VIDEO STEGANOGRAPHY USING WAVELET TRANSFORM

DESSERTATION

Submitted in partial fulfillment of the
requirement for the Award of
Degree of

MASTER OF TECHNOLOGY

IN

Electronics & Communication

Engineering

Submitted by

Sonali Rana

Regd. No:-11510781

Under the Guidance of

Mrs. Rosepreet Kaur Bhogal

Assistant Professor

Lovely Faculty of Technology and Sciences

School of Electrical and Electronics Engineering, (SEEE)

Lovely Professional University

Phagwara (Punjab), India

MAY-2017

ABSTRACT

"It is often my nature to be abstract, hidden in plain sight or nowhere at all" *Gerard Way*

Fundamental obligation of concealing data from intruders is mastered by the use of steganography, which is an art of concealing and protecting data. The propounded work is an application to conceal and protect covert data in a carrier video file. The research is concerned with imbedding the covert data inside the harmless cover media is an efficient and robust way. Data is a salient virtue for any firm or an individual entity and it must be secured from earwigs, this can be accomplished with the aid of steganography. Steganography conceals and secures data without any noticeable alterations and variations. Therefore, importance of reducing the chance of the information being detected by some earwig is the fundamental grail nowadays. So we need a system that secures our data from eavesdroppers and this will lead to the confidentiality of the hidden data. In the research, a study on Steganography is done; with its implementation technique has been discussed in detail, along with the different types in practice. In order to transmit data securely to destination, Steganography can be implemented. LSB algorithm and DWT (Discrete Wavelet Transform) on image is been performed in order to hide the message or text. A comparison between the PSNR and MSE values, DET (Data Encryption Data), DDT (Data Decryption Data), Imbedding Payload, MSD (Mean Standard Deviation) of six different cover images with covert and concealed data imbedded inside it is also demonstrated. Moreover, comparison is drawn between the imbedding capacities of two proffered algorithms.

ACKNOWLEDGEMENT

Foremost, I would like to express my sincere gratitude towards my guide, **Mrs. Rosepreet Kaur Bhogal**, who gave her full support in the working of this dissertation work with her stimulating suggestions and encouragement all the time. She has always been a source of ideas.

I am thankful to management of Lovely Professional University for giving me an opportunity to carry out studies at the university and providing the proper infrastructure like internet facility which is pool of vast knowledge to work in.

I owe my heartiest thanks to my mother, late father, sister and brother-in-law & all those guidepost who really acted as lightening pillars to enlighten my way throughout this research that has led to successful and satisfactory completion of my research.

At last but not the least I am thankful to all my friends, who have been instrumental in creating proper, healthy and conductive environment and including new and different innovative ideas for me during this research. Without them, it would have been extremely difficult for me to do this research in a time bound structure.

I would like to thank God for the strength that keeps me standing and for the hope that keeps me believing that this research is possible.

Sonali Rana
Regd. No: - 11510781
School of Electrical and Electronics Engineering
Lovely Professional University

DECLARATION STATEMENT

I hereby declare that this submission is my own work and that to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which has been accepted for the award of any other degree or diploma of the university or other institute of higher learning, except where the acknowledgement has been made in the text.

Date:

Sonali Rana
Regd. No: - 11510781
School of Electrical and Electronics Engineering
Lovely Professional University

CERTIFICATE

This is to certify that the Dissertation entitled “Video Steganography using Wavelet Transform” submitted by Sonali Rana in partial fulfillment of the requirement for the award of the degree of Master of Technology (M.Tech) in Electronics and communication engineering, is a record of bona-fide work carried out by her under my guidance.

Date:

Mrs. Rosepreet Kaur Bhogal
Supervisor
Assistant Professor
School of Electrical and Electronics Engineering
Lovely Professional University

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

HVS	Human Visual System
LSB	Least Significant Bit
AVI	Audio Video Interface
VOIP	Voice Over Internet Protocol
DCT	Discrete Cosine Transform
PVD	Pixel Value Differencing
PMM	Pixel Mapping Method
DWT	Discrete Wavelet Transform
FFT	Fast Fourier Transform
IOT	Internet Of Things
BCD	Binary Coded Decimal
MSE	Mean Square Error
BER	Bit Error Rate
IWT	Integer Wavelet Transform
PSNR	Peak Signal To Noise Ratio
SVD	Singular Value Decomposition
RGB	Red Green Blue
GUI	Graphical User Interface
MSD	Mean Standard Deviation
DET	Data Encryption Time
DDT	Data Decryption Time
IMP	Imbedding Payload

1

INTRODUCTION

"*The beginning of knowledge is the discovery of something we do not understand"- Frank Herbert*

Steganography is gleaned out of the Greek language for obscured and classified communication. It is a concoction of two words Steganos means 'protected'/'hidden' and graphy means 'writing 'or 'script'. It is an artistry of imbedding data inside a concealed medium like text, images and videos. It is a type of concealed communication that means 'covert handwriting' whether it consists of invisible ink on paper or may be information hidden in an audio file. Different description for steganography is 'disguised in lucid appearance' and it is a science of hiding information [5]. It is a 'long in the tooth' technique and was initially worn in 440 BC for covert communication by ancient Greece. This technique is implemented by substituting least significant bit and most superfluous bits of data in secret message. Steganography is not working with one peculiar law, still one should be apprehensive while picking and reusing the video and audio files for data hiding and concealing Steganography uses one flaw of 'Human Visual System' (HVS) as vantage i.e. human eyes can't recognize or detect slight changes in the cover medium [1].

Data collateral fundamentally aims at preserving the secrecy and preserving of data and protecting the data from unauthorized users or earwigs. Innumerable methods, for example, watermarking, cipher text, encryption and Steganography were fabricated retaining in mind that the finale goal to upgrade the data security. Cryptography is also a technique to protect and conceal the data; however it is assorted from Steganography. Cryptography wherewithal writing a message in a scrabbled or jumbled form to erect a covert code [1]. Intruders cannot foretell Steganography pertained on a cover; however one can easily depict the cryptographic code. Cryptography presents the data in the jumbled and scrambled form which allure the concern of some earwigs. Cryptography obfuscates information by scrambling it to figure texts utilizing an unknown key and transmitting it to the intended receiver. There are no laws associated with Steganography, but there are some laws and rules for cryptography. Steganography uses keys for concealed and protected communication at transmission and receiving end. These keys are may be private and public according to the proffered algorithm. Secret keys elucidate the confidentiality of the hidden data. Private Secret key uses a single key for both encryption and decryption. Public keys uses disparate key for encryption and decryption. The pivotal motivation of Steganography is to bestow secret communication to camouflage message or information from invaders or non-intended users and earwigs. Communication is the vital force of any organization and is a stick out amongst the most requisite obligations of people. The purpose of covert communication is as antiquate as communication itself. It is regularly visualized that communications can be made secure by utilizing encryption techniques; however this is not so much valid in practice. Encryption permits an undeniable way to deal with information collateral and surety, and encryption programs are promptly accessible. In any case, encryption plainly marks a message as containing interesting information, and the encrypted message gets to be subject to attack. Moreover, by and large it is attractive to send information without anybody noticing that information has been sent in form of secret/hidden information. The history teaches that is preferred hiding messages rather over enciphering them, since it arouses less suspicion. This preference persists in numerous operational contexts [2].

To conceal covert data in some variant source of data without vacating any evident and noticeable evidence of data modification, Steganographic techniques can be utilized. Nowadays in digital world, invisible ink and paper have been exchanged by considerably more flexible, adaptable and practical covers, exemplar given, digital documents, images, video, and audio files are employed for concealing messages. For whatsoever length of time that an electronic archive accommodates useless or redundant information, it can be utilized as a carrier for concealing covert messages [3]. The greater part of the traditional Steganography methods have slenderer data-concealing capacity about 10% or less. The aim of those methods was either to substitute all the least significant bits of an image with the covert data to substitute an extraordinary part of the recurrence components of the vessel image.

1.1 Need of Steganography

The fundamental obligation of Steganography is to yield protected, concealed and reliable communication within two parties and moreover to yield security. As we know from decades or centuries human uses covert communication like Romans do using some wax ink and invisible ink. Invisible ink is a composition of milk and fruit juices. In ancient times concealed and protected communication was very prominent. This is the era of technology where secrecy and confidentiality for accessing the data is the fundamental interest. In this current era every human is accessing the internet for communication and updation of data, so some kind of secret communication technique is required through which it can be secretly transmit and receive the intended data [4]. Steganography is being used around the world on computer systems for secret communication and security. It uses ciphers to conceal the data. Other obligation of Steganography is to secure the world from terrorist attacks. As 9/11 attackers and intruders used Steganography techniques and encryption for planning the bomb blasts in U.S.A. In order to anticipate their steps, therefore some kind of a secure technique is enforced that conceals the data in plain sight but also provides extra security and reliability.

1.2 Growth of Steganography

Steganography as a technology yields contemporary data compression, spread spectrum, information theory and cryptography technologies which are concocted together to satisfy the obligation for privacy on the Internet. Steganography has become a hot and popular technology to provide electronic privacy and copyright protection. Many companies are using steganographic methods as they require secrecy, information security and integrity. Therefore, it is a fundamental interest for companies and firms. For high level of confidentiality companies fuse Steganography and cryptography to augment and improve the security, secrecy of data or message [1].

1.3 Principles of Steganography

Steganography is an effective method of hiding data in plain sight. This technology is easy to use and difficult to crack or detect. Even if some hacker hacks or suspects the data, there is no proof of its existence. There are three core principles are used to judge the effectiveness of the steganographic technique-amount of data, difficulty of detection and difficulty of removal. Amount of data tells how much efficient is the technique, so more the data you will hide better will be the technique. Difficulty level of detection tells how easily your hidden data is detectable by some unintended user and earwig. There is a direct relationship between the amount of data can be hidden and how easily it is detectable and traceable by third party. As you increase the amount of data can be hidden more will be the chances of its detection by third party [4]. Difficulty of removal tells that some hacker intercepting the carrier file will not able to remove the hidden data contained in it.

1.4 Types of Steganography

Steganography is a fine artistry of concealing and protecting information in another medium. Steganography is turning out to be the important ingredient for security and privacy of present day technology and Internet. It is the most common method to conceal covert data. It uses image as a cover and conceals data in it [2]. It practices least significant bits to conceal the data in cover image and uses the most trivial flaw of human visual system, as our human eyes are not able to detect the changes made in the quality of the carrier image. In this luminance, brightness and intensity is amended by using LSB technique and it is not detectable by human eyes. One of them is grouping based on the sort of cover type and the description is as per the following:

1.4.1 Image Steganography

Images are employed as the ubiquitous carrier medium for steganography. Hiding and concealing information in image is known as image steganography. In this method pixels are used to hide the information. The carrier image is called envelop and packet. The carrier image hiding information inside it is called stego-image. A message is imbedded in a digital image employing an imbedding algorithm and also uses the secret key for enhancing secrecy. The following stego-image is dispatch to the receiver [4]. On the receiving side, it is processed by the extraction algorithm employing the same key. Amid the transmission of stego-image unintended persons can just perceive the transmission of an image still can't depict the existence of the hidden message [6]. To hide a message inside an image without changing its visible properties, the cover source can be altered in noisy areas with innumerable color differences, so less deliberation will be drawn to the modifications. The most widely identified methods to attain these modifications include the usage of the least significant piece or LSB, masking, filtering and transformations on the carrier image. These methods can be used on various sorts of image files with differing degrees of success.

1.4.2 Network Steganography

The term protocol steganography refers to imbedding information inside network protocols, for example, TCP/IP, UDP, and ICMP and so on. The network steganography is also known as protocol steganography. In the OSI network layer unveil that are some covert channels, where steganography can be achieved by concealing information in elective or unused header bits of TCP/IP fields [3].

1.4.3 Video Steganography

Video Steganography is a method to hide and protect any type of files in any extension into digital video format [7]. Video is a combination of images is used as a carrier for hidden information. Video steganography employs video formats, example given, H.264, Mp4, MPEG, AVI, and so on.

1.4.4 Audio Steganography

It is different form of data hiding. In this data is concealed inside an audio file. It is an untraceable and unnoticeable form of steganography. It uses one drawback of Human Auditory System that it cannot detect small changes in the quality of the audio file. In this frequency masking occurs because human ears cannot perceive small alterations in audio file i.e., low frequencies are masked by the higher frequencies. When choosing audio as a carrier for information concealing it is named as audio steganography. Due to the popularity of voice over IP (VOIP), audio has turned into a remarkable carrier medium. Audio steganography employs digital audio formats, example given as WAVE, MIDI, AVI, and MPEG or and so forth for concealing secret message.

1.4.5 Text Steganography

It is another kind of steganography in order to conceal and protect the secret message in a text file. It is a hard and strenuous form of steganography because the amount of data concealed in the text file is so small and less that one cannot perceive the covert message. Text steganography can be split in three categories- format based, random and statistical generation and linguistic technique. Format based technique used physical formatting of text as a place to hide secret data. In this secret steganographic text can be hidden in existing text files. This method can take the advantage of the fact that Human Visual System can't perceive small changes but computer systems can do. Random and statistical generation is generating cover text according to the statistical properties. Means this method is based on character sequences and word sequences. So hiding data in character sequences appears as random sequence of characters. Now linguistic method specifically considers the linguistic properties of generated and modified text. It uses linguistic structure as a place to hide intended data.

i. Line-Shift Coding
ii. Word-Shift Coding
iii. Feature Coding

1.4.5.1 Block Diagram of Steganography:-

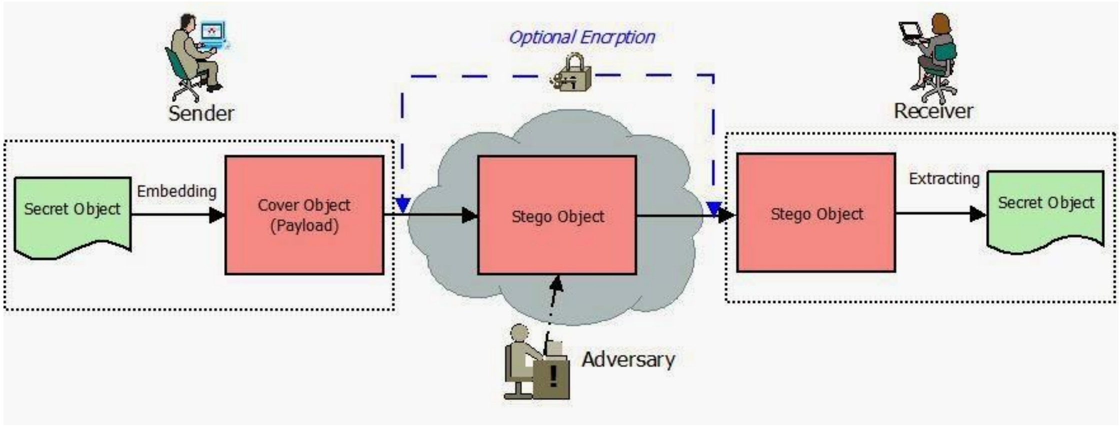


Fig.1.1- Steganography Mechanism

The above figure demonstrates a simple and easy representation of the generic embedding and extraction process in steganography. In this example, a secret data is being embedded inside a cover image to create the stego image. A key is frequently required in the embedding process. The embedding procedure is finished by the sender by utilizing the correct stego key. The recipient can extract the stego cover image with a specific end goal to see the secret data by utilizing the same key utilized by the sender. The stego image ought to look practically identical to the cover image.

1.4.6 Video Steganography

A video file as a cover has numerous vantage points over other cover extensions; video steganography method is presently an emerging area of research. It is a method to conceal and protect any type of files into a video file. The alteration in the video file is significantly more difficult to percept by the HVS. This technique is much more secure and robust than all the other techniques of steganography. As we know that a video is a collection of audio and images, so in this method the hidden message is imbedded into a video file. This technique occasionally uses the Discrete Cosine Transform (DCT). DCT entirety by marginally changing each of the images of video stream, but the change is so trivial that human eye can’t see and interpret [5]. The main advantage of video steganography is that it can hide a large amount of data in it. In this one can imbed message in audio as well as image files. Utilization of the video steganography is more beneficial than other multimedia files, as a result of its size and memory requirements. Thusly most of the current methods on images and audio can be attached to video files also.

Video steganography is the expansion of image steganography. A video file can simply be seen as a series of images. So information is hidden inside the video like in image in image steganography. There are numerous viewpoints that differentiate between video steganography and image steganography. As the video content is dynamic, so the detection of the hidden information is very less as compared with images [8]. In addition to the image attacks, there are significantly more attacks for videos; example given is lossy compression, change of frame rate, formats interchanging, addition or deletion of frames in the course of video processing. Taking care of a video stream as multiple two-dimensional images, does not consider the dependencies that exist among pixels in their three dimensions. The concealing limit is much higher on account of video. Videos give new heights to information hiding, for example, hiding messages in motion components. We can imbed message in audio as well as image files. So, the audio components of the video file can likewise be employed for information hiding.

1.5 Image Steganography Techniques

Image steganography procedure can be branched into following domains.

i. Spatial Domain
ii. Transform Domain
iii. Distortion Procedure
iv. Masking and Filtering

1.5.1 Spatial Domain Methods

There are diverse versions of spatial steganography, especially change a few bits in the image pixel values in concealing information. Least significant bit (LSB) - based steganography is one of the simplest techniques that conceals and protects a covert message in the LSBs of pixel values without offering diverse perceptible distortions. Small alterations and changes in the value of the LSB are imperceptible for human eyes. It manipulates the LSBs of the secret message with the LSBs of the carrier image. In this we can take the binary representation of the hidden data and then overwrite or embed the LSB of each byte within the cover or carrier image. Means we are manipulating the bits. Spatial domain techniques are extensively named takes after hinged on the techniques utilized for hiding information.

i. LSB
ii. PVD
iii. PMM

1.5.1.1. Least Significant Bit (LSB)

It is the easiest method for imbedding covert data in cover image is employing Least Significant Bits (LSB). The concept of the LSB computation is to imbed the bits of the concealed data especially into the LSB plane of the envelop image in a deterministic series. As the LSB method makes use of the pixel information of an image and therefore utilizes bits of every pixel as a part of the image. But it is essential to employ a lossless compression format because if the user will use lossy compression chances of the data loss will be higher. This method is more robust and best for grayscale image and if the hidden message length is smaller than the cover image or file. The LSB insertion alters according to the type of image are used. For an 8 bit image, the eight bit of every byte of the image is substituted with the bit of the covert message. For 24 bit image, the LSB bit of each of the red, green and blue color components are replaced. LSB works efficiently for BMP image because the compression in BMP is lossless. This also reduces the chance of the detection of the secret data from earwigs.

Let’s demonstrate an example for the operation of the LSB Hiding , take a 24-bit scheme image i.e.8- bit of Red plan, 8-bit of Green and 8- bit of Blue plane. In this scheme the amount of change will be minimum and obscure to the human visual system. Let us assume we have three adjacent pixels i.e., nine bits with following RGB scheme encoding:-

10010101	00001101	11001001
10010110	00001111	11001010
10011111	00010000	11001011

Let us take an example to conceal the successive 9 bits of data:- 101101101.So in order to overlap these ,9 bits over the LSB of the 9 bytes above, then will get:-

10010101	00001100	11001001
10010111	00001110	11001011
10011111	00010000	11001011

Now we have successfully hidden and concealed 9 bits by only changing 4 bits, or roughly 50%, of the LSB

Vantage points of LSB technique:

i. Easy.
ii. High imbedding capacity.
iii. Mere probability for deterioration of carrier image.

Demerits of LSB technique are:

i. Image manipulation can distort the concealed data. Hence it is less robust.
ii. Easy Stegoanalysis.
iii. Hidden data can be easily destroyed using simple attacks [7].

1.5.1.2. Pixel Value Differencing (PVD)

It is a method proffered, for imbedding a covert data; the real carrier image is divided into non covering blocks of two pixels. A difference value is enumerated from the values of the two successive pixels in each square. All credible difference values are represented into various reaches. In this technique the capacity of hidden data in edges is higher than that of smooth areas. The HVS are more responsive to noise in smooth area than in the edge area. The fluctuation value then is replaced by second attribute to imbed the value of a sub-stream of the covert data. The quantity of bits which can be embedded in a pixel merge is chosen by the breadth of the range that the fluctuation attribute has a place with.

The merits of method are:-

i. High imbedding capacity
ii. Good imperceptibility

PVD plot employs the difference attribute across two consecutive pixels in a piece to determine what number of secret bits ought to be imbedded. There are two sort of the quantization go table in Wu and Tasi's method. The first was based on selecting the range breadths of [8, 8, 16, 32, 64, 128], to give extensive capacity. The later was hinged on selecting the range breadths of [2, 2, 4, 4, 4, 8, 8, 16, 16, 32, 32, 64, 64], to give extreme subtlety.

1.5.1.3. Pixel Mapping Method (PMM)

It is another method to sketch data into image. It utilizes concept of pixel force and no of 1's in pixel to sketch data. The vantage point of this approach is:

i. Harvest better imbedding capacity.
ii. Suitable PSNR Value than PVD and GLM.

1.5.2 Transform Domain Technique

In this domain, the concealment of information is done inside an image or a video. The time domain steganography techniques allows more significant amount of data concealment, but it is less immune to Stegoanalysis attacks. Transform domain steganography, don't conceal the information behind image pixels especially rather transforming the image former masking the covert data. These techniques are more resistant to steganographic attacks as correlated to the time domain techniques. Disparate calculations and transformations are employed on the image to conceal information in it. Many systems nowadays work in the transform domain. Transform domain techniques concealed data by transforming significant areas of carrier image which makes this method robust against disparate image processing applications like compression, cropping, and enhancement or enrichment and so on. The essential way to deal with hiding data with DCT, FFT or Wavelet is to remodel the envelop image, twist the coefficients, and after that reverse the transformation. Few transform domain techniques don't come out to be rely on the image format and they may surpass lossless and lossy format coincide. TDT transforms are divided into:

i. DFT.
ii. DCT.
iii. FFT.

iv. DWT.

v. DCT.

vi. Embedding in coefficient bits.

1.5.2.1 Discrete Cosine Transform (DCT)

It is a technique in which the insertion of the covert data in carrier hinged on the DCT coefficients. Any DCT coefficient attribute above proper threshold is a potential place for mixture of covert data. In this method the Most Significant Bits of covert data are concealed in Least Significant bits of those pixels of cover image whose DCT coefficient value is highly outstanding than a specific threshold attribute. DCT transforms the image from time to frequency domain. It splits the image into small bands with respect to its visual calibre factor, i.e. high, mesial and low frequency attributes. DCT is a method to transform consecutive 88-pixel sections of the image from time domain to 64 DCT coefficients each in frequency domain. The LSBs of the quantized DCT attributes are employed as unused bits into which the concealed message is imbedded. The modification of a single DCT coefficient affects each of the 64 image pixels. Since this alteration occurs in the frequency domain and not in the spatial domain, there are no apparent visual differences. The main vantage point of DCT has over other transforms is the capacity to diminish and reduce the square like appearance eventuate when the boundaries across the 8x8 sub-images get to be visible and it is called hindrance relic.

1.5.2.2 Discrete Fourier Transform (DFT)

DFT gives the better and good evaluation of Fourier transform on discrete set of frequencies. The Discrete Fourier Transform is employed to get frequency part for every pixel value. Using DFT, all insertion is done in frequency domain. DFT is connected on source image to convert from spatial domain to frequency domain. Every 8 bit pixel in spatial domain is transformed into two parts i.e. real and another is imaginary part. The authenticating bits are inserted in real part of the frequency domain .The scheme is iterated for whole image matrix in a same way. In the wake of imbedding inverse DFT is executed to convert from frequency domain to time domain. Fast Fourier Transform (FFT) is the staunch technique of DFT because of high speed and productive technique.

1.5.2.3. Discrete Wavelet Transform (DWT)

It is a transform in which the wavelets are discretely sampled are called discrete wavelet transform (DWT). The prime vantage points of DWT are more than Fourier transforms because it gives both time-frequency representation. Wavelet transforms give results in floating point numbers. DWT gives best results for non-stationary signals like human speech etc. DWT can be implemented for both the 1-D and 2-D signals. Easiest and simplest form of DWT is Haar wavelet. A 2-dimensional Haar-DWT gives to two operations: First part is the horizontal operation and the other part is the vertical operation. These operations give sum and difference at level-1 decomposition. DWT decomposes in four distinct frequency sub bands, named as LL, LH, HL, and HH. LL is the nether resolution resemblance of the image and is the low frequency portion [12]. In Haar transform the details and approximations are multiplied by square root of two in order to preserve the energy of the signal. Execute the addition and subtraction operations on neighboring pixels and afterward store the sum on the top and the difference on the bottom. At long last we will get 4 sub-bands denoted as LL, HL, LH, and HH respectively.

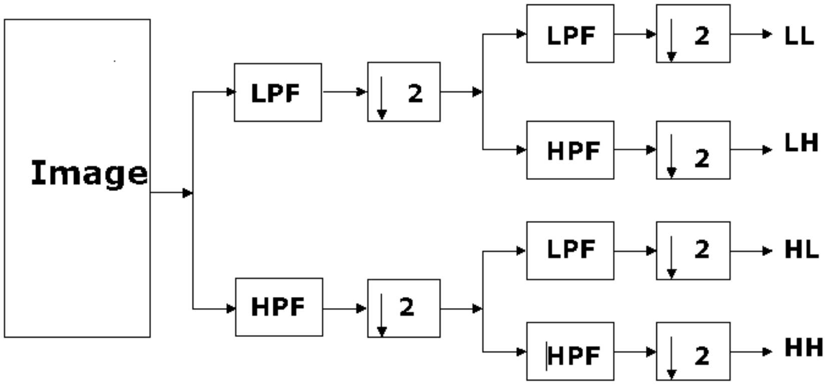


Fig1.2-Block diagram of DWT Decomposition

1.5.3. Distortion Techniques

Distortion techniques needs the information of the original carrier image during the decoding procedure, where the decoder function is to examine for the differences between the original cover and the distorted cover image with a specific end aspiration to restore and protect the covert data. The encoder unites a sequence of variation and alterations to the cover frame. Therefore, information is pictured as it is accumulated by flag aliasing. A stego image is made by implemented a series of alterations and editing to the carrier frame. The series of alteration is use to match the covert data which is demanded to transmit. The encoding scheme is for message to pseudo-randomly elect values of an image. But in real picture that the stego image is not the identical as the carrier image at the given message attribute value, the message bit is high i.e. 1. But originally, the message bit having a value is “0.” The encryption entity can edit the “1” value of image attributes in such a manner, that the statistical features of an image are not influenced [3]. Nonetheless, the necessity for sending the carrier image restricts the vantages and merits of this technique. In any concealed and protected system, the cover image can’t be employed more than once. There is a probability that an earwig do some alterations with the stego image by analysis features; the recipient can be discovered without any much of the effort.

1.5.4. Masking and Filtering

Masking and filtering method is a concealed method that uses disparate methodology for concealing a covert message. These methods camouflage information by using an image, in an indistinguishable way to form paper watermarks, putting points in an image. This can be procured by editing the brightness of the specific points of the carrier image. It is non-detectable to lossy techniques, as it won’t alter the covert message by replacing image coefficients. Even if masking alters the visible properties of an image, it is executed in a way that the Human Visual System (HVS) won’t see the changes and alterations [2]. After all masking employs visible parts of an image; it is more robust than LSB insertion with respect to compression, cropping and various forms of image processing. The information is imbedded in the more significant areas than normally concealing it into the noisy level of an image, which makes it more appropriate than LSB concealing method for lossy compression like JPEG. Masking and filtering method is typically restricted to 24 bits or grayscale images. Merits and demerits of Masking and filtering procedure are:

i. As the information is concealed in the visible portions of an image, with respect to compression this method is much more robust and good as compared to LSB replacement.

ii. Technique is only felicitous and confined to 24 bit and gray scale images.

*****

2

LITERATURE REVIEW

"If the facts don't fit the theory, change the facts." *-Albert Einstein*

Rear chapter gave glance of Steganography regarding data security and secrecy for obscured communication. In this review scholars gave suitable solution for enhancing data security for classified communication using steganography.

N. Jothy, et.al (2016): The proffered paper shows that the secret images/data can be withdraw without any distortion to the carrier image (i.e. cover image). As the secret data is imbedded inside the carrier images using IWT makes the presence of the data concealed. Higher PSNR value results in less distortion. This technique offers the high quality of the Stego-image with high PSNR values as compared to the other methods. Moreover, this method can facilitates us to transmit the secret information to the receiver independently and more securely [9].

Joanne Hwan Jie Yin, et.al (2015): Proffered paper explains, a new way of data hiding and securing is explained rooted on the image steganography, as IP camera of low processing and memory capability is used since IoT devices are employed to provide security. Due to the limitations of the smart devices, especially lower memory and computational power, the least significant bit technique is being adapted. With the use of steganography data tracking will be laborious for earwigs and intruders and it is easy in case of encryption because the format of data is changed in cryptography. With this method, changes in least significant bit would not result in any real degradation of quality through human perception and along with statistical analysis. For providing security and secrecy LSB insertion technique is used and also suggested that cryptography should be used along with steganography in order to enhance security and secrecy [10].

Ramadhan J. Mstafa, Khaled M. Elleithy (2015): Propounded paper demonstrates a high payload video Steganography algorithm in DWT domain based on BCH codes. In this Steganography algorithm divides the video into frames and then fragments each frame into three components Y, U and V. Before the imbedding process of data, the secret data is first encoded using BCH codes in order to augment and strengthen the security and efficiency of the algorithm. Afterwards 2D- DWT has been applied to each component but mesial and high frequencies components (HL, LH, and HH) are used for imbedding the secret data. Along with, this algorithm utilizes two keys at the time of imbedding and extraction, which improved and boosted the efficiency of the system. This algorithm is resistant against median filtering attack. In order to enhance more security and efficiency linear block codes can be implemented and to enhance or upgrade the video quality other techniques in the frequency domain can be implemented [11].

Ramadhan J Mstafa and Khaled M. Elleithy (2015): The proffered paper explains a secure video Steganography algorithm based on the principle of linear block code. Nine uncompressed video sequences are used as cover data and a binary image logo as a secret message. The pixel's positions of both cover videos and secret message are randomly reordered by using a private key to improve and enhance the security of the system. Then secret message is encoded by hamming codes (7, 4) before the imbedding process in order to make the message even more secure. The final outcome of the encoded message will be added to the random values by using XOR function. These steps make the message more secure and is ready to embed into the carrier video frames. In addition, the imbedding area in each frame is randomly selected and it will be disparate from others frames to improve and enhance the robustness of the Steganography scheme [12].

Yugeshwari Kakde, Priyanka Gonnade, and Prashant Dahiwale (2015): The presented paper explains data hiding in audio video file with the help of computer forensic technique provide better hiding and security to the secret information. Here different techniques like hiding image and text behind video and audio file extracted from an .avi file are discussed. For concealing image in video file DWT, SVD (Singular Value Decomposition) and random LSB are used. These techniques reduce distortion in the host audio file. Finally computer forensic technique is used to check security parameters by giving authentication code at the receiver side. It helps in tracking terrorist activities on web [13].

Saket Kumar, Ajay Kumar Yadav, Ashutosh Gupta and Pradeep Kumar (2015): The propounded paper explains that after Steganography of image on Video exact video is extracted which was given by user and difference between the input video and output video is very small. The process of CDT and LSB are really useful but there are some limitations in the process. The major limitation is the number of frames should be greater than 255 because in an image there are maximum 255 pixels and after applying CDT we will get maximum of 255 matrix of image. It means it will give maximum 255 frames of a single image. For Steganography process of an image on video by CDT (Component Division Technique) Technique, it requires the condition number of video frames>=number of Image frames. After Decoding the image we can get the exact RGB image due to help of colour map and unique matrix. The difference of the output RGB image and Input RGB image will be zero [14].

Ramadhan J. Mstafa, Khaled M. Elleithy (2015): The presented paper demonstrates a novel video algorithm in the wavelet domain based on algorithm and BCH codes. The proffered algorithm has four different steps. The first step is the preprocessing phase pursued by the face detection and tracking algorithm step. The last two steps are the data imbedding and process to extract the concealed image. Finally the proffered algorithm displayed high imbedding efficiency and imbedding payload features [15].

Kasim Tasdemir, Fatih Kurugollu and Sakir Sezer (2015): The proffered paper presents a design method for a video Stegoanalysis targeting pixel domain steganography based on HEVC video frames. A high correlation among neighboring pixels is displayed both in the temporal and spatial domain. The results attained display that the filters employed can capture both temporal and spatial distortions introduced by the stego techniques. In order to increase accuracy version 3 of HEVC can be used [16].

K. Thangadurai and G. Sudha Devi (2014): The propounded paper explains a comparison between the cryptography technique and the Steganography approach for concealing the secret data. From the above analysis inference made is that cryptography does nothing to conceal the presence of message to itself but just random the secret data, while Steganography emerges as an art of hiding information in such a way that its presence is unnoticed. LSB method is discussed in an extensive sense, displaying its efficiency to imbed information in the images and then its retrieval. In forthcoming data can be encrypted with a security key in order to boost the level of security and other techniques like DCT (Discrete Cosine Transform) and DWT (Discrete Wavelet Transform) can be used to increase and enhance the robustness and efficiency of the system [17].

Mennatallah M. Sadek & Amal S. Khalifa & Mostafa G. M. Mostafa (2014): The propounded paper presents a review of video Steganography techniques. A special attention and care was paid to applications related to video Steganography using disparate cover types. Depending upon domain such as spatial domain techniques, transform domain techniques a category was made for imbedding. A comparative analysis of results was presented, depicting the advantages and disadvantages of each domain [18].

Hamdy M. Kelash, Osama F. Abdel Wahab, Osama A. Elshakankiry and Hala S. El-sayed (2013): The proffered paper presents that Steganography algorithm based on histograms is used to reduce the faded pixels in each frame thereby increasing and enhancing the imbedding efficiency. Also the quality of the Stego-video is maintained as well as the secret message is made more secure. This method is more simple, easy and authenticated as compared to other techniques [19].

Rajesh G.R and A. Shajin Nargunam (2013): The propounded paper demonstrates that Steganography is a technique to imbedding secret data into unsuspected objects, has emerged like a rising technology for data concealing. This paper presents a visually undetectable, robust Steganography algorithm to conceal secret messages in moving videos. The video is used for the data transmission as it can hold large volume of the data. A new imbedding algorithm is propounded to conceal the secret data in moving videos. The 2D-DCT of the video is taken and the secret message is imbedded by checking the DCT coefficients of the video frame. The method entrusts on these characteristics to create a cover video that offers some robustness to geometric distortions. The PSNR value is taken as a performance measure to evaluate the quality of the video for any distortions. In forthcoming, a more secure Steganography algorithm and more appropriate, can be carried out by encrypting the secret message before imbedding in the moving videos [20].

Prabakaran.G, Bhavani.R (2012): The proffered paper presents a technique for steganography based on DWT (Discrete Wavelet Transform) are correlated with grayscale images. Proffered algorithm provides high data embedding capacity and enhances data security and integrity. Moreover stego-images are not perceived by intruders and shows robust results. In forthcoming other wavelet based techniques can be used for enhanced and secure results [21].

Souvik Bhattacharya and Gautam Sanyal (2012): The presented paper demonstrates a new approach named un-compressed Video Steganographic was proffered operating in the DWT domain. PMM was used to conceal data, thus providing high imbedding capacity and imperceptible Stego-image for human vision of the secret message. There is no degradation in visual quality of the video. Proffered algorithm gives good results with high imbedding capacity [22].

Feng Pan, Li Xiang, Xiao-Yuan Yang and Yao Guo (2010): The propounded paper presented the method that is used to embed large amounts of information and simultaneously maintain good video quality. The propounded method is less complex and not easily perceived by Human Visual System (HVS). Thus the embedding efficiency is improved to a large extent. In forthcoming Hamming code can be implemented and analyzed along with cryptography to enhance the security and secrecy [23].

Ozdemir Cetin, A. Turan Ozcerit (2009): The propounded paper demonstrates two new hidden embedding algorithms based on utilizing some histogram properties of raw digital video streams. A human visualization system makes it more attractive to analyze the results. Also we noticed that the block based techniques formed better results than frame based [24].

Abbas Cheddad, Joan Condell, Kevin Curan and Paul Mc Kevitt (2008): The proffered paper describes a new colour image Steganography method which executes the S- Tools and F5 in many aspects and features. Proffered algorithm enhances the system performance and is able to retrieve the secret data even after the presence of the noise. The approximate imbedding capacity is intensified to a great extent. In future 3-3-2 approach can be implemented along with an encryption [25].

Chen Ming, Zhang Ru, Niu Xinxin and Yang Yixian (2006): Presented paper describes that Steganography algorithms based on the spatial domain and transform domain are most commonly used by the present Steganography tools. For data hiding applications, LSB Steganography in spatial and transform domain is generally used. In forthcoming LSB hiding can be combined with linear codes to upgrade the security and robustness [26].

K.B. Raja, C.R. Chowdary, Venugoplal K R, and L.M. Patnaik (2005): Suggested paper explains that in order to achieve the secure stego-image the combination of LSB algorithms with DCT transformation has been used. Also compression techniques using quantization and runlength coding is executed on raw images. The LSB technique provides maximum payload which is imbedded into the cover-image to achieve the Stego-object. Runlength coding and quantization enhances the security of the system. DCT is applied to transform the Stego-object from the spatial domain into the frequency domain. In forthcoming other image compression techniques can implemented such as predictive coding and DPCM [27].

Venkatraman. S, Ajith Abraham and Marcin Paprzycki (2005): The presented paper indicates that the presence of high degree of redundancy in the digital multimedia can be used to meet the aspiration and idea of Steganography. This also suggests how variation of LSB algorithm and its alternatives aids in achieving better security, secrecy and robustness. It also represents that a combination of Steganography with cryptography ensures and provides higher degree of success in the secrecy of data. In future Wavelet transforms can be implemented to enhance and upgrades the security of the system [28].

*****

3

SCOPE OF STUDY AND OBJECTIVE

"The greatest challenge to any thinker is stating the problem in a way that will allow a solution." *-Bertrand Russell*

In the foregoing segment different types of steganographic algorithms like KLT, LSB, BCH, IWT, DWT were developed. The basic merits and demerits were taken into account while the designing of the steganographic algorithms. Consequently, in this section, the problem formulation and implementation is entailed through video steganography, formulated in DWT domain based on BCD codes. This technique ensures a suitable and reliable solution for data security in future.

3.1. Scope of study

The propounded work is hinged on video steganography in which wavelet transform domain and BCD codes are used. In the discrete wavelet transform (DWT) technique is applied to analyze the textural features of the input video and imbed text in the video to generate final steganographic video. The text which is embedded in the video will be in the encrypted form and to generate the encrypted data technique of BCD is applied and this technique uses the symmetric key for encryption and decryption. The following are the problems which minimize its efficiency in terms of security and accuracy.

i. The technique of wavelet transform is used which only analyze textural features of the input video. The video has also some other features like color features which are not used to generate steganographic video. This problem reduces the accuracy of text embedding and extraction from the input video.

ii. The second problem exits during the use of BCD codes to encrypt the input text. The BCD codes use the symmetric keys for encrypting and decrypting the text. The BCD codes generated the structure of encryption which is quite complex and need much time for execution.

3.2. Objectives

The principal need of the research is to build a secure interface for the users, while the data transmission. For secure communication security measures are required to be revised.

i. To study and analyze various video steganography techniques for data security.
ii. To propound improvement in wavelet domain transform (DWT) with the help BCD coding technique along with the enhancement in efficiency.
iii. The proposed improvement is based on to analyze color features for text embedding and use secure channel establishment algorithm to encrypt text.
iv. To implement propounded and existing schemes and compare results in terms of data encryption time, data decryption time, embedding payload, PSNR and MSE.

3.3. Workplan

Data security is an issue and problem for classified and obscure communication form past centuries. People need protection and certainty from inaccurate and wrong processing of data. Therefore in order to conceal and protect data from misuse and manipulations by earwigs and intruders, steganography is used to uphold the data integrity and certainty. Assorted steganographic algorithms are developed and implemented for classified and concealed communications.

From decades terrorist groups are practicing steganography for hidden communication in order to harm the world peace. Therefore, there is a fundamental need to construct efficient algorithms and techniques that could overkill the misuse of secret data. Thus steganography emerged as a successful tool for camouflaging the information from the outer world. Here the workplan is composed of two parts. First the delineation of the steganographic system was procured through LSB insertion technique followed by DWT method which was hinged on BCD codes. Various factors were studied in order to state the effectiveness of the selected methods. The workplan that was carried out throughout this dissertation is depicted with the help of below illustrated flowcharts:-

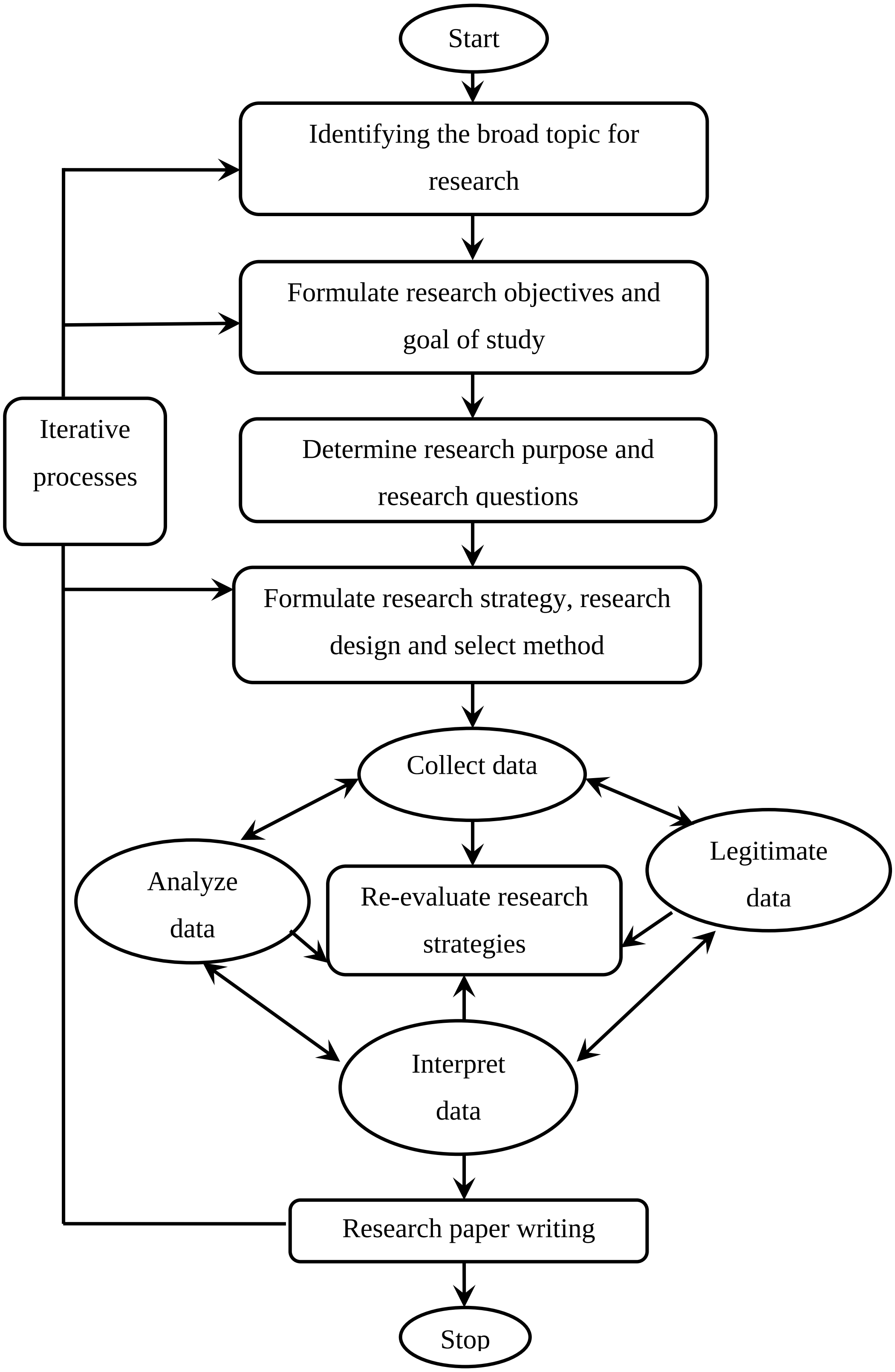

Start
Identifying the broad topic for research
Formulate research objectives and goal of study
Iterative processes
Determine research purpose and research questions
Formulate research strategy, research design and select method
Collect data
Analyze data
Re-evaluate research strategies
Legitimate data
Interpret data
Research paper writing
Stop

Fig 3.1. Design for the initial workplan

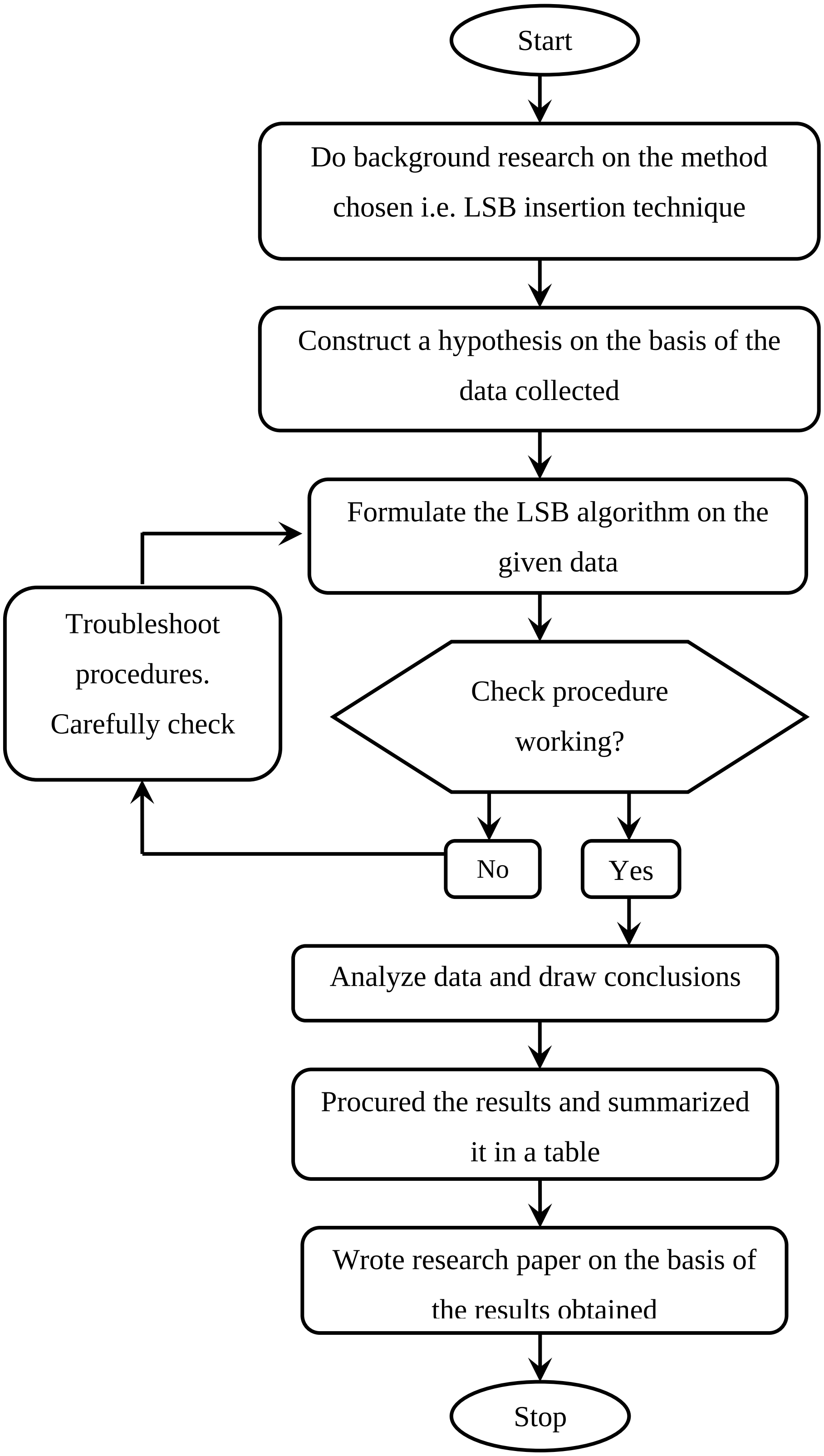

Start
Do background research on the method chosen i.e. LSB insertion technique
Construct a hypothesis on the basis of the data collected
Formulate the LSB algorithm on the given data
Troubleshoot procedures. Carefully check
Check procedure working?
No
Yes
Analyze data and draw conclusions
Procured the results and summarized it in a table
Wrote research paper on the basis of the results obtained
Stop

Fig 3.2 Design for the LSB approach workplan

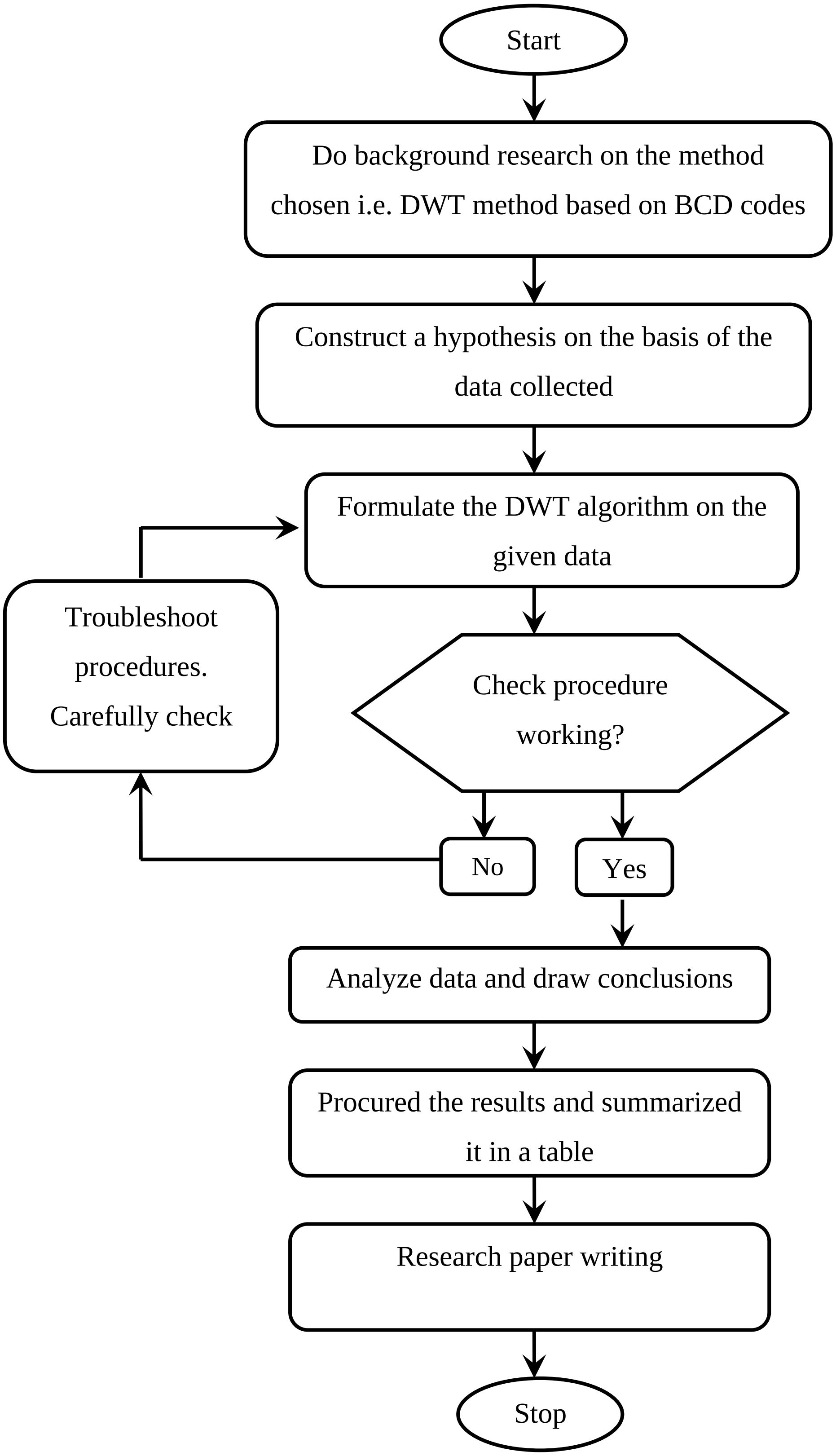

Start
Do background research on the method chosen i.e. DWT method based on BCD codes
Construct a hypothesis on the basis of the data collected
Formulate the DWT algorithm on the given data
Troubleshoot procedures. Carefully check
Check procedure working?
No
Yes
Analyze data and draw conclusions
Procured the results and summarized it in a table
Research paper writing
Stop

Fig 3.3 Design for the DWT approach workplan

The design method mentioned and explained above, define the workplan for the diverse methodology used while this whole research. The steps for the algorithms used are explained properly in the next section.

*****

4

RESEARCH METHODOLOGY

"If you steal from one author its plagiarism; if you steal from many its research"

Wilson Mizner

In the forgoing section problem formulation is composed and expounded. Two algorithms are discussed and implemented using different parameters of visual quality of an image like PSNR, MSE, data encryption time, data decryption time, imbedding payload. The implemented algorithms are LSB insertion method and DWT using BCD codes. From introduction of the steganography it can be inferred that the LSB hiding is good for concealing short message but for long message distortion is there. So in order to remove distortion from stego-image DWT came into existence. So many researchers had a research on LSB and DWT method and concluded that DWT is more robust and reliable as compared to LSB. DWT gives high PSNR as compared to LSB insertion method. Present section states proffered method and propounded algorithms, which are executed and explained in the form of flowcharts. The tool used to carry out the above work is MATLAB.

4.1 LSB INSERTION METHOD

LSB insertion technique is the easiest and simplest approach for data concealing using bit manipulation. It follows the procedure to manipulate LSBs of the secret message into the LSBs of the cover media. Due to the simplicity of the method it can have the capability of hiding long length messages. This method protects the very existence of the concealed data in a cover media. For BMP images it shows robust results, as the compression in BMP images is lossless. The covert message is in the form of a character string, which is to be converted into ASCII form. After which decimal numbers are converted into binary equivalents since the computer understands only binary language. In next step LSBs of the secret text is manipulated with LSBs of the image pixels. LSB works well for BMP and dark background images. Later compute the PSNR and MSE values for selected frames. In order to understand the basic formulation and steps of the LSB insertion technique, flowcharts and algorithmic procedure are depicted below.

4.1.1. Steps for LSB insertion method For Imbedding Phase:-

Step1:- Load the secret message and scan each and every character of the message.

Step2:- Then search for the ASIC equivalent of the character and the covert it into decimal number.

Step3:- Covert the decimal numbers into binary equivalent.

Step4:- Input the cover video and select few frames and take the values of its pixel in decimal form.

Step5:- Covert the decimal values of pixels into binary equivalent.

Step6:- Substitute the LSBs of the secret message into the LSBs of the cover image.

Step7:- Build the stego image after hiding the data inside the carrier image.

Step8:- Evaluate parameters like PSNR, MSE, imbedding payload etc.

4.1.2. Steps for LSB insertion method For Extraction Phase:-

Step1:- Load the stego video from the system or PC.

Step2:- Extract the frames from the video.

Step3:- Read the frames according to the list of rules.

Step4:- Take all the frames which have information and discard all other frames.

Step5:- Extract and decode the secret message from the frames by using LSB insertion method.

Step6:- If all the frames which contain message are not decoded, repeat step 5.

Step7:- Rearrange the bits extracted from the frames in form of bytes.

Step8:- Merge the secret message by going through the rule list in explicit format.

Step9:- Rebuild the secret message.

The algorithmic steps that are presented above, shows the working of the LSB technique. Further, the flowcharts of the imbedding and extraction phase are picturesque for better understanding of the above stated method. The flowcharts are presented in the below section:

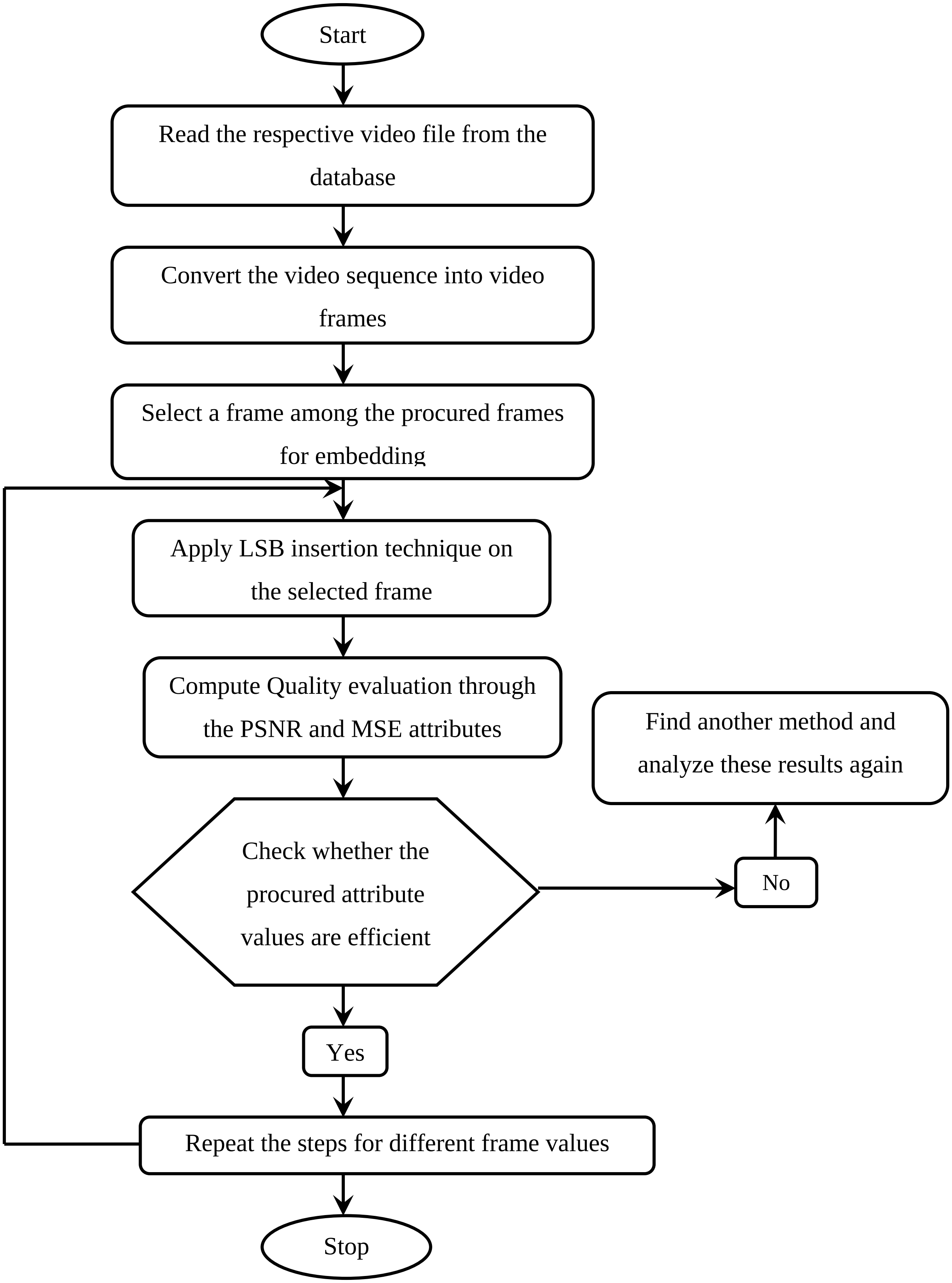

Start
Read the respective video file from the database
Convert the video sequence into video frames
Select a frame among the procured frames for embedding
Apply LSB insertion technique on the selected frame
Compute Quality evaluation through the PSNR and MSE attributes
Check whether the procured attribute values are efficient
No
Find another method and analyze these results again
Yes
Repeat the steps for different frame values
Stop

Fig.4.1 Flowchart of LSB Imbedding Algorithm

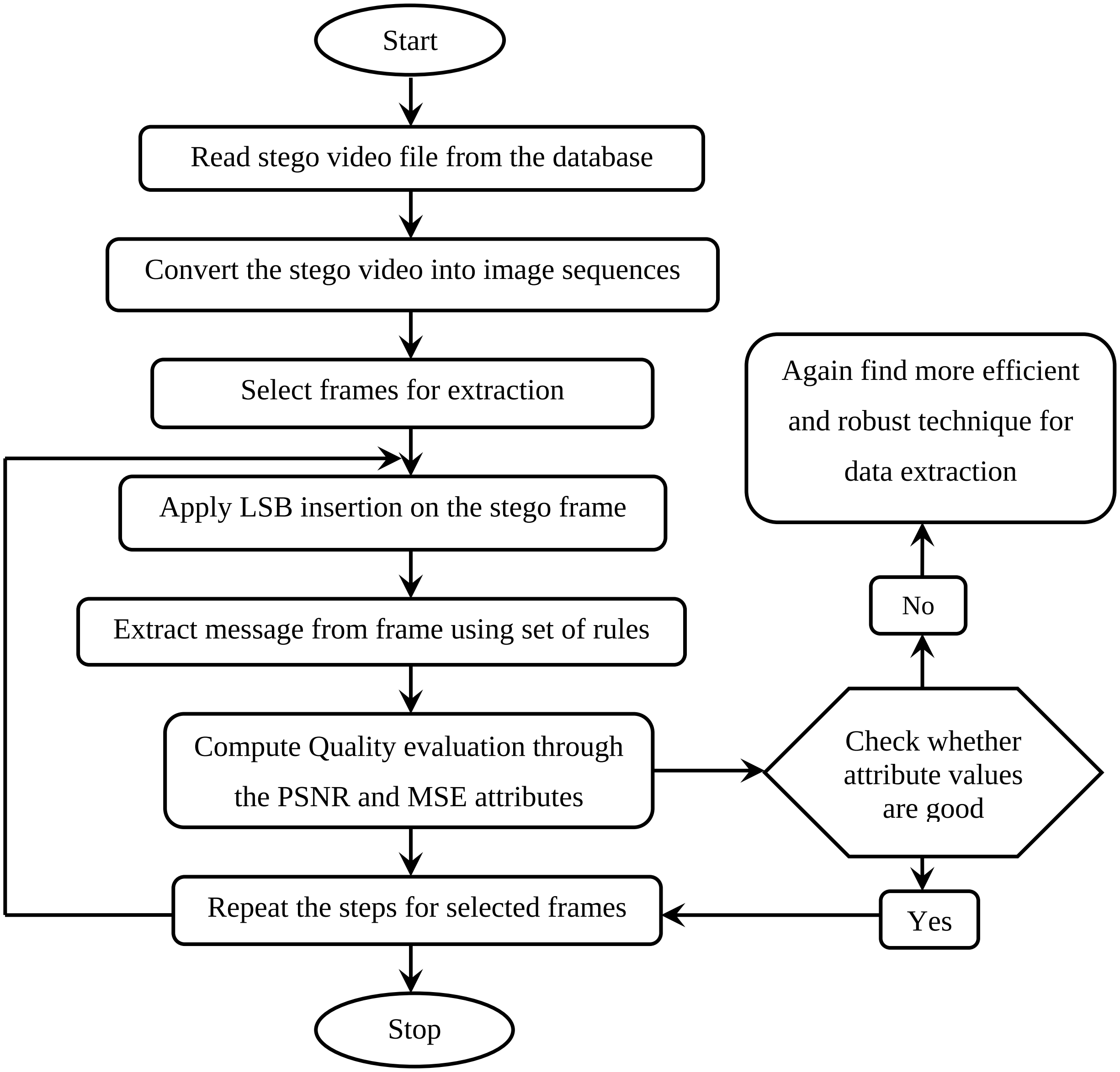

Start
Read stego video file from the database
Convert the stego video into image sequences
Select frames for extraction
Apply LSB insertion on the stego frame
Extract message from frame using set of rules
Compute Quality evaluation through the PSNR and MSE attributes
Check whether attribute values are good
No
Again find more efficient and robust technique for data extraction
Yes
Repeat the steps for selected frames
Stop

Fig.4.2 Flowchart of LSB Extraction Algorithm

4.2 DWT USING BCD CODES

DWT (Discrete Wavelet Transform) is a transform to enhance the textural features and edges of an image, where wavelets are discretely sampled in the transform. It transforms signal or image from spatial domain to frequency domain. Main vantage point of the transform is that it is localized in both time and frequency domains. The first form of DWT was the Haar transform which was designed by a mathematician named Alfred Haar. It decomposes the input values and stores them in the form of detail and fluctuations. DWT have an amazing property of scale and shift that was absent in other transforms, so researchers switched to this transform which helped in enhancing the edges, visual and textural features of the images along with data security and integrity. It imbeds the data in four frequencies LL, LH, HL and HH. But data is only imbedded into LH, HL and HH frequency sub-bands and LL sub-band is the close approximation of an image.

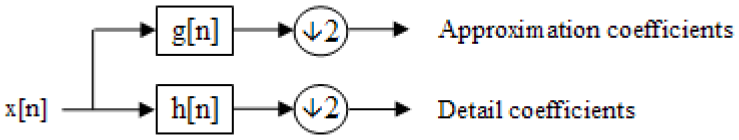


Fig. 4.2 DWT Decomposition

4.2.1. Steps for DWT method hinged on BCD codes Imbedding Phase:-

Step1: Input the cover video from system or PC.

Step2: Extract the frames from the cover video.

Step3: Input the secret message i.e. text file.

Step4: Change the positions of the bits of the secret message using secret key1.

Step5: Convert the covert message into 1-D array.

Step6: Encode the covert message with BCD encoder.

Step7: Apply 2-D DWT on the frames of the video.

Step8: Imbed the covert message in the middle and high frequency coefficients i.e. LH, HL, and HH frequency sub-bands.

Step9: Apply 2-D IDWT on the frames.

Step10: Rebuild the stego frames after data imbedding.

Step11: Rebuild the stego video from stego frames.

4.2.2. Steps for DWT method hinged on BCD codes Extraction Phase:-

Step1: Input the stego video from system or PC.

Step2: Extract frames from stego video.

Step3: Apply 2-D DWT on the stego frames.

Step4: Extract the encoded and concealed message from the LH, HL, and HH frequency sub-bands of the extracted frames.

Step5: Combine the whole encoded message.

Step6: Decrypt the encoded message using secret key1.

Step6: Decode the secret message with BCD decoder.

Step7: Extract the decoded message from the stego video.

Step8: Output the concealed message.

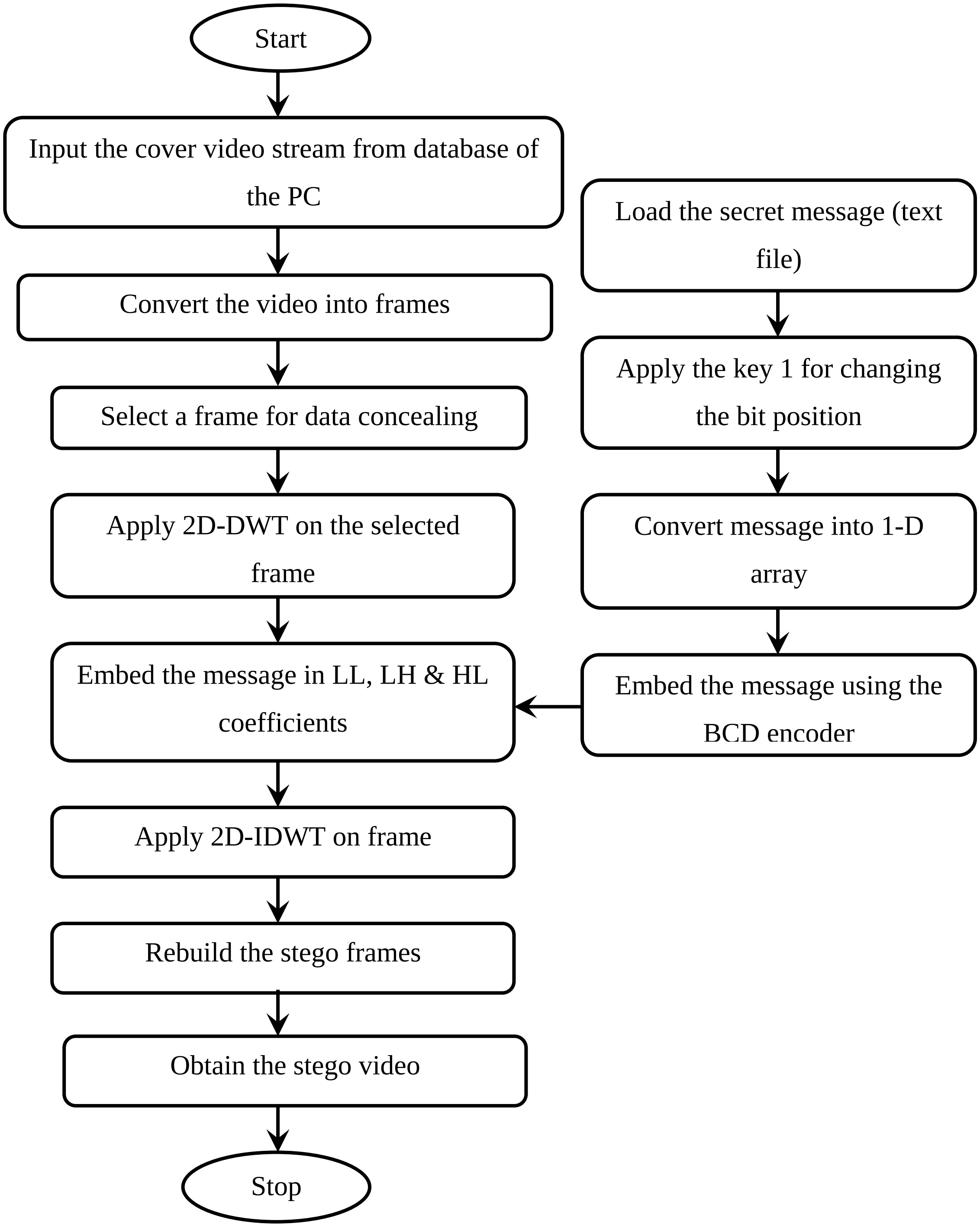

Start
Input the cover video stream from database of the PC
Convert the video into frames
Select a frame for data concealing
Apply 2D-DWT on the selected frame
Embed the message in LL, LH & HL coefficients
Apply 2D-IDWT on frame
Rebuild the stego frames
Obtain the stego video
Stop
Load the secret message (text file)
Apply the key 1 for changing the bit position
Convert message into 1-D array
Embed the message using the BCD encoder

Fig.4.3 Flowchart of Embedding phase DWT using BCD Algorithm

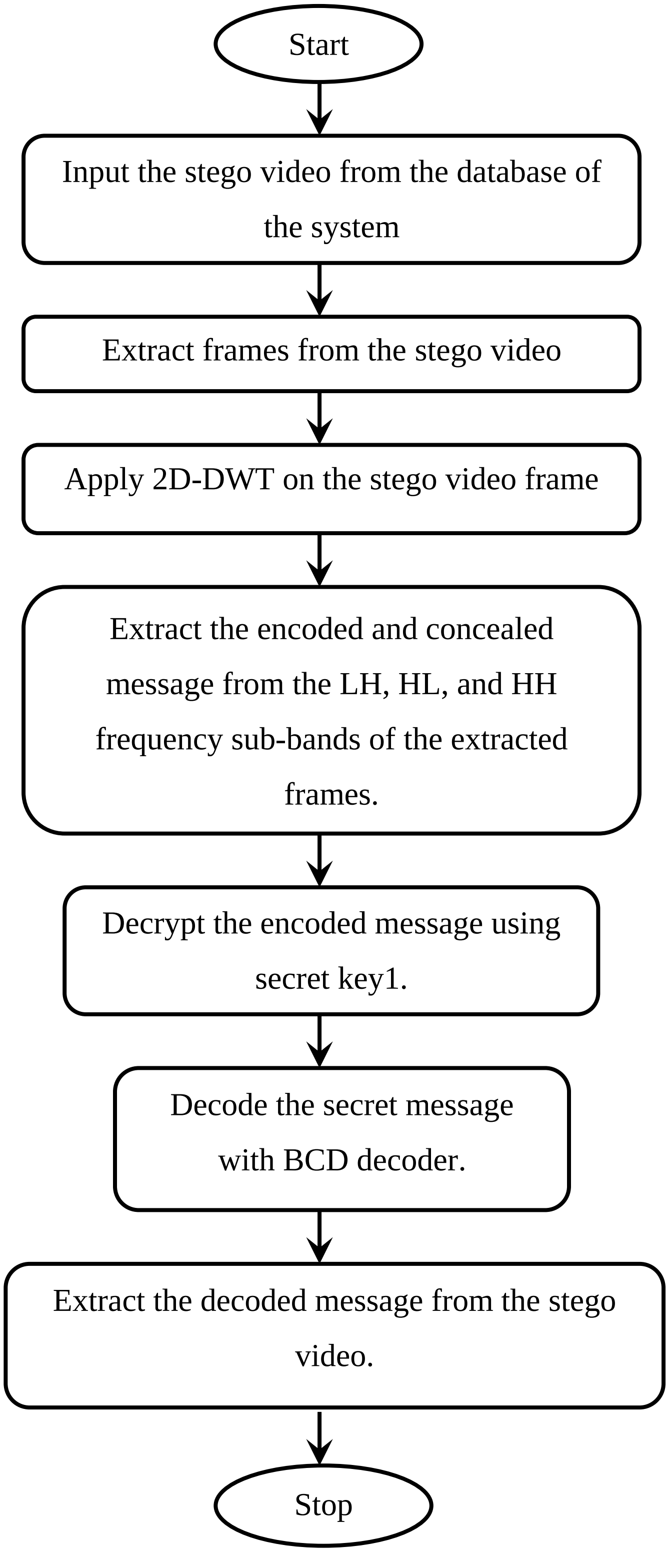

Start
Input the stego video from the database of the system
Extract frames from the stego video
Apply 2D-DWT on the stego video frame
Extract the encoded and concealed message from the LH, HL, and HH frequency sub-bands of the extracted frames.
Decrypt the encoded message using secret key1.
Decode the secret message with BCD decoder.
Extract the decoded message from the stego video.
Stop

Fig.4.4 Flowchart of Extraction phase DWT using BCD Algorithm

*****

5

RESULTS & DISCUSSIONS

"The more original a discovery, the more oblivious it seems afterwards" *Arthur Koestler*

This section consist of all the results that are obtained using two techniques i.e., LSB hiding and 2D-DWT using BCD codes on various video files. LSB hiding is implemented on the 'shuttle.avi' video file, which is then displayed using a graphical user interface (GUI). The GUI provides pushbuttons for loading the video file from which a frame is selected followed by text insertion in it, and finally creating a Stego frame image which is automatically saved in the database. When the video is loaded, the GUI also displays parameters like no. of frames, frame rate, time duration etc. Finally, calculate the PSNR and MSE values for four frames with different text imbedding in them.

In the 2D-DWT domain analysis using BCD codes, three video files are taken with different file extensions. The frames are extracted from the videos, after which one frame is selected from extracted frames, and applied 2D-DWT on the respective frame. Afterwards the encryption techniques (secret key) is employed for hiding text into the frame using the BCD encoding method and then embed the encrypted text into the frame obtained after 2D-DWT. After this, IDWT is applied on the frame with hidden text i.e., stego frame followed by rebuilding of the video known as the stego video.

The above process in video Steganography is termed as "Data Imbedding Phase" in which the secret message is imbedded in one of the frame and then sends it securely to the receiving end. Finally, the DWT using BCD code encryption gives the data more security than the LSB insertion alone. This is proved by the PSNR and MSE value that is calculated for both the algorithms, showing that for LSB technique, if the message length is increased than the values of PSNR decreases and MSE value increases but for DWT it remains almost same. Thus the imbedding capacity of DWT method is more than that of LSB insertion.

5.1 Parameters for Analysis:

For evaluating the effectiveness and efficiency of the steganographic algorithm various parameters are used like PSNR, MSE, embedding payload, data encryption time and data decryption time. These parameters help assessing the performance and coherence of the steganographic algorithm.

5.1.1 Visual Calibre Factor

The foremost hurdle in video steganography is to handle the visual transparency that is the distortion should be fairly small in the stego video. Visual calibre is also known as the impalpability factor that depends on the similarity between the stego carrier image and the original carrier image. A video file is also signified using the authenticity factor also which lies between the resemblance of the extracted secret text and the original secret text. The above parameters can be computed with the help of the quantitative index like Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR). For the three video files used the MSE and PSNR values are calculated using the below formulas.

5.1.1.1 PSNR

It is defined as the ratio of the quality computation among the original and the stego image. Higher the value of the PSNR superior will be the quality of the stego image.

$$PSNR = -10\log_{10}\frac{MSE}{S^2} \qquad (5.1)$$

5.1.1.2 MSE

It is defined as the difference between the pixel value of the cover image and the pixel value of the stego image. This difference should be less in order to get best results of data hiding.

$$MSE = \frac{1}{MN}\sum_{n=1}^{M}\sum_{m=1}^{N}[\overline{g}(n,m) - g(n,m)]^2 \qquad (5.2)$$

5.1.1.3 Data Encryption Time

It is elucidated as the time consumed to imbed the concealed data into an image of the video f over time interval t. It is measured based on the size of the concealed data.

$$Data\ encryption\ time = \frac{Concealed\ data}{t} \times f \qquad (5.3)$$

5.1.1.4 Data Decryption Time

It is expounded as the time consumed to retrieve the concealed data successfully and denoted as T.

$$Data\ decryption\ time = \frac{T(Concealed\ data)}{t} \times 100 \tag{5.4}$$

5.1.1.5 Imbedding Payload

It is described as maximum amount of data that could be carried by the concerned video file. It is advised that the input data i.e. text should be smaller than or equal to the total payload of the video.

$$Imbedding\ payload = \frac{9 \times m \times n \times f}{8 \times 10^{6}} \tag{5.5}$$

5.1.1.6 Mean Standard Deviation

The standard deviation is equivalent to the mathematical average deviation, besides the averaging is computed with power in lieu of amplitude. This is procured by squaring every deviation before computing the average. Further, the square root is employed to nullify the effect of initial squaring. It clearly defines the brightness probability distribution function.

$$S.Dev = [\frac{1}{m}\sum_{j=1}^{m}(y-\bar{y})^{2}]^{\frac{1}{2}} \tag{5.6}$$

5.2 Video Steganography using LSB hiding method (Imbedding Phase)

The implementation of Video steganography using LSB insertion is validated by the diversified steps in the figure below. The fundamental aspiration of implementing LSB hiding is to provide data security and certainty from earwigs and intruders over transmission channel. It is an easy and simplest approach to hide the covert data in a cover image without presenting numerous perceptible distortions. LSBs of some or all of bytes of a carrier image is changed and manipulated to the LSBs of the concealed data. Using this approach one can store 3 bits in a pixel (one bit of each plane i.e. red, green and blue). LSB works efficiently for BMP images, as this image type uses lossless compression.

5.2.1 Calculation of data hiding capacity of LSB method

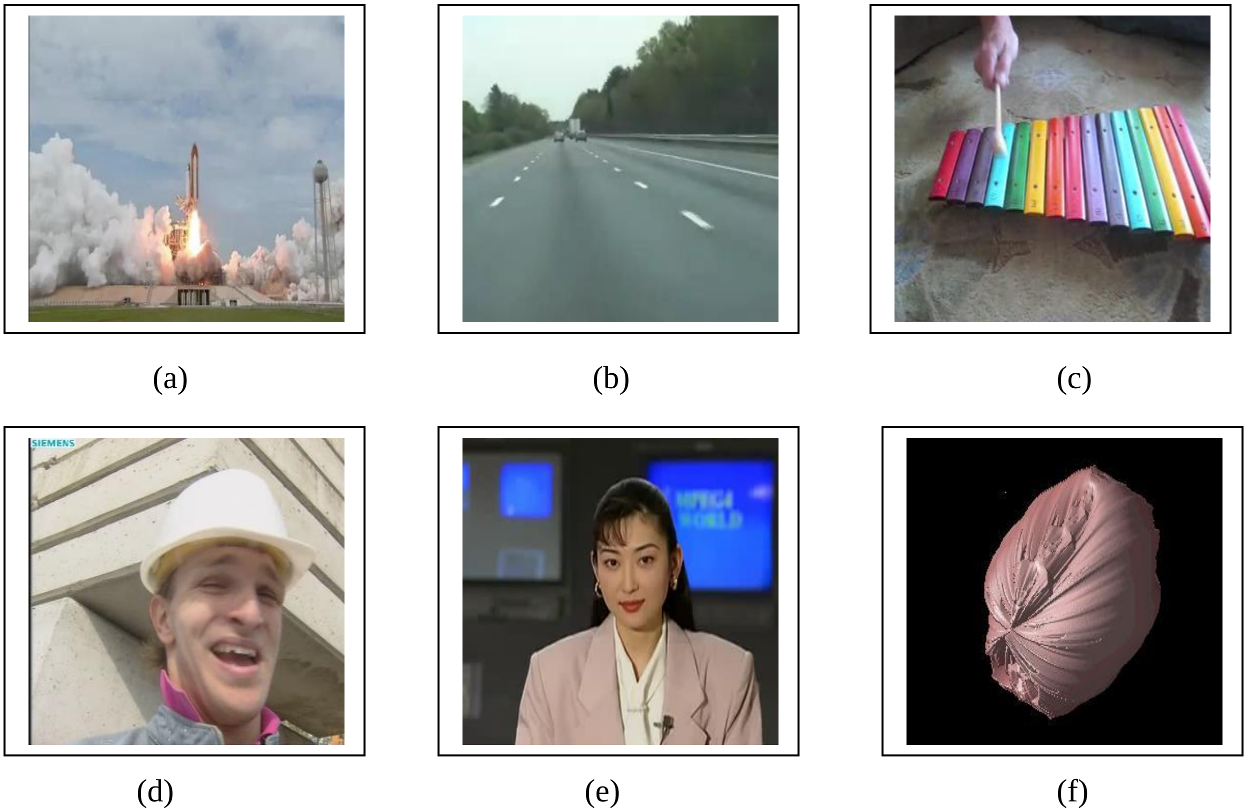
LSB is mostly famous for 24-bit scheme for insertion i.e. 3 bits/pixel. So the hidden ratio of data is:-

- (3 hidden bits/pixel)/ (24 data bits/pixel) =1 hidden bits/8 data bits

$$\frac{3\ hidden\ bits/pixel}{24\ data\ bits/pixel} = \frac{1\ hidden\ bit}{8\ data\ bits} \tag{5.7}$$

From above equation it is inferred that user can hide 1 bit of the imbedded message for every 8 bits of the carrier image.

5.2.2 Video types:



(a) (b) (c)

(d) (e) (f)

Fig.5.1 Frames of video (a) shuttle.avi (b) Vip.mp4 (c) Xylo.mp4 (d) Foreman.avi (e) Akiyo.mp4 (f) Super2.avi

In this segment different videos with disparate extension types are employed in order to analyze the LSB insertion method for data concealment in a carrier video.

The extension AVI stands for Audio Video Interleave and is employed to store both audio and video data in one file. This format is used to store multimedia data. It is less compressed in comparison to other methods.

The extension MP4 has a capability of storing audio, video and other data. This format uses high rate of compression but maintains the quality of data. It stands for MPEG-4 advanced video coding. It is well suited for video streaming in the internet.

Both the video extension has their merits and utilities. In avi compression ratio is very less, so the MSE value remains small in this. But the demerit of avi is, that sometimes it is not compatible with some of the media players e.g. VLC media player. On the other side compression ratio in the later type is high, so MSE value rises but it is compatible with all media players. In this segment the introductory part of video steganography is executed for different video types and is called video framing. Video framing is a process of extracting frames out of the carrier video. During the extraction of frames the GUI tool build for video steganography calculates the frame rate, the no. of bits procured, width and height of each frame. A total of 121 frames are there in the shuttle.avi, 337 frames in the viplanedeparture.mp4, 141 frames in the xylophone.mp4, 300 frames in the foreman.avi, 465 frames in the akiyo.mp4 and 25 frames are there in the videos from which a single frame is selected from all video and the process of data concealing is carried out on this respective frames.

The first and last video type is .avi which depicts that the compression is less in these videos, so the chances of degradation of the quality of the frames will be less during imbedding of the covert data. Other four video types are mp4, so there will be more compression; this means there are chances of degradation of image quality. In addition to at the time of imbedding covert data inside a carrier it can’t be commented whether image quality will degrade or not, only and only after extraction of covert data it can be explained and expounded through analysis. But the structural concept of higher PSNR obeys better quality image. The foremost aim of the LSB algorithm to bring out easy to implement and hard to retrieve.

The below mentioned Table.5.1 demonstrates the imbedding phase of the steganographic system and procured different parameters for evaluating the quality of the stego image and the distortions in the covert message. For better results PSNR values should be high and MSE value should be low to enhance the robustness of the propounded algorithm. MSD (Mean Standard Deviation) tells about the distortions in the covert message and also vindicates the efficiency of the system. That’s why imbedding of covert data is greatly depends on the MSD. Attribute DET (Data Encryption Time) depicts that how much time is taken by the algorithm to conceal the secret data inside the cover media. The last attribute Imbedding Payload (IMP) expounds about the maximum amount of covert data that could be carried by the concerned video media or file.

Table 5.1 Parameter values for LSB insertion imbedding phase

Parameters	Videos					
	Frames	Shuttle.avi	Vip.mp4	Xylo.mp4	Foreman.avi	Akiyo.mp4	Super2.avi
PSNR(dB)	Frame6	42.6557	32.0951	32.2894	34.6602	34.6602	32.2894
	Frame9	41.4063	31.4881	32.2894	37.0130	37.0130	32.8330
	Frame11	39.6454	32.5527	34.5939	32.1823	32.18238	32.2894
	Frame13	37.0130	32.3179	31.1696	32.7893	32.7893	31.3717
MSE	Frame6	1.67e-07	6.17e-04	5.908e-04	3.4196	3.4196	5.90e-04
	Frame9	1.56e-06	7.09e-04	5.908e-04	1.9892	1.9892	5.208e-04
	Frame11	1.43e-03	5.56e-04	3.472e-04	6.0500	6.0500	5.902e-04
	Frame13	1.74e-02	4.11e-04	7.638e-04	5.2609	5.2609	7.291e-04
MSD	Frame6	18.7378	28.2649	40.6622	44.9754	48.8632	45.0022
	Frame9	18.8411	32.8761	40.9129	45.2450	48.8611	51.2515
	Frame11	18.8916	35.6846	40.5464	45.6229	48.8350	56.5577
	Frame13	18.9692	35.6846	40.7516	46.3432	48.8262	46.8090
DET (secs)	Full video	25	48	21	24	20	12
IMP(MB)		14.4837	32.7564	12.1824	34.0213	53.4006	1.8432

The above expounded table demonstrates the PSNR values of the six different videos. PSNR values for four different frames are computed for six different videos. From above table it can be inferred that PSNR values of shuttle.avi, foreman.avi, and super2.avi are high as compared to vip.mp4, xylo.mp4, akiyo.mp4 due to the fact that compression is less in avi and more in mp4. Less compression means high PSNR values and higher PSNR values leads to less distortion in textural features of the stego image and also in originality of the covert message. AVI extension have less MSE values which means covert message is free from the distortion even after manipulating the LSBs of the covert message with the LSBs of the carrier image. But this doesn’t mean that mp4 extension is not good for data concealment, it can only be expounded after retrieving the covert message at the receiver side. Both extensions have their merits and demerits. Data Encryption time illustrates that how much time is taken by the steganographic system to conceal the covert message by substituting the LSBs of the covert message with the LSBs of the carrier media. Imbedding payload differs for different video extensions and their sizes. It can tell how much a video file can conceal and hold the covert data inside-it.

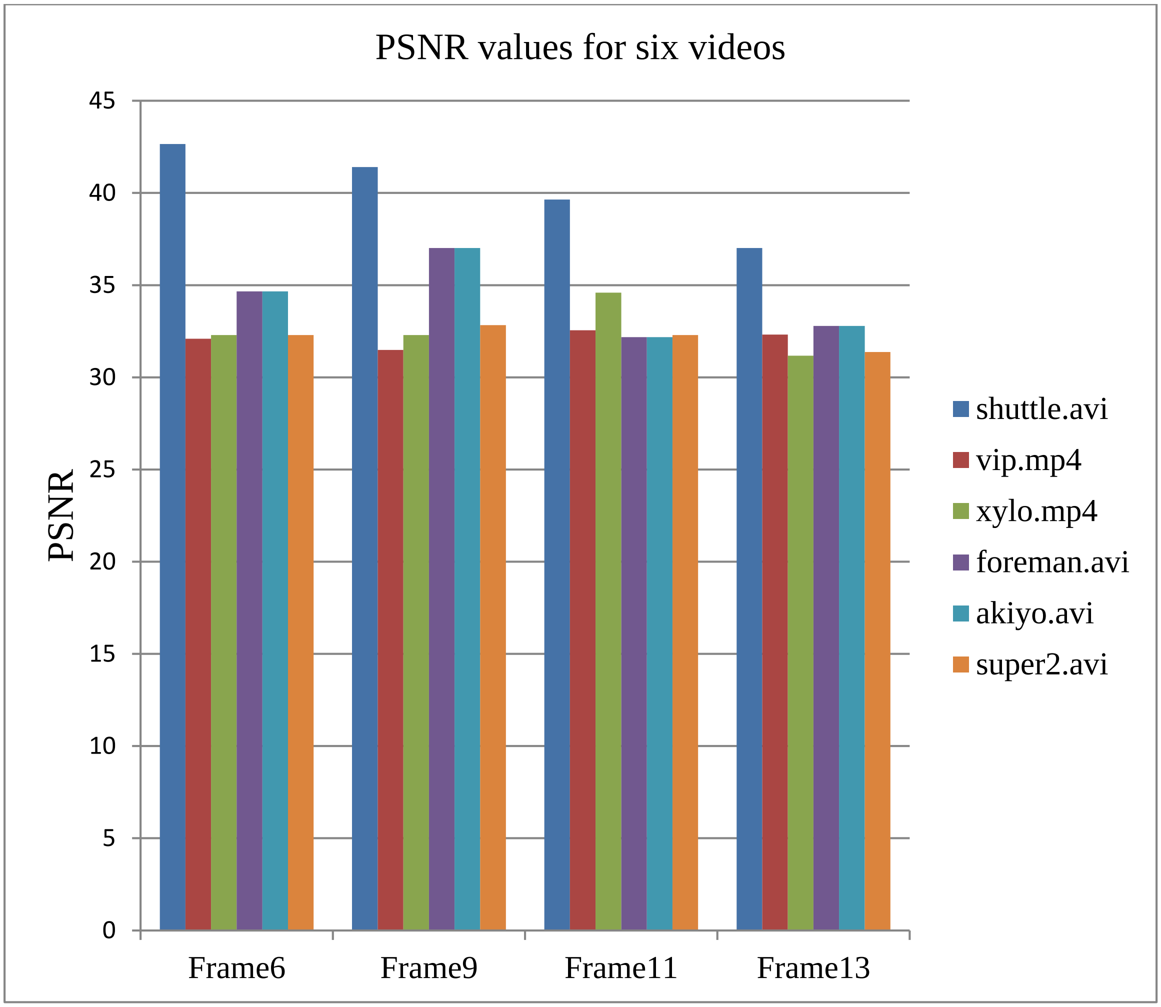


Fig 5.2 Plot of PSNR values of six different videos

PSNR is defined as the ratio of the quality computation among the original and the stego image. Higher the value of the PSNR superior will be the quality of the stego image. Above Fig 5.2, illustrates the PSNR values of six disparate videos. It expounds that for three videos with extension avi i.e. shuttle.avi, foreman.avi, super2.avi having high PSNR values as compared to other videos with extension mp4. This shows that system is giving good results for avi extensions due to less compression ratio in imbedding phase. Moreover it depicts that if PSNR is high MSE will be less. PSNR and MSE values are image quality measures, after imbedding data and extracting data these parameters are evaluated for respective frames. After evaluation these parameters efficiency and robustness of the system can be predicted and examined.

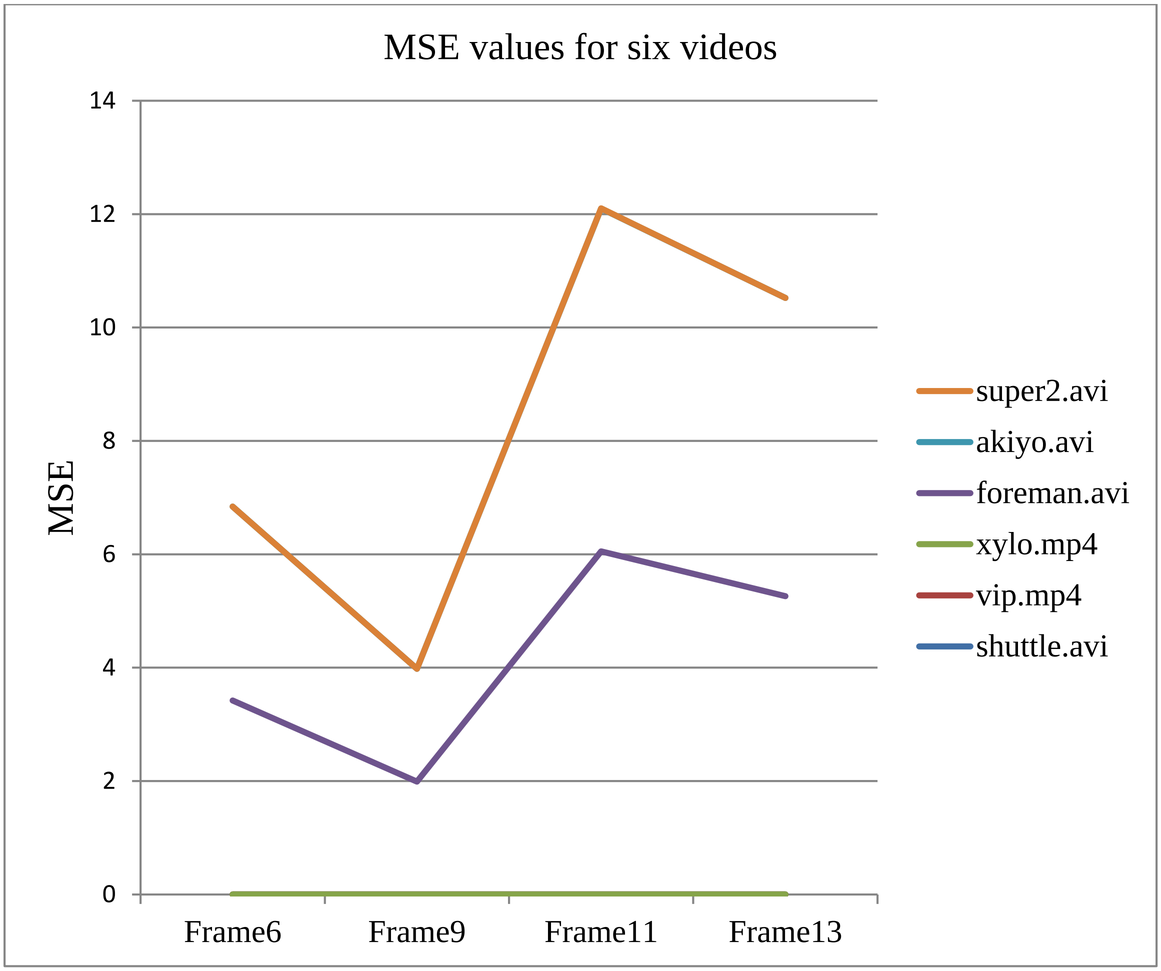


Fig 5.3 Plot of MSE values of six different videos

MSE is defined as the difference between the pixel value of the cover image and the pixel value of the stego image. This difference should be less in order to get best results of data hiding and protecting. The precedent Fig 5.3 presents that the MSE values are less for 3 videos i.e. foreman.avi, shuttle.avi, super2.avi and more for other three videos with extension mp4 due to high compression ratio. Low MSE value demonstrates that that there is no degradation in the quality of the stego image and originality of the covert message. The vip.mp4 having the highest MSE value for frame 6, but this doesn’t mean the extension is not suitable for data camouflaging. It can only depict after data extraction. Super2.avi having lowest MSE values for all four frames among all the videos.

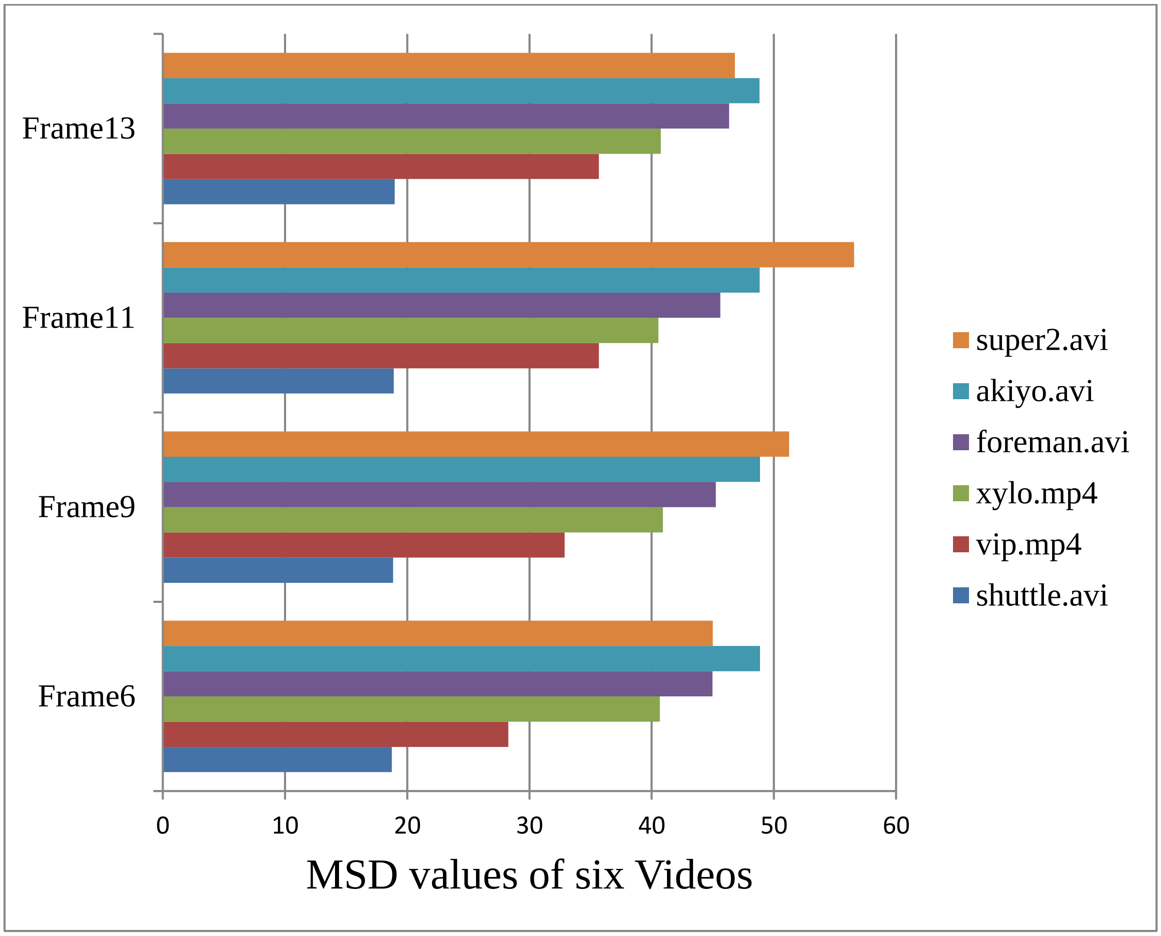


Fig 5.4 Plot of MSD values of six different videos

The standard deviation is equivalent to the mathematical average deviation, besides the averaging is computed with power in lieu of amplitude. This is procured by squaring every deviation before computing the average. Further, the square root is employed to nullify the effect of initial squaring. It clearly defines the brightness probability distribution function. From the foregoing Fig. 5.4 explains the MSD values for six different videos using disparate frames. In steganography it is quite frequent to use simple statistical representations of the images. The explanation of statistic is intimately associated to the approach of the standard deviation. For the given part which could feasibly be an entire image, the standard deviation function of the brightness in that region can be explained.

MSD is useful in telling the imbedding capacity of the algorithm. Therefore, its value should be high in both imbedding and extraction phase of the steganographic system.

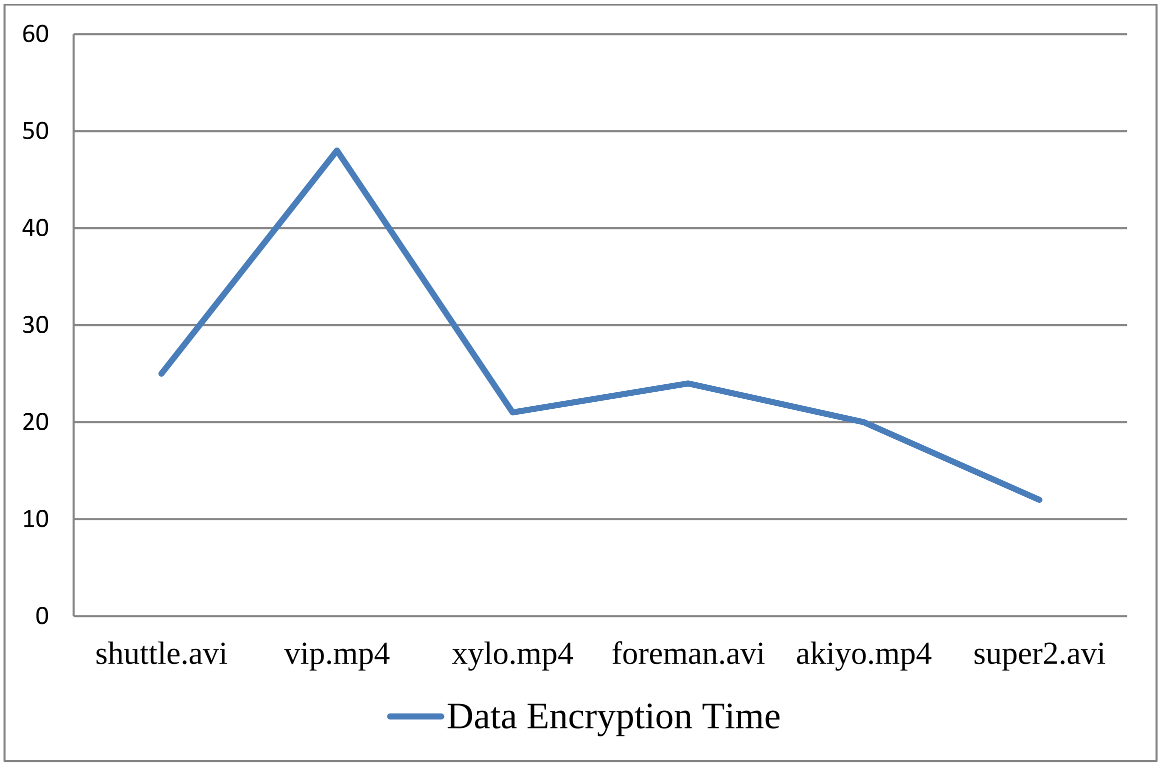


Fig 5.5 Plot of DET values of six different videos

DET (Data Encryption Time) is expounded as the time consumed to retrieve the concealed data successfully. Data encryption is a process of encrypting the covert text into something which emerges as redundant and random. The type of encryption is used in order to protect the covert data is symmetric. It protects and camouflages the important data from earwigs and eavesdroppers. In this a key is employed to scramble the data. The fundamental aim of encryption is to make the retrieval of covert data difficult. The foregoing Fig 5.5 demonstrates the six different videos with the DET for concealing data inside a cover image in an interval of time. It tells how much time a steganographic system is taking to conceal the covert data. This parameter varies according to the algorithm employed. Data encryption explains the ability of the algorithm to protect and secure data from attacks. Moreover it also depicts the speed of encryption of propounded algorithm and its efficiency. After the extraction secret data decryption time is also calculated and both DET and DDT (Data Decryption time) in order to conclude a point. According to DET values a comparison can be drawn between the propounded algorithms and also the efficiency of the system can be depicted and analyzed.

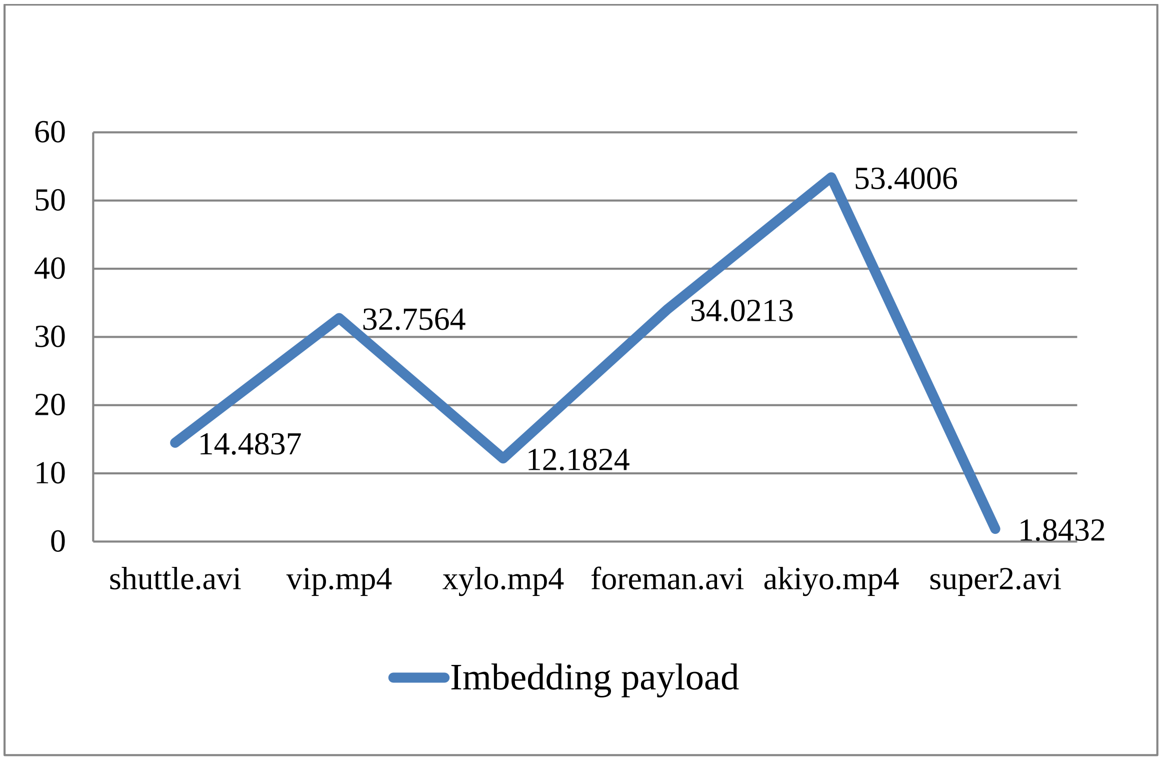


Fig 5.6 Plot of Imbedding Payload values of six different videos

Imbedding payload is described as maximum amount of data that could be carried by the concerned video file. It is advised that the input data i.e. text should be smaller than or equal to the total payload of the video. Six different videos holding covert data inside them are depicted by the Fig 5.6. From above graph it can be inferred that vip.mp4, foreman.avi and akiyo.mp4 having the highest imbedding payload.

5.3 Video Steganography using LSB hiding method of Extraction Phase

In the imbedding phase the covert data is concealed inside a cover image by manipulating and replacing the LSBs of the cover image and concealed data. It is indeed and undeniably important to extract the covert message securly for obscured and classified communication. This procedure of data conealing is easy and simple to implement. At the reciever side extraction process should be secure and reliable. This reliability is ensured by the PSNR and MSE attributes. If PSNR attribute having high value and MSE attribute having low value it signifies that the stego image quality is similar to that carrier image and there is no distortion in the retrieved covert message.

Parameters		Videos					
	Frames	Shuttle.avi	Vip.mp4	Xylo.mp4	Foreman.avi	Akiyo.mp4	Super2.avi
PSNR(dB)	Frame6	42.6557	32.0951	32.0411	34.6602	33.6608	31.8063
	Frame9	41.4063	31.6812	32.8330	34.0387	32.4114	32.2894
	Frame11	39.6454	33.9660	31.8063	33.4951	31.4423	32.2894
	Frame13	37.0130	37.3239	31.5836	34.0387	32.4114	32.0411
MSE	Frame6	2.419e+03	6.17e-04	6.25e-04	3.42e-04	4.30e-04	6.597e-04
	Frame9	1.56e-06	6.79e-04	5.208e-04	1.9892	5.73e-04	5.908e-04
	Frame11	1.43e-03	4.01e-04	6.597e-04	4.47e-04	7.17e-04	6.597e-04
	Frame13	1.74e-02	1.85e-04	6.946e-04	3.94e-04	5.73e-04	6.250e-04
MSD	Frame6	12.9200	28.2648	40.6622	45.1581	48.8632	45.0023
	Frame9	12.8252	32.8761	40.9129	45.1308	48.8612	45.5592
	Frame11	18.8916	34.3723	40.5464	45.3787	48.8350	46.8089
	Frame13	19.3230	35.6846	40.7517	45.5131	48.8262	47.0919
DDT (secs)	Full video	11	25	13	17	10	7
IMP(MB)		14.4837	32.7564	12.1824	34.0213	53.4006	1.8432

Table 5.2 for LSB insertion Extraction phase for different Parameters

The presented method uses the weakness of HVS as the vantage point i.e. it can’t perceive small changes and variation in the images. It can disguise the small changes in the carrier image. Retrieved message and recovered cover video are shown with the help of GUI. With the help of GUI the covert data is imbedded inside a cover video and recovered from the stego video with the aid of the pushbuttons.

The above table demonstrates information regarding PSNR and MSE values for six stego videos shuttle.avi, vip.mp4, xylo.mp4, foreman.avi, akiyo.mp4 and super2.avi. The PSNR and MSE values are image quality measures, after imbedding data and extracting data these parameters are evaluated for respective frames. If PSNR is good and MSE is low that means imbedding is efficient, but if PSNR is low then it means imbedding and extraction is not efficient and robust. This table depicts that PSNR is high for four frames for all videos but there is a sudden decrease and drop in MSE values and this makes presented method efficient and proficient for data concealing. This shows that the LSB insertion is an efficient and fine method for data security and collateral of the steganographic system.

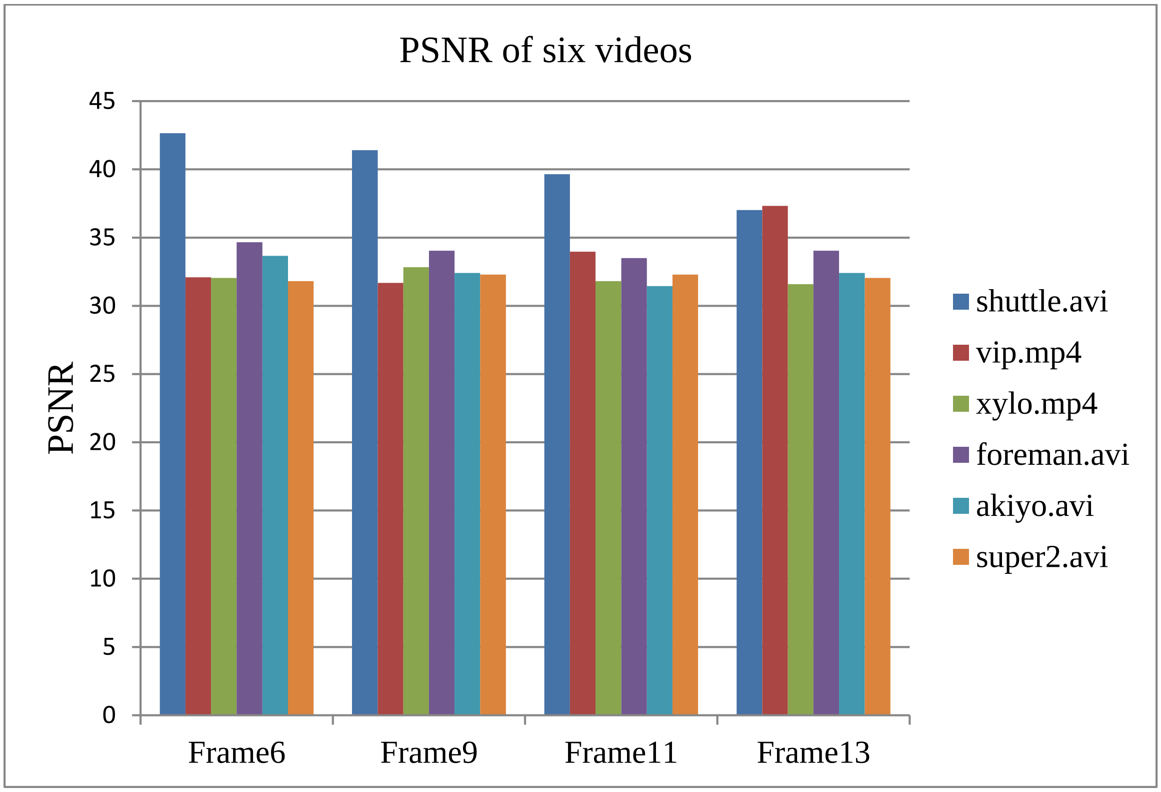


Fig 5.7 Plot of PSNR values of six different videos

From foregoing Fig 5.7 it can be inferred that shuttle.avi, vip.mp4 and foreman.avi is having highest PSNR values among all the videos during extraction of covert data. After extraction error of these two videos are less compared to other video files. High PSNR shows that system is efficient and there is no distortion involved after the retrieval of the secret text. Moreover these attributes depicts and explains the visual calibre factor i.e. the stego image is the fine approximation of the carrier image. This makes the steganographic system more proficient and excellent in data concealing and extraction.

From below demonstrated Fig 5.8 it can be gleaned that MSE values are only high for two videos vip.mp4, xylo.mp4 and super2.avi. This means rest three videos are more efficient for concealing data, as they have very less error which is negligible. It proves that the stego video is the close representation of the carrier video. For a steganographic system to be secure and protected MSE should be less. Below plot depicts that LSB method is easy to implement and is efficient and in addition to provides good results for data concealment.

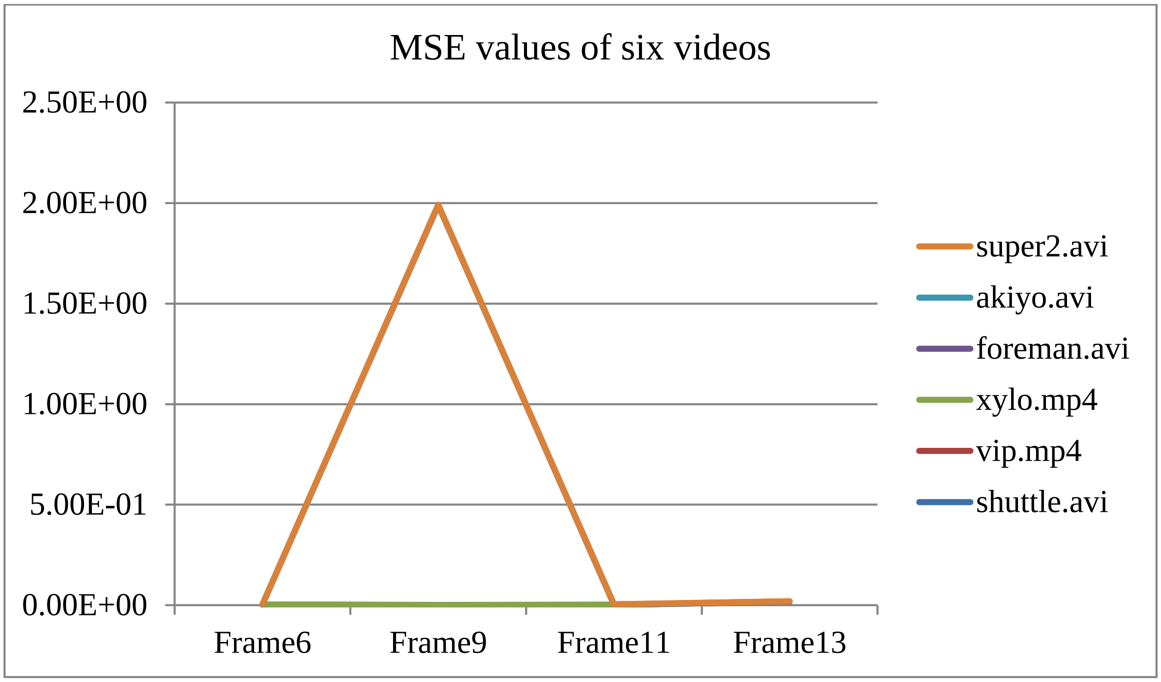


Fig 5.8 Plot of PSNR values of six different videos

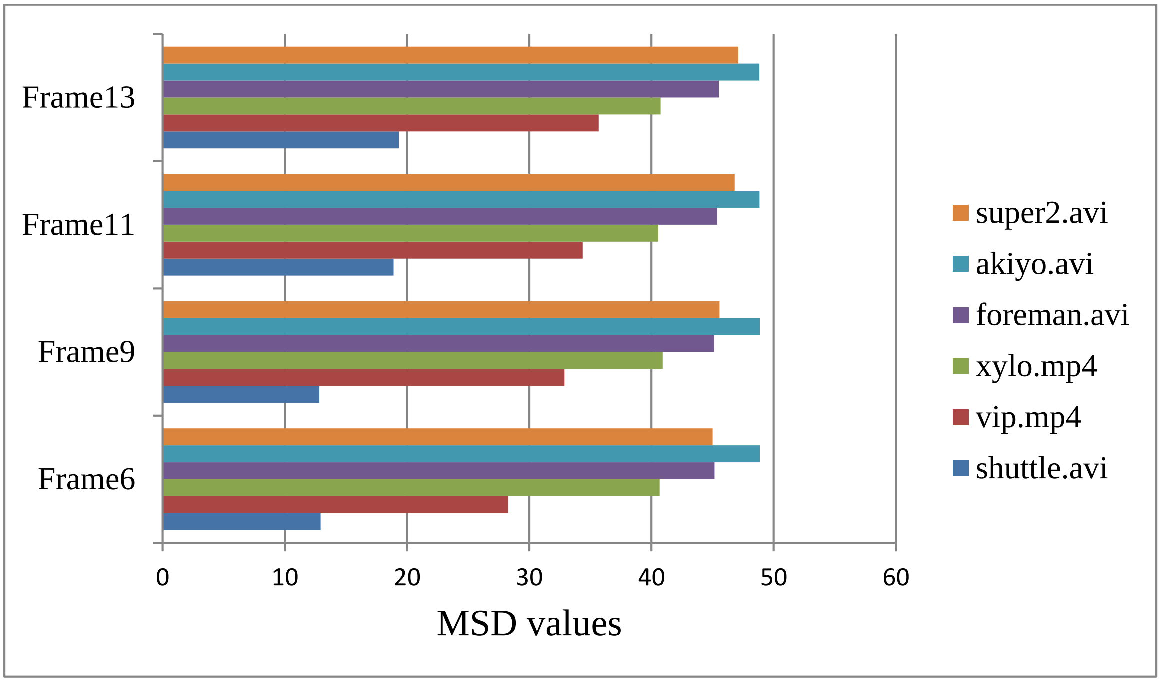


Fig 5.9 Plot of PSNR values of six different videos

The above mentioned values of MSD depicts that there is no distortion and alteration in the covert text after extracting it from the cover video. In addition to stego video is the close approximation the carrier video. Means chances of degradation of video quality are less. The explanation of statistic is intimately associated to the approach of the standard deviation. For the given part which could feasibly be an entire image, the standard deviation function of the brightness in that region of an image can be examined and explained.

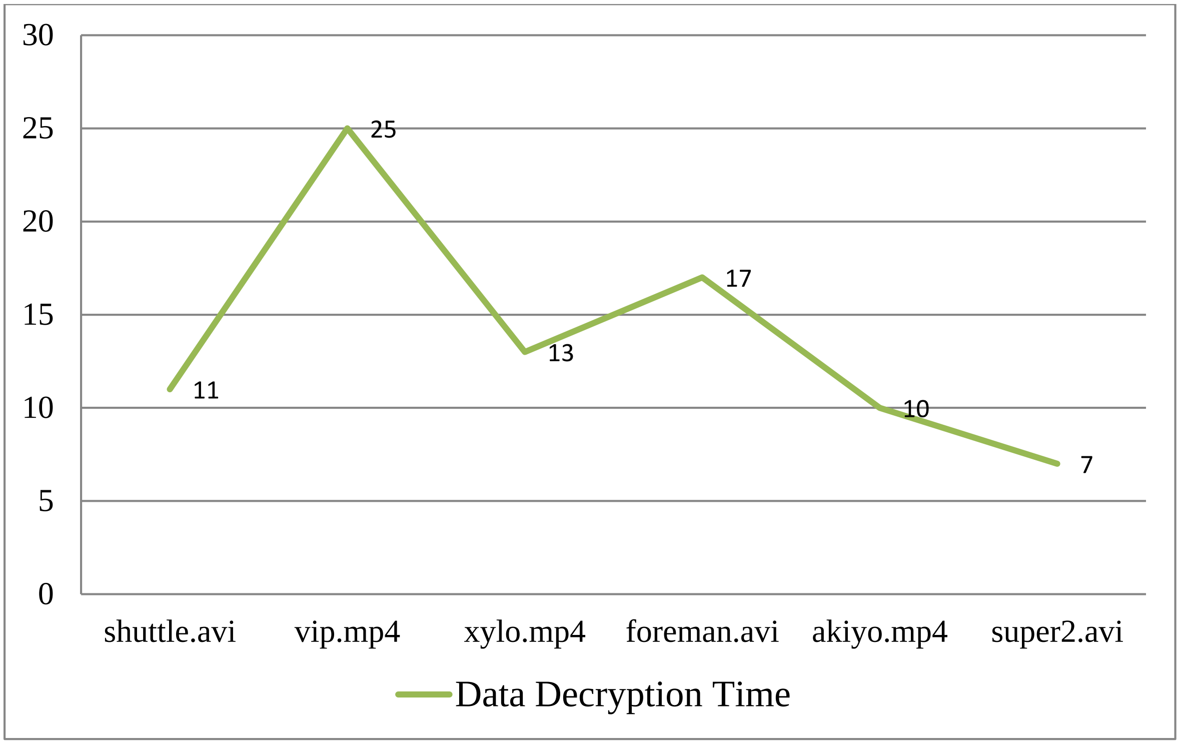


Fig 5.10 Plot of DDT values of six different videos

It is a process of retrieving and decrypting the covert data from the cover media by using some secret key. For symmetric decryption secret key should be private. Sender and receiver should know the secret key in order to encrypt the concealed data. In above Fig 5.10 the DDT (Data Decryption Time) for six videos is displayed. This plot shows that super.avi having the lowest decryption time for data retrieval. Afterwards akiyo.mp4, shuttle.avi, xylo.mp4, foreman.avi and at the last vip.mp4 having high DDT. But this parameter should be less since data retrieval should be fast. Less decryption time shows that the proffered method is useful and proficient in terms of data security and collateral. Difficult retrieval of covert data expounds that steganographic system is secure and protected. This parameter can't judge the robustness and proficiency of the encryption scheme, due to the presence of the various de-steganographic tools. Data security is not analyzed using only one parameters, other parameters are also responsible for robustness and efficiency of the algorithm and the system.

5.4 Video Steganograhy using DWT and BCD codes Imbedding Phase

The below flowchart show the steps that are followed for data concealing in the respective frame of the given video.Any successful steganography system should consider two important factors: imbedding payload and imbedding efficiency.

So, embedding payload demonstrated as the amount of covert information is to be imbedded inside the cover image and media.The imbedding efficiency includes the stego visual calibre factor.With this it can be infer that any algorithm is efficient and robust if it incur high imbedding payload i.e. its has large capacity to hide and conceal covert data.

In propounded algorithm frames are extracted from the cover video and one frame is taken for dataconcealing.But before imbedding secret message into the frames, encryption is applied on the text message using secret key1 and then BCD codes are applied for making secret data more random thus leads to increase the security of the system three times. The foremost merit of BCD codes is easy and simplest implementation. It is very easy to decode and encode the decimal numbers into BCD numbers and vice versa. It is simple to covert base-10 into base-2. Afterwards DWT is apllied on the cover frame of the input video for improving its textural features i.e. visual quality and calibre factor.The principle vantage point of using DWT is that it separates middle, high and low frequencies and its boundaries.In first level decomposition of DWT it splits the frequency coefficients od the frame into four sub-bands i.e. LL,LH,HL and HH. In level two decomposition it splits LL subband ino four subbands i.e. LLLL,LLLH,LLHL,LLHH. But it will discard LLLL subband as it contains less information and will store data in other three frequency subbands (LLLH,LLHL,LLHH). Succeedingly DWT imbeds the secret message into the cover image by transforming coefficient values. In last step stego video is rebulided by combining the frames. The following flowchart of “Imbedding Phase” mentioned below will demonstrates the full knowledge of the data concealing in a cover video.The propounded algorithm is implemented in MATLAB for visualizing and interpreting the exact results.

Example of the BCD coversion

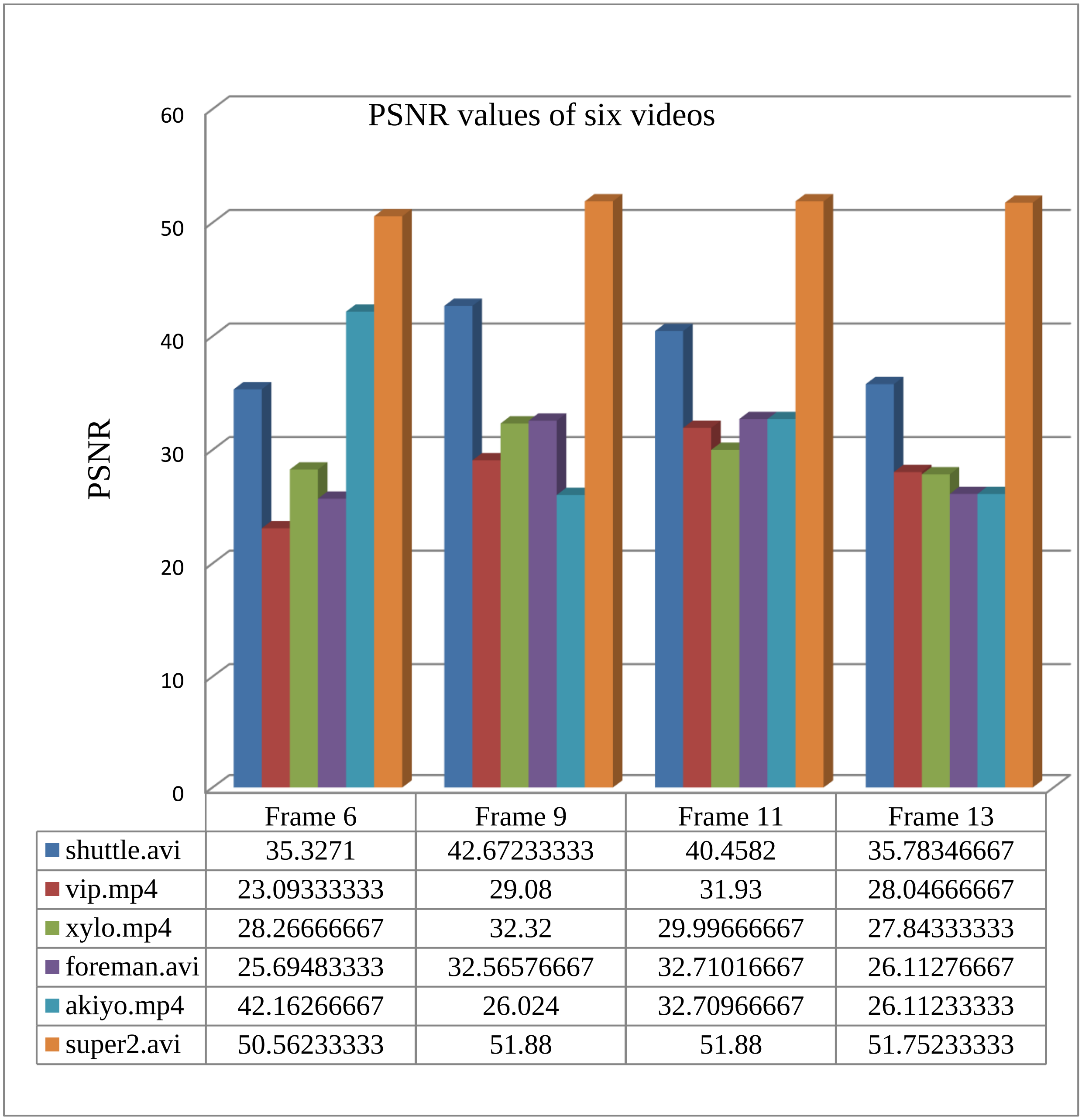
$(537)_{10}$ =0101 0011 0111

This example represents the 4-bit representation of the decimal numbers. This conversion is used to provide more security to the covert data.

Table 5.3 Attribute values of DWT using BCD codes imbedding phase

Parameters	Videos						
	Frames	Shuttle.avi	Vip.mp4	Xylo.mp4	Foreman.avi	Akiyo.mp4	Super2.avi
PSNR(dB)	Frame6	R=35.2299	R=23.49	R=29.05	R=25.3562	R=42.308	R= 50.880
		G=35.4519	G=22.96	G=28.10	G=25.8493	G=42.320	G=53.646
		B=35.2995	B=22.83	B=27.65	B=25.8790	B=41.860	B= 47.161
	Frame9	R=42.6062	R=29.19	R=32.82	R=32.3725	R=25.608	R=50.755
		G=42.8507	G=29.09	G=32.41	G=32.7149	G=26.153	G=54.134
		B=42.5601	B=28.96	B=31.73	B=32.6099	B=26.311	B=50.751
	Frame11	R=40.4563	R=31.76	R=31.02	R=32.6323	R=32.632	R= 50.755
		G=40.5659	G=32.04	G=29.70	G=32.8477	G=32.847	G= 54.134
		B=40.3524	B=31.99	B=29.27	B=32.6505	B=32.650	B=50.751
	Frame13	R=35.7487	R=28.02	R=28.42	R=26.0946	R=26.094	R=50.548
		G=35.8271	G=28.11	G=27.79	G=26.1912	G=26.191	G=53.953
		B=35.7746	B=28.01	B=27.32	B=26.0525	B=26.052	B=50.756
MSE	Frame6	R=19.5024	R=290.76	R=80.83	R=189.433	R=3.821	R=0.5309
		G=18.5304	G=328.2	G=100.52	G=169.104	G=3.810	G=0.2809
		B=19.1925	B=338.8	B=111.60	B=167.951	B=4.236	B=1.2502
	Frame9	R=3.5683	R=78.19	R=33.95	R=37.655	R=178.74	R=0.5465
		G=3.3730	G=80.13	G=37.27	G=34.800	G=157.66	G=0.251
		B=3.6064	B=82.48	B=43.61	B=35.652	B=152.04	B=0.5470
	Frame11	R=5.8540	R=43.35	R=51.38	R=35.468	R=35.468	R= 0.5465
		G=5.7081	G=40.58	G=69.52	G=33.752	G=33.752	G=0.2510
		B=5.9957	B=41.09	B=76.92	B=35.320	B=35.320	B= 0.5470
	Frame13	R=17.3064	R=102.53	R=93.44	R=159.81	R=159.81	R= 0.5732
		G=16.9970	G=100.3	G=108.15	G=16.301	G=156.30	G=0.261
		B=17.2038	B=102.7	B=120.40	B=120.401	B=120.40	B=0.5463
MSD	Frame6	R=20.5404	R=27.153	R=40.234	R=42.8011	R=45.6816	R=54.340
		G=18.1078	G=28.29	G=39.633	G=45.5853	G=39.7430	G=48.805
		B=17.8733	B=29.34	B=41.819	B=47.3418	B=61.0556	B=31.634
	Frame9	R=20.4711	R=31.515	R=40.234	R=42.8012	R=45.682	R=42.175
		G=18.1237	G=32.94	G=39.633	G=45.5853	G=39.759	G=46.656
		B=17.9260	B=34.16	B=41.819	B=47.3418	B=61.033	B=47.651
	Frame11	R=20.6386	R=33.509	R=40.234	R=42.8011	R=45.6493	R=42.175
		G=18.1477	G=33.84	G=39.633	G=45.5853	G=39.6939	G=46.656
		B=17.8797	B=35.75	B=41.819	B=47.3418	B=61.0721	B=47.651
	Frame13	R=20.8257	R=34.826	R=40.234	R=42.8011	R=45.6281	R=44.330
		G=18.2146	G=35.14	G=39.633	G=45.5853	G=39.6788	G=46.998
		B=17.8628	B=37.07	B=41.819	B=47.3419	B=61.0771	B=49.765
DET (secs)	Full video	20	17	16	21	20	18
IMP(MB)		14.4837	32.7564	12.1824	34.0213	53.4006	1.8432

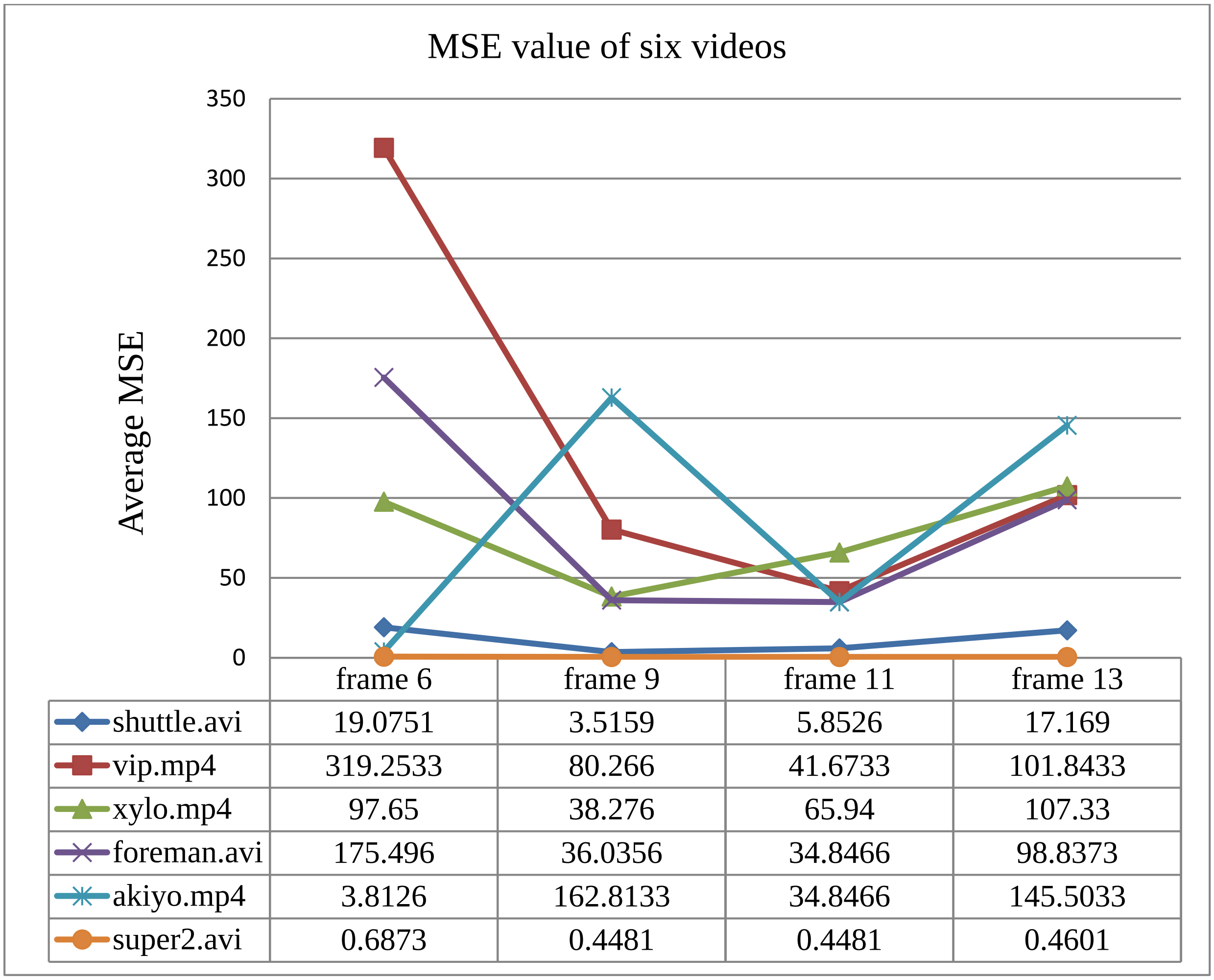
From the above table 5.3 it can be deduced that all the video are evaluated on different parameters for concealing data inside a carrier video by using DWT hinged on BCD codes. DWT gives best results as compared to LSB method even in imbedding phase. It is more robust and computed for all different parameters used for analysis. As DWT enhances the textural features and edges of the carrier image



	Frame 6	Frame 9	Frame 11	Frame 13
■ shuttle.avi	35.3271	42.67233333	40.4582	35.78346667
■ vip.mp4	23.09333333	29.08	31.93	28.04666667
■ xylo.mp4	28.26666667	32.32	29.99666667	27.84333333
■ foreman.avi	25.69483333	32.56576667	32.71016667	26.11276667
■ akiyo.mp4	42.16266667	26.024	32.70966667	26.11233333
■ super2.avi	50.56233333	51.88	51.88	51.75233333

Fig 5.11 Plot of PSNR values of six different videos

After the framing process of video, frames are taken random for imbedding the secret data inside the frame of video. This is executed by transforming the coefficients of the cover image and encrypting the secret data with key and then encode with BCD codes. In order evaluate the visual quality and textural features of the stego image PSNR and MSE values are computed. The above fig.5.11 shows the PSNR values for a total of 4 frames for six different videos. The table depicts that PSNR values for three videos are high i.e. shuttle.avi, foreman.avi and super2.avi and other videos have comparatively PSNR values. In this method PSNR values are high which means there is no degradation in the quality of the stego image. PSNR values are more for avi files and less for mp4 files.



	frame 6	frame 9	frame 11	frame 13
◆ shuttle.avi	19.0751	3.5159	5.8526	17.169
■ vip.mp4	319.2533	80.266	41.6733	101.8433
▲ xylo.mp4	97.65	38.276	65.94	107.33
× foreman.avi	175.496	36.0356	34.8466	98.8373
✳ akiyo.mp4	3.8126	162.8133	34.8466	145.5033
● super2.avi	0.6873	0.4481	0.4481	0.4601

Fig 5.12 Plot of MSE values of six different videos

From the Fig 5.12 it can be inferred that there is a sudden increment in the values of MSE values for videos such as vip.mp4. But this doesn’t mean mp4 extension is not appropriate for data concealing. After extraction of data real scenario can be explained and predicted. Moreover the MSE values also depend upon the background of the images. So the extraction of the concealed data is an import asset of steganographic system.

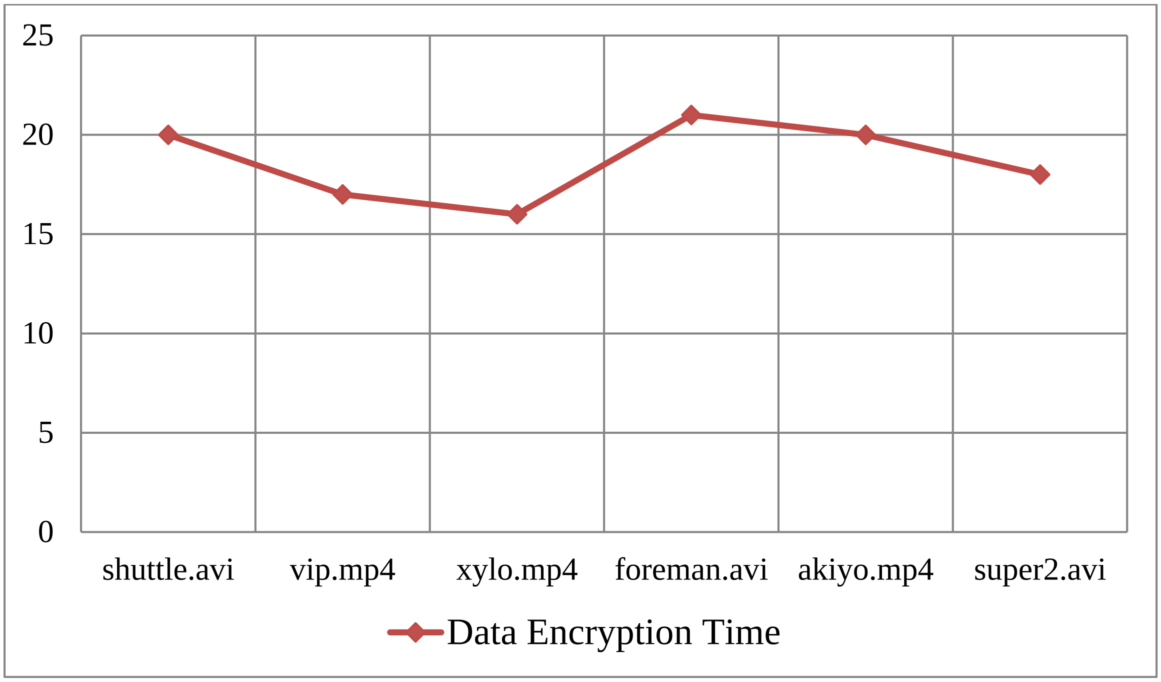


Fig 5.13 Plot of DET values of six different videos

This parameter greatly depends on the type of the algorithm employed, for DWT it is less for all video bit for LSB it was more. This shows the efficiency and security of the propounded algorithm. The above Fig 5.13 depicts that DET is less for all videos as compared to the LSB insertion method. This also displays that DWT is more robust and secure than LSB insertion method.

Imbedding payload is described as maximum amount of data that could be carried by the concerned video file. It is advised that the input data i.e. text should be smaller than or equal to the total payload of the video. Six different videos holding covert data inside them are depicted by the Fig 5.14. From below Fig 5.14 it can be inferred that vip.mp4 and akiyo.mp4 having the highest imbedding payload in DWT hinged on BCD codes. This parameter remains same for both the proffered algorithms. In DWT one can hide as much as data due to the property of enhancing the visual and textural details along with edges of the cover media. Moreover use of BCD codes makes this algorithm more reliable and secure as compared to previous one. Vantage point of using BCD codes is there easy and simple implementation.

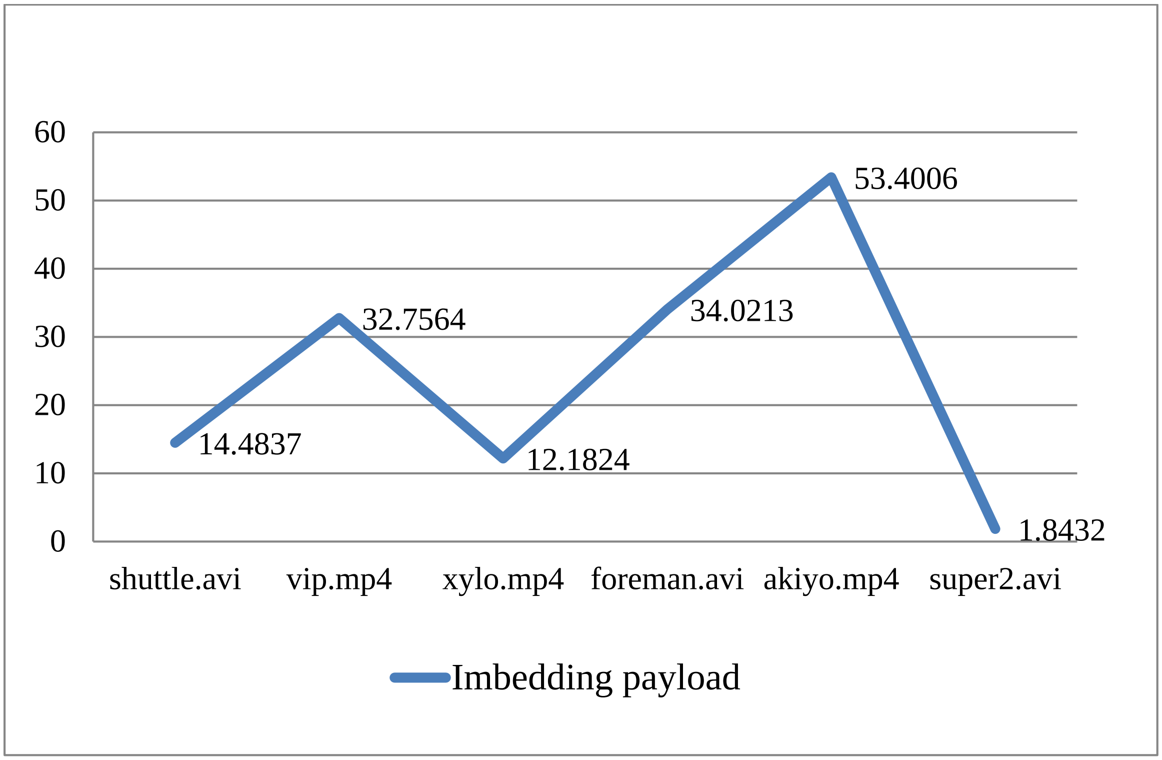
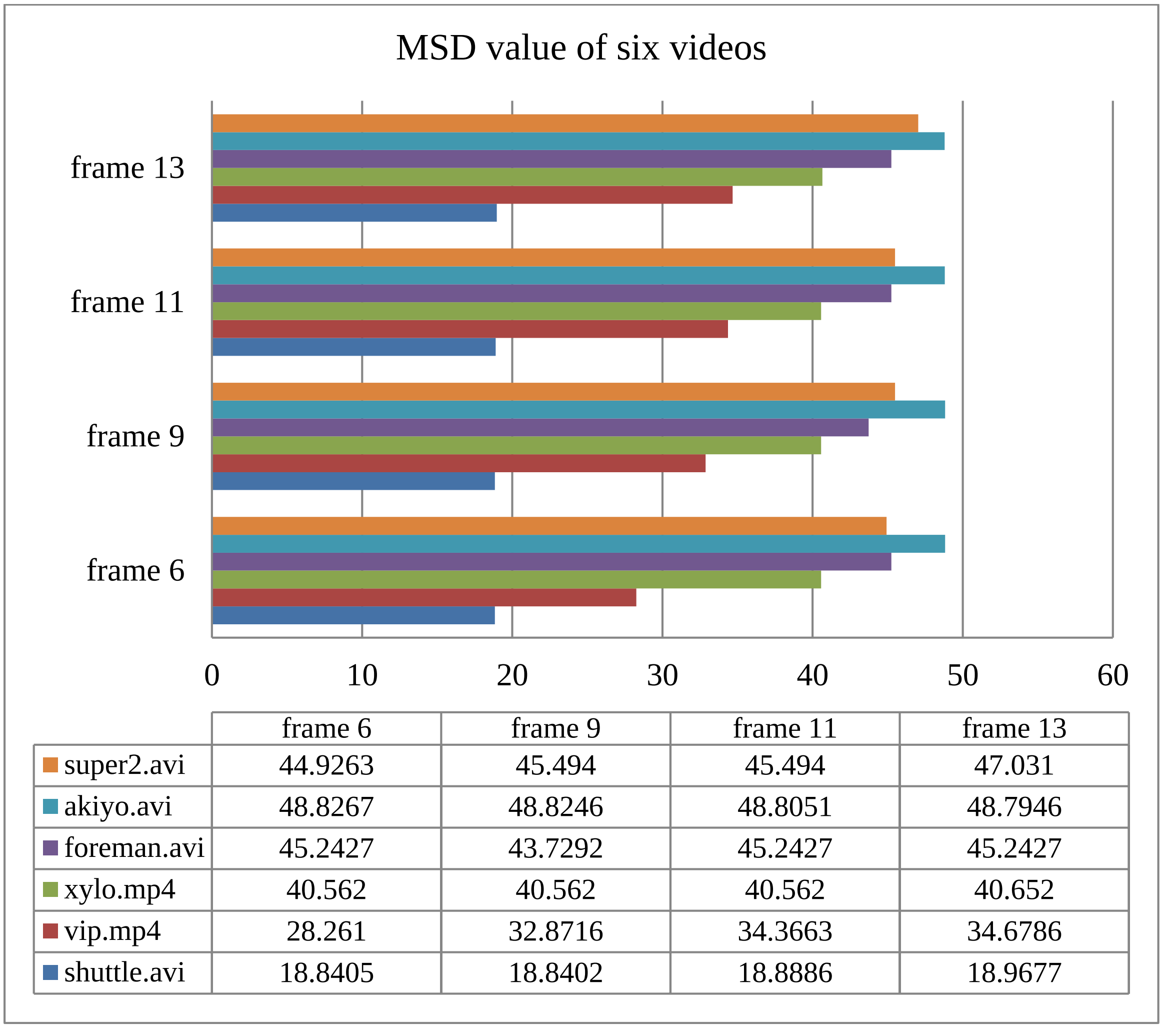


Fig 5.14 Plot of Imbedding Payload of six different videos

The below mentioned values of MSD in Fig 5.15 depicts that there is no distortion and alteration in the visual quality of the cover media after imbedding the covert data inside it. In addition to stego video is the close approximation the carrier video. Means chances of degradation of video quality are less. The explanation of statistic is intimately associated to the approach of the standard deviation. For the given part which could feasibly be an entire image, the standard deviation function of the brightness in that region of an image can be examined and explained. This attribute ensures the security and collateral of the concealed text inside a cover media. This parameter explains the least value of the MSD for shuttle.avi and it is high for all other five videos. MSD is an easy and simple way to secure the concealed data. The imbedding also depends on this parameter. In DWT one can hide as much as data due to the property of enhancing the visual and textural details along with edges of the cover media. Moreover use of BCD codes makes this algorithm more reliable and secure as compared to previous one. BCD codes are easy to implement. Due to this property of DWT, MSD is high in this imbedding phase.



	frame 6	frame 9	frame 11	frame 13
🟧 super2.avi	44.9263	45.494	45.494	47.031
🟦 akiyo.avi	48.8267	48.8246	48.8051	48.7946
🟪 foreman.avi	45.2427	43.7292	45.2427	45.2427
🟩 xylo.mp4	40.562	40.562	40.562	40.652
🟥 vip.mp4	28.261	32.8716	34.3663	34.6786
🟦 shuttle.avi	18.8405	18.8402	18.8886	18.9677

Fig 5.15 Plot of MSD of six different videos

5.5 Video Steganograhy using DWT and BCD codes Extraction Phase

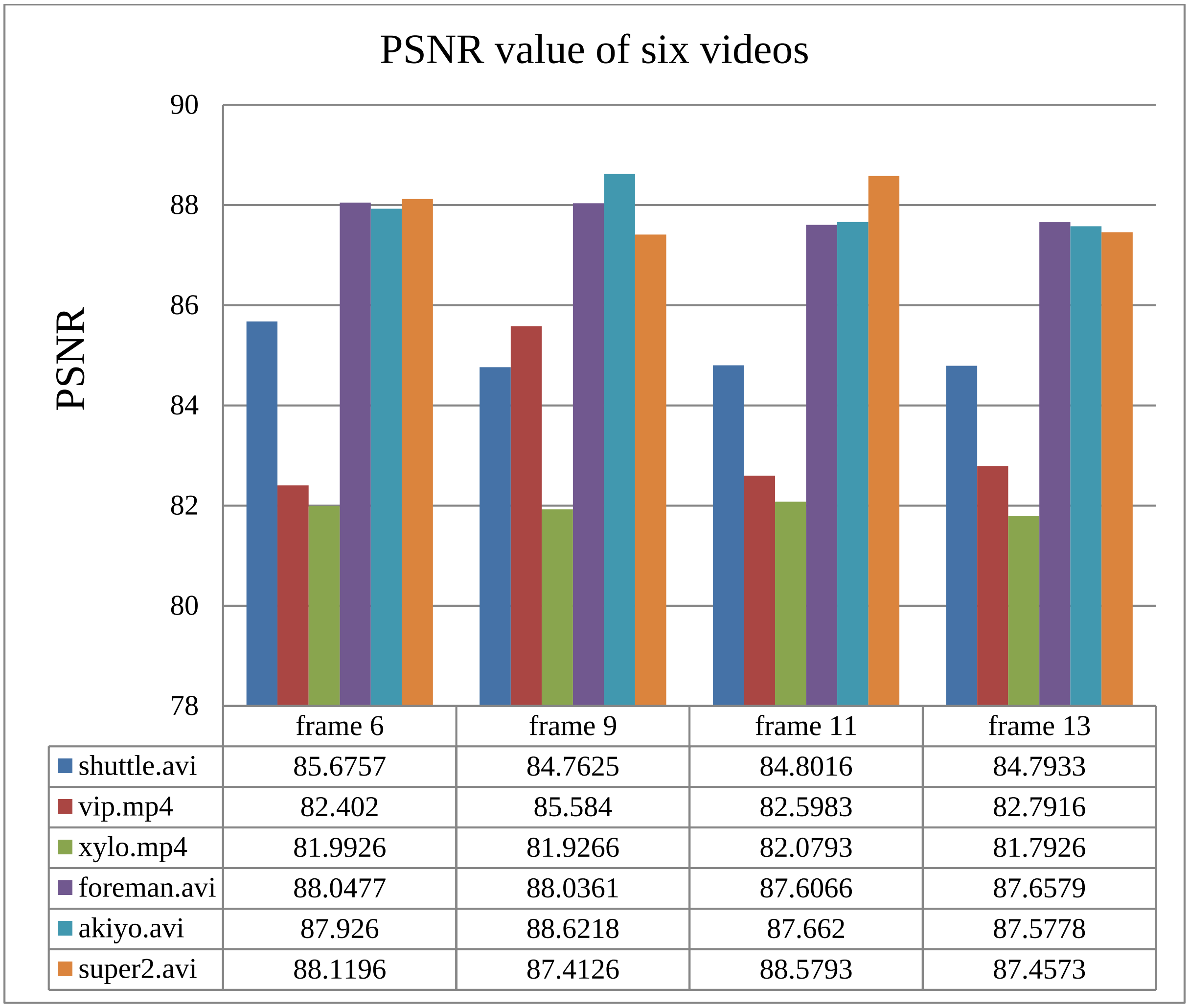
Any successful steganography system should consider two important factors: imbedding payload and imbedding efficiency. The imbedding payload demonstrated as the amount of covert information is to be imbedded inside the cover image and media.The imbedding efficiency includes the stego visual calibre factor.With this it can be infer that any algorithm is efficient and robust if it incur high imbedding payload i.e. its has large capacity to hide and conceal covert data.

In propounded algorithm frames are extracted from the stego video and stego frames are taken for data extraction. Afterwards 2D Inverse DWT is applied on the stego frames. It is only applied on thec LH, HL and HH frequency sub-bands. As the LL subband is near approximation the image.In the next step decryption is applied on the frames using secret key1 in ordedr to decrypt the secret data. Further apply BCD decoder on the decrypted covert message and decode the secret message.Analyze the recovered carrier video and extracted message The fundamental advantage of the BCD codes is easy and simplest implementation. It is very easy to decode and encode the decimal numbers into BCD numbers and vice versa. It is simple to covert base-10 into base-2. Afterwards DWT is apllied on the cover frame of the input video for improving its textural features i.e. visual quality and calibre factor.The principle vantage point of using DWT is that it separates middle, high and low frequencies and its boundaries.In first level decomposition of DWT it splits the frequency coefficients od the frame into four sub-bands i.e. LL,LH,HL and HH. In level two decomposition it splits LL subband ino four subbands i.e. LLLL,LLLH,LLHL,LLHH. But it will d0iscard LLLL subband as it contains less information and will store data in other three frequency subbands (LLLH,LLHL,LLHH). Succeedingly DWT imbeds the secret message into the cover image by transforming coefficient values. In last step stego video is rebulided by combining the frames. The following flowchart of “Extraction Phase” mentioned below will demonstrates the full knowledge of the data extraction from a stego video.The propounded algorithm is implemented in MATLAB for visualizing and interpreting the exact results.

From the below Table.5.4 it can be inferred that after extracting secret message from the cover video there is sudden rise in the PSNR and fall in the MSE values. This shows the propounded algorithm has high imbedding payload and capacity. It is efficient in terms of visual quality of cover video and originality of the secret message. There is no difference between the carrier image and the stego image. Less error depicts that the propounded algorithm is robust and competent. This method shows high PSNR values for six different videos in the range of (81-88 dB) and also proved that PSNR doesn’t depends on the type of video file extension. It gives the best results for all the extension used. The high value of PSNR shows that there is no degradation in the visual quality and textural features of the cover image along with the fact that there is no possible alteration in the concealed text after the retrieval from the cover image. This depicts the robustness and proficiency of the steganographic system.

Table 5.4 Attribute values for Extraction phase of DWT using BCD codes

Parameters	Videos						
	Frames	Shuttle.avi	Vip.mp4	Xylo.mp4	Foreman.avi	Akiyo.mp4	Super2.avi
PSNR(dB)	Frame6	R=84.5886	R=81.736	R=81.627	R=88.4898	R=87.8123	R=88.331
		G=84.2948	G=82.13	G=81.461	G=87.1635	G=87.5320	G=86.314
		B=85.1438	B=83.34	B=82.890	B=88.4898	B=88.4337	B=89.714
	Frame9	R=84.3767	R=81.932	R=81.421	R=87.5207	R=87.1428	R=87.953
		G=84.4603	G=81.85	G=81.58	G=87.7762	G=89.3613	G=86.842
		B=85.4505	B=82.97	B=82.779	B=88.8116	B=89.3613	B=87.442
	Frame11	R=84.4183	R=82.535	R=81.461	R=87.2794	R=87.5320	R=89.994
		G=84.5886	G=81.97	G=81.887	G=87.0507	G=87.0205	G=86.57
		B=85.3979	B=83.29	B=82.890	B=88.4898	B=88.4337	B=89.714
	Frame13	R=84.3356	R=82.535	R=81.302	R=88.0478	R=87.3983	R=86.842
		G=84.3767	G=81.97	G=81.186	G=87.2794	G=86.9015	G=86.570
		B=85.6677	B=83.87	B=82.890	B=87.6466	B=88.4337	B=88.96
MSE	Frame6	R=2.26e-04	R=4.3e-04	R=4.4e-04	R=9.20e-05	R=1.07e-04	R=9.5e-05
		G=2.4e-04	G=3.9e-04	G=4.6e-04	G=1.24e-04	G=1.1e-04	G=1.5e-04
		B=1.9e-04	B=3.0e-04	B=3.3e-04	B=9.20e-05	B=9.3e-05	B=6.9e-05
	Frame9	R=2.37e-04	R=2.3e-04	R=4.6e-04	R=1.15e-04	R=1.04e-04	R=1.04e-04
		G=2.3e-04	G=1.8e-04	G=4.5e-04	G=1.08e-04	G=1.2e-04	G=1.3e-04
		B=1.8e-04	B=3.6e-04	B=3.4e-04	B=8.54e-05	B=7.5e-05	B=1.1e-04
	Frame11	R=2.35e-04	R=4.1e-04	R=4.6e-04	R=1.21e-04	R=1.1e-04	R=6.5e-05
		G=2.2e-04	G=3.0e-04	G=4.2e-04	G=1.28e-04	G=1.2e-04	G=1.4e-04
		B=1.8e-04	B=3.6e-04	B=3.3e-04	B=9.20e-05	B=9.3e-05	B=6.9e-05
	Frame13	R=2.39e-04	R=3.6e-04	R=4.8e-04	R=1.01e-04	R=1.1e-04	R=1.3e-04
		G=2.3e-04	G=4.1e-04	G=4.9e-04	G=1.21e-04	G=1.3e-04	G=1.4e-04
		B=1.7e-04	B=2.6e-04	B=3.3e-04	B=1.11e-04	B=9.3e-05	B=8.24e-05
MSD	Frame6	R=20.5404	R=27.153	R=40.234	R=42.8011	R=45.6816	R=54.340
		G=18.1078	G=28.29	G=39.633	G=45.5853	G=39.7430	G=48.805
		B=17.8733	B=29.34	B=41.819	B=47.3418	B=61.0556	B=31.634
	Frame9	R=20.4711	R=31.515	R=40.234	R=42.8012	R=45.682	R=42.175
		G=18.1237	G=32.94	G=39.633	G=45.5853	G=39.759	G=46.656
		B=17.9260	B=34.16	B=41.819	B=47.3418	B=61.033	B=47.651
	Frame11	R=20.6386	R=33.509	R=40.234	R=42.8011	R=45.6493	R=42.175
		G=18.1477	G=33.84	G=39.633	G=45.5853	G=39.6939	G=46.656
		B=17.8797	B=35.75	B=41.819	B=47.3418	B=61.0721	B=47.651
	Frame13	R=20.8257	R=34.826	R=40.234	R=42.8011	R=45.6281	R=44.330
		G=18.2146	G=35.14	G=39.633	G=45.5853	G=39.6788	G=46.998
		B=17.8628	B=37.07	B=41.819	B=47.3419z	B=61.0771	B=49.765
DDT (secs)	Full video	11	11	12	17	10	12
IMP(MB)		14.4837	32.7564	12.1824	34.0213	53.4006	1.8432



	frame 6	frame 9	frame 11	frame 13
■ shuttle.avi	85.6757	84.7625	84.8016	84.7933
■ vip.mp4	82.402	85.584	82.5983	82.7916
■ xylo.mp4	81.9926	81.9266	82.0793	81.7926
■ foreman.avi	88.0477	88.0361	87.6066	87.6579
■ akiyo.avi	87.926	88.6218	87.662	87.5778
■ super2.avi	88.1196	87.4126	88.5793	87.4573

Fig 5.16 Plot of PSNR of six different videos

Data Decryption Time is a process of retrieving and decrypting the covert data from the cover media by using some secret key. For symmetric decryption secret key should be private. Sender and receiver should know the secret key in order to encrypt the concealed data. In above Fig 5.17 the DDT (Data Decryption Time) for six videos is displayed. This plot displays that akiyo.avi having the lowest decryption time of 10 seconds for data retrieval. Afterwards plot displays that the akiyo.mp4, shuttle.avi, xylo.mp4, vip.mp4, and at the last foreman.avi having high DDT. This parameter can’t judge the robustness and proficiency of the encryption scheme. But this parameter should be less since data retrieval should be fast. This parameter expounded that DDT is less than DET in the imbedding phase. This comparison depicts that the encryption of the concealed text is reliable, secure and good in imbedding process of data concealing.

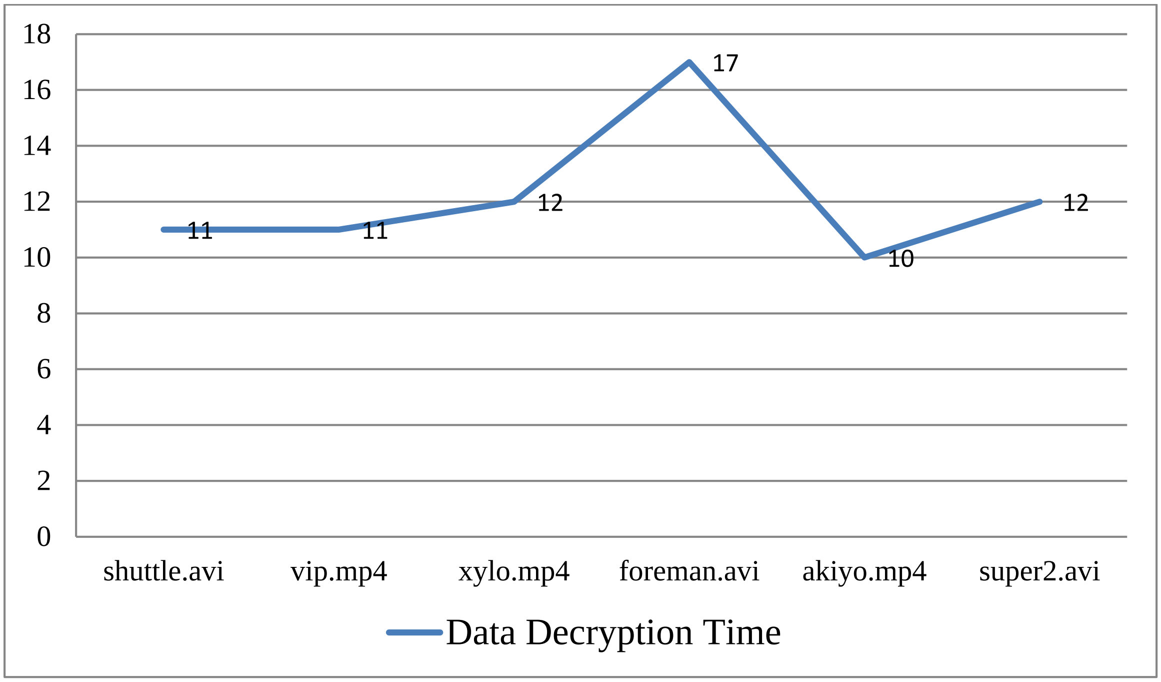


Fig 5.17 Plot of DDT of six different videos

As the MSE values are very small this shows that the steganographic system using DWT is more robust as compared LSB. It is more secure and reliable than LSB manipulation method, therefore the chances of image degradation and message distortion is very less.

5.6 Comparison between the above two algorithms:-

Present day is an age of technology in which people want security and secrecy regarding their personal whereabouts. So steganography came into existence and solved all the issues regarding data integrity and security. It can be implemented using time domain and frequency domain methods. In this work both domains are compared and an analysis is made according to their performances. The performance parameters are PSNR, MSE, data encryption time, data decryption time and imbedding payload. Above analysis demonstrates that LSB method works well for BMP images due to less compression and also shows that it has PSNR values up to 33 to 40 ranges. On the other side DWT works really well for all cover images and shows high PSNR values up to 80 to 89 ranges. Moreover DWT enhances the visual and textural features and edges of the stego image in order to minimize the distortion. According to results DWT using BCD code encryption gives more security and collateral to data than the LSB insertion method. This is proved by the PSNR and MSE value that is calculated for both the algorithms, showing that for LSB technique, if we increase the message length than the values of PSNR decreases and MSE value increases but for DWT it remains almost same. Thus the imbedding capacity of DWT method is more than that of LSB insertion.

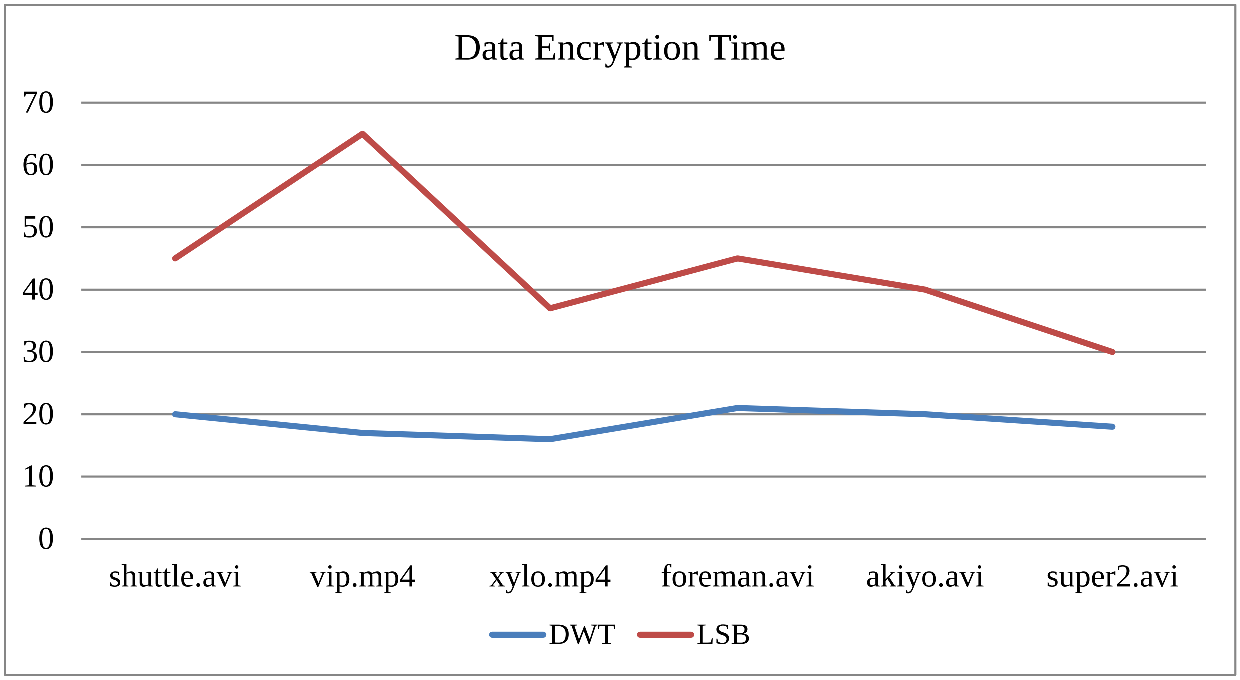


Fig 5.18 Plot of DET of six different videos

The DET defined the time required for concealing covert data inside the cover image. It is calculated in seconds and it greatly depends on the amount data to be concealed. This above Fig 5.18 depicts the comparison between the Data Encryption Time of LSB insertion and DWT hinged on BCD codes. According to this comparison the DET of DWT is less than the LSB insertion method because it is more efficient and good to implement, on the other side LSB method is very inefficient. The conjecture of this section is that DWT is more good and efficient than LSB method.

The DDT defined as the time required for retrieving the covert data from the cover image. It is calculated in seconds and it greatly depends on the amount data to be extracted. The underneath Fig 5.19 defines the DDT for both LSB and DWT method. Data Decryption Time is less for DWT as compared to LSB method. This depicts the efficiency of DWT method over LSB insertion method.

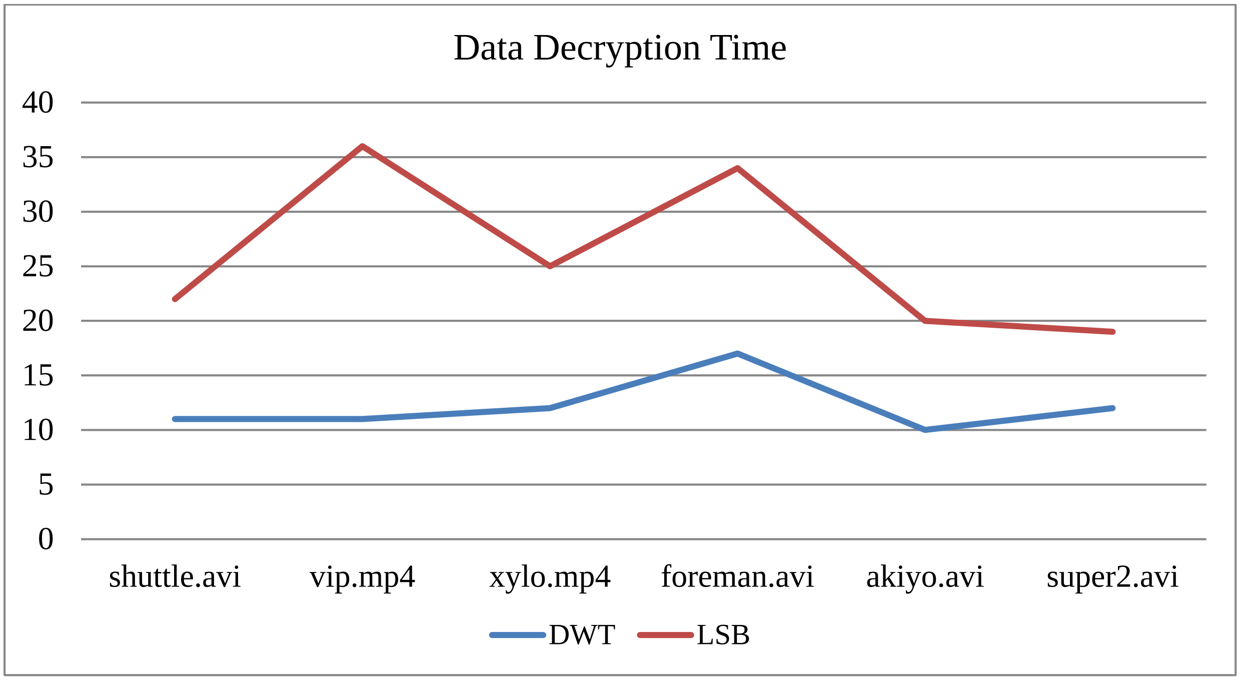


Fig 5.19 Plot of DDT of six different videos

*****

6

CONCLUSION & FUTURE SCOPE

"Success is a science; if you have the conditions, you get the result" *Oscar Wilde*

In this research, a comprehensive study of video steganography is procured with the aid of two different algorithms i.e. LSB insertion method and DWT hinged on BCD codes. The conjecture drawn on the basis of two algorithms is stated below. Further the future scope of the research is expounded and discussed.

6.1 Conclusion

In this dissertation, a cumulative study on video steganography is procured based on the formulation process of two algorithms i.e. LSB insertion method and DWT using BCD codes. These methods help in analyzing the visual calibre factors related to an image through which the quality of an image after concealing and extracting the covert message is judged. The higher PSNR value signifies that there is least distortion in the image quality. Through the DWT approach employed, the results show a considerable increase in the value of PSNR along with least MSE values. Whereas, for the LSB insertion the value procured for the calibre factors are not high enough in comparison to the DWT method used. Thus it is inferred from the simulation results that the DWT using BCD codes method gives far superior results in lieu to the LSB insertion technique exploited. Also concealing diverse amount of data in a video file using DWT method reveals that there is no effect on the textural features and edges of the stego image. A total of six videos for the LSB insertion technique and five videos for DWT using BCD codes method were considered in order to formulate the results. Also the different extension video files were used through which it is illustrated that the .avi files impose less compression on the image in comparison to the .mp4 video files. But the .avi files are not compatible with media players so .mp4 is considered more for analysis.

Further the data encryption time and data decryption time is computed for various videos using the two algorithms i.e. LSB insertion technique and DWT hinged on BCD codes. This signifies that for a video file of large size, encrypting and decrypting the concealed data takes more amount of time as compared to a file of less size. Also based on the algorithms used, the data encryption and decryption time procured shows that for LSB insertion method the values were more in comparison to the DWT hinged on BCD method used. Therefore, the performance estimation divulges that the data encryption and data decryption rates for various video formats lead to divergent level of concealment.

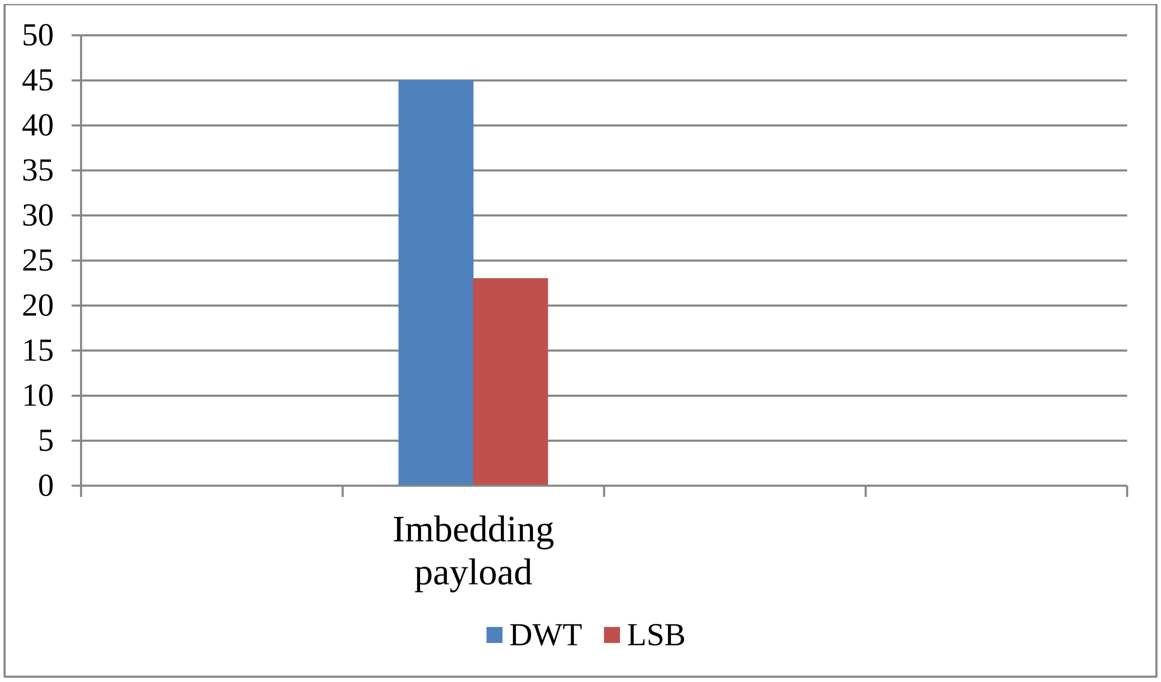


Fig 6.1 Comparison of Imbedding Capacity of Two algorithms

The below Fig 6.1 depicts the imbedding capacity of the two propounded algorithms. LSB method is having less imbedding capacity as compared to DWT method. As it is a fact that LSB insertion is a spatial domain method and DWT is a frequency domain method, the hiding capacity of the LSB is less because it only replacing the LSBs of the secret text and cover image. This leads to the distortion of the image quality and gives hint to earwigs that something is not normal with the image. On the other side DWT transforms the coefficients of an image that’s why there is no degradation in the image quality after imbedding the covert data inside a cover image. The conjecture of this discussion is that DWT is better than LSB insertion method in term of hiding data inside a cover media.

6.2 Future Scope

In forthcoming researches, the DWT method could be implemented using linear and cyclic error correction codes such as Reed Mullers code. Another idea for future is to seek and ordain diverse options for the users in efficiently choosing cover media and identifying techniques for embedding huge amount of covert data. Further diverse transformation techniques can be employed like lifting scheme that analyze the visual calibre attribute of an image. In future, imbedding payload capacity can be enhanced imbedding more number of bits to edges pixels as compared to non- edge pixels of a carrier image.

*****

REFERENCES

1. Eric Cole, Hiding in Plain Sight: Steganography and the Art of Covert Communication, Canada: Wiley, 2003

2. J. Anderson and Fabien A. P. Petitcolas," On the Limits of Steganography", IEEE Journal on Selected Areas in Communications, Vol. 16, No. 4, 1998

3. Gregory Kipper, Investigator's Guide to Steganography, New York: Auerbach, August 2004.

4. J. Lim, "Two-Dimensional Signal and Image Processing", Prentice-Hall, Englewood Cliffs, NJ, 1990

5. Mohamed Elsadig Eltahir, Miss Laiha Mat Kiah, Bilal Bahaa Zaidan, Aos Alaa Zaidan, "High Rate Video Streaming Steganography," IEEE, pp. 550-553, 2009

6. Manoj Kumar Ramaiya, Naveen Hemrajani, Anil Kishore Saxena, "Security Improvisation in Image Steganography Using DES," IEEE, pp. 1094-1099, 2012

7. Ross 3. M.A. Alavianmehr, et al, "A lossless data hiding scheme on video raw data robust against H.264/AVC compression," Computer and Knowledge Engineering (ICCKE), pp. 194-198, 2012

8. D. E. Dudgeon and R. M. Mersereau, Multidimensional Digital Signal Processing, Prentice-Hall, Englewood Cliffs, NJ, 1983

9. N.Jothy, et.al, "A Secure Color Image Steganography Using Integer Wavelet Transform", 2016

10. Joanne Hwan Jie Yin, et.al, "Internet of Things: Securing Data using Image Steganography", IEEE,2015

11. Ramadhan J. Mstafa, Khaled M. Elleithy, "A high payload Video Steganography Algorithm in DWT Domain Based on BCH Codes (15, 11)" IEEE, pp. 1-9, Mar. 2015

12. Ramadhan J Mstafa and Khaled M. Elleithy, "A highly secure video Steganography using Hamming codes (7, 4)," IEEE, pp. 1-6, 2015

13. Yugeshwari Kakde, Priyanka Gonnade, Prashant Dahiwale, "Audio-Video Steganography", 2015

14. Saket Kumar, Ajay Kumar Yadav, Ashutosh Gupta and Pradeep Kumar, "RGB Image Steganography on Multiple Frame Video using LSB Technique," IEEE, pp. 226-231, 2015

15. Ramadhan J. Mstafa, Khaled M. Elleithy, "A Novel Video Steganography Algorithm in the Wavelet Domain Based on the KLT Tracking Algorithm and BCH Codes" IEEE, pp. 1-7, 2015

16. Kasim Tasdemir, Fatih Kurugollu and Sakir Sezer, "A Stegoanalysis System Utilizing Temporal Pixel Correlation of HEVC Video," IEEE, 2015

17. K. Thangadurai and G. Sudha Devi, "An analysis of LSB Based Image Steganography Techniques," IEEE, pp. 1-4, 2014

18. Mennatallah M. Sadek & Amal S. Khalifa & Mostafa G. M. Mostafa, "Video Steganography: a comprehensive review" SPRINGER, pp. 1-32, 2014

19. Hamdy M. Kelash, Osama F. Abdel Wahab, Osama A. Elshakankiry and Hala S. El-sayed, "Hiding Data in Video Sequences Using Steganography Algorithms," IEEE, pp. 353-358, 2013

20. Rajesh G.R and A. Shajin Nargunam, "Steganography Algorithm Based On Discrete Cosine Transform for Data Embedding Into Raw Video Streams" IEEE, 2013

21. Prabakaran.G, Bhavani.R (2012)

22. Souvik Bhattacharya and Gautam Sanyal, "A Novel Approach of Video Steganography Using PMM" SPRINGER, vol. 292, pp. 644-653, 2012

23. Feng Pan, Li Xiang, Xiao-Yuan Yang and Yao Guo, "Video Steganography using Motion Vector and Linear Block Codes,", IEEE, pp. 592-595, 2010

24. Ozdemir Cetin, A. Turan Ozcerit, "A new Steganography algorithm based on color histograms for data embedding into raw video streams" ELSEVIER, pp. 670-682, 2009

25. Abbas Cheddad, Joan Condell, Kevin Curan and Paul Mc Kevitt, "Skin Tone Based Steganography in video files exploiting the YCBCR colour space," IEEE, pp. 905-908, 2008

26. Chen Ming, Zhang Ru, Niu Xinxin and Yang Yixian, "Analysis of Current Steganography Tools: Classifications & Features," IEEE, pp.1-4, 2006

27. K.B. Raja, C.R. Chowdary, Venugoplal K R, L.M. Patnaik, " A secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images" IEEE, pp. 171-176, 2005

28. Venkatraman. S, Ajith Abraham and Marcin Paprzycki, "Significance of Steganography on Data Security," IEEE, pp. 1-5, 2005

*****