ISSN : 2231-0711

Swetha V et al | IJCSET(www.ijcset.net) | June 2015 | Vol 5, Issue 6,206-213

Data Hiding Using Video Steganography -A Survey

Swetha V
Department of Computer Science and Engineering
Jawaharlal College of Engineering and Technology

Prajith V
Department of Computer Science and Engineering
Palakkad Institute of Science and Technology

Kshema V
Department of Computer Science and Engineering
Jawaharlal College of Engineering and Technology

***Abstract*—Digital data communication has become an integral part of infrastructure nowadays. In this tech era, with the increasing importance of internet and the fast communication techniques, the security and the confidentiality of the sensitive data has become of prime concern. This has resulted in an unpredictable growth in the field of information hiding. Cryptography and steganography are the two popular methods available to provide security. One hides the existence of the message and the other distorts the message itself. Steganography is a technique to hide secret information in some other media without leaving any apparent evidence of data alteration. It comes under the assumption that if the feature is visible, the point of attack is evident, thus the objective of steganography is always to conceal the very existence of the secret data. This paper provides a state-of-the-art review and analysis of the different existing methods of video steganography and also covers classification and applications.**

Keywords- **Cover Media, Cryptography, Data Hiding, LSB, Security, Steganography**

I. INTRODUCTION

The cutting edge of technology and the Internet have made a breakthrough in the existence of data communication. Communication is the lifeblood of any organization and is one of the most important needs of human beings. The concept of secret communication is as old as communication itself. It is often thought that communications can be made secure by using encryption techniques, but this is not really true in practice. Encryption provides an obvious approach to information security, and encryption programs are readily available. However, encryption clearly marks a message as containing interesting information, and the encrypted message becomes subject to attack. Furthermore, in many cases it is desirable to send information without anyone even noticing that information has been sent secret information. The history teaches that is better hiding messages rather than enciphering them, because it arouses less suspicion. This preference persists in many operational contexts till up this day.

Data security basically aims at preserving the confidentiality and integrity of data and protecting the data from unauthorized users or hackers. Many techniques such as digital watermarking, cryptography and steganography were developed in order to enhance the data security. Cryptography is an art or science of ciphers that use mathematics to scramble the original text into a seemingly unreadable format for others. Steganography is the art of invisible communication. Its purpose is to hide the very presence of communication by embedding messages in such a way that a third person cannot even sense the presence of the hidden message. While cryptography is a method to conceal information by encrypting it to cipher texts using an unknown key and transmitting it to the intended receiver, steganography provides further security by hiding the cipher text into another cover medium.

Digital watermarking and fingerprinting related to steganography are basically used for intellectual property protection. Watermarking is the practice of imperceptibly altering work to embed a secret message. A digital watermarking is a process of covertly embedding into a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. The main aim of digital watermarking is to protect the integrity and authenticity of digital media. In fingerprinting; different and specific marks are embedded in the copies of the work that different customers are supposed to get. In this case, it becomes easy for the property owner to find out such customers who give themselves the right to violate their licensing agreement when they illegally transmit the property to other groups

To hide secret information in some other source of information without leaving any apparent evidence of data alteration steganographic techniques can be used. In today's digital world, invisible ink and paper have been replaced by much more versatile and practical covers such as digital documents, images, video, and audio files are used for hiding messages. As long as an electronic document contains perceptually irrelevant or redundant information, it can be used as a cover for hiding secret messages. All of the traditional steganographic techniques have limited information-hiding capacity approximately 10% or less. This is because the principle of those techniques was either to replace all the least significant bits of a multivalued image with the secret information or to replace a special part of the frequency components of the vessel image. Data containing both the cover signal and the embedded information is known as stego data. Occasionally, especially when referring to image Steganography, the cover image can be called as Vessel or Container. Steganographic technologies are a very important part of the future of Internet security and privacy

on open systems such as the Internet. Security, capacity and robustness are three main aspects of steganography. All these factors are inversely proportional to each other creating steganographic dilemma.

II BACKGROUND STUDY

Steganography is a fine art of hiding information in something else to enable them to pass unobserved and is an unusual aspect of security that is not commonly known, despite having a history that dates back thousands of years. The roots of steganography date back to 440 BC. Although the term was only coined at the end of 15th century, the use of steganographic techniques dates back several millennia. The term is derived from two Greek words, "stegano" which means covered or secret and "grafia" which means writing or drawing. Despite the Greek origin, the word "Steganography" does not appear in the literature until when Johannes Trithemius uses the word in a trilogy published in Frankfurt in 1606.

A. *Early Evidence of Steganography*

The concept of hiding and concealing messages has existed for thousands of years, even though term steganography is only few years old. In ancient times, the secret messages were hidden in different ways such as tattooed on the scalp of slaves, hidden on tablets covered with wax, or written on the stomachs of rabbits. The earliest known written account of steganography being used was quoted by Herodotus during 484-425 BC. He tells how his master, Histiaeus, sent a slave to the Ionian city of Miletus with a message concealed on his body. The messenger's or slave's head was shaved and the secret message was tattooed on his scalp. After allowing his hair to grow concealing the message, the slave was sent to the Ionian city of Miletus. In order to reveal the message, slave's head was shaved once he reached there. Herodotus also documented how Demeratus notify Sparta that Xerxes intended to invade Greece. In ancient Greece, wax covered tablets were used for writing text. To preserve the message's confidentiality and avoid capture, he scraped the wax off of the tablets and on the underlying wood he wrote the message. The tablet was covered with wax again. As the tablets appeared to be blank and unused they passed inspection by sentries without question. The hidden message can be only revealed by scraping away all of the wax. Another steganographic technique was proposed by Aeneas Tactician, who was a Greek writer well-known for his various steganographic approaches and techniques .His idea was to conceal information in women's earrings, or using pigeons to deliver secret messages.

B. *Linguistic Steganography*

Linguistic steganography is possibly one of the oldest forms of steganography. Aeneas Tactician, who described many linguistic techniques, laid the foundation of linguistic steganography. Some of the techniques he proposed were to alter the height of letters or mark particular letters with dots or small holes. Linguistic steganography has been used prolifically throughout history, and in the modern era, variants of these techniques still exist. Linguistic steganography can the considered as the pioneer of text steganography. In 14th Century a poet named Giovanni Boccaccio, encoded over 1500 letters taken from three sonnets, into his acrostic poem, Amorosa Visione. This can be possibly considered as one of the largest examples of linguistic steganography. It was Francis Bacon who proposed the most interesting linguistic technique. Bacon's method allows messages to be encoded using a binary representation, by using normal or italic font. This scheme is a precursor to modern steganographic techniques. A photographic technique was proposed by Brewster in 1857. The technique would allow text to be shrunk down to a dirt-sized speck. The message is readable only under very high levels of magnification. The Germans used this technique to conceal large messages in the corner of post cards during World War I. The "microdot" technique used by the Germans was capable of hiding entire pages of text and even photographs, making them a powerful container of covert information .Null cipher is another variation of linguistic steganography.

C. *Modern Steganography*

Steganography is becoming more and more widespread and relevant with the advent of modern technology and Internet. Different multimedia files such as image, video and audio present interesting digital file formats for concealing secret information. The growth in communication technology and usage of public domain channels such as Internet has greatly facilitated transfer of data. The internet applications demands secure data transmission. Due to interception and improper manipulation by eavesdropper, data transmission in public communication system is not secure. An attractive solution for this problem is Steganography, which is the art and science of writing hidden messages in such a way that no one, apart from the sender and intend recipient, suspects the existence of the message. Media files are large in size and facilitate more embedding capacity. There are many criteria for classifying steganography. One of them is classification based on the type of cover object and the classification is as follows:

1) Image Steganography: Images are used as the popular cover medium for steganography. Hiding information in image is known as image steganography. Generally, in this technique pixel intensities are used to hide the information. The cover image can be called as Vessel or Container. The image after hiding information is called stego-image. A message is embedded in a digital image using an embedding algorithm, using the secret key. The resulting stego-image is send to the receiver. On the other side, it is processed by the extraction algorithm using the same key. During the transmission of stego- image unauthenticated persons can only notice the transmission of an image but can't predict the presence of the hidden message. To hide a message inside an image without changing its visible properties, the cover source can be altered in noisy areas with many color variations, so less attention will be drawn to the modifications. The most common methods to achieve these modifications involve the usage of the least-significant bit or LSB, masking, filtering and transformations on the cover image. These techniques can be used on different types of image files with varying degrees of success.

2) Network Steganography: The term protocol steganography refers to embedding information within network protocols such as TCP/IP, UDP, ICMP etc... The network steganography is also known as protocol steganography. In the OSI network layer model there exist covert channels where steganography can be achieved by hiding information in optional or unused header bits of TCP/IP fields.

3) Video Steganography: Video Steganography is a technique to hide any kind of files in any extension or information into digital video format. Video which is the combination of pictures is used as carrier for hidden information. Video steganography uses video formats such as H.264, Mp4, MPEG, AVI, etc.

*4) Audio Steganography***:** When taking audio as a carrier for information hiding it is called audio steganography. Due to popularity of voice over IP (VOIP), audio has become a significant cover medium. Audio steganography uses digital audio formats such as WAVE, MIDI, AVI MPEG or etc. for hiding secret message.

5) Text Steganography: The text steganography is a method of using written natural language to conceal a secret message. It can be achieved by altering the text formatting, or by altering certain characteristics of textual elements. The objective of designing coding methods was to develop alterations that are largely indiscernible to the reader and reliably decodable even in the presence of noise. General technique in text steganography is to use number of tabs, white spaces, capital letters, just like Morse code and etc to achieve information hiding. After the introduction of Internet and different type of digital file formats text steganography has decreased its importance. Text steganography lost its importance due to the fact that the text files have very small amount of redundant data. Examples for coding techniques are given below. The techniques can be used either jointly or separately. Each technique enjoys certain advantages or applicability of its own.

- Line-Shift Coding
- Word-Shift Coding
- Feature Coding

III **VIDEO STEGANOGRAPHY**

As a video container file has numerous advantages not exhibited by other container formats, video steganography is now a growing area of research. Video Steganography is a technique to hide any kind of files into a video file. The Alteration in the video file is significantly more difficult to detect by the human visual system, as frames are displayed on screen in an extremely faster rate. Furthermore, since video frames are not sharply focused images or crisp, variations in pixel color induced by steganography will blend into the frame very easily. Use of the video based steganography can be more eligible than other multimedia files, because of its size and memory requirements. The video has 2 components and they are an audio stream and a picture stream. Therefore most of the existing techniques on images and audio can be applied to video files too.

IV **IMAGE STEGANOGRAPHY**

Image steganography techniques can be divided into following domains.

- Spatial Domain Methods
- Transform Domain Technique
- Distortion Techniques
- Masking and Filtering

A. Spatial Domain Methods

There are many versions of spatial steganography, all directly change some bits in the image pixel values in hiding data. Least significant bit (LSB)-based steganography is one of the simplest techniques that hides a secret message in the LSBs of pixel values without introducing many perceptible distortions. Changes in the value of the LSB are imperceptible for human eyes. Spatial domain techniques are broadly classified as follows based on the techniques used for hiding data.

1. Least significant bit (LSB)
2. Pixel value differencing (PVD)
3. Edges based data embedding (EBE)
4. Quantization index modulation(QIM)
5. Random pixel embedding (RPE)
6. Pixel Mapping method
7. Multiple-Based Notational System
8. Difference Expansion Technique
9. Gray level modification (GLM)
10. Labelling or connectivity method
11. Pixel intensity based method
12. Texture based method
13. Histogram shifting methods

1) Least Significant Bit (LSB)

The simplest approach for embedding information in cover image is using Least Significant Bits (LSB). The idea of the LSB algorithm is to insert the bits of the hidden message directly into the least significant bit plane of the cover image in a deterministic sequence. As the LSB method is designed by taking the advantage of human vision system and as the amplitude of the change is small, modulating the least significant bit does not result in human-perceptible difference. Because this method uses bits of each pixel in the image, it is necessary to use a lossless compression format, otherwise the hidden information will get lost in the transformations of a lossy compression algorithm. The Least Significant Bit insertion varies according to the type of image. For an 8 bit image, the 8^{th} bit of each byte of the image is replaced with the bit of secret message. For 24 bit image, the LSB bit of each of the red, green and blue color components are changed.

Since the compression in BMP is lossless, LSB is effective in using BMP images. But for hiding the secret message inside BMP image using LSB algorithm it requires a large cover image. GIF formats also supports LSB substitution, but the problem with the GIF image is that whenever the least significant bit is changed the whole color palette will be changed. This problem can be solved by using the gray scale GIF images since the gray scale image contains 256 shades and the changes will be done gradually so that it will be very hard to detect. Since JPEG uses lossy compression, the direct substitution of steganographic techniques is not possible in JPEG images. So it uses LSB

substitution for embedding the data into images. General advantages of spatial domain LSB technique are:

- Simple
- More embedding capacity
- Less chance for degradation of the original image.

Disadvantages of LSB technique are:

- Image manipulation can distort the hidden data .Hence less robust.
- Easy steganalysis
- Hidden data can be easily destroyed using simple attacks.

2) Pixel Value Differencing (PVD)

The pixel-value differencing (PVD) method was proposed by Wu and Tsai. . In this technique, for embedding a secret message, the original cover image is partitioned into non overlapping blocks of two pixels. A difference value is calculated from the values of the two consecutive pixels in each block. All possible difference values are classified into a number of ranges. The selection of the range intervals is done by taking the advantage of the characteristics of human vision's sensitivity to gray value variations from smoothness to contrast. A larger difference in the original pixel values allows a greater modification. The block with large difference value is considered in edge area and with small difference value is considered in smooth area where the small or large values are taken depending upon some pre-specified threshold value. The human eyes are more sensitive to noise in smooth area than in the edge area. The difference value then is replaced by a new value to embed the value of a sub-stream of the secret message. The number of bits which can be embedded in a pixel pair is decided by the width of the range that the difference value belongs to. The advantages of this technique are:-

- High embedding capacity
- Outstanding imperceptibility

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. There are two types of the quantization range table in Wu and Tasi's method. The first was based on selecting the range widths of [8, 8, 16, 32, 64, 128], to provide large capacity. The second was based on selecting the range widths of [2, 2, 4, 4, 4, 8, 8, 16, 16, 32, 32, 64, 64], to provide high imperceptibility.

3) Quantization Index Modulation (QIM)

Quantization index modulation (QIM) is a commonly used data embedding technique in digital watermarking and it can be employed for steganography. Because of its information-theoretic optimality against a large class of attacks and robustness, QIM techniques have been gaining popularity in the data hiding community. It quantizes the input signal x to the output y with a set of quantizers, i.e., Qm (.). Using which quantizer for quantization is determined by the message bit m.

4) Random Pixel Embedding Method (RPE)

Least Significant Bits (LSB) is the simplest and most straight forward approach to spatial domain steganography. But, LSB hides the message in a way that the humans do not distinguish it, and still possible for the opponent to retrieve the message due to the simplicity of the technique. Therefore, LSB technique must be enhanced. In random pixel embedding method, the message is inserted in the images in random manner in the pixels of a cover image. RPE can be considered as improvement of LSB scheme in which message bits are inserted into a set of random in each pixel within the image, not in the least significant bit. The least significant bit sign to extract data from the image. In this method message bit is not only inserted to least bit but also to other bits in the pixel in the random manner. This can be done by comparing the message bit to the pixel bit randomly chosen from second to the last bit. Based on this comparison, 1 is inserted in the least significant bit if the message bit identical to that of the image, whereas, 0 is inserted if the message bit didn't match with the chosen bit from the image.

5) Pixel Mapping Method (PMM)

Pixel mapping is a new method to map data into image proposed by Bhattacharyya, synal et.al.It uses concept of pixel intensity and no of 1's in pixel to map data. The advantages of this approach are:

- Produces better embedding capacity
- Better PSNR Value over PVD and GLM

6) Multiple-Based Notational System (MBNS)

Zhang and Wang proposed an adaptive steganographic scheme with the Multiple-Based Notational System (MBNS) based on human vision sensitivity (HVS). The scheme, converts secret data into symbols by representing variable bases in a notational system .The hiding capacity of each image pixel is determined by its so called local variation. In the MBNS based scheme, a secret message is embedded into the cover image by modifying pixel values in a particular order derived from a key. A rule of thumb is that the more the variation of pixel-values in the vicinity of a pixel, the more the pixel can tolerate steganographic modification, allowing a greater change to be introduced. As such, we let each pixel carry one symbol of the secret message in a multiple-base notational system, with the corresponding base being proportional to the degree of variation in the pixel's immediate neighbourhood. Thus, pixels in busy areas carry more information and statistically undergo more modification than those in smooth areas. A secret key, which is shared by the message hider and the receiver, determines a specific path of pseudorandom walk over the pixels.

7) Difference Expansion Technique (DE)

Difference Expansion (DE) is a simple and efficient reversible data-embedding method used for digital images. Here the redundancy in the digital content is explored to achieve reversibility. In this method, one bit can be embedded into two consecutive pixels. So the maximum embedding capacity will be 0.5 bpp. The difference expansion technique was later generalized so that n -1 bits can be embedded into n pixels, resulting the maximum embedding capacity (n-1)/n bpp. However, the difference expansion based reversible data hiding methods could not gain much popularity as the method double the differences between pixels in successive iteration. The distortions were larger and hence DE was vulnerable to statistical attacks.

DE based technique had low payload capacity. The technique could not be used for applications demanding high visual quality. The advantages of the steganography method based on difference expansion are:

- It discovers extra storage space by exploring the redundancy in the image content.
- Better payload capacity limit.
- Better visual quality of embedded images.
- Low computational complexity

8) Gray Level Modification (GLM)

GLM (Gray level modification) steganographic technique was proposed by Potdar et al. Gray level modification Steganography is a technique to map data by modifying the gray level values of the image pixels. The technique does not hide or embed data. GLM technique uses the concept of odd and even numbers to map data within an image. It is a one-to-one mapping between the binary data and the selected pixels in an image. From a given image, based on a mathematical function, a set of pixels are selected. The gray level values of those pixels are examined and compared with the bit stream that is to be mapped in the image.

B. Transform Domain Technique

This is a more complex way of hiding information in an image. The spatial domain steganography techniques allow greater amount of data to be hidden but they are less resistant to steganalysis attacks. Transform domain steganography techniques do not hide the information behind image pixels directly rather they transform the image before masking data. These techniques are more resistant to steganalysis attacks when compared to those embedding principles that operate in the time domain. Various algorithms and transformations are used on the image to hide information in it. Most of the strong steganographic systems today operate within the transform domain. Transform domain methods hide messages significant areas of cover image which makes them robust against various image processing operations like compression, cropping, enhancement etc... The basic approach to hiding information with DCT, FFT or Wavelet is to transform the cover image, tweak the coefficients, and then invert the transformation. Some transform domain techniques do not seem dependent on the image format and they may outrun lossless and lossy format conversions. If the choice of coefficients is good and the size of the changes is manageable, then the result is pretty close to the original. Transform domain techniques are broadly classified into:

- Discrete Fourier transformation (DFT).
- Discrete cosine transformation (DCT).
- Fast Fourier transformation (FFT).
- Discrete Wavelet transforms (DWT).
- Lossless or reversible method (DCT)
- Embedding in coefficient bits

1) Discrete Cosine Transform (DCT)

In DCT based technique insertion of secret information in carrier depends on the DCT coefficients. Any DCT coefficient value above proper threshold is a potential place for insertion of secret information. Here the Most Significant Bits of secret image are hidden in Least Significant bits of only those pixels of cover image whose DCT coefficient value is greater than a certain threshold value. The Discrete Cosine Transform (DCT) transforms the image from spatial domain to frequency domain. It separates the image into spectral sub-bands with respect to its visual quality, i.e. high, middle and low frequency components. DCT is a mechanism to transform successive 88-pixel blocks of the image from spatial domain to 64 DCT coefficients each in frequency domain. The least significant bits of the quantized DCT coefficients are used as redundant bits into which the hidden message is embedded. The modification of a single DCT coefficient affects all 64 image pixels. Because this modification happens in the frequency domain and not the spatial domain, there are no noticeable visual differences. The advantage DCT has over other transforms is the ability to minimize the block-like appearance resulting when the boundaries between the 8x8 sub-images become visible (known as blocking artifact).

2) Discrete Fourier Transform (DFT)

DFT gives the better approximation of Fourier transform on discrete set of frequencies. The Discrete Fourier Transform is used to get frequency component for each pixel value. The Discrete Fourier Transform (DFT) of spatial value f(x, y) for the image of size M x N is represented as F(u,v) which is given by the equation:

$$F(u,v) = \frac{1}{\sqrt{M.N}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) e^{-j2\pi \left(\frac{ux}{M}+\frac{vy}{N}\right)}$$

The inverse Fourier transform is thus given by,

$$f(x,y) = \frac{1}{\sqrt{M.N}} \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} F(u,v) e^{j2\pi \left(\frac{ux}{M}+\frac{vy}{N}\right)}$$

In DFT steganography, all insertion is done in frequency domain. DFT is applied on source image to convert from spatial domain to frequency domain. Each 8 bit pixel in spatial domain is transformed into two parts one part is real and another is imaginary part. The authenticating bits are inserted in real part of frequency domain .The process is repeated for whole image matrix in the same manner. After embedding IDFT (Inverse DFT) is performed to convert from frequency domain to spatial domain. Fast Fourier Transform (FFT) is the fastest method of DFT. FFT is a high speed and efficient technique.

3) Discrete Wavelet Transform (DWT)

Any wavelet transform for which the wavelets are discretely sample are called discrete wavelet transform (DWT). The key advantage DWT has over Fourier transforms is temporal resolution. A 2-dimensional Haar-DWT consists of two operations: One is the horizontal operation and the other is the vertical one. At first, scan the pixels from left to right in horizontal direction. Then, perform the addition and subtraction operations on neighboring pixels. Store the sum on the left and the difference on the right .Repeat this operation until all the rows are processed. The pixel sums represent the low frequency part denoted as symbol L while the pixel differences represent the high frequency part of the original

image denoted as symbol H. Secondly; scan the pixels from top to bottom in vertical direction. Perform the addition and subtraction operations on neighboring pixels and then store the sum on the top and the difference on the bottom. Repeat this operation until all the columns are processed. Finally we will obtain 4 sub-bands denoted as LL, HL, LH, and HH respectively. The LL sub-band is the low frequency portion and hence looks very similar to the original image.

C. Distortion Techniques

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. In this technique, a stego-image 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." The encoder can modify the "1" value pixels in such a manner that the statistical properties of the image are not affected. However, the need for sending the cover image limits the benefits of this technique. In any steganographic technique, the cover image should never be used more than once. If an attacker tampers with the stego-image by cropping, scaling or rotating, the receiver can easily detect 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.

D. Masking and Filtering

Masking and filtering techniques is a steganographic method that takes a different approach to hiding a message. These techniques hide information by marking an image, in the same way as to paper watermarks, creating markings in an image. This can be achieved by modifying the luminance of parts of the image. Even if masking changes the visible properties of an image, it is done in such a way that the human eye will not notice the anomalies. Since masking uses visible aspects of the image, it is more robust than LSB modification with respect to compression, cropping and different kinds of image processing. The information is embedded in the more significant areas than just hiding it into the noise level, which makes it more suitable than LSB modifications in case a lossy compression algorithm like JPEG. The hidden message is more integral to the cover image. Masking and filtering technique is usually restricted to 24 bits or grayscale images. Advantages of Masking and filtering techniques are:

- Since the information is hidden in the visible parts of the image, with respect to compression this method is much more robust than LSB replacement.

Disadvantages of Masking and filtering techniques are:

- Technique is only applicable to gray scale images and restricted to 24 bits.

V AUDIO STEGANOGRAPHY

In audio steganography, secret message is embedded into digitized audio signal as noise at a frequency out of human hearing range. The embedding process will result a slight alteration of binary sequence of the corresponding audio file but the alterations made to the audio file are perceptually indiscemible. The characteristics of audio signal such as unpredictable nature and characteristic redundancy make them ideal candidate to be used as a cover for covert communications to conceal secret messages. The audio steganographic process mainly consists of following two steps:

1) Identification of redundant bits in the audio file:- Redundant bits are those bits that can be modulated without destroying the integrity or corrupting the quality of the cover media. Hence those redundant bits are chosen as the candidate for holding secret information.

2) Embedding the secret information in the audio file:- The redundant bits in the cover file is replaced by the bits of the secret information.

Due to the existence of advanced audio steganography schemes and the very nature of audio signals to be high-capacity data streams, audio steganalysis is very difficult and requires scientifically challenging statistical analysis. There have been many techniques for hiding information or messages in audio some of the common approaches include

A. Low-Bit Encoding

It is also known as LSB encoding. The low-bit encoding replaces the least significant bit in some bytes of the digitized audio file to hide a sequence of bytes containing the secret data. Since the LSB substitution doesn't cause significant quality degradation, such as in 24-bit bitmaps, this is usually an effective technique. In computing, the least significant bit (LSB) is the bit position in a binary integer giving the units value, that is, determining whether the number is even or odd. The LSB is sometimes referred to as the right-most bit, due to the convention in positional notation of writing less significant digit further to the right. Though this method is simple and have greater embedding capacity, the method cannot provide protection to the hidden message against small modifications that can arise as a result of format conversion or lossy compression.

B. Phase Coding

In phase coding technique, the phase of a cover audio segment is replaced with a reference phase that represents the secret information. In order to preserve the relative phase between segments, the remaining segments phase is adjusted. In terms of signal to noise ratio, Phase coding is one of the most effective coding methods. This method relies on the fact that the phase components of sound are not as perceptible to the human ear as noise is. Message bits are encoded as phase shifts in the phase spectrum of a digital signal. This leads to inaudible encoding in terms of the Signal-to-Perceived Noise Ratio (SPNR) and the secret message gets camouflaged in the audio signal, not detectable by the steganalysis methods based on SPNR. Thus, phase coding addresses the disadvantages of the noise-inducing methods of audio steganography. When there is a drastic change in the phase relation between each

frequency component, noticeable phase dispersion will occur. However, as long as the modification of the phase is sufficiently small, an inaudible coding can be achieved.
Phase coding is explained in the following procedure:

1) Decompose the original audio signal into smaller segments such that lengths are of the same size as the size of the message to be encoded.
2) Matrix of the phases is created by applying Discrete Fourier Transform (DFT).
3) Compute the phase differences between every pair of consecutive segments.
4) Phase shifts between adjacent segments are easily detectable. Although, we can change the absolute phases of the segments, the relative phase differences between adjacent segments must be preserved. So the secret information is embedded only in the phase vector of the first signal segment.
5) Create a new phase matrix using the new phase of the first segment and set of the original phase differences.
6) Reconstruct the sound signal by applying the inverse Discrete Fourier Transform using the new phase matrix and original magnitude matrix and then concatenating the sound segments back together.

The receiver must know the segment length to extract the secret information from the sound file. Then the receiver can use the DFT to get the phases and extract the secret information. The disadvantages of phase coding are:-

- Low data transmission rate owing to the fact that the secret message is encoded only in the first segment of the audio signal.
- The phase coding method is normally used only when a small amount of data as an increase in the length of the segment would have a ripple effect by altering the phase relations between the frequency components of the segment; thereby making detection easier.

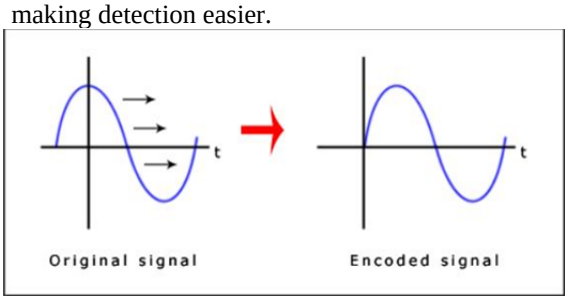

Figure 1: Phase Coding

C. Spread Spectrum Coding

In audio steganography, the basic spread spectrum (SS) method attempts to randomly spread bits of the secret message across the frequency spectrum of the audio signal. This is similar to a system which uses an implementation of the LSB that spreads the message bits randomly over the entire sound file. However, unlike LSB coding, the spread spectrum method spreads the secret information over the frequency spectrum of the sound file using a code which is independent of the actual signal. As a result, the final signal occupies a bandwidth which is more than what is actually required for transmission. The spread spectrum method is capable of contributing a better performance than LSB coding and phase coding techniques by virtue of a moderate data transmission rate coupled with a high level of robustness against steganalysis techniques. The one main disadvantage of the spread spectrum method is:-

- It introduces noise into a sound file like LSB coding method. This vulnerability can be tapped for steganalysis.

D. Echo Hiding

Echo hiding technique embeds secret information by introducing an echo into the discrete audio signal. To successfully hide the secret message, three parameters of the echo need to be altered. They are, amplitude, decay rate and offset or delay time from the original signal. As all the three parameters are set below the human audible threshold limit, the echo cannot be easily resolved. Also, the offset is altered to represent the binary message to be hidden. The first offset value represents a binary one, and the second offset value represents a binary zero. If only one echo was produced from the original signal, only one bit of secret information could be encoded. Hence, before the encoding process begins the original signal is broken down into blocks. Once the encoding process is done, all blocks are concatenated back together to create the final signal. The advantages of echo hiding are:-

- High data transmission rate.
- Superior robustness.

E. Parity Coding

Parity coding is one of the robust audio steganographic techniques. Instead of breaking a signal down into individual samples, this method breaks a signal into separate regions samples and encodes each bit of the secret message in a sample region's parity bit. The process inverts the LSB of one of the samples in the region, if the parity bit of a selected region does not match the secret bit to be encoded. Thus, the sender has more of a choice in encoding the secret bit. The decoding process extracts the secret message by calculating and lining up the parity bits of the regions used in the encoding process. The sender and receiver can use a shared secret key as a seed in a pseudorandom number generator to produce the same set of sample regions. Even parity is desired. There are two main disadvantages associated with the use of methods like LSB coding or parity coding. There are two main disadvantages associated with the use of parity coding. They are:-

- The human ear is very sensitive and can often detect even the slightest bit of noise introduced into a sound file, although the parity coding method does come much closer to making the introduced noise inaudible.
- Less robust. If the audio file embedded with a secret message using parity coding was resampled, the embedded information would be lost.

VI STEGANOGRAPHIC APPLICATIONS

Steganographic technique can be used anytime one wants to hide data. The most important reason to hide data is to prevent unauthorized persons from becoming aware of the existence of a message. Steganography is employed in various useful applications such as copyright control of

materials, enhancing robustness of image search engines and smart IDs where individual's details are embedded in their photographs. Other applications are TV broadcasting, video-audio synchronization, TCP/IP packets and checksum embedding and safe circulation of secret data. Steganography would provide an ultimate guarantee of authentication that no other security tool may ensure.

In the business world, data hiding can be used to hide a secret chemical formula or plans for a new invention. Steganography can also be used in the non-commercial sector to hide information that someone wants to keep private. It can be used in forensic applications for inserting hidden data into media files for the authentication of spoken words and other sounds, and in the music business for the monitoring of the songs over broadcast radio. Steganography also have some contemporary applications, one of which was in Medical Imaging Systems where a separation is considered necessary for confidentiality between patient's image data or DNA sequences and their captions, e.g., physician, patient's name, address and other particulars A link however, must be maintained between the two. Thus, embedding the patient's information in the image could be a useful safety measure and helps in solving such problems.

Inspired by the notion that steganography can be embedded as part of the normal printing process, the Japanese firm Fujitsu3 has developed a technology to encode data into a printed picture that is invisible to the human eye, but can be decoded by a mobile phone with a camera. The process takes less than one second as the embedded data is merely 12 bytes. Hence, users will be able to use their cellular phones to capture encoded data. This application can be used for doctor's prescriptions, food wrappers, billboards, business cards and printed media such as magazines and pamphlets or to replace barcodes. Protecting scanned documents from forgery using self-embedding techniques is also an important application of data hiding. The method not only points out forgery but also allows legal or forensics experts to gain access to the original document despite being manipulated.

VII CONCLUSION

In the era of fast information interchange using internet and World Wide Web, steganography has become essential tool for information security. Steganography can be classified based on many criteria and one among them is based on the type of cover media. This paper presented a review work in video steganography methods its major types and classification which have been proposed in the literature during last few years. As video is a bunch of images combined with audio, all existing image and audio steganographic techniques are applicable to video steganography. Pros and cons of different steganography algorithm were also discussed.

REFERENCES

[1] Masoud Nosrati , Ronak Karimi Mehdi Hariri,"*An introduction to steganography methods"*, World Applied Programming, Vol 1, August 2011.

[2]. J. Tian, "*Reversible data embedding using a difference expansion.*" IEEE Transactions on Circuits and Systems for Video Technology, 13, 8, PP 890–896, 2003.

[3] Wu D. C and Tsai W. H. (2003), "*A steganographic method for images by pixel-value differencing", Pattern Recognition Letters,* Vol. 24, no. 9-10, pp. 1613-1626.

[4] Wu H.C., et al., "*Image Steganographic scheme based on pixel-value differencing and LSB replacement methods"*, VISP(152), 2005

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

[6] N. F. Johnson and S. Katzenbeisser, "*A Survey of steganographic techniques. in Information Hiding Techniques for Steganography and Digital Watermarking*,S.Katzenbeisser and F.Petitcolas, Ed. London: Artech House, pp. 43-78,2000.

[7] H. S. Majunatha Reddy and K. B. Raja, *High capacity and security steganography using discrete wavelet transform.* International Journal of Computer Science and Security. pp. 462-472,2009.

[8] S. C. Katzenbeisser. *Principles of Steganography. in Information Hiding Techniques for Steganography and Digital Watermarking"*, S. Katzenbeisser and F. Petitcolas, Ed. London: Artech House, pp. 43-78,2000.

[9] P. Kruus, C. Scace, M. Heyman, and M. Mundy., *A survey of steganography techniques for image files* . Advanced Security Research Journal,2003, pp. 41-52.

[10] Jayaram P, Ranganatha H R, Anupama H S, *"Information hiding using audio steganography – A survey"*,The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011 ,DOI : 10.5121/ijma.2011.3308 86.

[11] B.C. Nguyen, S.M. Yoon et H.-K. Lee : *Multi bit plane image steganography*. Proc. Digital Watermarking, 5th International Workshop, IWDW 2006, volume 4283 de Lecture Notes in Computer Science, pages 61 –70, Jeju Island, Korea, novembre 2006. Springer.

[12] D.C. Wu. and W.H. Tsai.,"A steganographic method for images by pixel value differencing, Pattern Recognition Letters, 24:1613–1626, 2003.

[13] Potdar V.and Chang E. "*Gray level modification steganography for secret communication*". In IEEE International Conference on Industria l Informatics. pages 355–368, Berlin, Germany, 2004.

[14] Xinpeng Zhang and Shuozhong Wang. *"Steganography using multiple-base notational system and human vision sensitivity"*. IEEE Signal Processing Letters, 12(1):67{70, 2005.

[15] B. Chen and G.W. Wornell. "*Quantization index modulation: A class of provably good methods for digital watermarking and information embedding*". IEEE Transactions on Information Theory, 47(4):1423{1443, 2001.

[16] K. Gopalan and S. Wenndt, *"Audio Steganography for Covert DataTransmission by Imperceptible Tone Insertion"*, WOC 2004, Banff,Canada July 8 10, 2004.

[17] Prince Kumar Panjabi, Parvinder Singh,Ph.D,, "An Enhanced Data Hiding Approach using Pixel Mapping Method with Optimal Substitution Approach", International Journal of Computer Applications (0975 – 8887) Volume 74– No.10, July 2013

[18] http://www.steganosaur.us/

[19] Souvik Bhattacharyya and Gautama Sanyal. "*Study and analysis of quality of service in different image based Steganography using PMM"*. International journal of applied information system – foundation of computer science, New York, USA 2012

[20] Souvik Bhattacharyya and Gautam Sanyal. ''*PMM (Pixel Mapping method) Based Bit plane complexity onsegmentation (BPCS) Steganography'*. 2011 – IEEE