© 2017 IJSRSET | Volume 3 | Issue 7 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section:Engineering and Technology
National Level Technical Conference on Advanced Computing Technologies- n'CACT'17, Department of Computer Science & Engineering,
Ammini College of Engineering, Kannampariyaram, Mankara, Palakkad, Kerala, India
In association with
International Journal of Scientific Research in Science and Technology

Recent Review of Reversible Data Hiding in Steganography

Rasmi. A*1, Dr. Mohanapriya M2

*1Research Scholar, Department of Computer Science and Engineering, Karpagam University ,Karpagam Academy of Higher Education Tamilnadu, India

2Associate Professor, Department of Computer Science and Engineering & IT, Coimbatore Institute of Technology, Coimbatore, Tamilnadu, India

ABSTRACT

In the electronic era because of the wide spread usage of network technology, security measures play, a vital role for data transmission between sender and receiver. Steganography is the science of masking data bits in a secure manner using cover file,for various purposes. This paper explores and analyses some of the existing steganographic reversible data hiding methods from its earliest instances through potential future application.

Keywords: Steganography, Reversible data hiding, Spatial domain, Embedding capacity ,data hiding, stego,cover image

I. INTRODUCTION

Steganography is an art and science of concealed communication in a statistically unnoticeable way. It was first used and experienced by Greek people for exchanging secret data between sender and receiver for various purposes. In this type of data hiding the sender hides the secret information to be sent into the digital file where only the intended user can recover it .The word steganography is originated from the greek words “steganos ” and “graphia” means covered writing. Different application areas of steganography are :confidential communication and secret information storing, protection of data alteration ,transport highly private records between International Governments, and terrorists can use this to keep their communication secret and coordinate attack .[1,2,3]. It can be used in military for secret communication purpose. Various data hiding methods are watermarking, steganography and cryptography. The features of the embedding techniques can be defined by features like capacity, robustness and imperceptibility. The vital requirement for steganography is its undetectability and robustness. The main elements of a steganographic system are cover image, embedding algorithm, message, extraction algorithm and stego image .A general form of steganography is shown in figure .1.

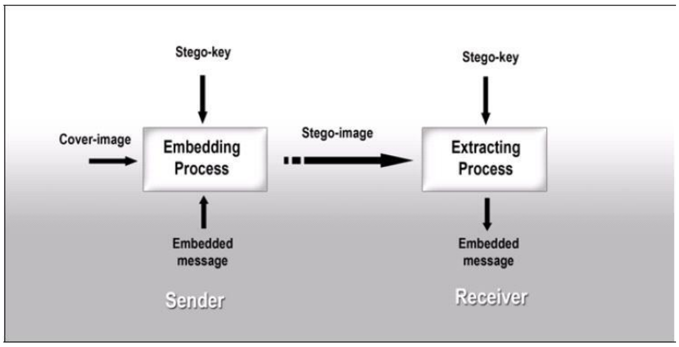


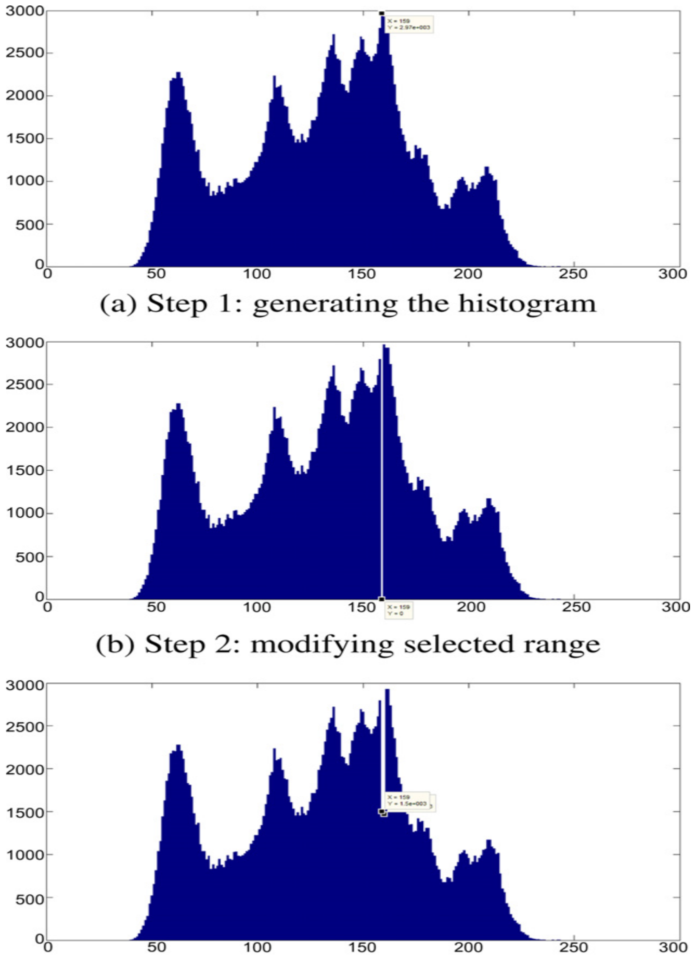
Figure (1) a general form of steganography

Cover file may be image, text, video or audio, which is used as a carrier in the data transfer. The secret data that the sender wants to be sent, is the information, it may be in different format as the carrier file. The secret information is also termed as payload [4,5].The insertion of payload into cover file gives, the resultant stego image. Steganographic techniques can be classified into two types and it named as spatial domain and transform domain, if manipulations are done at the pixel intensity based values, then it comes under spatial domain, while if it is based on the coefficient of pixel value it falls under frequency domain techniques. In spatial domain secret data is embedded directly whereas in transform embedding is in indirect way. Based on the nature of cover file used steganography can be termed as image steganography, text steganography, audio steganography, video steganography and network steganography.[6,7]

II. REVIEW OF LITERATURE

Information hiding can be graded into reversible or lossless data hiding and irreversible data hiding schemes. Most of the commonly used data embedding methods are not reversible based techniques .Reversible data hiding helps to retrieve the exact input data at the extraction phase without altering the content. Reversible data hiding is also known as lossless data hiding because it restores the cover content perfectly .It provides a perfect balance between the image quality and the payload. The major challenges in data embedding are associated with how efficiently inserting can be implemented in a cover file ,without affecting the visual properties .So before hiding data certain parameters has to be checked such as the size of secret data should never exceed the size of cover file ,if it is exceeding it can be easily detectable by the intruder. Embedding capacity means the number of bits can be embedded in a cover file without altering the structure of it .The quality of the stego image can be evaluated by using the peak signal to noise ratio (PSNR) which denotes the maximum power of a signal and the power of the corrupting noise. It is expressed in the logarithmic unit dB. The regular singular scheme first segments an image into non overlapping parts, then divide the parts into 3 sections named as regular(R),singular(S),and unusable(U),and by using some operations we can convert R to S and S to R ,and can insert the secret data into it but U remains as it is, without any change.[8,9,10]

Different types of existing reversible data hiding methods are regular singular scheme, the integer wavelet transform based method, histogram modification scheme and difference expansion scheme. In difference expansion technique the image is divided into pair of pixels, after that inserts one bit of data into each pair. Integer wavelet transform uses the least significant bit technique for high frequency integer wavelet coefficient by selecting a proper threshold value. Histogram based method gives the complete tonal representation of the image, which employs the redundancy information of the cover image to hide the secret message. It mainly depends upon peak value and zero point, then after selecting the peak point ,we are simply incrementing or decrementing 1 in all pixel values which are lesser or greater than peak point value. It prevents the overflow and underflow by applying the modulo addition. In this one it takes the minimum or zero point values of histogram then varying it slightly to insert the information bits .Figure (2) shows histogram modification of Lena image. In this the number of bits can be inserted into an image depends on the peak value of the histogram shifting. The most commonly used image formats are internet are Graphics interchange format (GIF) and Joint photographic experts group (JPEG), because of its better hiding power. Security of data embedding could be improved by using certain factors like proper selection of cover image, reducing the payload distortion and improving the message embedding capacity.



(a) Step 1: generating the histogram

(b) Step 2: modifying selected range

(c) Step 3: embedding hidden data

Figure (2) shows histogram modification technique

Reversible data hiding employs techniques like compression decompression, encryption decryption ,and information embedding and extraction. In prediction based steganography embedding can be done by the technique of predictive coding approach .In this pixel intensity values are predicted using predictor , and prediction error values (EV) are changed to insert secret message.[11,12,13]

III. CONCLUSION

This paper reviews image steganography and reversible data hiding in an effective way and discussing different parameters to increase the performance of the data embedding techniques. It applies different compression and encoding mechanisms to improve the visual quality and efficiency of the reversible data hiding methods.

IV. REFERENCES

[1] Z. Zhao, H. Luo, Z.-M. Lu, J.-S. Pan, Reversible data hiding based on multilevel histogram modification and sequential recovery, Int. J. Electron. Commun. 65 (2011) 814–826.B.

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

[3] B. Cong, N. Sang, M. Yoon, H.-K. Lee, Multi bit plane image steganography, in: International Workshop on Digitalforensics and Watermarking, vol. 4283 of Lecture Notes in Computer Science, pp. 61–70.

[4] E. Kawaguchi, R.O. Eason, Principle and applications of BPCS steganography, in: Proc. of Multi-media Systems and Applications, in: SPIE, vol. 3528, 1998, pp. 464–473.

[5] V.M. Potdar, E. Chang, Gray level modification steganography for secret communication, in: Proc. of 2nd IEEE International Conference on Industrial Informatics, pp. 223–228.

[6] D Tseng, Y.C. , Chen Y.Y. Pan H.K.:'A secure data hiding scheme for binary images', IEEE Trans. Commun., 2002, 50,pp. 1227-1231 .

[7] Pawan R Sharma, Jitendra Mishra“ A Comprehensive Survey on Data Hiding Technique” IRJET e-ISSN: 2395 -0056 Volume: 02 Issue: 04 July-2015.

[8] Gurpreet Kaur, Kamaljeet Kaur “Digital Watermarking and Other Data Hiding Techniques” IJITEE ISSN: 2278-3075, Volume-2, Issue-5, April 2013 ,181.

[9] Provos, N. &Honeyman, P., “Hide and Seek: An introduction to steganography”, IEEE Security and Privacy Journal, 2003.

[10] Y.K. Lee, L.H. Chen, “High capacity image steganographic model”, IEEE Proceedings on Vision, Image and Signal processing, Vol. 147, No.3,pp. 288-294, 2000.

[11] X. Liao, Q. Wen and J. Zhang, ”A steganographic method for digital images with four-pixel differencing and modified LSB substitution”, Journal of Visual Communication and Image Representation, vol 22, no 1, pp. 18, 2011 .

[12] A. Rashid and M. K. R. Rashid, “Stego-Scheme for Secret Communication in Grayscale and Color Images”, British Journal of Mathematics and Computer Sciences, vol. 10, no, 1 (2015), pp. 1-9.

[13] Sandeep Kaur ,Arunjot Kaur &Kulwinder Singh” A Survey of Image Steganography” IJRECE, Volume 2-Issue 3 June 2014, e-ISSN 2321-3159 p-ISSN 2321-3159.