Volume 3, Issue 6, June-2016, pp. 347-351 ISSN (O): 2349-7084
International Journal of Computer Engineering In Research Trends
Available online at: www.ijcert.org

Investigation of Various Image Steganography Techniques in Spatial Domain

[1]Gunjan, [2] Er. Madan Lal

Department of Computer Engineering
Punjabi University, Patiala,India
gun3007@gmail.com , mlpbiuni@gmail.com

Abstract: In this internet era the security of information has become a big concern. People are communicating over internet. Their communication can be made secure through information hiding technique known as steganography .It is a Greek world which literally means enclosed writing. Image steganography is very popular because it exploits the weakness of human visual system and also large amount of redundant bits are present in digital representation of an image. In this paper various image steganography techniques in spatial domain are investigated.

Keywords: LSBM, LSBMR, Steganalysis, stego-image

1. INTRODUCTION

Steganography is art and science of hiding information which provides a promising way of safe electronic communication .It uses a cover (image, text, video and audio) to hide the information. For steganography we must have some message to be embedded and a cover image in which message is to be hide. The cover image can be of any size and can be in any format. More the size it is easier to hide the message and much bigger message can be hide. We must have a key which is used to select the random pixels on which data is to hide. By using a message, a cover image and stego key a stego image is generated which is send to another person. On the receiver side the stego image is processed and extraction of message takes place with the help of secret key. The key is the one by which receiver knows the position of the pixel on which message is embedded.

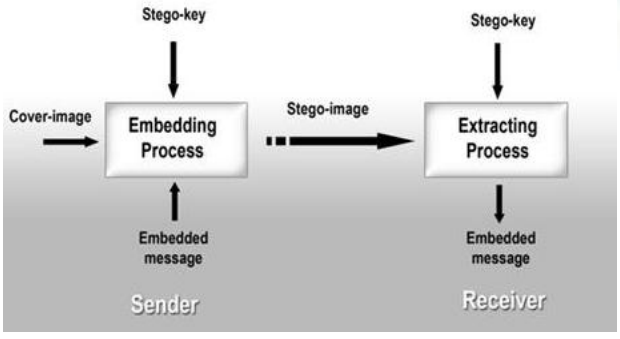

Figure 1 : Block diagram of steganography

Steganography is not the same as cryptography. Steganography and cryptography share a common goal but their usage is different. Steganography is hidden writing whereas cryptography is secret writing. This paper focuses on spatial domain image steganography techniques. Important issues that must be considered in stenographic system are Robustness, Capacity and Imperceptibility. Their relationship can be expressed by Measurement triangle of steganography shown in figure2.

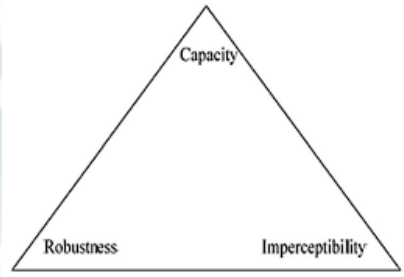

Figure 2: Measurement triangle of steganography.

Robustness: Robustness is the ability of embedded data to remain undamaged if the stego image undergoes transformations, such as linear and non-linear filtering, scaling and rotations, addition of random noise, sharpening or blurring, lossy compression, cropping or decimation and conversion from digital to analog form and then reconversion back to digital form.

Capacity: Capacity is the maximum amount of secret information can be embedded in a cover image. Capacity can be defined as an absolute value in term of number of bits which can be embedded in cover image, while the obtained stego-image remains undetectable. In order to improve one element, you have to sacrifice one or the other two elements. If you improve capacity, you sacrifice the security.

Imperceptibility: Imperceptibility refers to the inability of person to distinguish the original and the stego-image. The invisibility of a steganographic algorithm is the primary requirement but if one can distinguish the original and stego-image then the steganography algorithm is compromised.

2. IMAGE STEGANOGRAPHY

Image steganography: Spatial and Frequency domain are two popular domain of image steganography. In spatial domain the information bits is inserted directly while in frequency domain cover is first transformed to frequency domain.

2.1. Spatial domain Steganography: In this method, the pixel value is directly modified for data hiding. The various approaches to achieve embedding in spatial domain are shown in the Fig. 3.

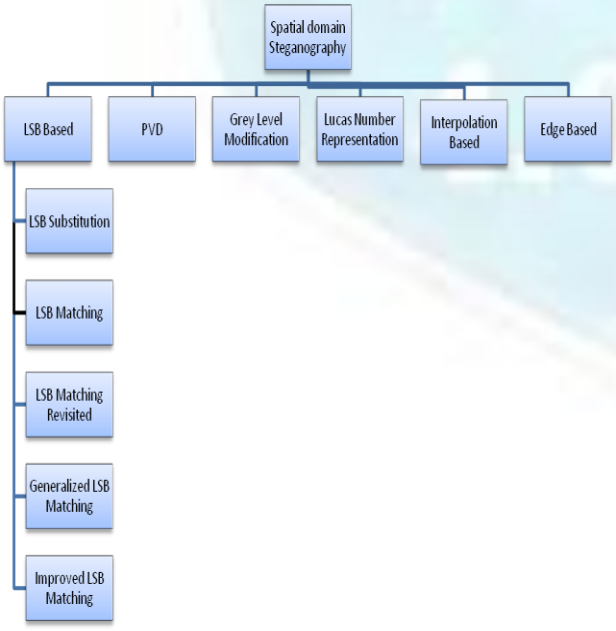

Figure 3: Various techniques of spatial domain steganography

2.1.1. LSB Based Steganography

2.1.1.1 LSB Substitution:

LSB substitution is most simplest and popular image steganography method. LSB of a cover image is replaced with the message bits. Cover-image with the secret message embedded in it is called stego-image. The advantage of LSB substitution method is its simplicity and highest capacity. However LSB substitution is extremely sensitive to any kind of filtering or manipulation of the stego-image. Stego-image is sensitive to Scaling, rotation, cropping as it will destroy the message. Steganalysis of LSB method is very easier. Therefore, it is suggested that the message should be first encrypted before the embedding it into cover image. In Lee-Ming Cheng et. al's [1] research paper authors proposed a LSB substitution with an optimal pixel adjustment process (OPAP) .

2.1.1.2 LSB matching:

LSB Replacement causes POV (Pair of Values) on intensity histogram of stego- image which makes it easier for analyzers to detect the secret messages. LSB matching is a modification of LSB replacement. In LSB matching, if the message bit does not match the LSB of cover image then instead of replacing the LSB of cover image the one is randomly added or subtracted from the value of cover pixel. It has only few detection methods like HCF-COM and ALE which can detect a message embedded using LSB matching.

2.1.1.3 LSB Matching Revisited:

LSBMR uses a pair of pixels as a unit in which the LSB of the first pixel carries one bit of information and the relationship of the two consecutive pixels carries another bit of Information. This proposed method causes fewer changes to the cover image and show better performance than LSBM in terms of resistance against steganalysis [3].

2.1.1.4 Gernalized LSB Matching:

It reduces the expected number of modification per pixel (ENMPP) as compare to LSB matching algorithm. Generalized LSB matching generalizes LSB matching and Mielikainen's scheme [3] and it is more secure [4].

2.1.1.5 Improved LSB Matching:

In LSB matching stego-image histogram has less power in high frequency than histogram of cover image. It is important to minimize the histogram alteration caused by steganography. Improved LSB matching minimizes the alteration of histogram by embedding two bits in a pair of pixels with adjacent intensity. Proposed method resists 1D histogram attack but do not work for two dimensional features [6].

2.2 Pixel Value Differencing :

In PVD cover image is partitioned into non-overlapping blocks of two consecutive pixels. A difference value d is calculated from these two consecutive pixels of a cover image. The difference value is mapped into range table, which is divided into different ranges of specific width. The width of the range determines the number of bits which can be embedded in a pixel pair. This method provides an easy way to produce a more unnoticeable result than those yielded by LSB replacement method [2]. In J. K. Mandal et.al's [11] authors proposed a method in which color images are used for embedding secret data by pixel value differencing technique. This method eliminate the overflow problem (the pixel values in the stego-image may exceed the range 0~255) of PVD technique. To improve security different no of bits are embedded in different pixel component. This method provides better image quality than the PVD technique. In H. C. Wu et.al's [12] authors proposed a method which combined the advantage of LSB and PVD. LSB+PVD combination gives high capacity and high security. In LSB+PVD method two pixel blocks are used. If the difference is less than or equal to 15, 3-bit LSB substitution is used. If the difference is more than 15, then PVD method is used. LSB+PVD approach has limitation that it embed more number of bits in smooth areas than edge areas, which contradicts to the principle that in "edge areas more number of bits can be hidden". In C. H. Yang et.al's [13] authors proposed a method which modifies LSB+PVD method. In this method risk of the RS-steganalysis detection program is reduced. This method had removed the limitation LSB+PVD method and provides more security.

2.3 Grey Level Differencing:

Grey level differencing is used to map data by modifying the gray levels of pixels. Based on some mathematical function, a set of pixels is selected for mapping. This technique uses the notion of odd and even numbers to map data within a cover image e.g. 0 is mapped with even value and 1 is mapped with odd values. Advantages of this method include low computational complexity and high information hiding capacity.

2.4 Lucas Number Representation:

In F. Akhter [5] author proposes a method in which Lucas number representation of pixel is used for embedding the message bits. Decomposition of cover image pixel using Lucas number provides higher bit plane for embedding message bits. Proposed method has high capacity as compare to [1, 2, and 3] and high peak signal to noise ratio.

2.5 Interpolation Based:

In Jie Hu et. al's [9] authors proposed a steganography technique which is reversible and uses extended image interpolation technique. In this scheme difference between the neighboring pixels is maximized to increase the capacity. The IMNP scheme has low computational complexity and high capacity. In Mingwei Tang et.al's[10] authors proposed an adaptive steganography technique which uses AMBTC compression and interpolation technique (ASAI). By AMTBC compression the input image is changed down into ¼ of its initial size. The compressed image is expanded up to four times into the cover image by interpolation technique. Proposed method offer higher hiding capacity and better image quality. In future more optimized algorithm can be made by designing a new idea based on AMBTC compression and interpolation technique.

2.6 Edge Based:

In H.A Dmour et. al's [8] authors proposed a steganography technique based on edge detection and XOR coding. Edge detection algorithm detects sharp edges in cover image. Human visual system is less sensitive to changes in sharp contrast. Therefore edges are used for embedding message bits. To reduce the difference between cover and stego-image XOR coding is used. Experimental results shows that this method has better imperceptibility results as compared to other methods. In P. Thiyagarajan et. al's [7] authors proposed reversible steganography algorithm using graph coloring. This method is resistant against transformations such as

cropping, rotation and scaling. It used dynamic, tough and unpredictable key which is obtained by solving 3 colorable graphs. In 3 colorable graph, coloring is done to the vertices such that connected vertices should not have the same color. Hash value is calculated using MD5 algorithm.

3. DISCUSSION

Table 1. Spatial domain Steganography Methods listed in chronological order starting from latest

S. N	Author	Year	Method used	Key features
1	Mingwei Tang et.al's [10]	2015	Image interpolation (ASAI) and AMBTC compression	Higher capacity and better image quality
2	Jie Hu et. al's[9]	2015	IMNP	Low computational capacity, Reversible and Improved capacity
3	H.A Dmour et. al's[8]	2015	Edge detection and XOR coding.	Better imperceptibility and security
4	P. Thiyagarajan et. al's[7]	2013	3 colorable graphs	Resistance Against Transformations such as cropping,rotation &scaling.
5	F. Akhter [5]	2013	Lucas number	High capacity
6	J. K. Mandal et.al's [11]	2012	PVD for color images	Better image quality than the PVD[2] technique
7	Ling Xi et. al's [6]	2010	Improved LSB matching algorithm	Resists 1D histogram attack
8	C. H. Yang et.al's [12]	2010	Modified LSB+PVD	Removes the limitation of [11] and provides more security
9	Xiaolong Li et. al's [4]	2009	Sum and difference covering set(SDCS) of finite cyclic group is used	G-LSB-M is more secure than LSB matching and LSBMR[6]
10	J. Mielikainen [3]	2006	LSBMR	Decreases the probability of detection for the HCF-OM detectors compared to LSB matching.
11	H. C. Wu et.al's [12]	2005	LSB+PVD	More capacity and security
12	Lee-Ming Cheng et. al's [1]	2004	LSB Substitution with OAOP	High capacity
13	D. C. wu et.al's [2]	2003	Pixel value differencing	More security

4. CONCLUSION

Steganography is very much useful to have a secret communication in the internet. In this paper

different Spatial Domain Techniques are investigated .The LSB techniques give high capacity, whereas PVD techniques give high security. The LSB and PVD techniques can be combined together to get both high capacity and high security. Reversible Steganography techniques [7, 9] are those which produces a lossless recovery of the host image when the secret data is extracted. Every year new steganographic techniques are being proposed and new steganalysis techniques are also found. The research to made strong steganographic and steganalysis technique is a continuous process.

REFERENCES

[1] Chan, Chi-Kwong, and Lee-Ming Cheng "Hiding data in images by simple LSB substitution", Pattern recognition, 2004, pp 469-474

[2] D. C. Wu, and W. H. Tsai, "A steganographic method for images by pixel-value differencing", Patter Recognition Letters, vol.24,2003, pp.1613-1626.

[3] J. Mielikainen,"LSB matching revisited." Signal Processing Letters, IEEE, Vol 13, Issue 5, 2006, pp 285-287.

[4] Li, Xiaolong, et al. "A generalization of LSB matching" Signal Processing Letters, IEEE, Vol 16, Issue 2, 2009, pp 69-72.

[5] Fatema Akhter "A Novel Approach for Image Steganography in Spatial Domain" Global Journal of Computer Science and Technology Graphics & Vision,Vol.13 ,Issue 7,2013,

[6] Ling Xi, Xijian Ping, Tao Zhang "Improved LSD Matching Steganography Resisting Histogram Attacks", Computer Science and Information Technology(ICCSIT),Vol.1,2010,pp 203-206.

[7] P. Thiyagarajan, G. Aghila "Reversible dynamic secure steganography for medical image using graph coloring", Health Policy and Technology, vol. 2,Issue 3,sep 2013,pp 151–161.

[8] Hayat Al-Dmour, Ahmed Al-Ani "A Steganography Embedding Method Based On Edge Identification and XOR coding", Expert System with Applications, vol. 46, March 2016,pp 293-306.

[9] Jie Hu , Tianrui "Reversible Steganography using extended image interpolation technique", Computers and Electrical Engineering Vol.46, Issue C, August 2015,pp 447-455.

[10] Mingwei Tang, Shenke Zeng, Xiaoliang Chen, Jie Hu, Yajun Du "An adaptive steganography technique using AMBTC compression and interpolation technique," International Journal for Light and Electron Optics, Vol.127, Issue 1, January 2016,pp 471-477.

[11] J. K. Mandal and Debashis Das "Colour Image Steganography Based on Pixel Value Differencing in spatial domain," International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4, July 2012. pp. 83-93.

[12] 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", IEEE Proceedings Vision, Image and Signal Processing, vol.152, No.5,2005, pp.611-615.

[13] C. H. Yang, C.Y. Weng, S. J. Wang, and H. M. Sun "Varied PVD+LSB evading programs to spatial domain in data embedding", The Journal of Systems and Software, vol.83,2010, pp.1635-1643.

