MATEC Web of Conferences **57**, 02003 (2016) DOI: 10.1051/matecconf/20165702003
ICAET-2016

A Survey on different techniques of steganography

Harpreet Kaur[1, a] and Jyoti Rani[1]

[1]*CSE Department, GZSCCET Bathinda, Punjab, India*

Abstract - Steganography is important due to the exponential development and secret communication of potential computer users over the internet. Steganography is the art of invisible communication to keep secret information inside other information. Steganalysis is the technology that attempts to ruin the Steganography by detecting the hidden information and extracting. Steganography is the process of Data embedding in the images, text/documented, audio and video files. The paper also highlights the security improved by applying various techniques of video steganography.

1 Introduction

A Steganography is the science or art of hide the messages into other sources of information like text/documents, audios, videos and images etc. so that it is not visible to unauthorized users. It is known as invisible communication. A Steganography system made up of three components: cover-object means which hides the secret message, the secret message and the stego-object means which is the cover object with message embedded inside it. Video consist of collection of image. A digital image is represented by using a 2-D matrix of the color intestines at each grid points. The gray images use 8 bits, whereas colored utilizes 24 bits to describe the color model, such as RGB model. The different types of techniques are used in the Steganography is to hide the messages in the cover images. These techniques provide the best challenge for digital forensics investigations. Before transmission the message is encrypted and with the help of a key, the message is decrypted at receiver side. Nobody can describe the content of the key except one having the key. The message is known as the plain text and message in the encrypted form is known as the cipher text. At the time of transmission the message is protected. After decryption, the message becomes

Unprotected and it can be copied and distributed. The Secret or encrypted message may be a text file, a cipher text, audio or images [1].

Applications for a data-hiding scheme include in-band captioning, communication conversion, image tamper Proofing, revision tracking, enhance robustness of image search engines and smart Ids or identity cards where individual's details are embedded in their photographs.

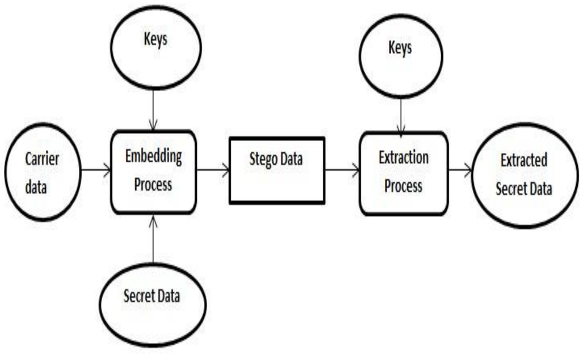


Figure 1 . Steganography Process

1.1 Cryptography and Steganography

Cryptography made up of Krypto's means hidden and Graphene means Writing. Steganography consist of Stegano's means Covered and Graphene means Writing. The Cryptography scrambles the messages so it is not easily understandable. Steganography diverge from cryptography.

Harpreet Kaur: kaurharpreet732@gmail.com

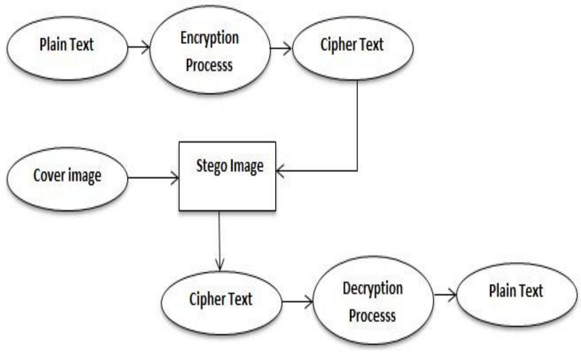


Figure 2. Combination of Cryptography and Steganography

The Goal of cryptography is to provide the secure communication by alter the data into a form that an eavesdropper cannot easily understand. A good steganography technique aims at three parameters i.e. capacity means the maximum information that can be hide inside the cover image , visual quality of stego-image cannot be change i.e. imperceptibility, robustness. Steganalysis is the technology that attempts to defeat the Steganography by detecting the hidden information and extracting [2].

2 Steganography in Digital Mediums

There are many Steganography techniques depending on the type of the cover object which are followed in order to obtain the security.

2.1 Text Steganography: The techniques in text steganography are number of tabs, white spaces, capital letters, just like Morse code is used to achieve information hiding.

2.2 Image Steganography: Taking the cover object as image in steganography is called image steganography. In this technique pixel intensities are used to hide the information. The 8 bit and 24 bit images are common. The image size is large then hides the more information. Larger images may require compression to avoid detection and the Techniques are LSB insertion and Masking and filtering [3]

Figure 3. Example of Image Steganography

2.3 Network Steganography: Taking cover objects as network protocol i.e. TCP, UDP, IP etc, where protocol is used as carrier is called network protocol steganography. In the OSI model there exist the channels where steganography can be achieved in unused header bits of TCP/IP fields

2.4 Audio Steganography: Taking audio as carrier for information hiding is called audio steganography. It is very important medium due to voice over IP (VOIP) popularity. It is used for digital audio formats such as WAVE, MIDI, and AVI MPEG for steganography. The methods are LSB coding, echo hiding, parity coding etc [4].

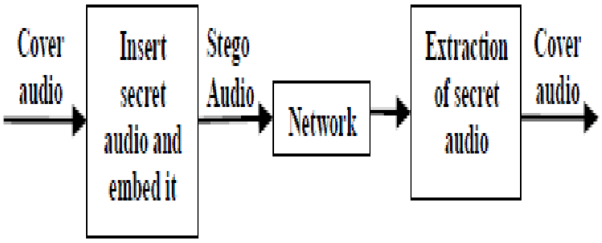


Figure 4. Example of Audio Steganography

2.5 Video Steganography: It is a technique to hide any type of files or information into digital video format. Video i.e. the combination of pictures is used as carrier for hidden information. The discrete cosine transform i.e. DCT change the values e.g., 8.667 to 9 which is used to hide the information in each of the images in the video, which is not justified by the human eye. It is used such as H.264, Mp4, MPEG, AVI or other video formats [5].

DOI: 10.1051/matecconf/20165702003

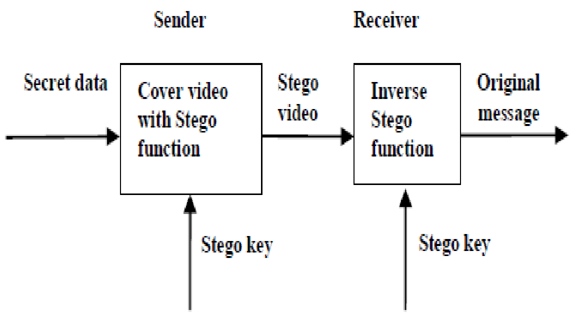


Figure 5. Example of Video Steganography

3 Techniques of Steganography

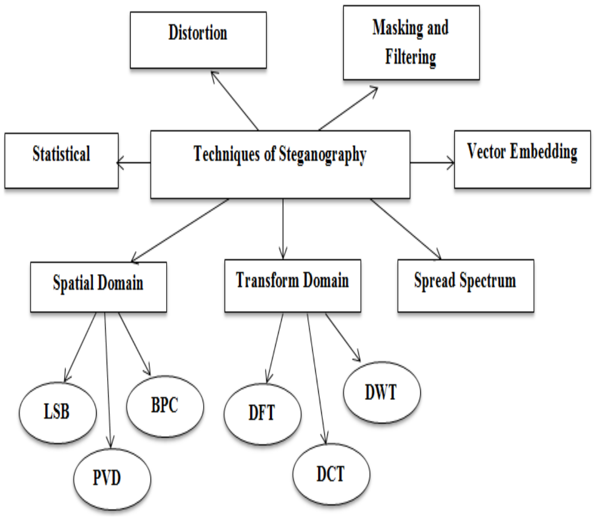


Figure 6 . Techniques of Steganography

3.1 Spatial Domain Methods: spatial domain Steganography technique refers to methods in which data hiding is performed directly on the pixel value of cover image in such a way that the effect of message is not visible on the cover image. The spatial domain methods are classified as following:

3.1.1 LSB: LSB is one the technique of spatial domain methods. LSB is the simple but susceptible to lossy compression and image manipulations. Some bits are change directly in the image pixel values in hiding the data. Changes in the value of the LSB are imperceptible for human eyes. Eg:

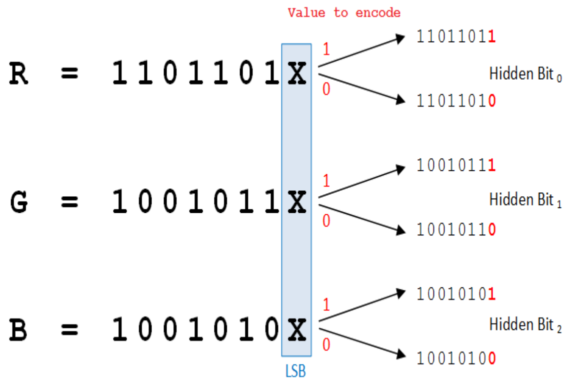


Figure 7. Example of LSB Conversion

In the spatial domain LSB technique there is less chance for degradation of the original image, more information can be stored in an image and covert communication of sensitive data.

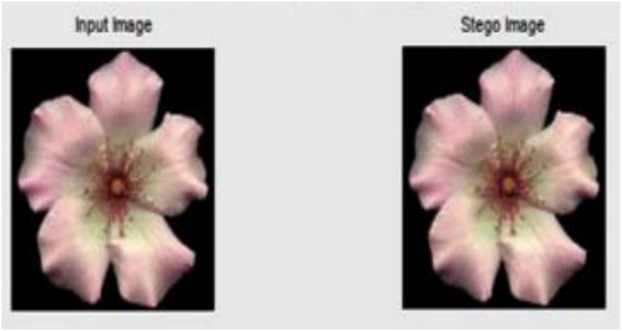


Figure 8 . LSB Conversion

3.1.2 Pixel Value Differencing: To embedding the data in PVD the two consecutive pixels are selected. Whether the pixels are determine from smooth area or an edge area. Payload is determined by calculating the difference between two regular pixels.

3.1.3 BPC: The Binary Pattern complexity approach is used to measure the noise factor in the image complexity. The noisy portion is replaced by binary Pattern and it is mapped from the secret data. The image will remain same when the reverse noise factor will determined.

3.2 Transform Domain Steganography: It is a more complex way to hides the information in an image. The different algorithms and transformations are used to hide information in the images. In the frequency domain, the process of embedding data of a signal is much stronger than embedding principles that operate in the time domain. The transform domain techniques over the spatial domain techniques is to hides the information in the images that are less exposed to compression, image processing and cropping. Some transform domain techniques are not depending on the image format and they run the lossless and lossy format conversions. Transform domain techniques are classified into various categories such as Discrete Fourier transformation (DFT), discrete cosine transformation (DCT), Discrete Wavelet transformation (DWT)

3.2.1 The Discrete Fourier Transform (DFT):

Discrete Fourier transform is the transform that are purely discrete: discrete-time signals are converted into discrete number of frequencies. DFT converts a finite list of equally spaced samples of a function into the list of coefficients of a finite combination of complex sinusoids ordered by their frequencies. It can be said to convert the sampled function from its original domain often time or position along a line to the frequency domain. The Discrete Time Fourier transforms uses the discrete time but it converts into the continuous frequency. The algorithm for computing the DFT is very fast on modern computers. This algorithm is known as Fast Fourier Transform i.e. FFT and it produces the same result as of the DFT by using the Inverse Discrete Fourier Transform.

3.2.2 The Discrete Cosine Transform (DCT): This method is similar to the Discrete Fourier Transform. DCT transform the signal or image from spatial domain to the frequency domain. The mathematical transforms convert the pixels in such a way as to give the effect of “spreading” the location of the pixel values over part of the image. The DCT is used in steganography as the Image is broken into 8×8 pixel blocks and transforms these pixel blocks into 64 DCT. Working from left to right, up to down, the DCT is applied to each block. Through quantization table each block is compressed to scale the DCT coefficients and message is embedded in DCT coefficients. The array of compressed blocks that constitute the image is stored in drastically reduced the amount of space. When desired, image is reconstructed through decompression, a process that uses the Inverse discrete cosine transform i.e. IDCT [6].

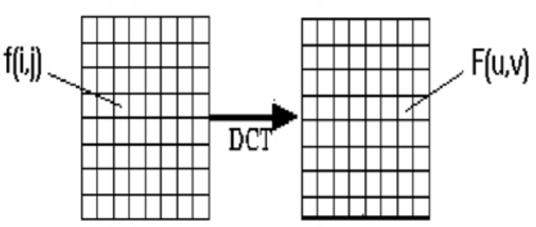


Figure 9 . Process of DCT

3.2.3 Discrete Wavelet Transform (DWT):

It is used to transform the image from a spatial domain to the frequency domain. In the process of steganography DWT identifies the high frequency and low frequency information of each pixel of the image. It is mathematical tool for decomposing an image hierarchically. It is mainly used for processing of non-stationary signals. The wavelet transform is based on small waves, Known as wavelets, of different frequency and limited duration. It provides both frequency and spatial description of the image. Wavelets are created by translations and dilations of a fixed function are known as mother wavelet. DWT performs in one dimension and in the two dimensional plane. The DWT is the accurate model than the DFT or the DCT and it is multi resolution description of the image. The current image compression standard JPEG 2000 is based on the wavelet transforms [7].

3.3 Vector Embedding: A vector embedding method that uses robust algorithm with codec standard (MPEG-1 and MPEG -2) .This method embeds audio information to pixels of frames in host video. It is based on the H.264/AVC Video coding standard. The algorithm designed a motion vector component feature to control embedding, and also to be the secret carrier. The information embedded will not significantly affect the video sequence's visual invisibility and statistical invisibility. The algorithm has a large embedding capacity with high carrier utilization, and can be implementing fast and effectively [8].

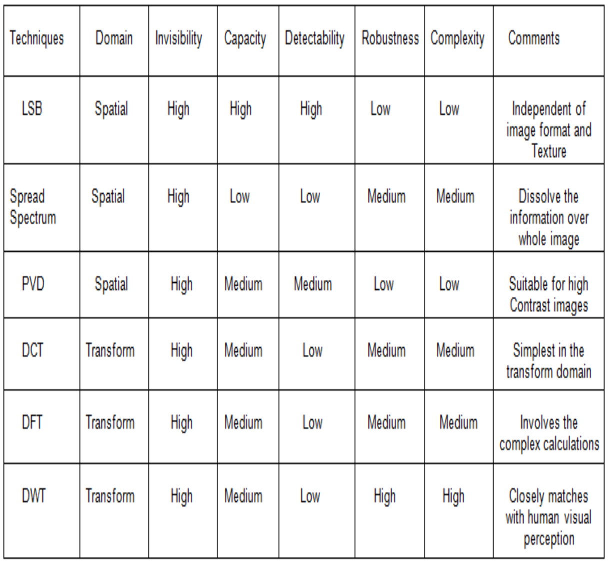
3.4 Spread spectrum: The concept of spread spectrum is used in this technique. In this method the secret data is spread over a wide frequency bandwidth. The ratio of signal to noise in every frequency band must be so small that it becomes difficult to detect the presence of data. Even if parts of data are removed from several bands, there would be still enough information is present in other bands to recover the data. Thus it is difficult to remove the data completely without entirely destroying the cover .It is a very robust approach used in military communication.

3.5 Statistical Technique: In the technique message is embedded by changing several properties of the cover. It involves the splitting of cover into blocks and then embedding one message bit in each block. The cover block is modified only when the size of message bit is one otherwise no modification is required.

3.6 Distortion Techniques: The distortion method is used to store the secret data by distorting the signal. An encoder applies a sequence of modifications to the cover image and the decoder phase decodes the encrypted data to the original data with the secret data by using some secret key.

3.7 Masking and Filtering: This approach is used to hides the data by marking an image. This approach is valuable where watermarks become a portion of the image. The data will be embedded where the more significant part of the image rather than hiding it into the noisy portion. The watermarking techniques are more integrated into the image and it can be applied without the fear of destruction of the image. This technique is used in 24 bit and grey scale images [9].

Table 1. Comparison of Various Techniques of Steganography.



Techniques	Domain	Invisibility	Capacity	Detectability	Robustness	Complexity	Comments
LSB	Spatial	High	High	High	Low	Low	Independent of image format and Texture
Spread Spectrum	Spatial	High	Low	Low	Medium	Medium	Dissolve the information over whole image
PVD	Spatial	High	Medium	Medium	Low	Low	Suitable for high Contrast images
DCT	Transform	High	Medium	Low	Medium	Medium	Simplest in the transform domain
DFT	Transform	High	Medium	Low	Medium	Medium	Involves the complex calculations
DWT	Transform	High	Medium	Low	High	High	Closely matches with human visual perception

4 Factors Include in Steganography

The effectiveness of steganography technique can be determined by comparing cover-image with the stego Image. The various factors are:

4.1 Robustness: Robustness refers to the ability of embedded data to remain intact if the stego- image undergoes transformations, such as linear and non-linear filtering, sharpening or blurring, addition of random noise, rotations and scaling, cropping or decimation, lossy compression.

4.2 Imperceptibility: The imperceptibility means invisibility of a steganography algorithm. Because it is the first and foremost requirement, since the strength of steganography lies in its ability to be unnoticed by the human eye.

4.3 Bit Error Rate: The hidden information can be successfully recovered from the communication channel. It must be ideal but for the real communication channel, the error comes while retrieving hidden information and this is measured by BER. It is the ratio of the number of errors to the total no of bits sent in an image.

4.4 Mean Square Error: It is computed by performing byte by byte comparisons of the two images. The representation of pixel with 8 bits and the representation of grey level images upto 256 levels. The distortion in the image can be measured using MSE. Let I be the cover image, K be the stego image and m*n be the total number of pixels.

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \qquad (1)$$

4.5 Peak Signal to Noise Ratio: The image steganography system must embed the content of hidden information in the image so that the quality of the image should not change. PSNR is commonly used to measure the quality of reconstruction of lossy compression techniques Larger the PSNR value indicates the better quality of image i.e. less distortion. PSNR is the ratio of the maximum signal to noise in the stego image [10].

5 Conclusions

The paper surveys the different types of Steganography and techniques to detect the steganography. In this basically Video steganography techniques are discussed. All the techniques discussed in this paper are able to secure the hidden data. On the other hand some algorithms have a very high time complexity and very less amount of data stored in the images. So, there is a need to develop efficient and accurate Steganography algorithms, either by combining the existing techniques or by developing new techniques. It helps in detecting terrorist activities on web.

References

1. P. Selvigrija and E. Ramya, *"Video by Linked List Method,"* no. March, (2015)
2. M. Hussain and M. Hussain, *"A Survey of video Steganography Techniques," Int. J. Adv. Sci. Technol.*, vol. **54**, pp. 113–124, (2013)
3. G. Kaur and A. Kochhar, *"A Steganography Implementation based on LSB & DCT,"* vol. **4**, no. 1, pp. 35–41, (2012)

4. P. Chen and H. Lin, *"A DWT Based Approach for Image Steganography," Int. J. of Applied Sci. Eng.*, vol. **4**, no. 3, pp. 275–290, (2006)
5. M. Juneja and P. S. Sandhu, *"An Improved LSB Based Steganography Technique for RGB Color Images," Int. J. Comput. Commun. Eng.*, vol. **2**, no. 4, pp. 513–517, (2013)
6. kaur Amandeep kaur, manpreet, *"Improved Security Mechanism of Text in Video using Steganographic Technique," Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. **7782**, no. 5, pp. 44–51, (2014)
7. M. Dixit, N. Bhide, S. Khankhoje, and R. Ukarande, *"Video Steganography," 2015 Int. Conf. Pervasive Comput.*, vol. **00**, no. c, pp. 1–4, (2015)
8. R. J. Mstafa and I. Studen, *"A High Payload Video Steganography Algorithm in DWT Domain Based on BCH Codes (15 , 11),"* (2015)
9. J. Gupta, *"A Review on Steganography techniques and methods,"* vol. **1**, no. 1, pp. 1–4, (2015)
10. C. Science and B. Bridgeport*, "A Novel Video Steganography Algorithm in the Wavelet Domain Based on the KLT Tracking Algorithm and BCH Codes,"* (2015)