The Non-Tangible Masking of Confidential Information using Video Steganography

Ramandeep Kaur
Mtech Scholar (CSE)
CTIEMT, Shahpur
Jalandhar (Punjab)

Pooja
Assistant Professor (CSE)
CTIEMT, Shahpur
Jalandhar (Punjab)

Varsha
Assistant Professor (CSE)
CTIEMT, Shahpur
Jalandhar (Punjab)

ABSTRACT
Video Steganography is a new research area which is playing an important role in information hiding criteria. Nowadays security of confidential information is major issue over the internet. To protect the secret information from cyber criminals like attackers, hackers and data thefts, a secure and standardized methodology is used that is known as steganography. It is beneficial for society to secure private data from being misused by unauthorized person. It is used for providing authentication to right users. For example, we can protect our confidential emails from our rivals over network using steganography concept. In this paper, we present a basic review about video steganography. Our aim is to provide a full-fledged knowledge about the basis of video steganography. This paper includes basic information about video steganography, its techniques and steganalysis with all type of attacks and applications of steganography in real life.

General Terms
Information Hiding, Image, Video, Quality, Security, Perceptibility, human Visual system (HVS).

Keywords
Steganography, Watermarking, Cryptography, LSB, DCT, DWT, Steganalysis attacks.

1. INTRODUCTION
In the digitized environment, security and privacy are major concern while sharing the private information over the network. Hackers are always be ready to gain access over our confidential information and may harm or misused it for their own profits. To protect our data from such type of cyber criminals or thefts, we use the concept of data hiding. Data hiding is a very secure phenomenon to secure confidential information by hiding it from human visual system (HVS) either by encrypting or behind a physical or logical medium. There is various information security techniques are available to protect significant information from active or passive attacks such as cryptography, Digital watermarking and Biometrics. Steganography is a major part of information security techniques [1].

1.1 Steganography
Steganography is an art and science of invisible communication, which is used to hide information and provide secret communication between two parties without being noticed by third party member. It is an information hiding technique that hides the presence of secret information inside a media. The steganography word is originated from Greek work, which is the combination of two words i.e. 'Steganós' means covered/secret and 'G*rafi*s' means writing. Literally, it is known as covered writing in which we conceal the secret message behind a cover. The information should be hidden in such a manner that it should not be visible and there should be no distortion in the secret message [2]. Steganography can be divided into two types:

a) **Fragile**: In this type of steganography, we embed information into a file which can be destroyed if the file is modified by attackers. I.e. cryptography and encryption.
b) **Robust**: Its aim is to embed information into a file which cannot easily be destroyed by hackers and can't be easily identify to make changes. I.e. digital watermarking and digital steganography.

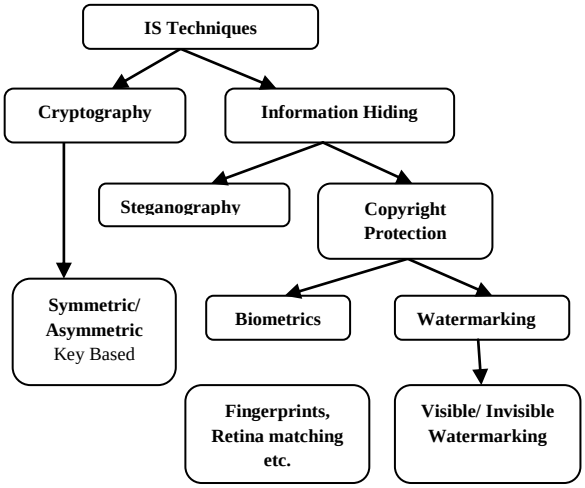


Fig 1: Classification of Information Security

2. HISTORY OF STEGANOGRPAHY
From the ascent time, steganography was used to hide secrets and for invisible communication. In *Histories* the Greek historian Histaeus write a secret message to his son-in-law, who wants to secretly communicate with him in Greece. He shaved the head of his most trustfully slave and tattooed the message ion his head. When the slave's hair grew back, he sent him with the hidden message. In the Second World War the Microdot technique was developed by the Germans. Candle and wax or some software's were used to embed secret information. But nowadays digital media is used to hide information behind any type of media file (image, text, video, audio etc). It is also known as digital steganography. Nowadays, Steganography is used for both legal and illegal purposes. People are using this process for spreading computer viruses, for hacking legal data of an organization, which is a very important concern of this field. So before procuring from cyber criminals, we must know the ways through which hackers are misusing steganography process.

2.1 Recent Advances in Steganography

- **9/11 Case**

The terrorists are said to have been using popular web locations to share crafted files containing hidden information.

- **Technical Magazine**

A technical magazine jahid was reported as a stego file that contained instructions on crafting Steganographic message.

- **Printer Steganography**

In 2004, a report emerged; revealing that certain printer manufactures enriched their products with the capacity to hide tracking information in printouts using yellow tracking dots coded machine ID number.

- **Photo Sharing websites (Picasa and Flicker)**

In 2010, scientists at Georgia Tech had created a method of communication by means of popular photo-sharing sites like Picasa and flicker to hide short text message in multiple pictures and from which data can retrieved by means of combining pictures using collage programs.

- **Hidden message in printed arrays of microbes**

Tufts University has showed in 2011 that information can be hidden within the aid of bacteria processing by changing color values of glowing pixels.

- **Malware and worms spreading**

Computer worms can be used to transfer hijacked data. Android malware (recent report on 30 Jan 2012) was created in which images are used to hide information on sending SMS.

- **Computer Games**

Multiplayer games may be good cover for covert communication.

3. COMPERISSION OF STEGANOGRAPHY WITH CRYPTOGRAPHY & DIGITAL WATERMARKING

As steganography, cryptography and watermarking are information hiding tools. But still they have some difference which is described as below:

3.1 Steganography vs. Cryptography

Both are information security techniques but both have different perceptive. Cryptography scrambles/move a message bits in an unreadable format using encryption algorithm. But attackers can easily sniff the packets by applying various attacks. Whereas steganography hides the presence of secret message using covert channel and can't be seen by human eye. To provide more security to our data, we can use both techniques together to provide one layer more protection to data. Cryptography hides the original information of message by modifying the content into unreadable format and steganography hides existence of secret message.

3.2 Steganography vs. Digital Watermarking

Steganography is a concept of one - to – one communication because it is the communication between sender and receiver only and supports to uncasting mechanisms. Whereas watermarking is a concept of one - to - many communications, in which we broadcast the watermarked data to multiple users at a time [16]. Generally, cryptography is about protecting the content of secret messages; steganography is about concealing the presence of secret message behind cover media file. The breaking concept of both systems is different i.e. cryptographic and Steganographic system (watermarking systems). Both cases are explained as follow:

- In cryptographic system, attackers can easily break the encrypted code by applying various attacks & can read the secrete message by using words transposition and line shifting methods.
- A Steganographic/watermarking system can be broken in to two stages: either the attacker can visually detect that steganography/watermarking has been used; or the attacker can read, modify or remove the hidden message by applying various attacks.

Steganography methods do not deal with robustness because they have no need to provide more security against the attempts of removing hidden message. But, Watermarking methods must have high robustness to provide resistance against the attempt of removing and modification of a hidden message. Watermarking is used to protect media file from being pirated whereas steganography is used to protect the secret message behind media file.

Table1. Differences between Crypto, Stegno, and Watermark systems

Parameters	Crypto	Stegno	Watermark
Goal	Modification of data for security	Protect and hide secret information	Protect carrier from being pirated
Type of carrier	Text	Digital Files(Text, image, audio, video)	Multimedia Files
Imperceptible	No	Yes	Yes
Robustness	No	May be	Yes
Attacks	Detection is easy	Resist to attacks	Complex detection

4. CATEGORIES OF STEGANOGRAPHY

On the basis of digital media, steganography is categorized into four categories as shown below: [4]

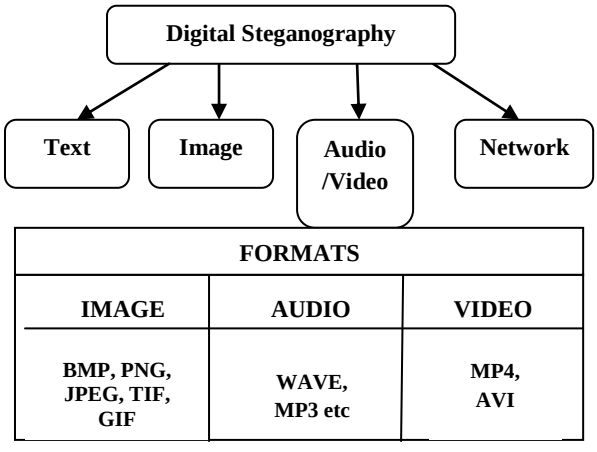


Fig 2: Categories of Steganography

4.1 Text Steganography

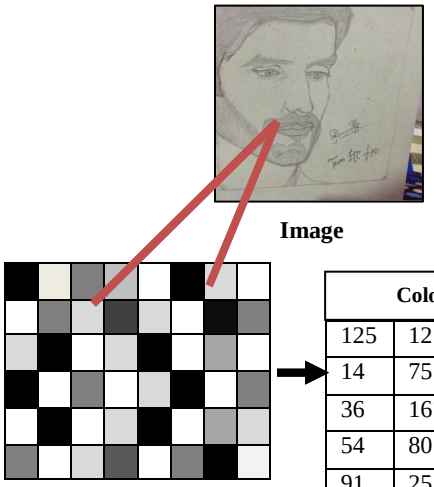
In text steganography a text file is used to embed a secret data using substitution and transposition of characters method. But it has one limitation that attackers can easily identify the presence of secret message by applying visual attacks. Text steganography methods are Line Shift Coding Protocol, Word Shift Coding, and White Space Manipulation etc.

4.2 Image Steganography

An image is used as media to hide secret message. Image can be of any format like Bitmap or JPEG etc. Image is a set of pixels having three or four color components .i.e. RGB and CMYK. There are three types of images [4]:

4.2.1 Binary images

In these images 1 pixel contains 1bit (either 0 or 1), where o indicates black color and 1 indicates white color pixels. They are also known as black/white images and monochrome images because there is no presence of light.



Color Pixel Values				
125	12	0	1	25
14	75	75	0	85
36	167	45	27	97
54	80	67	142	71
91	255	0	123	4

Fig 3: Image pixels

4.2.2 Gray scale images

It contains 0 to 255 gray color shades and 127 0r 128 values define a pure gray color. In these images, 1 pixel= 8 bits (either 0 or 255) so they are also known as 8 bit format images as black color = 00000000 and white = 11111111.

4.2.3 RGB color images

These images contain three color channels i.e. red, blue and green. They can be in two formats:

- **16 Bit color format**: where distribution of bits in R, G, B channels is 5 - 6 - 5 bits respectively. G channel contains one additional bit as it is more soothing to human eyes from all these color compounds.
- **24 Bit-color format**: Here R, G, B channels contain 8- 8- 8 bits respectively. These images are also known as 24- bit color images.

4.2.4 Image formats

An image is a collection of pixels in the form of a grid, in which each pixel has number of bits containing some color values ranges from 0 to 255. An image has various formats such as:

- **JPEG –** stands for Joint Photographic Expert Group. It is a lossy compression method. Every digital camera store image file in this format which supports 8- bit gray scale or 24 bit color images. JPEG format based files suffer from degradation effects, when repeatedly edited and saved. So it decreases the quality of images.
- **TIFF** – stands for Tagged image file. It is a lossy, lossless & flexible format that saves 8 or 16 bits per color (R, G, and B) for 24- bit color images. OCR generally generates this type of images.
- **GIF –** It stands for graphics interchange format**,** consist of 8-bit or 256 color values. It is suitable for storing graphics with few colors (black and gray) such as simple diagrams, logos and various shapes like circle, eclipse, parabola etc. It is supported by animated images or carton related images & also used to provide image animation effects .e.g. CAD.
- **BMP** – All the graphic files used in window O.S, are mostly stored in the form of bitmap format. This format based files are usually uncompressed and large and support to lossless compression.
- **PNG – Portable Network Graphics** supports 8-bit images and 24-bit true color (16 million colors) & work well for viewing online applications from web browsers**.**

4.3 Audio Steganography

Data is hidden by modifying sample data. Compressed audio formats like WAV, BWF & MBWF and uncompressed audio formats (i.e. lossy: MP3, AAC & lossless: FLAC, DST) are used to hide data in bits per sample. It is also known as sound steganography. Spread spectrum techniques are used for this type of Steganographic. And they are secure enough to hide data [15].

4.4 Network Steganography

In network steganography, a telecommunication network is used as medium to exchange the steganograms. Data is hidden by modifying the TCP/IP protocols. This type of steganography protects us from network theft and cyber criminals.

In this paper, we are focusing on the concepts of video steganography. Video steganography is a novel research area for hiding secret information because of high embedding capacity. It is the combination of audio and video frames. So, both can be used to hide secret information. Hiding the secret data inside audio frames is a difficult task because it works on the basis of signals and frequency waves. Our main motive is to explain the concept of video steganography using image frames instead of audio frames.

5. VIDEO STEGANOGRPHY

Video steganography has become very popular research area to hide secret data. It is a non- tangible masking of confidential information behind the video file. Video is a combination of audio and multiple image frames so can be used to embed large amount of data. To generate a video file, we need 16 frames per second (16 fps) or for HD videos, 25 fps are required. The main goal of video steganography is to embed the secret data behind video in such a manner that it should not be perceptible to HVS and no degradation in the quality of video. A good video steganography must have three parameters i.e. Security, Capacity and imperceptibility [5].

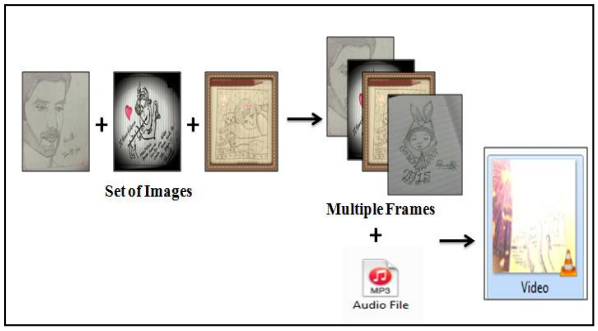


Fig 4: Video Frames

5.1 Video Formats

Various video formats are used as a carrier video such as avi, FLV, Mp4 etc.

- **Avi –** It is a video based format, stands for audio – video interleaved and store files with .avi extension. It is a container that includes audio and video frames in a single file and playback them simultaneously. It has a simple architecture, due to which it supports all operating systems like Windows operating system (XP, Vista, and window 7 or 8), Mac, and Linux (RHEL 6). It is supported by all web-browsers like Mozilla, chrome etc. Technically, this format is based on the Resource Interchange File Format (RIFF) and it fragments the file's data into small chunks.
- **H.264** – It is a high definition video format that provides good quality of video files at low bit rate without any distortion in quality of video and used for HDTV (High definition Television) broadcasting. E.g. Video LAN cards & VLC/ Windows media players.
- **3GP -** 3GP is a video file format stands for 3rd Generation Partnership Project and used for smart mobile phones. It provides various facilitates like creating, editing, transferring and viewing of video and audio files. This format is supported by various smart phones, such as the Apple phones (phone 4, 5, 6), android handsets etc. Some common examples of applications that support this type of format are Quick time player, VLC & Windows Media Players.
- **Flv** - The Flash Video format is a standard video format that supported by all Adobe player systems. It is used with all operating systems except IOS (apple's OS), such as the Adobe Flash Player and internet based web browsers inbuilt plug-in.
- **MPEG - 4 (m4v) - T**he M4V is another type of video and audio format. It was initiated by Apple Company to provide best quality of videos with high level resolution. The Video contents downloaded from apple app store or from iTunes are likely to be in M4V format. It contains Apple's DRM protection.
- **Mkv & mov –** It stands for Matroska multimedia container that holds the multimedia files (like audio, video, images and subtitle tracks) within it. It can store high amount of multimedia files. Mov is another video file format, which is mostly preferred by apple and quick time player related application programs.
- **MPEG-4 Part 14 or MP4** – It contains multimedia files. MP4 is a container that stores number of video, audio and subtitle data within a file and supported by iPod and PlayStation Portable (PSP).

6. PROCESS OF VIDEO STEGANOGRAPHY

Video steganography works in two phases i.e. embedding process and extraction process. Firstly, we extract the frames from cover video file and then select the random or sequential frames from all frames to embed the secret message. Audio files contain free and some unused bits in signals and these bits are used to hide secret information and it is very difficult to identify its presence in-between the wave signals.

6.1 Embedding Process

This process is carried out at sender side in which, a secret message is embedded inside the cover video using embedding algorithm and generate a stego video.

6.2 Extraction Process

Extraction process is a reverse process of embedding algorithms in which a secret message is extracted from stego video using stego key at receiver side.

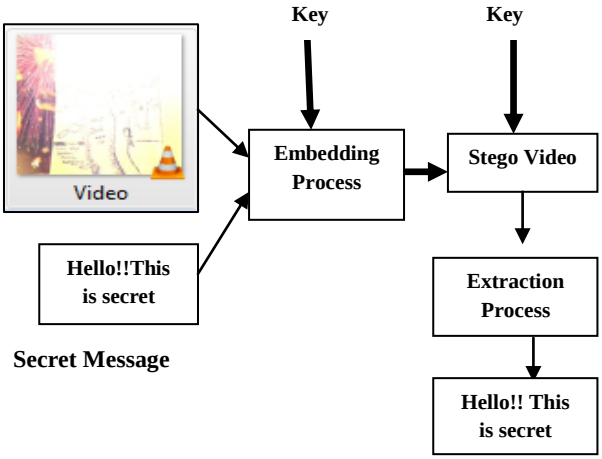


Fig 5: Process of Video Steganography

7. ELEMENTS OF VIDEO STEGANOGRAPHY

Video steganography process contains five components, which plays major role in data hiding process. They are as following:

- **Cover-Video (C):** Original video which is used as a carrier for hidden information.
- **Secret Message (M)**: Actual information which is used to hide inside cover video. Message can be a plain text, image or audio/video file.
- **Stego-Video (S)**: After embedding message into cover video, a new video file is generated, which actually contains secret message behind it, known as stego-video.
- **Stego-Key (K)**: This key is used for embedding or extracting the messages from cover-video and stego-video.

8. CHARACTERISTICS OF VIDEO STEGANOGRAPHY

A good steganography must have three prosperities i.e. Capacity, perceptual transparency and security. These are the main parameters that affect the concept of video

steganography. Most commonly used properties are following:

8.1 Capacity

It means total amount of data or number of bits that can be hide inside carrier video. It defines the maximum size of secret message or its length [18].

$$\textbf{Capacity} = \frac{No.of\ pixels\ of\ secret\ vidoe\ \ that\ are\ hidden}{No.of\ pixels\ of\ cover\ video\ that\ are\ used\ to\ hide\ data} \quad \textbf{(1)}$$

8.2 Perceptual transparency (Perceptibility)

The data should be hidden in such a manner that it should not be visible to human visual system. So it should be transparent. If we increase the capacity of data then its transparency will be affected. Perceptual transparency is of two types: Quality and fidelity.

8.3 Quality

It is an important factor of steganography and calculated by PSNR and MSE. PSNR is a peak to signal noise ratio used to measure quality of stego video. It is measured in decibel (dB). And MSE is a mean error ratio, which shows errors between cover and original video. PSNR should be high and MSE should be low for achieving good quality video.

$$\textbf{MSE}=\frac{1}{PQ}\sum_{i=1}^{P}\sum_{j=1}^{Q}(a(i,j)-b(i,j))^2 \quad \textbf{(2)}$$

In equation (2), P & Q are number of rows and columns. a and b are original and stego images respectively.

$$\textbf{PSNR}=10log_{10}\frac{255}{\sqrt{MSE}} \quad \textbf{(3)}$$

In equation (3), 255 is a fluctuation value in gray levels and its can be represented by R or L.

SSIM = 1/MSE, shows similarity between original and stego video. SSIM is inversely proportional to MSE

8.4 Video Fidelity

It defines as the perceptual similarity between signals before or after processing.

$$\textbf{IF} = 1-\sum_{i,j}(Io(i,j)-Is(i,j))^2 \Big/ \sum_{i,j} Io(i,j)^2 \quad \textbf{(4)}$$

8.5 Security

Attackers can extract the important information by applying various attacks. So security of video steganography must be high using various encryption and security algorithms.
BER (Bit error rate) = 1/PSNR, if BER is low then higher will be the reliability of algorithm.

9. TECHNIQUES

The major work of video Steganography is hide secret message without affecting the visual quality, and architecture of video file. Various methods are used for video steganography on the basis of spatial domain and frequency domain. In spatial Domain, secret data bits are directly replaced with the cover file bits. LSB substitution is a basic methodology used in spatial domain. In frequency domain, the manipulation of co-efficient is done using various transformations like Fourier transformation, cosine and wavelet transformations [17].

9.1 LSB Substitution Method

LSB means least significant bits are used to embed secret message. In this technique, secret bits are directly replaced with least significant bits of cover media. LSB bits are more secure for hiding information then MSB (most significant bits) [25]. If we hide data in most significant bits then it will distort the frames and affect the quality of video frames. So, secrete message becomes slightly visible like Visible watermarking. Also MSB bits contain important information so if we replace these bits it will damage the image/frame scenes. LSB substitution can be done in two ways either by replacing LSB or by matching. In LSB replacement (LSBR) we flip the last bits of image pixel with secret data and in LSB matching (LSBM), randomly increment or decrement the data values [3].

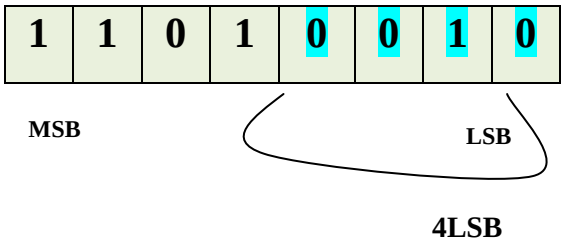


Fig 6: LSB and MSB Bits

The hiding of bits can be done either at bit level or byte level. At bit level, firstly we convert the bytes into bits and then hide the secret message bits in the places of least significant bits of video frame pixels. This process enhances the security of data hiding technique. If we hide data in between the MSB bits, then it will affect the quality of video. so we prefer LSB bits to hide data and maintains quality of video by changing low resolution.

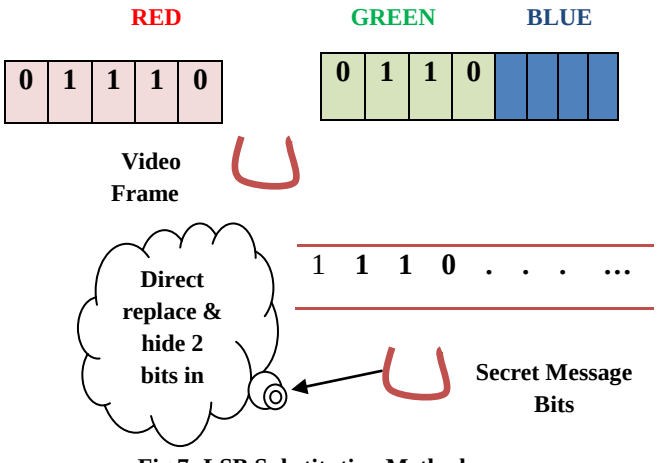


Fig 7: LSB Substitution Method

In 24 bit (RGB) images, Red color channel represents LSB bits and Green & blue channels are Most Significant bits. From which, Green, & Blue channels are used to hide secret message, because these bits has minimum visual perceptibility as compared to red bits. So 24- bit color images have high hiding capacity than 8- bit gray level images. For example: if R is secret information & we want to hide secret data inside

video frames. Firstly, we have to perform conversion process i.e. convert our secret data characters into ASCII code values and then convert into binary format (contains bit values). Then after this process, we perform embedding process in which we hide our secret data bits in between the frame's pixel values but one by one.

Cover Image: 11001010 00110101 00011010 00000000

Secret Image: 01 10 11 01

Stego Image: 11001001 00110110 00011011 00000001

Fig 8: Example of LSB

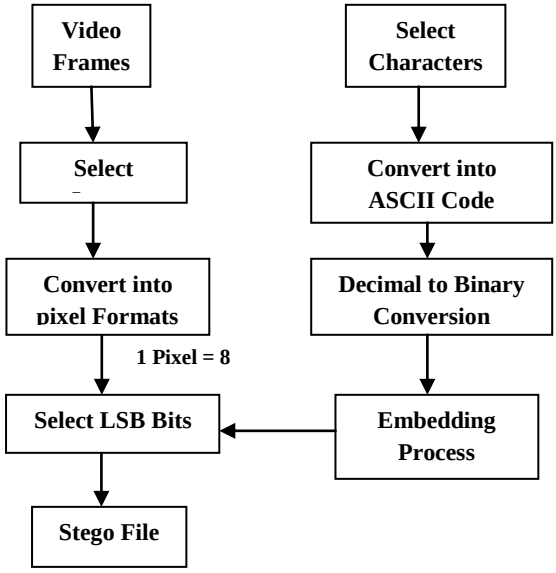


Fig 9: Flow chart of LSB

9.2 DCT (Discrete Cosine Transformation)

DCT stands for as Discrete Cosine Transformation. The secret data is embedded by manipulating the coefficient of image frame pixels.

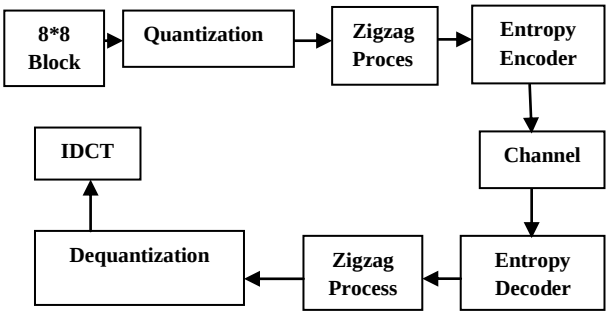


Fig 10: DCT Method

9.3 DWT (Discrete Wavelet Transformation)

DWT is based on sub-band coding and it is easy to implement because it reduces the resources requirements, time complexity and processing time. DWT is of two types. 1-DWT transforms contains High (H) and low (L) frequency bands. A 2-D DWT transforms or divides an image into four sub bands i.e. LL, LH, HL & HH sub bands. The LL band contains less important information, which is not useful to represent an image frame. But, the other three sub-bands give the important information about the image. So, we hide data in LL (High) bands because there are no compression data losses and also not reduce the quality of image frames [18].

10. VIDEO STEGANALYSIS

The main motive of steganalysis is to detect the presence of secret message inside media file like image and video. Its play an important role in computer forensics department for security purpose and find out whether coming media is fake media files or not. If yes, then it helps to track the cyber criminals by analyzing the parameters such as contrast checking, height, width, size and frame number & histogram analysis of secrete message before & after hiding process [1].

10.1 Challenges of Steganalysis

There are various challenges of steganalysis. These challenges are need to be completed by computer forensics to avoid hacker's attacks such as:

- It analyzes whether media file contains secret message or not in a hidden manner.
- Analyze the type of steganography, if message is embedded or not.
- Identify length and size of secret message.
- Extract message from medium.
- Check encryption of message.
- Check noise added in signals of file and decrypt it.

10.2 Steganalysis Techniques

There are various steganalysis techniques, which are used to detect the presence of hidden messages behind digital media files over network. Some of techniques are described as follow:

10.2.1 Histogram analysis

The histogram analysis is to detect significant changes in frequency values of the colors by comparing the cover video with the stego video. This analysis is carried out on the basis of four components of any image frames i.e. Brightness, Sharpness and RGB color contrast [1].

10.2.2 Authentication check

It means identify a stego video and access it using some labeling information i.e. password verification, by analyzing the embedded logo as watermark and pass key. Until you are not authorized you can't extract secret message.

10.2.3 By applying attacks

Various attacks are applied on stego videos to break its security. These attacks main purpose is to determine stego media files by comparing original and modified files.

10.3 Types of Attacks

By applying various attacks, we can remove hidden message by modifying characters and destroying the hidden information at bit or byte level. Three main classes of attacks are Visual, Statistical & Structured.

10.3.1 *Visual attacks*

Identify the existence of secret message by visually identifying the carrier medium. A steganography concept should be resist to visual attacks so that human eye can't predict the difference between original and stego video file.

a) **Active Attack-** these attacks Identify stego key algorithms & data location, which are used to embed the message without any modification in file. Attackers can alter the important information according to their need.
b) **Passive Attack-** these attacks identify the existence or absence of message and remove them.

10.3.2 Statistical attacks

The presence of message is identifying by analyzing the image behavior using histogram analysis, Chi- square attack, RS- Analysis. Steganography process must have resistance to these attacks. These attacks are of two types:

a) **Targeted Steganalysis:** It studies the image frames, analyze the embed algorithm and find statistics changes in these frames after embedding the secret message. It gives accurate results and secures enough. But, it is inflexible in nature and work only with specific type of stego systems.
b) **Blind Steganalysis:** It analyzes the presence of secret message by random guessing method (i.e. Hit and Trail Method). It learns the difference in statistical properties of original and stego images. Learning process is done by large database based training machines and it works with all type of stego systems such as outguess and YASS. Blind analysis is very expensive and less accurate than target ones. So semi blind steganalysis is also used for finding fake or hidden data from specific type stego systems.

10.3.3 Structured attacks

Format of data files changes as the data is embedded. It basically identifies the characteristic structure changes in image. Some Basic attacks used in steganography:

- **Steganography only attack** – only, carrier medium is known for analysis.
- **Known - carrier attack** - cover media and stego media both are known.
- **Known - message attack** – only secret data is known for analysis.
- **Chosen - steganography attack** – stego medium, algorithm and steganography tools are known.
- **Chosen - message attack**- algorithm and stego tools are known.
- **Known- steganography attack** - carrier, stego, algorithm and tools are known.

11. APPLICATIONS OF STEGANOGRPAHY

- It is used in computer forensics to identify whether a video is fake one or not. And also track the cyber criminals.
- Digital Watermarking is an important application of steganography as it is used to embed watermark like logo inside the media files for their copy right protection and to avoid pirated videos and audio files.
- Used in biometrics to embed fingerprint detail for verification, or eye's verification related data inside a digital file.
- Medical field used the steganography concept to embed patient details inside the image and helps to maintain large information inside a cover media [14].
- Copyright Protection mechanisms that avoid data, typically digital data, from being copied.
- In Military field for secret communication [9].
- In smartcards to embed person details.
- It can be used to embed metadata. Metadata refers to additional information that you want to embed inside cover media [17].

12. CONCLUSION

Video steganography is a new research area used for protecting covert communication from hackers using various embedding algorithms for hiding the secret message inside multimedia files. It works with a lot of applications for hiding different kind of information and for providing security. We can embed large amount of data behind selected frames of video, hence it is very difficult to find out that which part of video contains hidden data. We can easily detect the fake videos, which are transferring over internet from sender to receiver by using computer forensic check. Security protection in steganography is very high from cryptography and it is very useful to explore stego videos to avoid cyber crimes and for breaking the planning strategies of terrorists. Video steganography is a very popular research field as it can done work with multiple domains like digital image processing (DIP), network security or information security. Protection of private information from attackers is still more challenging task. So, future work is to embed high capacity data inside video frames with high security to resist various steganalysis attacks and with minimum degradation in quality of video.

13. ACKNOWLEDGMENTS

The authors would like to thanks to the earlier work regarding different video Steganography methods that contribute the work made in this paper. All work done in this paper will help to the researchers for doing future work based on video steganography.

14. REFERENCES

[1] Sunil. K. Moon, Rajeshree. D. Raut, "Analysis of Secured Video Steganography Using Computer Forensics Technique for Enhance Data security", IEEE Second International Conference on image information processing, pp 660-665, 2013.

[2] K.Parvathi Divya, K.Mahesh, "Various Techniques in Video Steganography-A Review", International Journal of Computer & organization Trends, Vol.5, pp 8-10, February 2014.

[3] Hemant Gupta, Setu Chaturvedi, "Video Steganography through LSB Based Hybrid Approach", International Journal of Computer Science and Network Security, Vol.14, Issue 3, pp 99-106, March 2014.

[4] Mehdi Hussain and Mureed Hussain, "A Survey of Image Steganography Techniques", International Journal of Advanced Science and Technology, Vol. 54, pp 113-124, May, 2013.

[5] Babloo Saha and Shuchi Sharma., "Steganographic Techniques of Data Hiding using Digital Images", Defense Science Journal, Vol. 62, Issue 1, January 2012, pp 11-18.

[6] A. Swathi 1, Dr. S.A.K Jilani, "Video Steganography by Substitution Using Different Polynomial Equations", International Journal of Computational Engineering Research, Vol.2, Issue 5, September 2012.

[7] Geetha C.R., H. D. Giriprakash, "Image Steganography by Variable Embedding and Multiple Edge Detection

using Canny Operator", International Journal of computer Applications, Vol.48, Issue 16, June 2012.

[8] Saurabh Singh, Ashutosh Datar, "Improved Hash Based Approach for Secure Color Image Steganography using Canny Edge Detection Method", International Journal of Computer Science and Network Security, Vol.14, Issue 7, (July. 2014).

[9] K.V.Vinodkumar, V. Lokeswara Reddy, "A Novel Data Embedding Technique for Hiding Text in Video File using Steganography", International Journal of Computer Applications, Vol.77, Issue 17, September 2013.

[10] M. Pavani, S. Naganjaneyulu, C. Nagaraju, "A Survey on LSB Based Steganography Methods", International Journal of Engineering and Computer Science, Vol.2, Issue 8, August 2013 pp. 2464-2467.

[11] K. Naveen BrahmaTeja1, Dr. G. L. Madhumati 2, K. Rama Koteswara, "Data Hiding Using EDGE Based Steganography", International Journal of Emerging Technology and Advanced Engineering, Vol.2, Issue 11, November 2012.

[12] Souvik Bhattacharyya, Indradip Banerjee and Gautam Sanyal, "A Survey of Steganography and Steganalysis Technique in Image, Text, Audio and Video as Cover Carrier", Journal of Global Research in Computer Science, Vol.2, Issue 4, April 2011.

[13] Neethu Prabhakaran, D.Shanthi, "A New Cryptic Steganographic Approach using Video Steganography", International Journal of Computer Applications, Vol.49, Issue 7, July 2012.

[14] Dimple Anandpara, Amit D. Kothari, "Working and Comparative Analysis of Various Spatial based Image Steganography Techniques", International Journal of Computer Applications, Vol.113, Issue 12, March 2015.

[15] M.Jyotheeswari, V. Lokeswara Reddy, "A Novel Steganographic System for Data Hiding in Video/Audio", International Journal of Computer Application, Vol.82, Issue 11, November 2013.

[16] Ranjeet Kumar Singh, Shikha Gupta, and Deepak Gupta, "A Secure Authentication Technique using Edge Detection in Watermarking", International Journal of Computer Applications, Vol.61, Issue 11, January 2013.

[17] Anjula Gupta, Navpreet Kaur Walia, "A Survey on Data Hiding and Steganographic Techniques", International Journal for Scientific Research & Development, Vol. 2, Issue 2, 2014.

[18] Parul, Manju and Dr. Harish Rohil, "Optimized Image Steganography using Discrete Wavelet Transform (DWT)", International Journal of Recent Development in Engineering and Technology, Vol.2, Issue 2, February 2014.

[19] Shivani Khosla, Paramjeet Kaur, "Secure Data Hiding Technique Using Video Steganography and Watermarking", International Journal of Computer Applications, Vol.95, Issue 20, June 2014.

[20] Pooja Yadav, Nishchol Mishra, Sanjeev Sharma," A Secure Video Steganography with Encryption Based on LSB Technique", IEEE International Conference on Computational Intelligence and Computing Research, 2013.

[21] Arijit Basu, Gaurav Kumar, Soumyajit Sarkar, "A Video Steganography approach using Random Least Significant Bit Algorithm", International Journal of Science and Research (IJSR), Vol.3, Issue 6, June 2014.

[22] Vijay Kumar Sharma, Vishal Shrivastva, "A steganography algorithm for hiding image in image improved LSB substitution by minimize Detection", Journal of Theoretical and Applied Information Technology, Vol. 36, Issue 1, February 2012.

[23] Atallah M. Al-Shatnawi, "A New Method in Image Steganography with Improved Image Quality", Applied Mathematical Sciences, Vol. 6, Issue 79, pp .3907 – 3915, 2012.

[24] Mamta Juneja and Parvinder Singh Sandhu, "Improved LSB based Steganography Techniques for Color Images in Spatial Domain", International Journal of Network Security, Vol.16, No.6, pp.452-462, Nov. 2014.