XV International Conference on Recent Trends in Engineering Science and Management
Osmania University Centre for International Program, Hyderabad (India) (ICRTESM-18)
20th October 2018 www.conferenceworld.in ISBN:978-93-87793-51-4

A steganographic technique for combining LSB substitution in color images

Annu Sharma[1] A.K. Chaturvedi[2], Kalpana Sharma[3]

[1] *Research Scholar, Computer Department , Bhagwant University, Ajmer, India*
[2] *MCA Deptt, Govt. Engineering College, Ajmer, India*
[3] *CSE Deptt., Bhagwant Univ., Ajmer, India*

Abstract

Information Security is a major concern in today's modern era. Almost all the communicating bodies want the security, confidentiality and integrity of their personal data. But this security goal cannot be achieved easily when we are using an open network like Internet. Steganography provides one of the best solutions to this problem. Image steganography is the art of hiding information into a cover image. in the recent past some steganography techniques by combining least significant bit (LSB) substitution and pixel value differencing (PVD) have been proposed to improve upon the hiding capacity and peak signal-to-noise ratio (PSNR). In this paper proposes a steganographic technique by using both LSB substitution and PVD with in a block. The image is partitioned into 2×2 pixel blocks in a non-overlapping fashion. For every 2×2 pixel block the upper-left pixel is embedded with k-bits of data using LSB substitution. Many noticeable hiding strategies proposed by researchers are presented here, but more research is required with the objectives of achieving high embedding payload. In this paper we bring some of the technique for it.

Keywords:- *Steganography, hidden,histogram, LSB least Singnificant Bit, PVD.*

Introduction

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. Steganography has various useful applications. However, like any other science it can be used for ill intentions. It has been propelled to the forefront of current security techniques by the remarkable growth in computational power, the increase in security awareness by, e.g., individuals, groups, agencies, government and through intellectual pursuit. Steganography's ultimate objectives, which are undetectability, robustness (resistance to various image processing methods and compression) and capacity of the hidden data, are the main factors that separate it from related techniques such as watermarking and cryptography. This paper provides a state-of-the-art review and analysis of the different existing methods of steganography along with some common standards and guidelines drawn from the literature. This paper concludes with some recommendations and advocates for the object-oriented embedding mechanism. Steganalysis, which is the science of attacking steganography, is not the focus of this survey but nonetheless will be briefly discussed. Steganography is a Greek origin word meaning

"Concealed Writing". It can be considered as a way to hide secret information in cover image pixels such that it cannot be detected by Human Visual System (HVS) and nobody know about its existence without the intended sender and receiver. Steganography requires three main components named as carrier object, secret data and steganographic algorithm. Sometimes a secret key and cryptographic algorithm is also required in order to increase the security levels and introduce multiple barriers in the way of an attacker.

Steganography can be used for many useful applications like online voting security, secure transmission of top-secret data between national and international governments, online banking security, military and intelligent agencies security and safe circulation of secret documents among defense organizations. On the other hand, Steganography is also very nefarious; it is used by terrorists and criminals for their secure communication and sending viruses and Trojan horses to compromise machines.

Types of Steganography with respect to Carrier Object There are five different types of steganography based on the carrier object that is used for embedding the secret information. The carrier object may be images, text, videos, audios or network protocol packets. If the image is used as a carrier, it is called image steganography. Similarly if video is used for hiding secret messages, we call it video steganography and so on. The diagrammatic representation of different types of steganography is shown in Fig. 1.The types of steganography are:

a. Audio Steganography
b. Image Steganography
c. Video Steganography
d. Text Steganography
e. Network Steganography

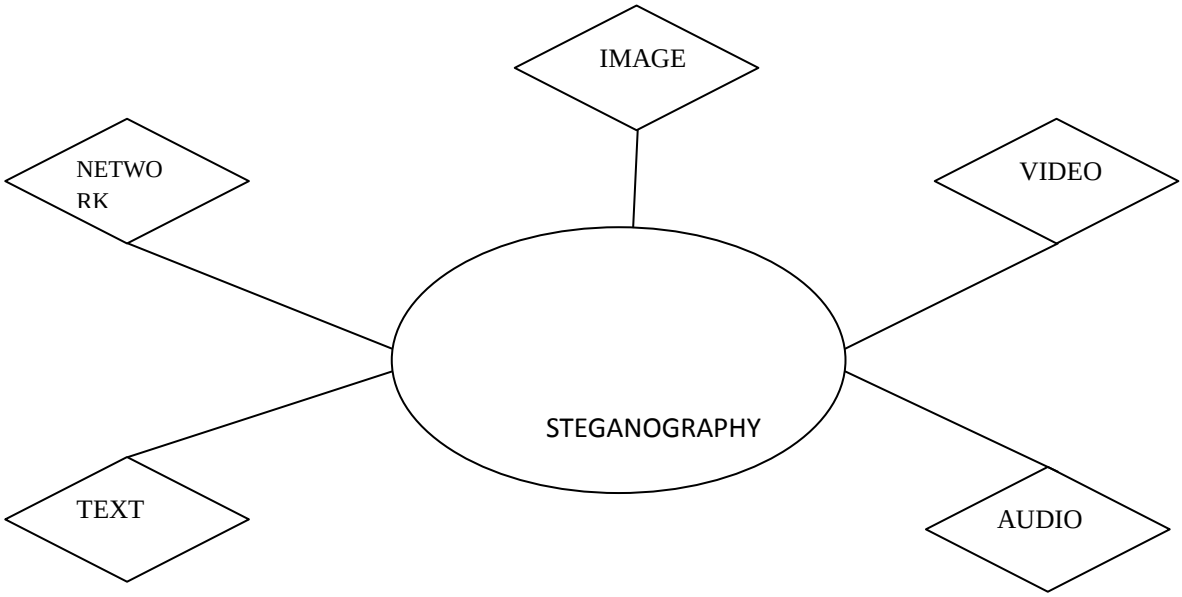

Fig.1:- Types of Steganography with respect to carrier object

Spatial Domain Techniques

In spatial domain techniques, the carrier object (image, video etc) pixels are directly changed in order to hide secret data inside it. These techniques have high payload and bring minor changes in the carrier object but are vulnerable to even simple statistical attacks like cropping, scaling, rotating, compression etc. Some of the techniques that belong to spatial domain are:

a. Least Significant Bit (LSB)

b. Gray-Level Modification (GLM)

c. Pixel Value Differencing (PVD)

d. Edges based Embedding (EBE)

REVIEW OF LITERATURE

A novel reversible data hiding scheme in encrypted image. The content owner encrypts the original image with the encryption key to achieve privacy protection for image content, and then, each block of the encrypted image is embedded with one secret bit by the data hider using the data-hiding key. Through the elaborate selection for partial pixels to be flipped, data hiding process only conducts slighter modifications to each block, which leads to significant improvement of visual quality for the decrypted image. Experimental results demonstrate the effectiveness of the proposed scheme. An effective reversible data hiding scheme with privacy protection capability for image content is proposed. During data embedding, the data hider has no idea about the principle image content since the content owner first encrypts the original image with the encryption key before submitting it to the data hider. The data hider only modifies the 3 LSB layers of some elaborately selected pixels in the encrypted image according to the secret bits for embedding, and the number of the modified pixels is fewer than half of the total image pixel number. Through the encryption key, the receiver can obtain the decrypted, marked image that is visually similar to the original image .The embedded secret bits can be correctly extracted and the original image can be reversibly recovered by the data-hiding key. Thus, the privacy of image content for the content owner is protected, and the operation of reversible data hiding can also be achieved. The experimental results show that, compared with the reported schemes, our scheme has better visual quality of the decrypted image and higher accuracy of secret extraction and image recovery. Therefore, how to parse the compressed stream of the image and make the encrypted bit stream have the compatible structure with the original is important. Also, how to exploit suitable positions in the encrypted JPEG/JPEG2000 bit stream for reversible data embedding deserves in-depth investigations.[6]

A novel method to embed a series of ternary secret data into a cover image based on an improved Least-Significant-Bit (LSB) scheme using the modulo three strategy. Our new method can hide two ternary numbers into each grayscale pixel, normally only modify the two LSBs of the pixel, while it may cause overflow/underflow and a carry/borrow. We solve these problems by adding 1 to the pixel or subtracting 1 from the pixel before embedding. Extensive experimental results indicated that our new method is capable of getting a higher PSNR than traditional LSB scheme when the embedding capacity is greater than 3 bpp, and it has

higher resistance ability against the chosen steganalysis algorithm when the embedding capacity is low. a novel steganography method that is suitable for a ternary number system and achieves high embedding payload with capacity greater than 3bpp. When the embedding capacity is low, our method does not perform better than the traditional LSB scheme, but our proposed scheme is less detectable against the modern detector SPAM.**[7]**

When the embedding capacity is greater than 3bpp, our method performs much better than the traditional LSB scheme. The experimental results confirmed that the proposed method is outstanding in achieving a high PSNR when the embedding payload is high, i.e., we present are versible data hiding (RDH) algorithm for color image. The traditional RDH technique regarding color image embeds data into each color Channel independently. Considering that the color channels correlate with each other, we propose a RDH algorithm based on prediction-error expansion that can enhance the Prediction accuracy in one color channel through exploiting the edge information from Another channel. Extensive experimental results demonstrate that the Proposed algorithm out performs the traditional RDH methods independently embedding data into each channel. a PEE-based RDH algorithm specially designed for color image. This work is based on an observation that the three color channels have similar edge distribution, though their values are not obviously close to each other. With the edge information obtained from another channel, we can adopt a more suitable prediction method for the current channel. So our most important contribution is improving the prediction accuracy through exploiting the correlation between color channels. In addition, we also improve the traditional sorting strategy through taking the overflow/underflow problem into consideration. Experimental results demonstrate that the proposed algorithm obviously outperforms the traditional methods that independently hide data into each channel. Finally, we point out that because the PEE and histogram shifting are used in our proposed RDH algorithm, it is hard to escape from steganalysis. In our future work, we will try to improve the efficiency and security of the RDH algorithm.**[8]**

A new fragile watermarking scheme with high-quality recovery capability based on overlapping embedding strategy. The block-wise mechanism for tampering localization and the pixel- wise mechanism for content recovery are collaborated in the proposed scheme. With the assist of inter- leaving operation, reference bits are derived from mean value of each overlapping block, and then are dispersedly embedded into 1 LSB or 2 LSB layers of the image, corresponding to horizontal-vertical mode and diagonal mode, respectively. Authentication bits are hidden into adaptive LSB layers of the central pixel for each block according to block complexity. The proposed scheme can achieve better quality of recovered image compared with some of state-of-the-art schemes. The overlapping block-wise mechanism for tampering detection and the pixel-wise mechanism for content recovery are proposed. Reference bits are derived from the mean value of each overlapping block through the information interleaving, and dispersedly hidden into the 1 or 2 LSB according to two different embedding modes. Authentication bits are embedded into the center pixel in each overlapping block, and the embedding capacity is determined by the complexity of the block. After detecting tampered blocks and reconstructing mean-value bits, according to the locations of the tampered pixels in each overlapping block, three

corresponding manners of pixel-wise recovery are utilized to recover the pixels with the assist of different neighboring, over- lapping blocks, Compared with some reported schemes, the proposed scheme can achieve superior performance of tampering recovery even for larger tampering rates. [9]

PROPOSED METHOD

In this paper, a more secure steganographic technique is presented which hides secret data in the LSBs of cover image pixels in a randomized cyclic manner. The order in which secret bits are embedded in cover image pixels' planes is RED, GREEN, BLUE, RED, GREEN, and BLUE and so on. This randomized and cyclic approach increases the robustness of the proposed algorithm and randomly disperses the secret data inside the cover image pixels. Due to this reason it is difficult for a malicious user to extract the original secret data from the stego image.

Embedding Algorithm

Input: Color Image and secret data

Output: Stego Image

Step 1: Take the cover color image and secret data.

Step 2: Separate the RED, GREEN and BLUE planes from the cover image.

Step 3: Convert secret data into 1-D array of bits.

Step 4: Set channelFlag = 1 initially (channelFlag determines the channel for embedding).

Step 5: If channelFlag = 1

Replace the LSB of RED channel with secret bit Else if channelFlag = 2

Replace the LSB of GREEN channel with secret bit Else if channelFlag = 3

Replace the LSB of BLUE channel with secret bit End

Step 6: Increment channelFlag by 1.

Step 7: If channelFlag = 3

Set channelFlag = 1;

End

Step 8: Repeat Step 5 to Step 7 until all secret data bits are embedded.

Step 9: Combine all three planes to form the resultant stego image.

CONCLUSIONS

Using three different directional edges can hide more secret data into the cover image than the PVD method. Also, we have presented an optimal selection approach for the reference point with adaptive rules to reduce the quality distortion of the stego-image. Experiment results demonstrate that the secret data embedded in the stegoimage is imperceptible for human vision while compared with the cover image. A steganographic technique based on LSB substitution and three directional PVD in 2×2 pixel blocks is proposed. There are two variants of this proposed technique. The extraction process is very simple and does not require the original cover

image. This technique can be further extended to 3×3 pixel blocks. Still a lot of research is needed for this topic and future researcher may bring some new technique.

REFERENCE

1. Chang CC, Tseng HW. A steganographic method for digital images using side match. Pattern Recognition Letters. 2004, 25(12):1431-1437.
2. Swain G, Lenka SK. Steganography using two sided, three sided, and four sided side match methods. CSI Transactions on ICT. 2013, 1(2):127-133.
3. Swain G. Steganography in digital images using maximum difference of neighboring pixel values. International Journal of Security and Its Applications. 2013,7(6):285-294.
4. Tseng HW, Leng HS. A steganographic method based on pixel-value differencing and the perfect square number. Journal of Applied Mathematics, 2013, article ID 189706.
5. Wu HC, Wu NI, Tsai CS, Hwang MS. Image steganographic scheme based on pixel-value differencing and LSB replacement methods. IEEE Proceedings Vision,Image and Signal Processing. 2005, 152(5): 611-615.
6. Yang CH, Weng CY, Wang SJ, Sun HM. Varied PVD+LSB evading programs to spatial domain in data embedding systems. The Journal of Systems and Software. 2010, 83:1635-1643.
7. Liao X, Wen QY, Zhang J. A steganographic method for digital images with four-pixel differencing and modified LSB Substitution. Journal of Visual Communication and Image Representation. 2011, 22:1-8.
8. Swain G. Digital image steganography using nine-pixel differencing and modified LSB Substitution. Indian Journal of Science and Technology. 2014, 7(9):1444-1450.
9. Luo W, Huang F, Huang J. A more secure steganography based on adaptive pixel-value differencing scheme. Multimedia Tools and Applications. 2010, 52:407-430.
10. Balasubramanian C, Selvakumar S, Geetha S. High payload image steganography with reduced distortion using octonary pixel pairing scheme. Multimedia Tools and Applications. 2013, doi: 10.1007/s11042-013-1640-4.
11. Chen J. A PVD-based data hiding method with histogram preserving using pixel pair matching. Signal Processing: Image Communication. 2014, 29:375-384.
12. Wang CM, Wu NI, Tsai CS, Hwang MS. A high quality steganographic method with pixel-value differencing and modulus function. Journal of Systems and Software. 2008, 81(1):150–158.
13. Joo JC, Lee HY, Lee HK. Improved steganographic method preserving pixel-value differencing histogram with modulus function. EURASIP Journal on Advances in Signal Processing. 2010, doi:10.1155/2010/249826.
14. Shen SY, Huang LH. A data hiding scheme using pixel value differencing and improving exploiting modification directions. Computers & Security. 2015, 48:131-141.

15. Khodaei M, Faez K. New adaptive steganographic method using least-significant-bit substitution and pixel-value differencing. IET Image processing. 2012,6(6):677-686.
16. Ahmad J, Sajjad M, Mehmood I, Rho S, Baik S W (2015) Describing Colors, Textures and Shapes for Content Based Image Retrieval-A Survey. *arXiv preprint arXiv:1502.0704*
17. Al-Taani AT, Al-Issa AM (2009) A novel steganographic method for gray-level images. Int J Comput Inform Syst Sci Eng 3:1 2009
18. Amirtharajan R, Archana P, Rajesh V, Devipriya G, Rayappan J (2013) Standard deviation converges for random image steganography. In: *Information & Communication Technologies (ICT), 2013 I.E. Conference on*. pp 1064–1069
19. Amirtharajan R, Behera S K, Swarup M A, Rayappan J B B (2010) Colour guided colour image steganography. *arXiv preprint arXiv:1010.4007*
20. Amirtharajan R, Mahalakshmi V, Nandhini J, Kavitha R, Rayappan J (2013) Key decided cover for random image steganography. Res J Inf Technol 5:171–180
21. Anees A, Siddiqui AM, Ahmed J, Hussain I (2014) A technique for digital steganography using chaotic maps. Nonlinear Dyn 75:807–816
22. Bailey K, Curran K (2006) An evaluation of image based steganography methods. Multimedia Tools Appl 30:55–88
23. Chan C-K, Cheng L-M (2004) Hiding data in images by simple LSB substitution. Pattern Recogn 37:469–474
24. Chang C-C, Hsiao J-Y, Chan C-S (2003) Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy. Pattern Recogn 36:1583–1595
25. Cheddad A, Condell J, Curran K, Mc Kevitt P (2010) Digital image steganography: survey and analysis of current methods. Signal Process 90:727–752
26. Chen W-Y (2008) Color image steganography scheme using DFT, SPIHT codec, and modified differential phase-shift keying techniques. Appl Math Comput 196:40–54
27. Chen W-J, Chang C-C, Le T (2010) High payload steganography mechanism using hybrid edge detector. Expert Syst Appl 37:3292–3301
28. Cheng W-C, Pedram M (2004) Chromatic encoding: a low power encoding technique for digital visual interface. Consum Electron IEEE Trans 50:320–328
29. Dumitrescu S, Wu X, Wang Z (2003) Detection of LSB steganography via sample pair analysis. Signal Process IEEE Trans 51:1995–2007
30. Fakhredanesh M, Rahmati M, Safabakhsh R (2013) Adaptive image steganography using contourlet transform. J Electron Imaging 22:043007
31. Fang Y, Zeng K, Wang Z, Lin W, Fang Z, Lin C-W (2014) Objective quality assessment for image retargeting based on structural similarity. IEEE J Emerg Sel Top Circ Syst 4:95–105
32. Ghasemi E, Shanbehzadeh J, Fassihi N (2012) High Capacity Image Steganography Based on Genetic Algorithm and Wavelet Transform. In: Intelligent Control and Innovative Computing. Springer. pp 395–404
33. Grover N, Mohapatra A (2013) Digital Image Authentication Model Based on Edge Adaptive Steganography. In: *Advanced Computing, Networking and Security (ADCONS), 2013 2nd International Conference on*. pp 238–242
34. Gutub AA-A (2010) Pixel indicator technique for RGB image steganography. J Emerg Technol Web Intell 2:56–64
35. Gutub A, Ankeer M, Abu-Ghalioun M, Shaheen A, Alvi A (2008) Pixel indicator high capacity technique for RGB image based Steganography. In: WoSPA 2008–5th IEEE International Workshop on Signal Processing and its Applications. pp 1–3

36. Hamid N, Yahya A, Ahmad RB, Al-Qershi OM (2012) Image steganography techniques: an overview. Int J Comput Sci Secur (IJCSS) 6:168–187
37. Hong W (2013) Adaptive image data hiding in edges using patched reference table and pair-wise embedding technique. Inf Sci 221:473–489
38. Hong W, Chen T-S (2012) A novel data embedding method using adaptive pixel pair matching. Inform Forensic Secur IEEE Trans 7:176–184
39. Huang F, Li B, Huang J (2007) Attack LSB matching steganography by counting alteration rate of the number of neighbourhood gray levels. In: *Image Processing, 2007. ICIP 2007. IEEE International Conference on*. pp I-401-I-404
40. Ioannidou A, Halkidis ST, Stephanides G (2012) A novel technique for image steganography based on a high payload method and edge detection. Expert Syst Appl 39:11517–11524
41. Jan Z, Mirza AM (2012) Genetic programming-based perceptual shaping of a digital watermark in the wavelet domain using Morton scanning. J Chin Inst Eng 35:85–99
42. Jassim F A (2013) A novel steganography algorithm for hiding text in image using five modulus method. *arXiv preprint arXiv:1307.0642*
43. Kanan HR, Nazeri B (2014) A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm. Expert Syst Appl 41:6123–6130
44. Karim M (2011) A new approach for LSB based image steganography using secret key. In: *14th International Conference on Computer and Information Technology (ICCIT 2011)*. pp 286–291
45. Ker A D (2005) A general framework for structural steganalysis of LSB replacement. In: *Information Hiding*. pp 296–311
46. Ker AD (2005) Steganalysis of LSB matching in grayscale images. Signal Proc Lett IEEE 12:441–444
47. Laaksonen J, Koskela M, Laakso S, Oja E (2000) PicSOM–content-based image retrieval with self-organizing maps. Pattern Recogn Lett 21:1199–1207
48. Lee Y-P, Lee J-C, Chen W-K, Chang K-C, Su I-J, Chang C-P (2012) High-payload image hiding with quality recovery using tri-way pixel-value differencing. Inf Sci 191:214–225