International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

A Study and Review of Techniques of Spatial Steganography

Ravneet Kaur[1], Bhavneet Kaur[2]

[1]Department of Computer Science and Engineering, CGC Technical Campus, Jhanjeri (Mohali), Mohali, India

[2]Asst Professor, Department of Computer Science and Engineering, CGC Technical Campus, Jhanjeri (Mohali), Mohali, India

Abstract: ***Steganography is the technique of hiding secret information within any media like text, images, audio/video and protocol based network. This paper studies and reviews various data hiding techniques based on spatial domain image steganography like Least Significant Bit, Most Significant Bit, Parity check, Pixel value differencing. It elaborates an overview of steganography and illustrates the process of steganography. Various classifications of steganographic techniques are discussed. The image domain/ spatial domain techniques are discussed in detail. As privacy concerns continue to develop along with the digital communication domain, steganography will undoubtedly play a growing role in society. For this reason, it is important that we are aware of digital steganography technology and its implications. Equally important are the ethical concerns of using steganography and steganalysis. Steganography enhances rather than replaces encryption.***

Keywords: Data hiding, Steganography, Cover-media, Cover-object, Stego-image, Stego-key

1. Introduction

Steganography is the process of hiding the messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message. So steganography is the art and science of invisible communication as it hides the existence of communication information.

The word Steganography is originated from Greek words "Stegós" means "Covered", and "Grafia" means "Writing", which literally means "cover writing".

The idea of hiding information has a long history. In Histories the Greek historian Herodotus writes of a nobleman, Histaeus, who needed to communicate with his son-in-law in Greece. He shaved the head of one of his most trusted slaves and tattooed the message onto the slave's scalp. When the slave's hair grew back the slave was dispatched with the hidden message In the Second World War the Microdot technique was developed by the Germans in which information, especially photographs, was reduced in size until it was the size of a typed period. But now-a-days , with the change in technology steganography systems uses the multi-media objects like image, audio, video etc as cover-object because people often transmit or share the digital data over the internet via email or any other communication application.

Steganography is often confused with cryptography as they both are used to secure confidential information, but are different from each other as cryptography hides the content of information by encrypt and decrypt the data whereas steganography hides the existence of message/information.

Two other technologies are also closely related to the steganography that are watermarking and fingerprinting..

2. Overview of Steganography

To provide the overview of steganography, firstly some terms and concepts are explained and then its types are discussed.

A. Steganography terms and concepts

1) Steganography Terminologies

Steganography terminologies are as follows:-

- **Cover-Object**: Original objects which are used as a carrier for conceal the information.
- **Message:** Actual information which is used to be hide. Message could be a text or some other image.
- **Stego-object:** After embedding message or secret information into cover object is known as stego-object.
- **Stego-Key:** A key is used for embedding or extracting the messages from cover-object and stego-objects.

2) Steganography Concept

The aim of steganography is to hide a secret message within a cover-media in such a way that others cannot suspect the presence of the hidden message. Technically in simple words "steganography means hiding one piece of information within another".

Modern steganography uses the opportunity of hiding information into digital multimedia files(images,audio/video and text) and also at the network packet level.

Concealing the information into a media requires following elements

- Let C be the cover object that will hold the hidden data
- And M represents the secret message (M) that may be text, image or any type of data

- Suppose Fe be the stego function and its inverse is Fe-1.
- Also considers an optional stego-key (K) or password that may be used to hide and unhide the message.

The stego function operates over cover object and the message to be hidden, along with a stego-key (optionally) to produce a stego-object [3]. The diagrammatic view of steganographic operation is shown below.

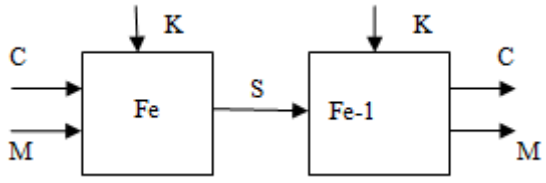

Figure 1: The Steganographic operation

B. Types of Steganography

Depending on the type of the cover object there are different types of steganographic techniques are used in order to conceal the data or to obtain security which are as follow.

1) Image Steganography:

In steganography, when taking the cover object as digita image to hide the data, then it is known as image steganography. Generally, in this technique pixel intensities are used to hide the information as the image is acollection of color pixels [19].

2) Network Steganography:

When taking cover object as network protocol, such as TCP, UDP, ICMP, IP etc, where protocol is used as carrier, is known as network protocol steganography. In the OSI network layer model there exist covert channels where steganography can be achieved in unused header bits of TCP/IP fields [19]

.

3) Video Steganography:

Video Steganography is a technique to hide any kind of files or information into digital video format such as H.264, Mp4, MPEG, AVI or other. Video is used as carrier for hidden information where video is a combination of pictures [19].

The schematic representation of different types of steganography is shown below.

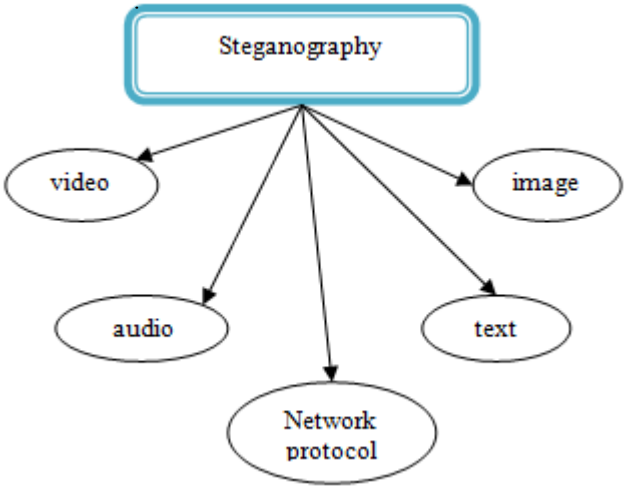

Figure 2: Digital Medium to Achieve Steganography

4) Audio Steganography:

When taking audio as a covert for hiding information then it is called audio steganography. It has become very significant medium due to voice over IP (VOIP) popularity. Audio steganography uses digital audio formats such as WAVE, MIDI, AVI MPEG or etc for steganography.

5) Text Steganography:

In text steganography the general technique is to use number of tabs, white spaces, capital letters, just like Morse code and etc to achieve information hiding.

3. Existing Steganographic Techniques

The steganographic algorithms can broadly be classified into two categories.

1. Spatial Domain Techniques
2. Transform Domain Techniques

Each of these techniques is covered in detail in the next two subsections.

A. Spatial Domain

These techniques use the pixel gray levels and their color values directly for encoding the bits of message. These techniques are some of the simplest schemes in terms of embedding and extraction complexity. The major drawback of these methods is amount of additive noise that creeps in the image which directly affects the Peak Signal to Noise Ratio and the statistical properties of the image. Moreover these embedding algorithms are applicable mainly to lossless image compression schemes like TIFF images. For lossy compression schemes like JPEG, some of the message bits get lost during the compression step.

The most common algorithm belonging to this class of techniques is the Least Significant Bit (LSB) Replacement method in which the least significant bit is used to represent the message bit of the binary representation of the pixel gray levels. This kind of embedding leads to an

addition of a noise of 0:5p on average in the pixels of the image where p is the embedding rate in bits/pixel. This kind of embedding also leads to an asymmetry and a grouping in the pixel gray values (0, 1); (2, 3); . . . (254,255). This asymmetry is exploited in the attacks developed for this technique as explained further in section 2.2. To overcome this undesirable asymmetry, the decision of changing the least significant bit is randomized i.e. if the message bit does not match the pixel bit, then pixel bit is either increased or decreased by 1. This technique is popularly known as LSB Matching. It can be observed that even this kind of embedding adds a noise of 0:5p on average. To further reduce the noise, [2] have suggested the use of a binary function of two cover pixels to embed the data bits. The embedding is performed using a pair of pixels as a unit, where the LSB of the first pixel carries one bit of information, and a function of the two pixel values carries another bit of information. It has been shown that embedding in this fashion reduces the embedding noise introduced in the cover signal.

In [4], a multiple base number system has been employed for embedding data bits. While embedding, the human vision sensitivity has been taken care of. The variance value for a block of pixels is used to compute the number base to be used for embedding. A similar kind of algorithm based on human vision sensitivity has been proposed by [5] by the name of Pixel Value Differencing. This approach is based on adding more amount of data bits in the high variance regions of the image for example near "the edges" by considering the difference values of two neighboring pixels. This approach has been improved further by clubbing it with least significant bit embedding in [6].

According to [15], "For a given medium, the steganographic algorithm which makes fewer embedding changes or adds less additive noise will be less detectable as compared to an algorithm which makes relatively more changes or adds higher additive noise." Following the same line of thought Crandall [7] have introduced the use of an Error Control Coding technique called "Matrix Encoding". In Matrix Encoding, q message bits are embedded in a group of $2^q - 1$ cover pixels while adding a noise of $1 - 2^{-q}$ per group on average. The maximum embedding capacity that can be achieved is $q/2^{q-1}$. For example, 2 bits of secret message can be embedded in a group of 3 pixels while adding a noise of 0:75 per group on average. The maximum embedding capacity achievable is 2/ 3 = 0:67 bits/pixel. F5 algorithm [16] is probably the most popular implementation of Matrix Encoding.

LSB replacement technique has been extended to multiple bit planes as well. Recently [3] has claimed that LSB replacement involving more than one least significant bit planes is less detectable than single bit plane LSB replacement. Hence the use of multiple bit planes for embedding has been encouraged. But the direct use of 3 or more bit planes leads to addition of considerable amount of noise in the cover image. [8] and [9] have given a detailed analysis of the noise added by the LSB embedding in 3 bit planes. Also, a new algorithm which uses a combination of Single Digit Sum Function and Matrix Encoding has been proposed. It has been shown analytically that the noise added by the proposed algorithm in a pixel of the image is 0:75p as compared to 0:875p added by 3 plane LSB embedding where p is the embedding rate.

B. Transform Domain

These techniques try to encode message bits in the transform domain coefficients of the image. Data embedding performed in the transform domain is widely used for robust watermarking. Similar techniques can also realize large-capacity embedding for steganography. Candidate transforms include discrete cosine Transform (DCT), discrete wavelet transform (DWT), and discrete Fourier transform (DFT). By being embedded in the transform domain, the hidden data resides in more robust areas, spread across the entire image, and provides better resistance against signal processing. For example, we can perform a block DCT and, depending on payload and robustness requirements, choose one or more components in each block to form a new data group that, in turn, is pseudo randomly scrambled and undergoes a second-layer transformation.

Modification is then carried out on the double transform domain coefficients using various schemes. These techniques have high embedding and extraction complexity. Because of the robustness properties of transform domain embedding, these techniques are generally more applicable to the "Watermarking" aspect of data hiding. Many steganographic techniques these domain have been inspired from their watermarking counterparts.

F5 [16] uses the Discrete Cosine Transform coefficients of an image for embedding data bits. F5 embeds data in the DCT coefficients by rounding the quantized coefficients to the nearest data bit. It also uses Matrix Encoding for reducing the embedded noise in the signal. F5 is one the most popular embedding schemes in DCT domain steganography, though it has been successfully broken.

The transform domain embedding does not necessarily mean generating the transform coefficients on a block of size 8 X 8 as done in JPEG compression techniques. It is possible to design techniques which take the transforms on the whole image [10]. Other block based JPEG domain and wavelet based embedding algorithms have been proposed in [11] and [17] respectively.

4. Classification of Spatial Domain Techniques

Spatial domain techniques can be classified into [7]:

1. Least significant bit (LSB)
2. Pixel value differencing (PVD)
3. Edges based data embedding method (EBE)
4. Random pixel embedding method (RPE)
5. Mapping pixel to hidden data method
6. Labelling or connectivity method
7. Pixel intensity based method
8. Texture based method

9. Histogram shifting methods

A. Least Significant Bit Method (LSB)

Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image in least significant bit position. The least significant bit is the 8 of the bytes inside an image. It is changed with bit of the secret message. When using a 24-bit image, a bit of each of the red, green and blue color components can be used, since they are each represented by a byte. In other words, one can store 3 In other words; one can store 3 bits in each pixel. An 800 × 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data[18].

For example to embedding information in a cover image. The least significant bit or the 8th bit of some or all of the bytes inside an image is changed to a bit of the secret message. When using a 24-bit image, a bit of each of the red, green and blue colour components can be used, since they are each represented by a byte. In other words, one can store 3 bits in each pixel. An 800 × 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data. For example a grid for 3 pixels of a 24-bit image can be as follows:

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

When the number 200, which binary representation is 11001000, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

(00101101 00011101 11011100)
(10100110 11000101 00001100)
(11010010 10101100 01100011)

Although the number was embedded into the first 8 bytes of the grid, only the 3 underlined bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size. Since there are 256 possible intensities of each primary colour, changing the LSB of a pixel results in small changes in the intensity of the colours. These changes cannot be perceived by the human eye - thus the message is successfully hidden. With a well-chosen image, one can even hide the message in the least as well as second to least significant bit and still not see the difference.

In the above example, consecutive bytes of the image data – from the first byte to the end of the message – are used to embed the information. This approach is very easy to detect. A slightly more secure system is for the sender and receiver to share a secret key that specifies only certain pixels to be changed. Should an adversary suspect that LSB steganography has been used, he has no way of knowing which pixels to target without the secret key.

In its simplest form, LSB makes use of BMP images, since they use lossless compression. Unfortunately to be able to hide a secret message inside a BMP file, one would require a very large cover image. Nowadays, BMP images of 800 × 600 pixels are not often used on the Internet and might arouse suspicion. For this reason, LSB steganography has also been developed for use with other image file formats.

For Example of imagery steganography is

Figure 3: Example of imagery steganography. Left hand side image is the original cover image, whereas right hand side does embedding a text file into the cover image make the stego image.

General Advantages of LSB technique are:

- There is less chance for degradation of the original image.
- More information can be stored in an image.

Disadvantages of LSB technique are:

- Less robust, the hidden data can be lost with image manipulation.
- Hidden data can be easily destroyed by simple attacks.

B. Pixel value differencing Method (PVD)

The pixel-value differencing (PVD) scheme uses the difference value between two consecutive pixels in a block to determine how many secret bits should be embedded. This scheme provides high imperceptibility to the stego image by selecting two consecutive pixels and designs a quantization range table to determine the payload by the difference value between the consecutive pixels[18].

C. Parity Checker Method (PCM)

The Parity Checker Method (PCM) method uses the concept of odd and even parity for insertion and retrieval of message. In this method even value can be inserted at a pixel position to identify pixel has 1(odd) parity bits. It can be identical odd value insert at a pixel; if the pixel should be 0 (even) parity . If the close similarity parity do not exist at a pixel position for odd or even, then the pixel location can be added and subtracted such that the change in the image quality will not be Visible (to the human visual system)[18].

D. Moderate Significant Bit (MSB)

Moderate significant bit (MSB) [19] insertion is a common, simple approach to embedding information in a cover image at moderate significant bit position. Already we have least significant bit technique in which data is stored at least significant bit position but problem arises in case when image is compressed, LSB of image is discarded. So the receiver won't be able to extract the data. To overcome this problem we have moderate significant bit technique in which secret data is embedded at 4th, 3rd or 2nd moderately-significant-bit of pixel of an image [18].

E. Histogram shifting method

Histogram-based data hiding is another commonly used data hiding method. Data hiding can be done by using the difference value of adjacent pixels. It exploits the correlation between adjacent pixels that eventually results in a compact histogram that is characterized by a normal Gaussian distribution Instead of taking the whole image, the image is divided into blocks of where the residual image is calculated using adjacent pixels' difference. Then the secret data is embedded into the residual values, followed by block reconstruction.

5. Characteristics of Image Steganography

Generally image steganography is categorized in following aspects

- **High Capacity:** Maximum size of information that can be embedded into image represents its capacity and an digtal image has high capacity to hide the message.
- **Perceptual Transparency:** After hiding process into cover image, perceptual quality will be degraded into stego-image as compare to cover- image.
- **Robustness:** After embedding, data should stay intact if stego-image goes into some transformation such as cropping, scaling, filtering and addition of noise.

And it is represented as:

Figure 4: Different Aspects of Image Steganography

- **Temper Resistance:** It should be difficult to alter the message once it has been embedded into stego-image.
- **Computation Complexity:** How much expensive it is computationally for embedding and extracting a hidden message?

6. Conclusion

In this paper, we talked about steganography and its types. First we had a look at image, audio, video, network and text steganography and Then we got into steganography techniqes and then different spatial steganographic techniques are explained and at the end, the characteristics of steganography are given and in the next paper, we can combine it with another technique to utilize the hybrid combination so that we can increase the hiding capacity.

Acknowledgment

The author's wants to heartily thank their guide, Er. Bhavneet Kaur- Asst. Prof. – CGCTC, Punjab technical university for their critique discussion, constant encouragement, valuable suggestion and timely guidance.

References

[1] N. F. Johnson, and S. Jajodia, "Steganography: Seeing the Unseen", IEEE Computer, Feb. 1998, pp. 26-34.
[2] J. Mielikainen, "LSB Matching Revisited", IEEE Signal Processing Letters , vol. 13, no. 5, May 2006, pp. 285 - 287
[3] A. Ker, "Steganalysis of Embedding in Two Least-Significant Bits", IEEE Trans. on Information Forensics and Security, vol. 2, no. 1, March 2007, pp. 46-54.
[4] X. Zhang and S. Wang, "Steganography using multiple-base notational system and human vision sensitivity, IEEE Signal Processing Letters, vol. 12, Issue 1, Jan. 2005, pp. 67-70.
[5] D. C. Wu and W.H. Tsai, "A Steganographic method for images by pixel-value differencing", Pattern Recognition Letters, vol. 24, Jan. 2003, pp. 1613–1626.
[6] 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. Vision, Image and Signal Processing, vol. 152, Oct. 2005, pp. 611-615.
[7] R. Crandall, "Some Notes on Steganography", Posted on Steganography Mailing List, 1998.
[8] A. Sur, P. Goel, and J. Mukhopadhyay, "A Spatial Domain Steganographic Scheme for Reducing Embedding Noise", in Proc. 3rd International Symposium on Communications, Control and Signal Processing (ISCCSP 2008), St. Julians, Malta, 12-14 March, pp. 1024 - 1028.
[9] A. Sur, P. Goel and J. Mukhopadhyay, "A SDS based Steganographic scheme for reducing Embedding Noise", 15th International Conference on Advanced Computing and Communication, (ADCOM-2007), Guwahati, India, 18-21 Dec., pp. 771-775.

[10] I. J. Cox, J. Kilian, F.T. Leighton, T. Shamoon, "A Secure, Robust Watermark for Multimedia", in Proc. of the 1st Int. Workshop on Information Hiding, Cambridge, U.K, 30th May - 1 June 1996 ,pp. 185-206.
[11] E. Koch and J. Zhao, "Towards Robust and Hidden Image Copyright Labeling", in Proc. IEEE Workshop on Nonlinear Signal and Image Processing, Halkidiki, Greece, June. 1995, pp. 452-455.
[12] I. Avcibas, N. Memon, and B. Sankur, "Steganalysis using Image Quality Metrics", IEEE Trans. on Image Processing, vol. 12, Feb 2003, pp. 221-229.
[13] H. Farid, and L. Siwei, "Detecting Hidden Messages Using Higher-Order Statistics and Support Vector Machines", in Proc. 5th Int. Workshop on Information Hiding, Noordwijkerhout, The Netherlands, 7-9 Oct. 2002, pp. 340-354.
[14] J. Fridrich, "Feature-Based Steganalysis for JPEG Images and its Implications for Future Design of Steganographic Schemes", in Proc. 6th Int. Workshop on Information Hiding, Toronto, Canada, 23-25 May 2004, pp. 67-81.
[15] J. Fridrich, M. Goljan, P. Lisonek, and D. Soukal, "Writing on wet paper", IEEE Trans. on Signal Processing, Special Issue on Media Security, vol. 53, Oct. 2005, pp. 3923-3935.
[16] A.Westfeld, "High capacity despite better steganalysis (F5 - a steganographic algorithm)", in Proc. 4th Int. Workshop on Information Hiding, Pittsburgh, PA, USA, pp. 289-302, 25- 27 April 2001.
[17] X.G. Xia, C.G. Boncelet, and G.R. Arce, "A multiresolution watermark for digital images", IEEE Int. Conf. on Image Processing, Washington, DC, USA, 26-29 Oct. 1997.
[18] Igloo Jain1, P.S. Mann2, "Study and Review of Data Obscuring Techniques based on Spatial Image Steganography," International Journal of Engineering Science & Advanced Technology Volume-4, Issue-3, 280-284.
[19] Mehdi Hussain and Mureed Hussain, "A Survey of Image Steganography Techniques", International Journal of Advanced Science and Technology Vol. 54, May, 2013.
[20] Ronak Karimi, Mehdi Hariri and Masoud Nosrati," An introduction to steganography methods", World Applied Programming, Vol (1), No (3), August 2011. 191-195 ISSN: 2222-2510 ©2011 WAP journal.
[21] Soumyendu Das, Subhendu Das, Bijoy Bandyopadhyay and Sugata Sanyal, "Steganography and Steganalysis: Different Approaches", International Journal of Computers, Information Technology and Engineering (IJCITAE), Vol. 2, No 1, June, 2008, Serial Publications.
[22] T Morkel, JHP Eloff and MS Olivier, "An Overview of Image Steganography," in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, June/July 2005 (Published electronically)
[23] 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.
[24] 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.
[25] S. Channalli and A. Jadhav, "Steganography an Art of Hiding Data", International Journal on Computer Science and Engineering, IJCSE, vol. 1, no. 3, (2009).
[26] 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.
[27] 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