An Efficient Higher LSB Method for Hiding Encrypted Data into Guard Pixels Region of a Multicarrier Image Objects

Komal B. Bijwe, G. R. Bamnote

Department Of Computer Science & Engineering, PRMIT, Badnera, Amravati, Maharashtra, India

Abstract: ***Digital communication has become an essential part of infrastructure nowadays, a lot of applications are Internet-based and it is important that communication be made secret. As a result, the security of information passed over an open channel has become a fundamental issue and therefore, the confidentiality and data integrity are required to protect against unauthorized access and use. This has resulted in an unstable growth in the field of information hiding. Stegnography is a popular method to provide security. Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio and video files. It comes under the assumption that if the feature is visible, the point of attack is evident, thus the goal here is always to conceal the very existence of the embedded data. For hiding secret data in digital media, large varieties of steganographic techniques are available, some are more complex than others, and all of them have their respective pros and cons. This paper intends to give thorough understanding and evolution of different existing digital media steganography techniques of data hiding. It covers and integrates recent research work.***

Keywords: Steganography, *PVD,* LSB, DCT, Cover Image, Stego Image, Huffman Encoding

1. Introduction

Digital data embedding in digital media is an information technology field of rapidly growing commercial, as well as national security of interest. The transmission of digital multimedia products via internet is getting more and more popular. Because the digital medium can be conveniently transmitted and lossless copied, they also lead to an increase of digital piracy. To solve this problem different data hiding techniques are used [1] [2] [3] [4]. Covert communication or steganography, which literally means "covered writing" in Greek, is the process of hiding data under a cover medium (also referred to as host), such as image, video, or audio, to establish secret communication between trusting parties and conceal the existence of embedded data [5][6][7][8][9].i.e. The main objective of data hiding is to communicate securely in such a way that the true message which is embedded in any one of the digital media is not visible to the observer. That is unwanted parties should not be able to distinguish in any sense between cover-image (image not containing any secret message) and stego-image (modified cover-image that contains secret message). Thus the stego image should not deviate much from the original cover image. Different data hiding techniques can be evaluated on following four basic attributes of data hiding [10]: (i) payload - information delivery rate; (ii) robustness - hidden data resistance to noise/disturbance; (iii) transparency - low host distortion for concealment purposes; and (iv) security - inability by unauthorized users to detect/access the communication channel.

Recently, developing data hiding technologies, particularly in the form of steganography, are seen to pose a threat to personal privacy, commercial and national security interests [11]. The countermeasure technology to steganography security is frequently referred to as steganalysis, which can be classified into two categories: Passive and active. The primary task of passive steganalysis is to decide the presence or absence of hidden data in given media objects (binary hypothesis testing problem). Active steganalysis (also known as forensics steganalysis) refers to the effort by unintended recipients to extract/remove/modify the actual hidden data. In this context, active steganalysis is unlike attacks to watermarking security. In this work, we focus our attention on active spread-spectrum (SS) steganalysis and, in particular, we aim at recovering blindly secret data hidden in medium hosts via (multi-carrier/signature) direct-sequence SS embedding [12]-[19]. Neither the original host nor the embedding signatures (carriers or spreading sequences) are known (fully blind SS steganalysis).While passive steganalysis is being intensively investigated in the past few years, active steganalysis is a relatively new branch of research seeking methods that can blindly extract secret data. In blind active SS steganalysis the unknown host acts as a source of interference/ disturbance to the data to be extracted.

2. Literature Survey

Tung-Hsiang Liu and *Long-Wen Chang* [20] has proposed a simple data hiding technique for binary images in *2004*.The proposed method embeds secure data at the edge portion of host binary image. The Distance matrix mechanism is used to find the edge pixels of host binary image. Then the Weight mechanism is used to consider the connectivity of the neighborhood around changeable pixels for choosing the most suitable one. For the security and quality consideration, a random number generator is used to distribute the embedding data into the overall image. This method not only embeds large amounts of data into host binary image but also can maintain image quality.

In order to improve the capacity of the hidden secret data and to provide am imperceptible stego image quality *H.-C. Wu, N.-I. Wu, C.-S. Tsai* and *M.-S. Hwang* [21] has proposed a novel stenographic method based on Least Significant Bit (LSB) Replacement and Pixel Value Differencing (PVD) methods in *2005*.Pixel Value Differencing (PVD) method is

used to discriminate between edge areas and smooth areas of cover image. The secret data is hidden into the smooth areas of cover image by LSB method while using the PVD method in the edge areas. As, the proposed method not only store data in the edge areas but also in the smooth areas; therefore it can hide much larger information and maintains a good visual quality of stego image.

In *2005 M. Carli M.C.Q. Fariasy, E. Drelie Gelascaz, R. Tedesco & A. Neri* [22] has proposed a no-reference video quality metric that blindly estimates the quality of a video. They had used Block based Spread Spectrum embedding method to insert a fragile mark into perceptually important areas of the video frames. They used a set of perceptual features to characterize the perceptual importance of a region that are Motion, Contrast and Color. The mark is extracted from the perceptually important areas of the decoded video on receiver side. Then a quality measure of the video is obtained by computing the degradation of the extracted mark. So, in this way quality of a compressed video is estimated by using simple embedding system on perceptually important areas of the video frame.

In *2007 Hsien-Wen Tseng, Feng-Rong Wu*, and *Chi-Pin Hsieh* [23] has proposed a novel method for hiding data in binary images. A Weight mechanism is used to select the most suitable pixel for flipping. Additionally boundary check is performed to improve the visual quality of stego image as well as to prevent boundary distortion. This method achieved a good visual quality for watermarked image and has high capacity of embedding.

In *2008 Beenish Mehboob* and *Rashid Aziz Faruqui* [24]discussedthe art and science of Steganography in general and proposed a novel technique to hide data in a colorful image using least significant bit. Least Significant Bit or its variants are used to hide data in digital image. This technique chops the data in 8 bits after the header and used LSB to hide data. So, they proved LSB method is the most recommended for hiding data than other techniques which require masking and filtering.

M.B. Ould Medeniand & El Mamoun Souidi [25] has proposed a novel stenographic method for gray level images on four pixel differencing and LSB substitution in *2010*.They used K-bit LSB substitution method for hiding the secret data into each pixel where K is decided by the number of one in the most part of pixel. This method gave best values for the PSNR measure which means that there were no big difference between the original and the stegno image.

In *2012 Tasnuva Mahjabin,Syed Monowar Hossain* and *Md. Shariful Haque* [26] has proposed a data hiding method based on PVD and LSB substitution to improve the capacity of the secret data as well as to make stegnalysis a complicated task they made an effort to implement a robust dynamic method of data hiding. An efficient and dynamic embedding algorithm was proposed here that not only hides secret data with an imperceptible visual quality and increased capacity but also make secret code breaking a good annoyance for the attacker. This method achieved an increased embedding capacity and lower image degradation with improved security as compared to LSB substitution method and some other existing methods of data hiding.

Ankit Chaudhary and *JaJdeep Vasavada* [27] has proposed an improved stenography approach for hiding text messages in RGB lossless images in *2012*.The securitylevel is increased by randomly distributing the textmessage over the entire image instead of clusteringwithin specific image portions. They increased storage capacity byutilizing all the color channels for storinginformation and providing the source text messagecompression. The degradation of the images can beminimized by changing only one lease significant bitper color channel for hiding the message, incurring avery little change in the original image. So, this method increased the security level and improved the storage capacity while incurring minimal quality degradation.

Kousik Dasgupta & J.K. MandalandParamartha Dutta [28] have proposed a secured has based LSB technique for video stenography in *2012*.This technique utilizes cover video files in spatial domain to conceal the presence of sensitive data regardless of its format. After comparing the proposed technique with LSB technique it is found that the performance analysis of proposed technique is quite encouraging. The advantage of this method is that the size of the message does not matter in video stenography as the message can be embedded in multiple frames.

In *2012 Poonam V Bodhak* and *Baisa L Gunjal* [29] has proposed a method to hide data containing text in computer video file and to retrieve the hidden information. This can be designed by embedding the text file in a video file in such a way that the video does not lose its functionality using DCT & LSB Modification method. This method applies imperceptible modification. This proposed method strives for high security to an eavesdropper's inability to detect hidden information.

RigDas and *Themrichon Tuithung* [30] have proposed novel technique for image stenography based on Huffman Encoding in *2012*. Huffman Encoding is performed over the secret image/message before embedding and each bit of Huffman code of secret Image/message is embedded inside the cover image by altering the least significant bit (LSB) of each of the pixel's intensities of cover image. The size of the Huffman encoded bit stream and Huffman Table are also embedded inside the cover image, so that the Stego-Image becomes standalone information to the receiver.

In *2013 Ming Li,Michel K. Kulhandjian, Dimitris,A. Pados,,Stella N. Batalama,* and *Michael J. Medley* [31] has considered the problem of extracting blindly data embedded over a wide band in a spectrum (transform) domain of a digital medium (image, audio, video).We develop a novel multicarrier/signature iterative generalized least-squares (M-IGLS) core procedure to seek unknown data hidden in hosts via multicarrier spread-spectrum embedding. Neither the original host nor the embedding carriers are assumed available.

Table 1

S. No	Year	Author	Advantages
1	2004	Tung-Hsiang Liu Long-Wen Chang	Large amount of data can be stored in binary images as well as quality of an image is maintained.
2	2005	H.-C. Wu, N.-I. Wu, C.-S. Tsai M.-S. Hwang	Much larger information can be stored in images by using LSB method for storing data in smooth areas of image.
3	2005	M. Carli M.C.Q. Fariasy, E. Drelie Gelascaz, R. Tedesco, A.Neri	Quality of a compressed video is estimated by using simple embedding system.
4	2007	Hsien-Wen Tseng, Feng-Rong Wu,Chi-Pin Hsieh	This method achieved a good visual quality for watermarked image and has high capacity of embedding.
5	2008	Beenish Mehboob Rashid Aziz Faruqui	LSB method is used for hiding data in colorful images than other techniques which require masking and filtering.
6	2010	M.B. Ould Medeni El Mamoun Souidi	K-bit LSB substitution method used here gave best values for the PSNR measure.
7	2012	Tasnuva Mahjabin, Syed Monowar Hossain Md.Shariful Haque	PVD & LSB methods used here which achieved an increased embedding capacity and lower image degradation with improved security.
8	2012	Ankit Chaudhary JaJdeep Vasavada	1-bit LSB substitution method used which increased the security level and improved the storage capacity
9	2012	Kousik Dasgupta, J.K.MandalParamartha Dutta	It allows embedding the large size of data in multiple frames. Therefore size of the message does not matter.
10	2012	Poonam V Bodhak Baisa L Gunjal	DCT & LSB methods used which provide high security to embedded data.
11	2012	RigDas ThemrichonTuithung	Huffman Encoding is used for secret message which again improves the security level of hiding data.
12	2013	Ming Li, Michel K. Kulhandjian, Dimitris,A. Pados,,Stella N. Batalama, Michael J. Medley	M-IGLS procedure is used for extracting blindly data embedded over a wide band in a spectrum domain of a digital medium.

3. Proposed Methodology

Proposed Methodology has been divided in 2 Phases:

1) Data Hiding
2) Data Extraction

1) Data Hiding:

In this phase, we split the image in different parts. Then intensity of the image gets check to find whether it is closer to darkness or brightness. If it is closer then that image sample will be selected for hiding the data. For hiding the secrete data, firstly data is encrypted with shifting method and then segmented into equal parts. After that each data segment is hiding behind the specific sample of image. At last all the samples are concatenated which will give the stego image.

2) Data Extraction:

In this phase, whatever the data is hidden in first phase that is being extracted. Following steps will be performed:

i) First Split the image.
ii) Extract the data segment from image samples.
iii) Decrypt the data segments.
iv) Assemble the data obtain from data segment.

At last plain text will be obtain from the assembled data that is required secrete data.

4. Conclusion & Future Scope

Although only some of the main steganographic techniques were discussed in this paper, one can see that there exists a large selection of approaches to hiding information in digital media. All the major image file formats have different methods of hiding messages, with different strong and weak points respectively. Where one technique lacks in *payload capacity*, the other lacks in *robustness*. So, our future study and research includes developing the data hiding methods with high embedding capacity & robustness. This information might be useful for interested researchers to carry out further work in this research area.

References

[1] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding: A survey," *Proc. IEEE, Special Issue on Identification and Protection of Multimedia Information*, vol. 87, no. 7, pp. 1062–1078, Jul.1999.
[2] J. Cox, M. L. Miller, and J. A. Bloom, *Digital Watermarking*. San Francisco, CA, USA: Morgan-Kaufmann, 2002.
[3] F. Hartung and M. Kutter, "Multimedia watermarking techniques," *Proc. IEEE, Special Issue on Identification and Protection of Multimedia Information*, vol. 87, pp. 1079–1107, Jul. 1999.
[4] G. C.Langelaar, I. Setyawan, and R. L. Lagendijk, "Watermarking digital image and video data: A state-of-the-art overview," *IEEE Signal Process. Mag.*, vol. 17, no. 5, pp. 20–46, Sep. 2000.
[5] N. F. Johnson and S. Katzenbeisser, , S. Katzenbeisser and F. Petitcolas, Eds., "A survey of steganographic techniques," in *Information Hiding*. Norwood, MA, USA: Artech House, 2000, pp. 43–78.
[6] S. Wang and H. Wang, "Cyber warfare: Steganography vs. steganalysis," *Commun. ACM*, vol. 47, pp. 76–82, Oct. 2004.
[7] C. Cachin, "An information-theoretic model for steganography," in *Proc. 2nd Int. Workshop on Information Hiding*, Portland, OR, USA, Apr. 1998, pp. 306–318.
[8] G. J. Simmons, "The prisoner's problem and the subliminal channel," in *Advances in Cryptology: Proc. CRYPTO'83*, New York, NY, USA, 1984, pp. 51–67, Plenum.

[9] J. Fridrich, *Steganography in Digital Media, Principles, Algorithms, and Applications*. Cambridge, U.K.: Cambridge Univ. Press, 2010.
[10] Y. Wang and P. Moulin, "Perfectly secure steganography: Capacity, error exponents, and code constructions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2706–2722, Jun. 2008.
[11] Federal Plan for Cyber Security and Information Assurance Research and Development Interagency Working Group on Cyber Security and Information Assurance, Apr. 2006.
[12] H. S.Malvar and D. A. Florencio, "Improved spread spectrum: A new modulation technique for robust watermarking," *IEEE Trans. Signal Proc.*, vol. 51, no. 4, pp. 898–905, Apr. 2003.
[13] J. Cox, J. Kilian, F. T. Leighton, and T. Shannon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Process.*, vol. 6, no. 12, pp. 1673–1687, Dec. 1997.
[14] J. Hernandez, M. Amado, and F. Perez-Gonzalez, "DCT-domain watermarking techniques for still images: Detector performance analysis and a new structure," *IEEE Trans. Image Process.*, vol. 9, no. 1, pp.55–68, Jan. 2000.
[15] C. Qiang and T. S. Huang, "An additive approach to transform-domain information hiding and optimum detection structure," *IEEE Trans. Multimedia*, vol. 3, no. 3, pp. 273–284, Sep. 2001.
[16] C. Fei, D. Kundur, and R. H. Kwong, "Analysis and design of watermarking algorithms for improved resistance to compression," *IEEE Trans. Image Process.*, vol. 13, no. 2, pp. 126–144, Feb. 2004.
[17] M. Gkizeli, D. A. Pados, and M. J. Medley, "SINR, bit error rate,and Shannon capacity optimized spread-spectrum steganography," in *Proc. IEEE Int. Conf. Image Proce. (ICIP)*, Singapore, Oct. 2004, pp. 1561–1564.
[18] M. Gkizeli, D. A. Pados, S. N. Batalama, andM. J.Medley, "Blind iterativerecovery of spread-spectrum steganographic messages," in *Proc. IEEE Int. Conf. Image Proc. (ICIP)*, Genova, Italy, Sep. 2005, vol. 2,pp. 11–14.
[19] M. Gkizeli, D. A. Pados, and M. J. Medley, "Optimal signature design for spread-spectrum steganography," *IEEE Trans. Image Process.*, vol. 16, no. 2, pp. 391–405, Feb. 2007.
[20] Tung-Hsiang Liu and Long-Wen Chang, "An Adaptive Data Hiding Technique for Binary Images", *Proc.IEEE 17th Int.Conf. On Pattern Recognition (ICPR'04)* 2004.
[21] H.-C. Wu, N.-I. Wu, C.-S. Tsai and M.-S. Hwang," Image steganographic scheme based on pixel-value differencing and LSB replacement methods", *IEE Proc.-Vis. Image Signal Process.*, Vol. 152, No. 5, October 2005.
[22] M. Carli , M.C.Q. Fariasy, E. Drelie Gelascaz, R. Tedesco, A. Neri, "QUALITY ASSESSMENT USING DATA HIDING ON PERCEPTUALLY IMPORTANT" *IEEE* AREAS0-7803-9134-9/05/$20.00 ©2005.
[23] Hsien-Wen Tseng, Feng-Rong Wu,and Chi-Pin Hsieh," Data Hiding for Binary Images Using Weight Mechanism",*IEEE* 2007.
[24] Beenish Mehboob and Rashid Aziz Faruqui," A StegnographyImplementation", *IEEE* 2008 M.B. Ould MEDENI, El Mamoun SOUIDI," A Novel Steganographic Method for Gray-Level Images With four-pixel Differencing and LSB Substitution "*IEEE* 2010
[25] Tasnuva Mahjabin, Syed Monowar Hossain, Md. Shariful Haque," A Block Based Data Hiding Method in Images Using Pixel Value Differencing and LSB Substitution Method", *IEEE* 2012.
[26] Ankit Chaudhary, JaJdeep Vasavada,"A Hash Based Approach for Secure Keyless Image Steganography in Lossless RGBImages" , *IEEE* 2012.
[27] Kousik Dasgupta1, J.K. Mandal2 and Paramartha Dutta3," HASH BASED LEAST SIGNIFICANT BIT TECHNIQUE FOR VIDEO STEGANOGRAPHY (HLSB)", *International Journal of Security, Privacy and Trust Management (IJSPTM)*, Vol. 1, No 2, April 2012.
[28] Poonam V Bodhak, Baisa L Gunjal," Improved Protection In Video Steganography Using DCT & LSB", *International Journal of Engineering and Innovative Technology (IJEIT)* Volume 1, Issue 4, April 2012.
[29] RigDas, Themrichon Tuithung," A Novel Steganography Method for Image Based on Huffman Encoding", *IEEE* 2012.
[30] Ming Li, Michel K. Kulhandjian, Dimitris A. Pados, Stella N. Batalama, and Michael J. Medley," Extracting Spread-Spectrum Hidden Data From Digital Media", *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY,* VOL. 8, NO. 7, JULY 2013.

Author Profile

Ms. Komal B. Bijwe received B.E in Computer Science & Engineering from H.V.P.M College of Engineering & Technology, Amravati; in 2007 and pursuing M.E in Computer Science & Engineering From Prof. Ram Meghe Institute of Technology & Research, Bandera, Amravati.

Dr. G. R. Bamnote received PhD in Computer Science & Engineering in 2009. He is now working as a Head of Department (CSE) in Prof. Ram Meghe Institute of Technology & Research, Bandera, Amravati.