Journal of Basic and Applied Engineering Research
Print ISSN: 2350-0077; Online ISSN: 2350-0255; Volume 2, Number 10; April-June, 2015 pp. 854-859
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/jbaer.html

Information Hiding Using Image Steganography - A Survey

Fagul Pandey[1], Sayesha Gupta[2] and Sunil Kumar[3]

[1,2]Studnet of University of Petroleum and Energy Studies, Dehradun
[3]A.P., University of Petroleum and Energy Studies, Dehradun
E-mail: [1]fagul.pandey12@stu.upes.ac.in, [2]sayesha.gupta12@stu.upes.ac.in, [3]skumar@ddn.upes.ac.in

Abstract—*Communication Security is the discipline of preventing unauthorized interceptors from accessing confidential information. Steganography is one of the techniques that are used to hide the information in the form of text, audio, video and images etc. In Image-Steganography, secret communication is achieved by embedding a message into the pixels of the cover image called stego-image. Different techniques exist for image steganography. In this paper, author's intent is to discuss and compare the various existing techniques of Image-Steganography.*

Keywords: *Steganography, Information Hiding, image, LSB*

1. INTRODUCTION

1.1 Information Hiding Information hiding is a powerful technique used for transmitting secret messages by using the following techniques.

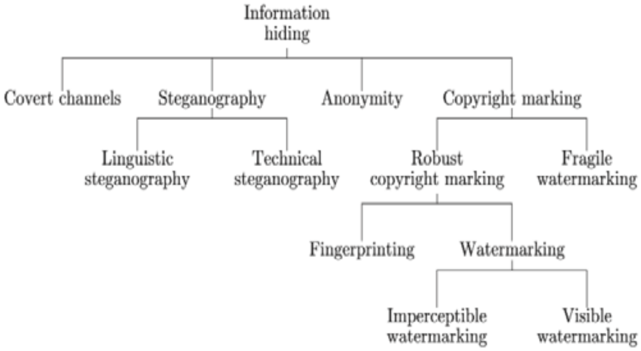

Fig1. Classification of Information Hiding Techniques [1]

1.1.1 Covert Channels

A covert channel is any communication channel that can be exploited by a process to transfer information in a manner that violates the system's security policy. [2]

1.1.2 Steganography

1.1.2.1. Linguistic steganography

Linguistic Steganography makes use of written natural language to conceal secret messages. The whole idea is to hide the very presence of the real messages. These algorithms embed messages into cover text in a covert manner such that the presence of embedded messages in the resulting stego-text cannot be easily discovered by anyone except the intended recipient. [3]

1.1.2.2. Technical steganography

Technical steganography uses scientific methods to hide a message, such as the use of invisible ink or microdots and other size-reduction methods. [6][4].

Types

- **Image -** Taking the cover object as image in steganography is known as image steganography. Generally, in this technique pixel intensities are used to hide the information.
- **Text -** General technique in text steganography such as number of tabs, white spaces, capital letters and Morse codes etc. are used to achieve information hiding.
- **Audio -** When taking audio as a carrier for information hiding it is called audio steganography. Audio steganography uses digital audio formats such as WAVE, MIDI, AVI & MPEG etc. for steganography
- **Video -** Video Steganography is a technique to hide any kind of files or information into digital video format. Video (combination of pictures) is used as carrier for hidden information. Video steganography uses such as AVI, Mp4, MPEG and other video formats.

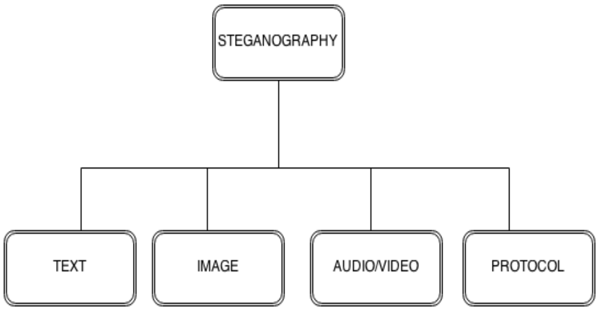

Fig. 2: Classification of Steganographic Techniques

1.1.3 Anonymity

Generally, computer security deals with privacy authentication, means whether the receiver is authorized to get access to the information or not. But, it is important to know that what content is being sent rather than the authentication. The identities of the people, who are the subjects of the data or other sensitive properties of the data, are protected. E.g., person specific information in hospitals and organizations. [5]

1.1.4 Copyright marking

The major concern in information hiding is that of copyright media such as audio, video etc. are available in digital form, due to which perfect copies can be formed, may lead to large scale unauthorized copying. This is great concern to the music, film, book and software publishing industries. Watermarks are hidden copyright messages i.e. used to prosecute against copyright violators whereas Fingerprints is used to hide serial number helps in identifying the copyright violators. [1]

2. IMAGE STEGANOGRAPHY

It is one of the most popular and easy ways to hide information, because images are easier to carry and transfer through web. The following shows the classification of the various types of algorithms implemented in image steganography.

Spatial Domain - Spatial domain techniques embed information in the intensity of the original image pixels directly. Basically, least significant bit (LSB) method is used to replaces the least significant bit of original pixel with the message bit.

Transform Domain - Transform domain also known as frequency domain where images are first transformed then the message is embedded in the image. The procedure of embedding data in the frequency domain of a signal is much stronger than embedding principles that operate in the time domain. Discrete cosine transformation (DCT) technique is used in JPEG images to achieve compression. DCT is a lossy compression transform where the cosine values cannot be generated as original, because DCT alter values to hide the information.

Compression Domain - Distortion techniques need knowledge of the original cover image during the decoding process where the decoder functions to check for differences between the original cover image and the distorted cover image in order to restore the secret message. The encoder adds a sequence of changes to the cover image. So, information is described as being stored by signal distortion. Using this technique, a stego-object is created by applying a sequence of modifications to the cover image. This sequence of modifications is use to match the secret message required to transmit. The message is encoded at pseudo-randomly chosen pixels. If the stego-image is different from the cover image at the given message pixel, the message bit is a “1” otherwise, the message bit is a “0”. [4]

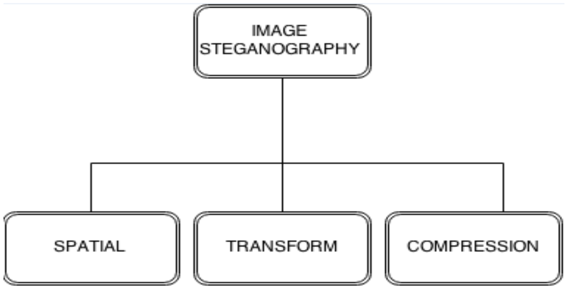

Fig. 2: Classification of Image Steganography

3. EXISTING TECHNIQUES IN SPATIAL IMAGE-STEGANOGRAPHY

Least significant bit - Least Significant Bit embedding is one of the most popular and simple technique to implement steganography. The technique works by replacing information in a pixel with secret information, embedding is performed on the least significant bit(s) of the pixel. Embedding in least significant bit assures minimum change in the colour value. For example if least significant bit is changed then it changes the colour value by one. Therefore, if embedding is performed on the last two significant bits of the pixel, colour value variation is by four. In a LSB embedding some information is always lost from the cover image. This can be stated as one of the effects of embedding data directly into the pixel.

Pixel Value differencing - In PVD method, gray scale image is used as a cover image with a long bit-stream as the secret data[2]. PVD uses the difference between the pixel and its neighbour to determine the number of bits to be embedded .Larger the difference, the more secret bits can be embedded into the cover image.

Image is scanned in zig-zag manner starting from the upper left corner. Then, the cover image is divided into large number of blocks where each block consists of two consecutive non-overlapping pixels. The difference of the two non - overlapping pixels in the block is used to determine the smoothness properties of the cover image. A small difference value states that the pixels are at smooth area whereas difference values between the pixels around edge area are large. Therefore, in PVD method a range table has been designed with n contiguous ranges Ri (where i=1,2,…,n) where the range is 0 to 255. The lower and the upper bound are denoted as li and ui respectively, then Ri∈ [li,ui]. The width of Ri is calculated as wi=ui-li+1. Width that is,wi decides how many bits can be embedded in a particular pixel block. The number of bits ‘bi’to be embedded in a block can be defined as bi=(log2wi), where wi is the width of the range.

This method enhances the embedding capacity but the disadvantage of this technique is that sometimes the pixel value in the stego-image may exceed the range 0-255 which leads to improper visualization of the stego image. It has security issues, embedding information in smooth areas etc.

Edge based data embedding method - This method is based on the theory that human eyes can very easily observe small changes made in the smooth areas but they cannot notice larger changes made at the edges of the image. Therefore, secret information is embedded into pixels around the edges of the image. For example in EDGE LEAST SIGNIFICANT BITEMBEDDING (ELSB) we identify the edge pixels . After obtaining the edge pixels data is hidden in the LSB bits of the edge pixels only and send the stego object to the receiver.

Mapping pixel to hidden data method - In this method a pixel pair value is taken as reference coordinate. Another pixel pair co-ordinate is searched in the neighbourhood of the reference coordinate depending upon the binary message digit. With this the reference coordinate will be replaced by the searched pixel value pair to conceal the message bit.

Labelling or connectivity method - In this method the image is converted into binary and then is labelled using the 4 connectivity or the 8- connectivity method. In the 8 connectivity method two pixels are part of the same object if their edges are connected vertically, horizontally or diagonally.[9][8]

Pixel intensity based method - In this method, all the three colour planes will be converted in to binary values. For each pixel in the image, the plane which has the minimum number of ones in its MSB will act as index plane and the other two colour planes are considered as data planes. This technique increases the capacity to hide more number of message bits in the cover image[7].

Texture based method – In this method the texture areas are divided into two groups, simple and complex. These are then used to hide important information.

Histogram shifting method - In this method, first a zero point and a peak point are identified. The gray scale value which no pixel in the cover Image assumes corresponds to minimum number of pixels also known as Zero point. Peak point corresponds to the gray scale value with the maximum number of pixels in the cover image. Once the zero-peak pair are found, the image is scanned in a sequential order. The gray scale value of pixels between peak and zero points are incremented by 1 unit. This is equivalent to shifting the gray scale values to the right by 1, leaving the gray scale value of peak points empty.

4. PARAMETERS OF IMAGE STEGANOGRAPHY[4]

- **Embedding capacity:** Maximum size of information that can be embedded into the cover media without deteriorating its integrity.
- **Perceptual transparency:** The embedding should occur without significant degradation or loss of perceptual quality of the cover media.
- **Robustness:** It refers to the ability of embedded data to remain intact if the stego-image undergoes various transformations such as scaling, rotation, cropping or compression.
- **Tamper resistance:** It refers to the difficulty to alter or forge a message once it is embedded in a cover-media, such as replacing a copyright mark with the one claiming legal ownership.
- **Computational complexity:** Computational complexity of steganography technique employed for encoding and decoding is another consideration and should be given importance.

5. FINDINGS

Table 1: Analysis of various image Steganography techniques[4]

Lit. Ref	Domain	Technique	Targetto					Advantage	Disadvantage
			Ca pa cit	Pe rc ep	R ob us	Te m	C o m		
[10]	Spatial	AdaptiveLSB	Y	N	N	N	N	Integrity of secret hidden informationwith HighCapacity	Hide extrabits ofsignature with hidden message
[11]	Spatial	Texture, Brightness and Edge based Adaptive LSB	Y	Y	N	N	N	High Hidden Capacity with Considering of Good Visual Quality	Experimental Dataset is limited

[12]	Spatial	Combine Pattern bits (Stego-Key)with Secret Message usingLSB	N	N	N	N	N	Security of Hidden Data	Hidden Capacity is Low
[13]	Spatial	PVD(on edges) with Adaptive LSB (smooth)	Y	Y	N	N	Y	High Hidden Capacity with Considering of Good Visual Quality	Computationally Complex
[14]	Spatial	MPD with LSB	Y	Y	N	N	N	Betterthan general PVD methods	Experimental Dataset is limitedand Threshold (Stego)Key Required for Bothends
[15]	Spatial	PVDwith **Adaptive LSB**	Y	Y	N	N	N	Histogram of **cover and stegoimage is almost same**	Dataset for **Experiments is too small.**
[16]	Spatial	Hybrid (canny + fuzzy) edge detection withLSB	Y	Y	N	N	N	HighPSNRwith high hidden capacity	Limited Dataset with ideal images and Extensive edgebased images may failed
[17]	Spatial	LSB substitutio n with Random pixel selection	N	N	N	N	N	Security of hidden message inStego-image	Embedding data without considering VisualQuality inRandom pixel selection
[18]	Spatial	Mapping pixel to hidden alpha-numeric letters	N	Y	N	N	N	Just Mappingof pixelwithletter no need ofimage processing (edge etc.)required.	Have to keep Matching Pattern for Extracting procedureplus OnlyusefulforLetter based hidden data
[19]	Spatial	LSB substitutingon Dark region of Image	N	Y	N	N	N	Usefulfor smoothregion withsolid boundaryof objectbased dataset	High computation requiredand not tested on hightexture areas
[20]	Spatial	LSB substitutio n with Median Filtering	Y	N	N	N	N	High hidden capacity	Computational ly complex (filtering) plusStego-key requirement

[21]	Spatial	Pixel indicator with variable LSB substitution	Y	N	N	N	N	Almost Same histogramof stego-image against cover image	Hidden capacity depended on Coverimage pixel intensities
[22]	Spatial	Simple and Complex Texture basedLSB substitution	Y	Y	N	N	N	High hidden Capacity	High hidden capacity degrade the visualquality PSNR
[23]	Transform	DCT Coefficient based	N	Y	N	Y	N	HighPSNR	Noticeable artifact of hidden data
[24]	Transform	DWT Coefficient permuted and embeddingin Spatial domain	N	N	N	N	N	Integrity of hidden data in stego-image	Computational ly complex
[25]	Transform	Secretbits plusBit- depth embedded into coded- block	N	Y	N	Y	N	Usefulforbinary image	NotforColor image support

6. CONCLUSION

Data security is protecting the secret information from the unwanted actions of unauthorized users and steganography is the way to achieve data security.In this paper, we have discussed about the Information Hiding along with its domains i.e covert channels, steganography, anonymity and copyright marking. Based on capacity, perceptual, robustness, temper and computation parametersvarious spatial and transform image steganography techniques are discussed and analyzed.PVD(on edges) with Adaptive LSB[4] is a better image steganography technique than its counterparts.

7. FUTURE SCOPE

Information hiding is a technique that is used for transmitting secret messages.Steganography is the sub-domain of information hiding which hides secret information in an image, audio, video etc. We look forward todesign and implement a better image steganographic technique which can be related to all spatial, transform and compression domains or satisfies parameters such as capacity, perceptual, robustness, temper and computation.

REFERENCES

[1] P. Fabien, J. Ross. Anderson, and Markus G. Kuhn. “Information Hiding – A Survey.” Proceedings of the IEEE, 87:7. 1062-1078. 1999.

[2] H.C. Wu, N.I Wu, C.S Tsai and M.S Hwang, “Image Steganographic scheme based on pixel value differencing and LSB replacement method”, IEEE Proceedings on Vision, Image and Signal processing, Vol. 152, No.5, pp.611-615,2005 .

[3] http://link.springer.com/chapter/10.1007%2F978-3-540-88961-8_16#page-2

[4] Mehdi Hussain and Mureed Hussain, A Survey of Image Steganographic Techniques, International Journal of Advanced Science and Technology Vol. 54, May, 2013

[5] https://epic.org/privacy/reidentification/Sweeney_Article.pdf

[6] BablooSaha and Shuchi Sharma, Steganographic Techniques of data hiding using digital imagesDefence Science Journal, Vol. 62, No., pp. 11-18, DOI: 10.14429/dsj.62.1436 2012, DESIDOC 1, January 2012

[7] M.Shobana, R.Manikandan EFFICIENT METHOD FOR HIDING DATA BY PIXEL INTENSITY, International Journal of Engineering and Technology (IJET) http://www.enggjournals.com/ijet/docs/IJET13-05-01-060.pdf

[8] H. Motameni, M. Norouzi, M. Jahandar, and A. Hatami, Labeling Method in Steganography, WASET International Journal of Computer, Control, Quantum and Information Engineering Vol:1, No:6, 2007

[9] http://www.researchgate.net/publication/239551978_Labeling_Method_in_Steganography

[10] Y. K. Jain and R. R. Ahirwal, “A Novel Image Steganography Method With Adaptive Number of Least Significant Bits Modification Based on Private Stego-Keys”, International Journal of Computer Science and Security (IJCSS), vol. 4, (2010) March 1.

[11] H. Yang, X. Sun and G. Sun, “A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution”, Journal: Radioengineering, vol. 18, no. 4, (2009), pp. 509-516.

[12] S. Channalli and A. Jadhav, “Steganography an Art of Hiding Data”, International Journal on Computer Science and Engineering, IJCSE, vol. 1, no. 3, (2009).

[13] C.-H. Yang, C.-Y. Weng, S.-J. Wang, Member, IEEE and H.-M. Sun, “Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems”, IEEE Transactions on Information Forensics and Security, vol. 3, no. (2008) September 3, pp. 488-497.

[14] K.-H. Jung, K.-J. Ha and K.-Y. Yoo, “Image data hiding method based on multi-pixel differencing and LSB substitution methods”, Proc. 2008 International Conference on Convergence

and Hybrid Information Technology (ICHIT '08), Daejeon (Korea), (2008) August 28-30, pp. 355-358.

[15] H. Zhang, G. Geng and C. Xiong, “Image Steganography Using Pixel-Value Differencing”, Electronic Commerce and Security, ISECS '09. Second International Symposium on (2009) May.

[16] W. J. Chen, C. C. Chang and T. H. N. Le, “High Payload Steganography Mechanism Using Hybrid Edge Detector”, Expert Systems with Applications (ESWA 2010), vol. 37, pp. 3292-3301, (2010) April 4.

[17] V. MadhuViswanatham and J. Manikonda, “A Novel Technique for Embedding Data in Spatial Domain”, International Journal on Computer Science and Engineering, IJCSE, vol. 2, (2010).

[18] M. A. Al-Husainy, “Image Steganography by Mapping Pixels to Letters”, Journal of Computer Science, vol. 5, no. 1, (2009), pp. 33-38.

[19] H. Motameni, M. Norouzi, M. Jahandar and A. Hatami, “Labeling Method in Steganography”, World Academy of Science, Engineering and Technology, France, (2007).

[20] B. Ahuja, M. Kaur and M. Rachna, “High Capacity Filter Based Steganography”, International Journal of Recent Trends in Engineering, vol. 1, no. 1, (2009) May.

[21] M. TanvirParvez and A. Abdul-Aziz Gutub, “RGB Intensity Based Variable-Bits Image Steganography”, IEEE Asia-Pacific Services Computing Conference, (2008), pp. 1322-1327.

[22] A. M. Hamid and M. L. M. Kiah, “Novel Approach for High Secure and High Rate Data Hidden in the Image Using Image Texture Analysis”, International Journal of Engineering and Technology (IJET): 0975-4042, (2009).

[23] M. Chaumont and W. Puech, “DCT-Based Data Hiding Method To Embed the Color Information in a JPEG Grey Level Image”, 14th European Signal Processing Conference (EUSIPCO 2006), Florence, Italy, copyright by EURASIP, (2006) September 4-8.

[24] K. S. Babu, K. B. Raja, K. Kiran Kumar, T. H. Manjula Devi, K. R. Venugopal and L. M. Pataki, “Authentication of secret information in image steganography”, IEEE Region 10 Conference, TENCON- 2008, (2008) November, pp. 1-6.

[25] S. Ohyama, M. Niimi, K. Yamawaki and H. Noda, “Lossless data hiding using bit depth embedding for JPEG2000 compressed bit-stream”, Journal of Communication and Computer, vol. 6, no. 2, (2009) February.