www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 7 July, 2014 Page No. 7341-7345

An Overview of Image Steganography Techniques

Amritpal Singh[1] , Satinder Jeet Singh[2]

[1]Guru Kashi University, Department of CSE,
Talwandi Sabo, Punjab, India
amritranu12@gmail.com

[2]Guru Kashi University, Department of CSE,
Talwandi Sabo, Punjab, India
Lali399@gmail.com

Abstract: ***Steganography is becoming an important area of research in recent years. It is an art and the science of embedding information into cover image viz., text , video, audio or multimedia content for military communication, authentication and many other purposes. It deals with the ways of hiding the communication message and its existence from the unintended user. In image steganography, secret communication is achieved through embedding a message into an image as cover file and generates a stego-image having hidden information. There are several image steganography techniques are used each have its pros and cons. This paper discusses various image steganography techniques such as Least significant bit, Discrete wavelet transformation, Pixel value differencing, Discrete cosine transformation, Masking and filtering etc.***

Keywords: Steganography, stego-image, Spatial domain methods, Transform domain techniques, Distortion techniques**.**

1. Introduction

With the development of computer and the rise of internet, the information is easily transferred from one location to another. But in some cases it is needed to keep the information must travel secretly. One of the grounds discussed in information security is the exchange of information through the cover media. Many different techniques like cryptography, encryption etc. have been developed to encrypt and decrypt information in order to keep the contents of message secret. But steganography have an advantage over these techniques, it keeps the existence of the message secret as well as secret the information [1].

Steganography is the process of hiding the one information into other sources of information like text, image, audio or video file, so that it is not visible to the natural view. Steganography is the art and science of invisible communication of messages by hiding information into other information. In image steganography the information is embedded into innocent looking cover image and the message implanted image is called a stego-image [2]. In history there are several secret communication methods are used like undetectable inks , microdots , character organization , digital signatures, spread spectrum etc. that conceal the existence of information. But now day's digital approaches are used so the steganography is mostly used on digital data. There are various steganography techniques used based on the information to be hidden. In this paper we describe brief review of several image steganography techniques.

2. Image Steganography Techniques

Image steganography is the process of hiding the sensitive information into the cover image with no degradation of the image and providing better security so that unauthorized user cannot access the hidden information. Figure 1 shows the various image steagnography techniques. Image steganography techniques are broadly classified into following-

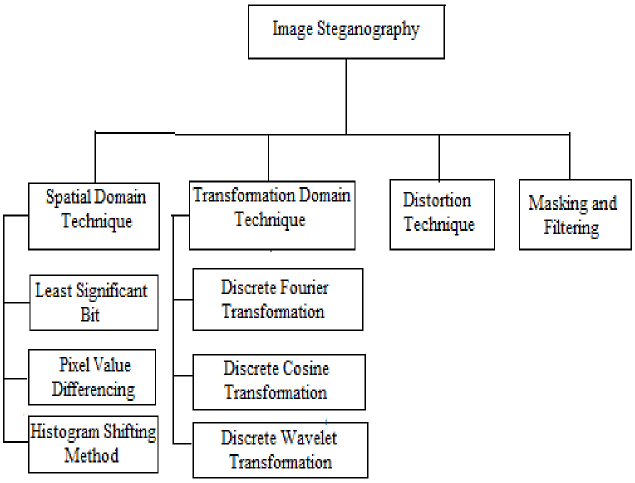
Image Steganography
Spatial Domain Technique
Transformation Domain Technique
Distortion Technique
Masking and Filtering
Least Significant Bit
Pixel Value Differencing
Histogram Shifting Method
Discrete Fourier Transformation
Discrete Cosine Transformation
Discrete Wavelet Transformation

Figure 1: Various Image Steganography Techniques.

2.1 Spatial Domain Methods

In spatial domain steganography method, for hiding the data some bits are directly changed in the image pixel values. Most used method in this category is least significant bit .Spatial domain techniques are classified into following-

2.1.1 Least Significant Bit (LSB)

LSB insertion is a common and simple approach for embedding information in a cover file. Digital images used as cover file are mainly of two types- 24-bit images and 8-bit images. In 24-bit images we can embed three bits of information in each pixel. In 8-bit images, one bit of information can be hidden into images. After applying the LSB algorithm the image obtained having secret message is called stego-image. LSB technique as the name implies replaces the least significant bit of the pixel with the information to be hidden. Since LSB is replaced there is no effect on cover image and hence unintended user will not get the idea that some message is hidden behind the image [3].However a little change in level of intensity of original and modified pixel, but it cannot be detected visually.

The following example explain how the letter A can be hidden into the three pixels i.e. eight bytes of an 24-bit image.

Pixels: (00100111 11101011 11001010)
(00100111 11011000 10101001)
(11001000 00110111 11011001)

A: 010100111

Result: (0010011$\underline{0}$ 11101011 11001010)
(00100111 11011000 1010100$\underline{0}$)
(1100100$\underline{1}$ 00110111 11011001)

The main advantage of LSB method is easy to implement and high message payload and there is less chance of degradation of quality of original image. The disadvantages are that the information can be easily extracted or destroyed by simple attacks and it is less robust, vulnerable to image manipulation.

2.1.2 Pixel Value Differencing (PVD)

In PVD method, gray scale image is used as a cover image with a long bit-stream as the secret data [4].It was originally proposed to hide secret information into 256 gray valued images. The method is based on the fact that human eyes can easily observe small changes in the smooth areas but they cannot observe relatively larger changes at the edge areas in the images. PVD uses the difference between the pixel and its neighbor to determine the number of embedded bits. The larger the difference amount is, the more secret bits can be embedded into the cover image.

It scans the image starting from the upper left corner in a zigzag manner. Then, it simply divides the cover image into number of blocks where each block consists of two consecutive non-overlapping pixels. The difference of the two pixels in the block is used to categorize the smoothness properties of the cover image. A small difference value indicates that the pixels are at smooth area whereas pixels around edge area have large difference values. The data is embedded mostly in the edge areas because the changes of the pixel values are more easily noticed by human eyes. Therefore, in PVD method a range table has been designed with n contiguous ranges Rk (Where k=1,2,3……n) where the range is between 0 to 255.The lower and upper bound are denoted as Ik and Uk respectively, then Rk €[Ik ,Uk]. The width Wk and Rk is calculated by WK= Uk-Ik+1 which decides how many bits can be hidden in pixel block. When extracting the embedded data from stego-image original range table is required.

This method is proposed to enhance the embedding capacity without improper visual changes in stego-image. But the disadvantage of the method is 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 also weak security performance due to non-adaptive quantization, embedding some information in smooth areas etc.

2.1.3 Histogram Shifting Method

Histograms are used for graphical representation of image. It represents the pixel value and density at a particular pixel. It plots the pixel for each part of the image. A histogram is useful to identify pixel distribution, density of colors and tonal distribution. A histogram provides the highest and lowest pixel values in graph. Histogram shifting is the technique which is used to modify or to extract a certain group of pixels from a image [11]. In histogram the highest value is called maxima and the lowest value is called minima. When the pixel value is modified for embedding process it should not cross the minima and maxima limit. There are several algorithm which supports histogram functionality in order to manipulate the image. The number of the pixels constituting the peak in the histogram of a cover image is equal to the hiding capacity because a single peak in a cover image is used [5].

Several histogram shifting techniques are enhanced by dividing the cover image into blocks to generate a respective peak for each block which provides more hiding capacity into the multiple blocks.

2.2 Transformation Domain Technique

Transformation domain methods hides message in the significant areas of the cover image which makes them more robust against various image processing operations like compression, cropping and enhancement. There are many transformation domain method exists. The basic approach used for hiding information is to transform the cover image, tweak the coefficients and then insert the transformation. Transformation domain techniques are broadly classified into following:

2.2.1 Discrete Fourier Transformation (DFT) Technique

In DFT all the insertion of hidden message is done in the frequency domain. It is a more complex way of hiding message into frequency domain of the image. The Discrete Fourier Transform of spatial value f(x,y) for an image of size M × N is defined in equation for frequency domain transformation [6].

$$f(u,v) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y)\; e^{-12\nabla \;\; \frac{ux}{M}+\frac{vy}{N}} \qquad (1)$$

Similarly inverse discrete fourier transform (IDFT) is used to convert frequency component of each pixel value to the spatial domain value and the equation for transformation from frequency to spatial domain is

$$f(x,y) = \frac{1}{\sqrt{MN}} \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} f(u,v)\ e^{12V\ \frac{ux}{M}+\frac{vy}{N}} \tag{2}$$

When DFT is applied it converts the cover image from spatial domain to frequency domain and each pixel in spatial domain is transformed into two parts: real and imaginary part. The hidden message bits are inserted in real part of frequency domain excluding first pixel. After embedding IDFT is performed frequency domain converted into spatial domain. During the extraction or decoding of the message image from spatial domain is transformed to frequency domain. After applying DFT and extraction algorithm the original source image is retrieved.

2.2.2 Discrete Cosine Transformation (DCT) Technique

The DCT transforms the image from spatial to frequency domain and separates the image into spectral sub-bands with respect to visual quality of the image, i.e. low, middle and high frequency components as shown in fig. 2. Here F_L and F_H is used to denote the lowest frequency components and higher frequency components respectively. F_M is used as embedding region to provide additional resistance to lossy compression techniques, while avoiding significant modification of the cover image [13].

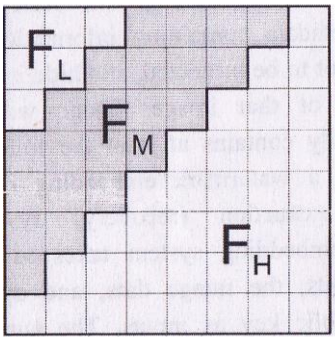

Figure 2: DCT Regions

It is used in the JPEG compression algorithm to transform successive 8 × 8 pixel blocks of the image into 64 DCT coefficients each in frequency domain. Each DCT coefficient F(u,v) of an 8 × 8 pixel block of image pixels f(x,y) is calculated by

$$F(u,v) = \frac{1}{4} C(u)\, C(v) \left[\sum_{x=0}^{7} \sum_{y=0}^{7} f(x,y) * \cos \frac{(2x+1)u\pi}{16}\ \cos \frac{(2y+1)u\pi}{16} \right] \tag{3}$$

Where $C(x)=1/\sqrt{2}$ when x=0 and C(x)=1 otherwise. The following quantization operation is performed after calculating the coefficients:

$$F^Q(u,v) = \left\lfloor \frac{F(u,v)}{Q(u,v)} \right\rfloor \tag{4}$$

Where Q(u,v) is a 64-element quantization table. The hidden message is embedded into the redundant bits, i.e. the least significant bits of the quantized DCT coefficients. A modification of a single DCT coefficient affects all 64 image pixels. In DCT based techniques, the secret data is embedded in the carrier image for DCT coefficients lower than the threshold value [7].Pixels having DCT coefficient value below threshold are known as potential pixels. Hence to avoid the visual distortion in image the potential pixels are used for data hiding.

2.2.3 Discrete Wavelet Transformation (DWT) Technique

The Discrete Wavelet Transformation Technique is the new idea in the applications of the wavelets. The standard technique of storing in the least significant bit of pixel still applies but the only difference is the information is stored into the wavelet coefficients, instead of changing the bits of actual pixels in the image. DWT have advantage over Fourier Transformation, it performs local analysis and multi-resolution analysis. Wavelet analysis can reveal signal aspects like discontinuities, breakdown points etc. more clearly than Fourier Transformation. The DWT splits the signal into two parts- high and low frequency. The information about the edge component is in high frequency part and the low frequency part is further split again into high and low frequency parts. A one dimensional DWT uses filter bank algorithm [12] and the information is convolved with high pass filter and low pass filter. Human eyes are less sensitive to high frequency so high frequency components are used for steganography.

In two dimensional applications, for each level of decompositions, we first perform the DWT in the vertical direction, followed by DWT in the horizontal direction [8]. As we can see in the fig.3, the first level of decomposition results into four classes or sub-band: approximate band(LL1), vertical band(LH1), horizontal band(HL1), diagonal detail band(HH1). The approximation band consists of low frequency wavelet coefficients which contains the significant part of the spatial domain image. The other bands consist of high frequency coefficients, which contain the edge details of the spatial domain image. For each successive level of decomposition, the approximate band of the previous level is used as the input. In second level of decomposition, the DWT is applied on LL1 band which decomposes it into four sub-bands: LL2, LH2, HL2 and HH2.

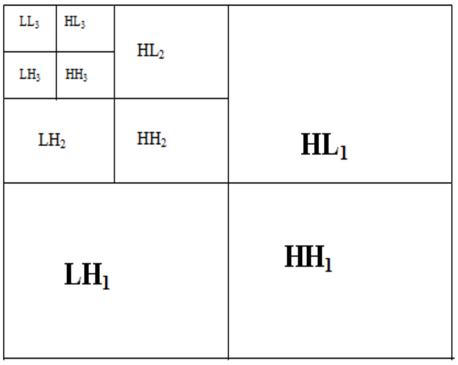

Figure 3: Three phase decomposition using DWT

2.3 Distortion Technique

In distortion techniques the information is stored by signal distortion. These techniques require the knowledge of the original cover image during the decoding process. The encoder applies series of modifications to the cover image and the decoder functions to check for the various differences between the original cover image and distorted cover image to recover the secret message. Using this technique, a stego object is created by the sender by applying a sequence changes to the cover image. This sequence of modification corresponds to a specific secret message required to transmit. The message is encoded at pseudo- randomly chosen pixels in the image. If the stego-image differ from the cover image at the given message pixel, the message bit is a “1” otherwise “0”. The sender can modify the “1” value pixels in such a way that the statistical properties of the image should not affected.

The receiver must have access to the original cover for retrieving the message; it limits the benefits of this technique. In every steganography techniques, the cover image should never be used more than once. If an attacker has access to the cover image the secret message can be easily detected by attacker from the stego-image by cropping, scaling or rotating it. In some cases, if the message is encoded with error correcting information, the change can even be reversed and the original message can be recovered [9].

2.4 Masking and Filtering

This technique is usually applied on 24 bits or grayscale images, uses a different approach to hiding a message. It hides information by marking an image, similar to paper watermarks. This technique actually extends an image data by masking the secret data over the original data as opposed to hiding information inside of the data [10]. These techniques embed the information in the more significant areas of the image than just hiding it into noise level. Watermarking techniques can be applied on the image without the fear of its destruction due to lossy compression as they are more integrated into the image.

This method is more robust than LSB modification with respect to compression and different kinds of image processing since the information is hidden into the visible parts of the image. The main drawback of this technique is that it can only be used on gray scale images and restricted to 24-bit images.

3 Conclusion

Image steganography is the way of secret communication through the digital images. In this paper we have discussed about steganography and several image steganography techniques. Every technique have its own importance and use for hiding the data in image. After the study of the all techniques it is easy to decide a particular one for secret communication.

References

[1] Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav, “Steganography Using Least Significant Bit Algorithm”, International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 3, pp. 338-341, 2012.

[2] Manu Devi, Nidhi Sharma, “ Improved Detection of Least Significant Bit Steganography Algorithm in Color and Gray Scale Images”, IEEE Proceedings of RACES UIET Panjab University Chandigarh, 2014.

[3] Nadeem Akhtar, Pragti Johri, Shabaaz Khan, “Enhancing the Security and Quality of LSB based Image Steganography”, IEEE International Conference on Computer Intelligence and Computer Networks(CICN), pp.385-389, 2013.

[4] 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.

[5] Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, and Wei Su, “ Reversible Data Hiding”, IEEE Transactions on Circuits and Systems for Video Technology, vol. 16(3), pp. 354–362, 2006.

[6] Inderjeet Singh, Sunil Khullar, Dr.S.C.Laroiya, “DFT Based Image Enhancement And Steganography”, International Journal of Computer Science and Communication Engineering, Vol.2, Issue 1, February, 2013.

[7] Hardik Patel, Preeti Dave, “Steganography Technique Based on DCT Coefficients”, International Journal of Engineering and Applications(IJERA), Vol.2, Issue 1, pp.713-717, 2012.

[8] Parul, Manju, Dr. Harish Rohil, “Optimized Image Steganography Using Discrete Wavelet Transform”, International Journal of Recent Development in Engineering and Technology (IJRDET), Vol. 2, Issue 2,2014.

[9] Mehdi Hussain, Mureed Husain, “A Survey of Image Steganography Techniques”, International Journal of Advanced Science and Technology(IJAST), Vol.54, May , 2013.

[10] Jammi Ashok, Y.Raju, S.Munishankaralah, K.Srinivas, “Steganography: An Overview”, International Journal of Engineering Science and Technology (IJEST), Vol.2 (10), 2010.

[11] Sapna Saini, Brindha K., “Improved Data Embedding into Images Using Histogram Shifting”, International Journal of Emerging Research in Management & Technology (IJERMT), Vol. 3, Issue 5, 2014.

[12] Barnali Gupta Banik, Prof. Samir K. Bandyopadhyay, “A DWT Method for Image Steganography”, International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), Vol. 3, Issue 6, 2013.

[13] J.R. Hernandez, M. Amado, and F. Perez Gonzalez, “DCT- Domain Watermarking Techniques for Still Images: Detector Performance Analysis and a New Structure,” IEEE Transactions on Image Processing, Vol. 9, pp. 55-68, 2000.

Author Profile

Amritpal Singh received his B.Tech degree in Computer Engineering from Punjabi University Patiala in 2012. Currently he is pursuing M.Tech degree in Computer Science from Guru Kashi University, Talwandi Sabo, Bathinda (Punjab). His research interests include Image Processing and Data Mining.

Satinderjeet Singh received his B.Tech degree from GGSCET, Talwandi Sabo and M.Tech from Punjabi University Patiala. Currently he is working as Assistant Professor in department of computer science at Guru Kashi University, Talwandi Sabo.