survey results show each technique has its advantage and disadvantages and the focus of all methods is on a high payload with less degradation of data. The performance can be evaluated by determining the visual quality of the image and by determining the PSNR of an algorithm. Data hiding in encrypted images provide more security for the data as cryptography and steganography are performed. By combining lossless and reversible data hiding techniques, more efficient data embedding can be done in encrypted images. The concept of data hiding and their applications in the security of digital data communication across the network is studied in this paper and a technical survey of recent methods in reversible data hiding is presented.

REFERENCES

[1]. Zhang, Xinpeng. "Reversible data hiding in encrypted image." IEEE signal processing letters 18, no. 4: 255-258, 2011.

[2]. Liao, X., & Shu, C., "Reversible data hiding in encrypted images based on the absolute mean difference of multiple neighboring pixels". Journal of Visual Communication and Image Representation, 28, 21-27, 2015.

[3]. Ni, Zhicheng, Yun-Qing Shi, Nirwan Ansari, and Wei Su. "Reversible data hiding." IEEE Transactions on circuits and systems for video technology 16, no. 3: 354-362, 2006.

[4]. Awrangjeb, Mohammad. "An overview of reversible data hiding." In Proceedings of the Sixth International Conference on Computer and Information Technology, pp. 75-79. 2003.

[5]. Varsaki, Eleni, Vassilis Fotopoulos, and A. N. Skodras. "A reversible data hiding technique embedding in the image histogram." Hellenic Open University Journal of Informatics 1, no. 2, 2006.

[6]. Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Transactions on Circuits Systems and Video Technology, Vol. 16, No.3, 2006, pp. 354–362.

[7]. M. Naseem, Ibrahim M. Hussain, M. Kamran Khan, Aisha Ajmal, "An Optimum Modified Bit Plane Splicing LSB Algorithm for Secret Data Hiding", International Journal of Computer Applications, Vol. 29, No. 12, 2011. Foundation of Computer Science, New York, USA, pp. 36-43.

[8]. Zhaoxia Yin, Andrew Abel, Xinpeng Zhang, Bin Luo, "Reversible Data Hiding In Encrypted Image Based On Block Histogram Shifting" IEEE, 2016.

[9]. Wen-Chung Kuo, Dong-Jin Jiang, Yu-Chih Huang, "A Reversible Data Hiding Scheme Based on Block Division", Congress on Image and Signal Processing, Vol. 1, 27-30 May, pp. 365-369, 2008.

[10]. P. H. Pawar and K. C. Jondhale "Histogram Based Reversible Data Hiding Using Block Division" International Conference on Advanced Communication Control and Computing Technologies ICACCCT, 2012, pp-295-299.

[11]. Sandipan Dey, Ajith Abraham, Sugata Sanyal, "An LSB Data Hiding Technique Using Prime Numbers", IEEE Third International Symposium on Information Assurance and Security, Manchester, United Kingdom, IEEE Computer Society Press, USA, 29-31 Aug. 2007, pp.101-106.

[12]. Rajkumar Rama Swamy and Vasuki Arumugam "Lossless Data hiding Based on Histogram Modification " The International Arab Journal of Information Technology, Vol 9, No. 5, Sept 2012, pp-445-451.

[13]. Wen-Chung Kuo, Dong-Jin Jiang, Yu-Chih Huang, "A Reversible Data Hiding Scheme Based on Block Division", Congress on Image and Signal Processing, Vol. 1, 27-30 May 2008, pp. 365-369

[14]. Rangarajan A. Vasudevan, Sugata Sanyal, Ajith Abraham, Dharma P. Agrawal, "Jigsaw-based secure data transfer over computer networks", Proceedings of International Conference on Information Technology: Coding and Computing, Las Vegas, Nevada, Vol. 1, 5-7 April 2004, pp. 2- 6.

[15]. Pei, Soo-Chang, and Jing-Ming Guo. "Hybrid pixel-based data hiding and block-based watermarking for error-diffused halftone images." IEEE transactions on circuits and systems for video technology 13, no. 8: 867-884, 2003.