# An Improved Data-hiding Approach using Skin-tone Detection for Video Steganography

*A dissertation submitted in partial fulfillment of requirement for*

*the award of degree of*

**Master of Engineering**

in

**Electronics and Communication Engineering**


**Submitted by:**

Pankaj Kumar

Roll No: 801561020

**Under the guidance of:**

Dr. Kulbir Singh

Professor

**ELECTRONICS AND COMMUNICATION ENGINEERING DEPARTMENT**

**THAPAR UNIVERSITY**

(Established under the section 3 of UGC Act, 1956) PATIALA–

147004 (PUNJAB)



JULY, 2017

# DECLARATION

I hereby declare that the work which is being presented in this dissertation, entitled **"An Improved Data-hiding Approach using Skin-tone Detection for Video Steganography"** for the award of degree of Master of Engineering in Electronics and Communication Engineering, is an authentic record of my own work carried out under the supervision of **Dr. Kulbir Singh (Professor),** ECED, Thapar University Patiala and refers other work which are listed in the reference section.

The results presented in this dissertation have not been submitted by me in part or full to any other University/Institute for the award of degree or diploma.

Pankaj Kumar

**Date:** 17-07-2017

Pankaj Kumar

Roll No. 801561020

It is certified that the above statement made by the candidate is correct to the best of my knowledge and belief.

**Date:** 17-07-2017

**Dr. Kulbir Singh**

Professor, ECED

Thapar University, Patiala

# ACKNOWLEDGEMENT

Though the work done for research purpose is hectic and time consuming and requires a lot of hard work, dedication, immense will power and proper knowledge of the field of research to complete the thesis but without the constant support and motivation, it can't be achieved.

I would like to take the opportunity to express my gratitude to my supervisor **Dr. Kulbir Singh**, Professor, Electronics and Communication Department, Thapar University, Patiala for his continuous advice, enthusiasm and inspiration throughout the thesis work.

I also want to thank **Dr. Alpana Agarwal**, Head of the department (ECE), **Dr. Hemdutt Joshi**, P.G Coordinator and **Dr. Amit Mishra**, Program Coordinator, M.E (ECE) for giving me moral support and adequate environment to complete the research work.

I wish to thank all my friends, faculty members of the department who helped me directly or indirectly and provided me their valuable knowledge, specially my mother for her never ending love, blessings and encouragement throughout my life.

**Pankaj Kumar**
801561020

# ABSTRACT

The secure transmission of data over internet is attained using steganography. It is an art and science of hiding information in undistinguishable cover media so as not to instigate and observer's suspicion. Steganography is a method to secure the secret information by just embedding the information within other information. Several types or formats of steganography are being used in modern era such as, image, text and audio/video. There are several steganography algorithms each having its own weakness or strength in terms of complexity and security. Some of them provide invisibility of secret information while some provides large embedding capacity. Securing the embedded data and diminishing the distortions in videos remain as challenging goals in data-hiding techniques. In this work, a steganographic approach is proposed to minimize the probability of detection of the embedded image data in cover video objects where human skin regions are considered as Regions of Interest (ROI) for embedding the secret data. The proposed technique works with both 2-D and 3-D secret images, which increases the adaptability of the proposed model to the various types of image data. Selective continuous pixel stacks are used to embed the secret data in the cover video object, which is performed over the third Discrete Wavelet Transform (DWT) component. The approximation coefficient has been entitled to be utilized for the purpose of embedding after the application of third Level DWT over the input video frame to enhance robustness and video quality. The frame matrix further undergoes the skin-map extraction to make the color-based pixel selection. Moreover, the proposed approach is designed with the amalgamation of 8-pixel stack extraction on the third Level DWT over the Red and Blue channels. Experimental results reveal that the proposed data-hiding scheme offers high imperceptibility and enhance the robustness against MPEG-4 compression.

# TABLE OF CONTENTS

*Declaration* *i*

*Acknowledgment* *ii*

*Abstract* *iii*

*Table of Contents* *iv*

*List of Abbreviations* *vii*

*List of Figures* *viii*

*List of Tables* *ix*

**CHAPTER-1: Introduction** **1-18**

1.1 Preamble 1

1.1.1 Overview of steganography 2

1.2 Types of information hiding 3

1.2.1 Cryptography 3

1.2.2 Steganography 4

1.2.3 Watermarking 4

1.2.4 Comparison of steganography techniques in different domains 4

1.3 Types of steganography 5

1.3.1 Text steganography 5

1.3.2 Audio steganography 6

1.3.3 Video steganography 7

1.3.4 Network steganography 7

1.3.5 Image steganography 8

1.3.6 Basic parameter of steganography methods 10

1.4 Domains of steganography 10

1.4.1 Spatial domain image steganography methods 11

1.4.2 Transform domain image steganography methods 13

1.5 Comparison of steganography techniques in different domains 14

1.6 Steganalysis 14

1.6.1 Steganalysis attacks 14

1.6.2 Steganalysis techiques 15

1.7 Applications of steganography 16
1.8 Motivation of the dissertation 17
1.9 Organization of the dissertation 18

**CHAPTER-2: Literature Review 19-31**
2.1 Introduction 19
2.2 Literature survey 19
2.3 Performance parameters 27
2.4 Research gaps 29
2.5 Problem formulation 30
2.6 Objectives of the dissertation 30
2.7 Methodology 30
2.8 Chapter summary 31

**CHAPTER-3: Data-hiding Approach using Skin-tone Detection 32-40**
3.1 System overview 32
3.2 Skin-block-map generation 33
3.3 Wavelet-based hiding 34
3.4 Secret-message embedding 36
3.5 Data-extraction procedure 38
3.6 Chapter summary 40

**CHAPTER-4: Results And Discussions 42-54**
4.1 Overview 42
4.2 Simulation scenario 42
4.3 Result evaluation 42
4.4 Comparison with other approaches 53
4.5 Chapter summary 54

**CHAPTER-5: Conclusion and Future Scope 55**
5.1 Conclusion 55
5.2 Future scope 55

**REFERENCES** **56-60**

**LIST OF PUBLICATIONS** **61**

# LIST OF ABBREVIATIONS

| | |
|---|---|
| **AES** | Advanced Encryption Standard |
| **DCT** | Discrete Cosine Transform |
| **DES** | Data Encryption Standard |
| **DWT** | Discrete Wavelet Transform |
| **GMSD** | Gradient Magnitude Similarity Deviation |
| **HH** | Horizontally and vertically high pass |
| **HL** | Horizontally high pass and vertically low pass |
| **HVS** | Human visual system |
| **IDWT** | Inverse Discrete Wavelet Transform |
| **IDCT** | Inverse Discrete Cosine Transform |
| **JPEG** | Joint Photographic Expert Group |
| **LH** | Horizontally low pass and vertically high pass |
| **LL** | Horizontally and vertically low pass |
| **LSB** | Least Significant Bit |
| **MPEG** | Moving Picture Expert group |
| **MSB** | Most Significant Bit |
| **MSE** | Mean square error |
| **Pixel** | Picture Element |
| **PSNR** | Peak Signal -to- Noise Ratio |
| **RGB** | Red, Green and Blue |
| **SSIM** | Structural Similarity Index |
| **YCbCr** | Luminance, Chroma: Blue, Chroma: Red |

# LIST OF FIGURES


| | | |
|---|---|---|
| **Figure 1.1** | Categorization of information hiding | 3 |
| **Figure 1.2** | Basic block diagram of steganography system | 8 |
| **Figure 1.3** | Basic reqiurement of steganography methods | 9 |
| **Figure 1.4** | Domains of steganography | 11 |
| **Figure 1.5** | Different techniques of steganalysis | 16 |
| **Figure 3.1** | Proposed data-hiding scheme for video steganography | 35 |
| **Figure 3.2** | Flowchart for embedding the secret image | 36 |
| **Figure 3.3** | Flowchart for data extraction | 39 |
| **Figure 4.1** | Secret image used in experiment | 43 |
| **Figure 4.2** | First frame of foreman video | 43 |
| **Figure 4.3** | First-level DWT application over first frame | 44 |
| **Figure 4.4** | Second-level DWT application over first frame | 44 |
| **Figure 4.5** | Third-level DWT application over first frame | 45 |
| **Figure 4.6** | Skin detection upon the first frame of test videos | 46 |
| **Figure 4.7** | Embedding capacity and bits per pixel (BPP) for foreman video | 46 |
| **Figure 4.8** | Embedding capacity and bits per pixel (BPP) for suzie video | 47 |
| **Figure 4.9** | Embedding capacity and bits per pixel (BPP) for car phone video | 47 |
| **Figure 4.10** | Embedding capacity and bits per pixel (BPP) for tennis video | 47 |
| **Figure 4.11** | Embedding capacity and bits per pixel (BPP) for akiyo video | 48 |
| **Figure 4.12** | Embedding capacity and bits per pixel (BPP) for trevor video | 48 |
| **Figure 4.13** | Embedding capacity and bits per pixel (BPP) for salesman video | 48 |
| **Figure 4.14** | PSNR comparison of test videos | 49 |
| **Figure 4.15** | MSE comparison of test videos | 50 |
| **Figure 4.16** | Skin-tone detection time for test videos | 50 |
| **Figure 4.17** | GMSD comparison of test videos | 51 |

# LIST OF TABLES


| | | |
|---|---|---|
| **Table 1.1** | A comparison of steganography techniques | 14 |
| **Table 2.1** | Number of bits to be used for hiding in HSFI image for given magnitude | 20 |
| **Table 2.2** | Comparative analysis of various approaches | 24 |
| **Table 4.1** | Result analysis for test videos | 52 |
| **Table 4.2** | Comparison of performance with other approaches | 53 |
| **Table 4.3** | Comparison of robustness with other approaches based on SSIM | 54 |

# Chapter-1
# Introduction

## 1.1 Preamble

In recent decades, the increase in usage of dominant internet has made the present society digitized and empowers us to communicate enormous multimedia information easily through global channels [1]. It enables us to download, upload, manipulate and exchange information. In our daily life large amount of data is frequently communicated over the internet [2, 3]. Nevertheless, it acknowledges a potential issue that may yield in disclosures of our privacy to other people, if the multimedia data is not protected securely. So, there is a critical necessity of safe communication manner to secure the confidential information transmitted through internet. Nowadays information hiding has a significant role. Due to its development in recent communication technologies it has caught much attention of researchers. In the today's modern world, everyone comes across the digital information. Internet is widely used and information/data is transferred through the network regularly. Security is the main issue of digital information since transmission of information over the internet is not secure and it goes through eavesdropping [3]. Encryption is also used to provide the security to the information and to encrypt the data in such a way so that intruder cannot decrypt the data on network.

Data hiding techniques are primarily divided into three types; cryptography, watermarking and steganography. Initially, cryptology was used for a reliable and safe transmission. However, the encrypted data which has meaningless message may actually evoke suspicion from illegal attackers. Watermarking is used to verify the integrity of digital contents such as images and videos. Steganography [4, 5] is invented to overcome the drawback of embedding confidential data within cover media without attracting any special attention from hackers. So, steganography is such technique which is used to provide more security to the confidential information. The existing steganography techniques suffer from the problems associated with lower similarity and PSNR value. Lower similarity and imperceptibility makes existing techniques vulnerable to the several steganalysis attacks. In this dissertation,

secure embedding stack selection method based on third level discrete wavelet transform (DWT) is used to provide better security and imperceptibility.

### 1.1.1 Overview of steganography

Steganography is a method to conceal the secret information within another information. It is executed on several types of data such as text, image, audio and video etc. In other version of data abstraction of data makes a covert channel that is utilized for different secure transmission channels for government, military and another type of information communication abilities [5]. The word steganography is originated from 2 Greek word stegano and graphy that means "covered writing". Steganography is the science of hiding the data in a manner so that not anyone apart from transmitter and receiver get to know about the hidden message [6]. Practically any text, image, audio/video can be hidden in the cover media by steganography. To accomplish it existence of data is concealed in apparently innocent cover or carriers. History shows that information hiding techniques were used by people since ancient times [4]. The most prominent example from ancient times is invisible ink and was lately used in World War II [5]. Greek prisoner Histiaeus utilized the technique of shaving one of slave's head for transmitting secret message to his son-in-law in $5^{th}$ century BC. [5].

During Mughal Emperor Akbar's rule, one of his slaves Benazir used text steganography for sending message to the rival party [5]. Images are made very small by microdot technology that they weren't distinguishable by human eye. In 1550 paper mask with holes method was proposed by the Italian mathematician to write the secret messages in it. The holes were utilized by arranging the mask on blank paper to hide the secret message [7]. China used a trick in which secret code ideogram was concealed in message carrier at a predefined position. In medieval Europe other similar idea was proposed. In this to conceal the message secret text data was covered with wooden template. In 1980's Margreth the prime minister of UK utilized a word processor that was programmed in a manner that identification of text document's author is encoded by itself and aided her in catching the miffed ministers and political parties involved [7].

## 1.2 Types of information hiding

Mainly information hiding techniques can be divided in three parts suchlike: Steganography, cryptography and watermarking. As there are no distinct bounds between watermarking and steganography. Therefore, these both come under same subclass [8]. Figure 1.1 represents the categorization of data hiding techniques.

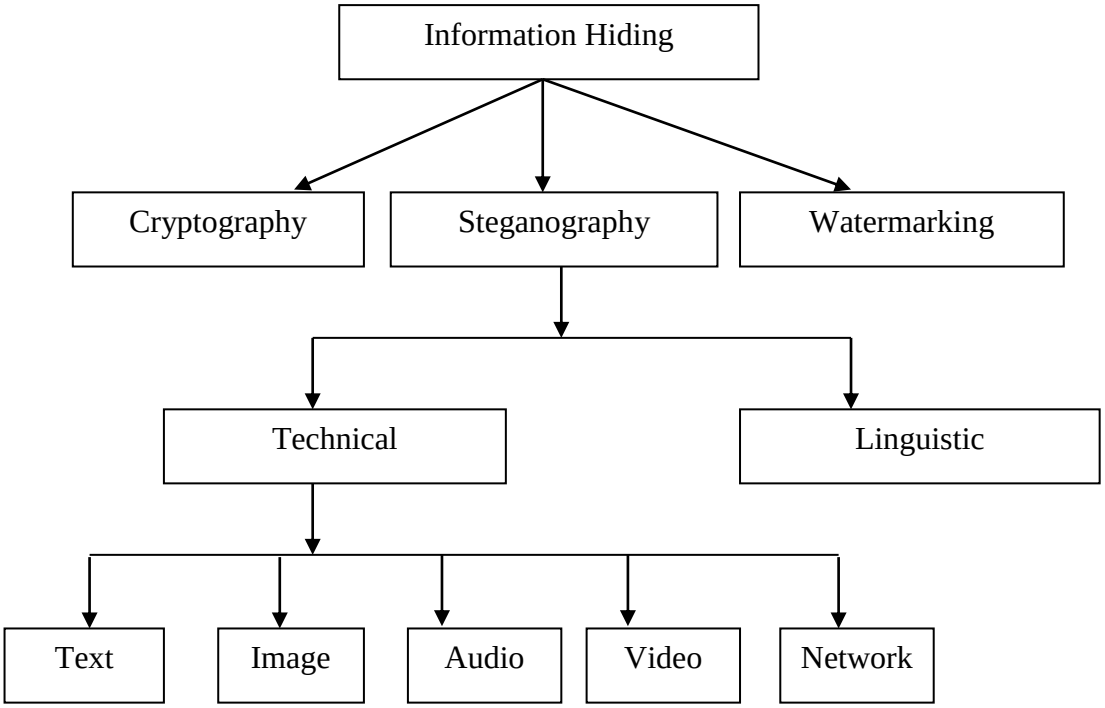



Figure 1.1: Categorization of information hiding [9]

### 1.2.1 Cryptography

Cryptography is used by sender to covert the plaintext into the cipher text using encryption key and identical key is applied at receiver end to decrypt the plaintext from the cipher text [10]. In cryptography encryption and decryption process is performed on secret message. Cryptography has grown a lot over the years and it comes under the highly developed technologies. The encryption algorithms work based on two primary principles such as substitution and transposition. In substitution each and every element in the plain text is modified to some another element which yields chiper text while elements of plain text are reordered to yield the cipher text in transposition [11].

### 1.2.2 Steganography

It is acquired from 2 Greek word stegano and graphy that means “covered writing”. It is the part of information security that is applied to conceal the information or another object from attacker [12]. Steganography is a science which hides the data in a manner so that not anyone other than transmitter and receiver notices the hidden secret message. Practically any form of data such that text, image and audio/video are concealed within the cover medium using steganography system.

### 1.2.3 Watermarking

Watermarking is the technique for embedding data within multimedia contents such as image, video etc. It is employed for verifying the integrity of digital contents or for identification of the multimedia content’s owner. Watermarking is used for various purposes [1].

Goals of watermarking are:

- Copyright protection
- Source tracking
- Broadcast tracking, such as watermarked videos from global news organizations
- Hidden communication

### 1.2.4 Comparison between steganography, cryptography and watermarking

Steganography is an obscure type of cryptography. Unlike Steganography, in cryptography secret message is scrambled by using encryption process in a manner so that no one other than transmitter and receiver notices it however if there is no compromise on the encryption key. Steganography and watermarking use same embedding process but they differ in their goals. All the methods have their own advantages and are very efficient [13].

Table1.2: Comparison of Steganography and cryptography, and watermarking [13]

| S. No. | Steganography | Cryptography | Watermarking |
|---|---|---|---|
| 1. | It is a type of secret or covered communication. | It is a type of protected data communication. | It is a type of one to many secret or covered communication. |
| 2. | It is an old technology except its modern digital form. | It is the technology of modern digital era. | It is the the technology to digital modern era. |
| 3. | Still being developed technology and advancing every day. | It is a developed technology comprising of a lot of strong algorithms for encryption. | Still being enhanced day by day. |
| 4. | The system is compromised once the secret message is detected | There is resistance of different algorithms against strong attacks such as Brute force. | System is compromised to some extent. |
| 5. | To crack embedding algorithm more time and computational power is needed. | To crack the system less computational power is needed. | Cracking the embedding algorithms needs more computational power. |

## 1.3 Types of steganography

It is divided into following categories on the basis of carrier media used.

### 1.3.1 Text Steganography

In this type of technique secret data is concealed in any text file. Text steganography is

divided into three categories explained below:

- **Line shift coding**

In line shift coding technique, to hide data text lines are shifted vertically to few extent. For the detection of marked line movement, it has 2 lines on both sides which are unmarked. A line is shifted up for hiding bit 0 while the line is shifted down for hiding bit 1. The marked lines centroid distance measurement is done to determine even if the line is shifted up or down. Hidden data can be destroyed if encryption of data is performed or whether OCR is utilized. Moreover, by applying specific instruments for distance estimation, distances are determined.

- **Word shift coding**

In word shift coding technique, to hide data words are shifted horizontally, that means data is shifted to left or right positions to depict bit 0 or 1 correspondingly. Detection of shifting of words is done by applying correlation technique in which a profile is treated as a waveform. The middle block of this waveform is shifted to left or right positions. This method may be recognized less, but if anyone gets to know about the distance algorithms, comparison of stego text and obtained concealed data can be done by the usage of difference. Moreover, hidden information get destroyed by applying encryption or OCR programs.

- **Feature coding**

In this technique, one or more features of text are altered to hide the secret data. Information is hidden by investigating the document and picking out all features which can be used to conceal the data. For instance, strike's dimension can be altered in the letters f and t, in letters i and j point can be changed or height of letters b, d, h etc. can be shortened or extended. If the OCR technique is applied or if data is retyped, hidden message will be lost. This is the major drawback of this technique.

### 1.3.2 Audio steganography

In audio steganography, secret data is concealed within audio files. Audio steganography is divided into three categories explained below:

- **Parity encoding**

In this technique, a signal is split into individual areas of samples rather than splitting the signal into separate samples and each secret data bit is encoded in the sample area's parity bit. The least significant bit of the samples in the area is flipped if the selected

area's parity bit is not matched to the secret bit that has to be encoded. Therefore, signal may be altered in more unobtrusive manner and for encoding secret bits there are many choices.

- **Phase encoding**

Phase encoding technique substitute the segment of initial audio with a reference phase which serve as the data. The relation between segments is preserved by adjusting subsequent segments. Observable phase dispersion occurs, when the phase relationship between every frequency component is drastically altered. Although, as long as alteration in the phase is adequately small experts in broadcast radio may discover alteration which is invisible to the fact that the phase component of sound isn't observable to the human ear as noise is. Instead of introducing disturbances, this method encodes the message bits as phase shift in phase spectrum of digital signal, achieves an imperceptible encoding in terms of perceived signal to noise ratio.

- **Echo hiding**

In echo hiding, An echo is introduced into discrete signal to embed the information in a sound file. Like the spread spectrum technique, it too offers advantages that is high data transmission rate and offers better robustness as compare to the noise inducing techniques. If only one echo was produced from the original signal, only a bit of information could be encoded. Therefore, the original signal is broken down into blocks the encoding process begins. Once the encoding process is completed, the blocks are concatenated back together to create the final signal.

### 1.3.3 Video steganography

Generally, video files are considered to be the collection of image and audio files. Video steganography is a combination of image and audio steganography. Using video steganography a large amount of data can be hidden due to the moving stream of image and audio files. Because of this any noticeable can remain unnoticed by the human eye.

### 1.3.4 Network steganography

In network steganography, communication protocols are used for embedding purpose open system interconnection (OSI) network model have different layers which contain covert channels and those channels are used for steganography. Basically, it includes modifications to the network protocol at any layer of OSI model e.g. data can be hidden

in the header of TCP/IP packets.

### 1.3.5 Image seganography

Images are the most accepted objects for the steganography. It overcomes the limitation of text steganography where in it boosts the volume of the data to a large extent. It is the most widely used technique for secret communication. The values provided in the image matrices are known as the pixels, and the representation of the pixel in the matrix form is called the pixel grid. The images consist of the square or rectangular shape in every case and every pixel value represents some of the color. An image may be 2-D, 3-D or hyper spectral (N-D) images, which depends upon the depth of the image. The image depth is measured in the planes in the images, for example, in the RGB image there are three primary planes, red, green and blue. Each one of the planes in the RGB images is the 2-D image and shows the gray scale pattern. The 2-D images are usually known as 8-bit pixel based images and 3-D images are known as the 24-bit pixel based images. The bit-map image (BMP) saves the file in the full size matrix, whereas the other formats are utilized to reduce the size on disk such as JPEG, PNG, etc. [14].

Images are used to hide the important information as the cover media in image steganography. As a lot of redundant information is contained into images so images are taken to be cover media. Bits in any image which are not detectable even when they are modified are called as redundant bits. For steganography image files are used as cover medium since they have large amounts of redundant bits. The main idea of image steganography is to secure the secret information from hackers. The basic image steganography model is shown below in Figure1.2.

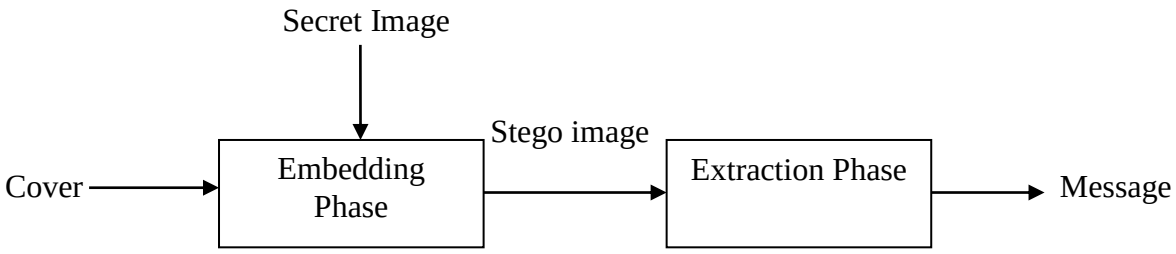



Figure 1.2: Basic block diagram of steganography system [14]

In Figure 1.2, secret image is concealed within cover medium to create a stego-medium

and this is transmitted to receiver and secret information is extracted from the stego-medium [14].

Following key terms are used in steganography:

- **Cover image:** Cover image is used as a carrier for embedding secret information or message to be sent to the receiving party.
- **Message:** Message is Secret data that the sender wishes to remain confidential. It can be plain text, cipher text, audio file or video file.
- **Stego key:** It is a key to integrate the information inside cover medium and extract same information from the stego medium.
- **Stego image:** It is the cover image with a hidden secret data inside it called the Stego image. It is employed at the receiver end to pull out the message hidden in it.

The general specifications that must be kept in mind, when implementing steganography, are described below:

- The embedded data must not downgrade the quality of cover media. Quality of cover media should be such that it must look like original media. The media size should not increase tremendously as it can look suspicious to the casual viewer. It must have good Peak Signal to Noise Ratio.
- The data that is to be hidden should be embedded in the information part of cover media, not in the header. The data must be temper resistance to the attacks of the third party.
- The integrity of data should be maintained, it must be robust enough so that it must not be modified in between the way.
- A cover file must be of enough size so that it can hide a large amount of message.
- The message hidden must be invisible to the viewer. The hidden message must be undetectable during steganalysis process.

### 1.3.6 Basic parameter of steganography methods

There are three basic measures to access the performance of the steganography:

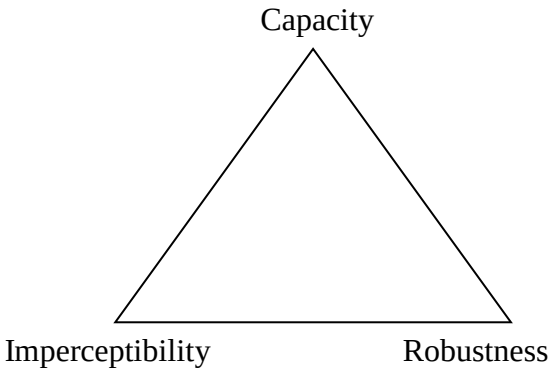



Figure 1.3: Basic requirement of steganography methods [14]

- **Payload capacity**

It can be determined as the maximal data that can be embedded in the cover medium. In other words it is defined as embedding the maximum amount of information into the carrier being used like image file or audio file without causing distortion and without any loss to the original information. Capacity can be measured in terms of bits per pixels which means what number of bits of a pixel of cover image has been utilized by the secret information.

- **Robustness**

Robustness is the ability of secret message to remain intact after the application of operations such cropping, filtering compression and rotation etc.

- **Imperceptibility**

It is defined as the quality of the stego-image. Imperceptibility is also known as invisibility. It means there is no decay in the quality of image before and after embedding the secret information. It makes hard for attackers to locate the secret message in cover medium. This factor depicts the stego-image quality and also checks that the number of distortions and irregularities in it are minimum.

## 1.4 Domains of steganography

Today image processing can be applied successfully to all possible types of imagery in any domain and many aspects are responsible for its success. There are two methods for the image steganography. First is Spatial Domain based techniques and second is

Transform Domain based techniques [15]. Techniques based on the Spatial Domain are also recognized as Least Significant Bit methods, cover image LSB bits are changed to conceal the secret information within it. In transform domain based methods, the cover image and secret image are transformed from spatial to transform domain first. Afterward the secret image is concealed within transformed coefficient. Wavelets are being utilized in mostly all steganography approaches. It has been noticed that discreet wavelet based approaches are better in robustness than spatial domain based approaches. Moreover, stego-image obtained by utilizing wavelet based approaches is good in quality. In image processing image enhancement is the first step and this means that any additional information is not added to the image but just subjective quality is enhanced by working on the existing data of image. So primarily in image steganography there are two domains such as Spatial and Transform Domains.

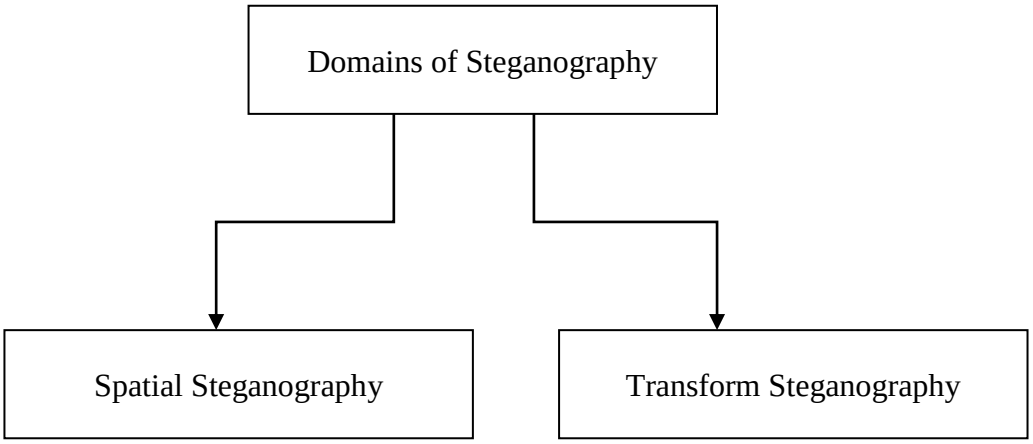



Figure1.4: Domains of steganography [15]

In spatial domain work is done on the pixel values of images. So it deals with the pixel values to get the new stego-image. While in transform domain work is done on the components of frequency in image.

### 1.4.1 Spatial domain image steganography methods

- **LSB technique:** It is an insertion method in which least significant bits of the pixels are utilized for embedding the secret information in noisy areas [16].

  Ex. Let us consider a set of three pixels for a 24-bit image.

  (00101101 00011100 11011100)

(10100110 11000100 00001100)

(11010010 10101101 01100011)

Now, assume a number '200' needs to embed in the least significant bits of pixels set mentioned above. Number 200 is represented as 11001000 in binary form. Resulting set of pixels after embedding process are:

(00101101 00011101 11011100)

(10100110 11000101 00001100)

(11010010 10101100 01100011)

In the technique mentioned above, just half of the entire bits of the color image are altered. Due to modification in LSB bits, intensity of colors changes slightly that is invisible to human visual system. So, in general it doesn't disturb the quality of the image.

- **Masking and filtering:** In this technique, a mask is applied on an image and consequently luminance of the masked region is changed [17]. This technique is more robust as compare to LSB insertion as this technique is more persistent to modification s like cropping, compression and some another image processing functions. Secret information is embedded in significant regions of the image than hiding information in noisy regions
- **MBPIS steganography:** In this technique, insertion is done in multiple bit planes of the image and it works as an extension of LSB insertion method [18].
- **MBNS steganography:** In this method, secret information is transformed into symbols which in notational system are depicted by variable bases. It is based on HVS and results in poor stego-image quality which is the prime loophole of this technique i.e. the modification done in the image are visible to human visual system. [19].
- **QIM:** It is the commonly used steganography technique based on quantized image modulation for embedding information. A set of quantizer is utilized for quantization of the input signal I to the output signal O. Quantizer is determined by the message bit m for quantization. The values of output are produced at the points of reconstruction in quantizer [20]. So, these are several steganography techniques based on the special domain.

  So these are various spatial domain image watermarking techniques. every technique have their own disadvantages and advantages. Some yields in higher payload capacity and whereas some are better in robustness.

### 1.4.2 Transform domain image steganography methods

The transform domain methods embed information in the frequency domain of an image. Numerous strong steganography systems these days operate in transform domain. The prime advantage of these methods over the spatial domain bases methods is that image is concealed in the region which is not exposed much to the image processing, compression and cropping. These methods run on lossy and lossless both image formats. Primary transform functions under this technique are; Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) and Discrete Wavelet Transform (DWT) [21]. Several methods under the transform domain are discussed below:

- **Jsteg:** It is Discrete Cosine Transform (DCT) based technique and makes usage of steganography which uses the simple LSB technique for embedding the data [22]. In this technique LSBs of non zero quantized coefficients of DCT are replaced successively with the bits of secret information. JPHide is another feasible form of Jsteg. It is other steganography tool which works in a similar way as Jsteg but performs so in a random manner.
- **F5 algorithm:** F5 algorithm is introduced by Westfield. In this technique the absolute value of coefficients of quantized DCT are modified after that it is decreased by 1 rather than replacing the LSBs of quantized DCT coefficient with the bits of secret message. The prime advantage of this technique is that the entire modifications that are needed to conceal a secret message of certain length is minimized [23].
- **Model based steganography:** It is the general method in which steganography and steganalysis both techniques are performed by utilizing statistical model of cover medium. This technique provides higher payload capacity and security to $1^{st}$ order statistical attacks.
- **YASS:** YASS stands for yet another steganography scheme [24]. It is another version of Jsteg technique. Unlike Jsteg technique, it splits input image of spatial domain into fixed sized blocks of image known as B-blocks instead of embedding information in DCT coefficients of JPEG. An 8×8 block is chosen randomly from this block that is known as H-block. Secret data is concealed in H-block by utilizing error correction codes. Image is compressed in the end and is sent to receiver party.

## 1.5 Comparison of steganography techniques in different Domains

In steganography one deal with two domains particularly spatial domain and the transform domain and the main requirements of any steganography system are robustness, payload capacity and imperceptibility [25]. These factors are according to the domain. There is a trade-off between robustness and the payload capacity. So for achieving one factor one has to compromise on other factor in any of the both spatial and transform domain. In author has given a survey on all the domains present for the basic requirements of any watermarking system that has been shown below in Table 1.1

Table 1.1: A comparison of steganography techniques [25]

| Parameters | Spatial Domain | Transform Domain | Spread Spectrum | Statistical techniques | Distortion technique |
|---|---|---|---|---|---|
| Imperceptibility | High | High | High | Medium | Low |
| Robustness | Low | High | Medium | Low | Low |
| Payload capacity | High | Low | High | Low | Low |

## 1.6 Steganalysis

It is the science which deals with the detection of hidden secret message which is concealed within image by using steganography techniques [35]. The goal of the steganalysis is to discover whether the innocent image has any secret message hidden within it or not. It aims to determine those statistical properties of the stego-image which are modified leading to failure in maintenance of steganography statistical properties. Hence, steganalysis succeeds if it distinguishes very easily that an image has secret message concealed within it. Steganalysis also tends to discover more information of image and hidden secret message which can be revealed and known such as length of secret message, content of secret message, method utilized for concealing, secret key and its length. Practically, any steganalyst always strives to verify whether any secret message is concealed within a image or not in such a way he can finally reach to his goal that is extraction and decryption of the secret message.

### 1.6.1 Steganalysis attacks

There are several types of steganalysis attacks. These attacks are classified in four types

and one assumption is made that steganalyst always has atleast the stego medium. steganalysis attacks are of following types:

- **Chosen stego attack:** Steganalyst is aware of the algorithm used for embedding the text into the image and put efforts to make stego image from the cover-image to match the intercepted stego-image. Therefore the steganalyst attempts to form the similar stego system by usage of this algorithm and it is matched with the existing stego-medium.
- **Stego only attack**: Steganalyst is aware about the stego medium intercepted only. He does not have any other information available apart from this. Practically, steganalyst tries to detect every possible attacks on current watermarking algorithms.
- **Known cover attack**: In this attack the stego medium, the original cover medium is available to the steganalyst. Steganalyst attempts to find the differences that are present between cover medium and the stego-medium. Known cover attack seems to be same as known plain text attack.
- **Known message attack**: In this attack the hidden message is known, now steganalyst can try to analyze the stego image for attacks in future. But, it is still quite hard to get steganography system, therefore this attack is considered as stego only attack.

### 1.6.2 Steganalysis techniques

Undoubtedly the several steganography methods such as spatial domain, transform domain functions like DCT, DWT and adaptive steganography techniques have developed practically for embedding secret data but at the same time these are yet vulnerable to attacks. Plenty of work is performed to analyze several steganography methods and from this it is concluded that these methods in some cases compromise the statistical properties of image and therefore returns the failure of steganography systems. In the specific detection considerable amount of work is done. Detection of LSB concealing methods is the priority here. Least significant bit technique conceals the bits of secret message by replacing the LSB of either value of pixels, or palette color indices, or coefficients of quantized DCT. Several techniques for steganalysis are classified in subjective techniques and statistical technique comprises of chi-square, histogram and RS analysis.

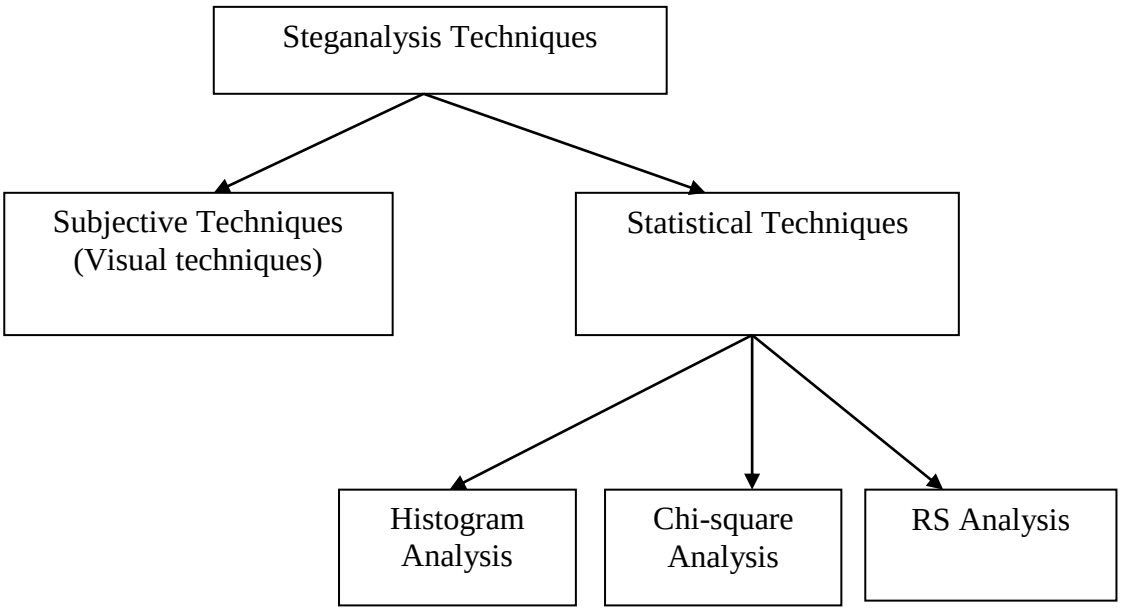



Figure1.5: Different techniques of steganalysis [27]

## 1.7 Applications of steganography

Steganography is being utilized nowadays in numerous applications. Most importantly it is used in the digital communication domain where transmission and reception of digital files are performed at every moment of the day. The major issue in digital communication is the data security. Therefore to accomplish this requirement steganography plays a vital role. Steganography techniques are utilized to put an additional security layer to the information transmission beside the cryptographic techniques that are used for the data scrambling. The significant applications of steganography are listed below:

- **Hidden communication**

In general, while information is communicated through cryptography attackers can attack because the message is visible. On the other hand in steganography information is communicated in a hidden manner and it makes steganography an adaptable and more secure method in the cases of very confidential data that is utilized for military purposes.

- **Copyright protection**

Copyright protection is other very major application of steganography. It is used for

eluding the misusage of owner legality.

- **Feature Tagging**

Feature tagging application is used for hiding different image features such as name of person in an image, content and location of the image.

- **Advanced data structures**

The secret or useful information can be embedded within the media, and this ends the need to extra data such as readme or information files with the distribution of the data. For example, the informative content about an image can be embedded within the image.

- **Medical Imagery**

The information about the patients can be embedded within the medical imagery such as MRI, CT scan, etc. in order to minimize the frauds related to the fake medical imagery and to prevent the chance of misguidance or wrong treatment, which could be otherwise caused by the medical imagery forgery.

- **Watermarks**

The visible or invisible watermarks can be embedded within the digital media, which can protect the originality of the content and can provide the information about the owner of the information.

Other applications of steganography are:

i. Enhancement of search engine's robustness based on image.
ii. Smart identity cards to embed individual person's identity details within it.
iii. Circulate the information securely in any environment or an organization.
iv. Audio and Video synchronization.
v. Checksum Embedding.
vi. TV broadcasting.

So, all this discussed above is the primary introduction to the steganography system including basic model of bits, definition, domains for steganography and various applications.

## 1.8 Motivation of the dissertation

The main motivation behind this dissertation and studying video steganography methods is to evade drawing attention to the secret information transmission. Some common reasons that infiltrators can be able to get unauthorized access of secret information and they can use it for other purpose, to modify and attack the secret information. As the

technologies are continuously developing due to possibilities of getting information hacked in modern era communication need certain protection from intruders. Providing additional security to computer network is important since most of the information is communicated over the internet.

## 1.9 Organization of the dissertation

This dissertation is ordered in the form of chapters as listed below:

Chapter 2: Literature Review, A study is done about numerous existing video steganography techniques. Existing steganography techniques are analyzed in the tabular form based on pros and cons of methods used. Work done in skin-tone detection based video steganography is also discussed.

**Chapter 3: Data-hiding Approach using Skin-tone Detection,** Steps related to work done in video steganography are discussed. Skin-tone detection, data embedding process and data extraction process are explained separately with flowcharts and algorithms. The detail of the method applied in each step is also provided.

**Chapter 4: Results and Discussions**, Results of skin-tone detection based video steganography are discussed in this chapter. Skin-tone detection results of video frames and collaborative graphs for evaluation measures are provided. Comparison with other approaches is discussed separately.

**Chapter 5: Conclusion and Future scope**, The work done is concluded in this chapter and based upon the observations future scope is given.

# Chapter-2

# Literature Review

## 2.1 Introduction

In last decades a lot of research has been done to develop various steganography models for transform domain and spatial domain as well. The field of steganography is evolving day by day and a lot of researches are being conducted on it. Several modified techniques have been proposed for embedding information. Although researches on other techniques are also being carried in spatial and transform domain such as multiple bit planes, masking and filtering. Different work conducted in these domains is discussed in this chapter.

## 2.2 Literature survey

Chen *et al*. [28], presented a data hiding technique in frequency domain. Secret messages were embedded within high frequency coefficients ensued from DWT, In the low frequency sub-bands coefficients were kept unchanged to improve quality. Before embedding the secret messages some basic mathematical operations were performed to keep the secret messages away from stealing and to provide better security [28]. In digital-media processing significant localization property is the important advantage of using wavelet transform, which is adequate for several image processing applications [29].

Bhattacharya *et al*. [30], presented a steganographic technique based on DWT and DCT which hides multiple secret images in a color cover image. Secret data of considerable amount were concealed within cover images by utilizing an entropy function. Embedding process was restrained by what amount of bit error rate is minimized.

Bhattacharyya *et al.* [31], presented a stegnographic technique where secret data are embedded in frequency domain without negotiating image quality; secret data are effectively extracted with least distortion. Although, the quality and capacity of cover-medium in this approach needs to be enhanced.

Sheikhan *et al.* [32], presented a stegnographic approach which uses the LSB of DWT. Although, utilization of a lower sub-band increases the computational burden and moreover decayed the quality of secret data. Another steganographic approach based on DWT was also presented in [33]; in this approach secret data are embedded in images utilizing a biometric feature, i.e, the skin tone region to which human visual system (HVS) is not sensitive. But this approach cannot keep images safe from distortions.

Jalab *et al.* [34], presented a steganographic method in which data are embedded within the noise region of MPEG videos by utilizing the bit-plane complexity segmentation method. This method works better for images having more complex textures than for images which are computer generated generally have uniform textures.

Table 2.1: Number of bits to be used for hidding in HSFI image for given magnitude [34]

| Magnitude of Pixel in HFSI image(M) | Kth MSB bit which is one | Number of bits that can be used for hiding information(k-2) bits |
|---|---|---|
| $0 \leq M < 2$ | 0 or 1 | 0 |
| $2 \leq M < 4$ | 2 | 1 |
| $4 \leq M < 8$ | 3 | 1 |
| $8 \leq M < 16$ | 4 | 2 |
| $16 \leq M < 32$ | 5 | 3 |
| $32 \leq M < 64$ | 6 | 4 |
| $64 \leq M < 128$ | 7 | 5 |
| $128 \leq M$ | 8 | 6 |

Wu *et al.* [35], presented a method to embed secret data within grayscale cover image. The grayscale image (cover) was divided into non overlapping blocks. Then 2 successive pixels in each block were selected to compute the difference in their values so as to embed data in the block when gray value falls off of the range of 0 through 255.In this, if value comes out to zero then it is marked as smooth block and

if it is 255 then it would be shapely edge block. The range intervals of the selection were based on the behavior of human visual system (HVS) for grayscale value variations from smoothness to contrast. It provides good quality of stego image, but does not provide any security against various types of attacks [35].

Ali *et al.* [36], improved the embedding capacity of steganographic scheme and acquired acceptable levels of image distortion and imperceptibility; nevertheless, the approach evokes high computational overhead.

Eltahir *et al.* [37], presented an adapted variant of the famous LSB scheme. They exploited the fact that the human visual system is more sensitive to the alteration in blue level color than to the green and red level colors. Their adaptation was to utilize 3-3-2 scheme which means, utilizing 3 least significant bits from green and 3 from red color however only 2 from blue color. This scheme is easy to implement, and exploits up to 33.3% of every frame for data embedding. However, this approach is not robust against compression.

Kapotas *et al.* [38], presented a steganographic method for H.264 video streams using scene-change detection. To conceal the scene change information within the encoded sequence H.264 encoder utilizes differently sized blocks during the inter prediction stage. An algorithm for MPEG videos to scene-change detection was developed in [39].

Wu *et al.* [40], presented a technique to utilize the amalgamation of two techniques PVD and LSB to enhance the PSNR and capacity for hiding the data. This method used difference between two consecutive pixel values to hide data. It utilizes an LSB substitution technique for hiding data at the smooth area and PVD to hide data at edges of image. The splitting between smooth area and edge areas of range width table used at sender and receiver end to increase security level, which made it difficult to guess the area at which the data hiding was done. In this, two pixels were embedded using LSB if difference falls into smooth area of range width table whereas few pixels were embedded by PVD if difference fall into higher level. This method has shown increase in imperceptibility and embedding capacity at image edge pixels as compared to the smooth area of image [40].

Singh *et al.* [41], in 2007 proposed a method for concealing encrypted data within the

image features instead of hiding the data in smooth region of cover medium. In this approach, message encryption was performed followed by edge detection and LSB embedding algorithm for hiding the encrypted message in non-adjacent and random pixel locations on edges of the image. The intruder did not have any suspicion that secret message bits were concealed in the cover image. This approach ensures the security. Blind LSB detection technique was not able to estimate the length of the secure message bits accurately [41].

Yang *et al.* [42], in 2008 proposed a steganographic technique based on the adaptive LSB embedding algorithm. Data was concealed within non continuous regions of the cover image in spatial domain. Secret data was embedded within gray scale image with minimal distortion and PVD technique was utilized to differentiate between non continuous and continuous regions in the cover image. Embedding at edge pixels of the image used k bit LSB substitution by greater value of the k than continuous area of the image. In this the range width table includes difference value which was divided into lower, middle and high level. This approach achieved highs imperceptibility, high capacity and PSNR. To find the embedding information relative attacks were executed on stego-image, but this doesn't afford resistance toward attacks [42].

Yang *et al.* [43], in 2009 presented a method for improving data hiding based on histogram by utilizing intercalating prediction for gray scale cover images. In this technique the values of error predicted similar to the pixels number in cover medium and thereafter entire values of prediction were transformed to histogram for enhancing PSNR and capacity for embedding the message. The pixel difference between cover image and stego image was always fall within the ±1 [43].

Luo *et al.* [44], in 2010 proposed an edge adaptive method for image steganography based upon least significant bit matched revisited. This method chooses the region for embedding secret message in accordance with the message size that was concealed within cover medium in 2 consecutive pixels by PVD in original image. It also preserves the statistical and visual attack feature. It provides resistance towards attacks. Visual quality and security of stego image was also high using this LSB revisited approach as compared to using the typical LSB substitution [44].

Chen *et al.* [45], in 2010 presented a high payload steganography technique by

utilizing detection of hybrid edge. LSB method, fuzzy logic and canny edge detection were paired in this technique. It has not only achieved higher payload capacity, but also improves quality of stego image. Any image or object edge boundary achieved by this hybrid edge detector was more precise than using a single edge detector either fuzzy logic edge detector or canny edge detector. It was implemented for grayscale images, not tested for color images. It has achieved higher payload capacity of 2.66bpp. It was also resistant to the steganalysis system that was based on the statistical attack analysis [45].

To further improve PSNR, Hussain *et al.* [46], proposed an approach to embed data within the cover image at edge boundaries. This paper was targeted on low capacity of data embedded with high PSNR and high level of imperceptibility. More data were embedded at edges of image instead of embedding it within smooth image regions. This method has low computational complexity and gives higher PSNR. For extracting feature and object segmentation it utilized the stego medium as native image. Canny edge detection with their default threshold parameter was used to detect the edge boundaries. In this horizontal edge pixel was used for data embedding and difference of horizontal edge pixel with the upper boundary pixel should be larger than the edge difference threshold. It was used for high PSNR but having the disadvantage of low embedding capacity and also used only for horizontal edge detection pixel boundaries [46].

Juneja *et al.* [47], in 2013 presented an approach based on adaptive LSB method to enhance the embedding capacity and PSNR for data hiding. To provide more security, AES was utilized for encryption of message that was embedded within cover medium. Instead of using the feature of smooth area, feature of edge areas like density, frequency, color and contrast was also used because of edge pixel changes were more tolerated than any changes in smooth areas of the image. In this fusion of canny edge detection and advanced Hough transforms used for edge pixel detection. The approach has provided more imperceptibility, high payload capacity, PSNR and high robustness. It was more resistance to steganalysis attack like chi-square, histogram and RS attacks [47].

Tseng *et al.* [48], in 2014 proposed a steganographic technique based on high embedding capacity block data hiding with minimal distortion by detecting hybrid

edge. To embed the more secret data within edge regions instead of concealing data in image at smooth regions algorithms based on canny and fuzzy block were used. It has achieved high embedding capacity by using fuzzy block based algorithm and achieved minimum distortion by using edge pixel of each 4×4 block with minimum MSR. By selecting the proper edge and non-edges, it also increases the imperceptibility [48].

Singla *et al.* [49], Presented an image steganography technique in 2015 for color images by detecting hybrid edge. In this approach, more data was embedded in contrast areas rather than doing embedding at brighter areas of the image. In this hybrid edge detection was a fusion of canny and fuzzy edge detection to discover the edges. 1-4-8 LSB method was utilized to perform the adaptive LSB substitution. AES was utilized for encoding the secret message to provide higher security [49].

Table 2.2: Comparative analysis of various approaches

| **Authors** | **Approach used** | **Pros** | **Cons** |
|---|---|---|---|
| Wu *et al.* [35] | • PVD (pixel value differencing) | • Embedding capacity: 50960 dB<br>• PSNR: 41.79<br>• Good quality of stego image | • It is not resistant towards the different attacks such as: analysis of statistical attack, chi-square test and RS attack analysis |
| Wu *et al.* [40] | • Fusion of LSB and PVD.<br>• LSB substitution | • Embedding capacity: 95755 dB<br>• PSNR:36.16 | • It is more susceptible towards stego attacks since |

| | | | |
|---|---|---|---|
| | method of concealing data within smooth regions.<br>• PVD to hide the data at the edges of image. | • Increase imperceptibility<br>• Embedding capacity at edge pixel was more as compared to the smooth area of image | range width table is sent to the receiver to extract the original image. |
| Singh *et al.* [41] | • Blind LSB detection technique<br>• Simplified data encryption standard (S-DES)<br>• Pseudo random number generator (PRNG) | • Ensures the security of data embedding in the feature of the image | • Low payload capacity<br>• Stego image quality degrades |
| Yang *et al.* [42] | • K bit LSB and PVD technique for embedding | • If 4-5 bits used for embedding then payload capacity:1,076,109<br>• PSNR: 32.42<br>• MSE:7.86 | • It provides no resistance toward the attacks |
| Yang *et al.* [43] | • Interleaving prediction for grey scale image | • Payload capacity : 99947<br>• PSNR : 48.82 dB<br>• Enhance reversible data hiding based on | • Sometimes problem occur in not obtaining correct prediction |

| | | | |
|---|---|---|---|
| | | histogram. | |
| Luo *et al.* [44] | • LSB matched revisited PVD and PRNG | • High PSNR<br>• Resistance towards the attacks<br>• Embedding rate was 50% with accuracy 83% | • Lower embedding rate<br>• Poor visual quality |
| Chen *et al.* [45] | • LSB substitution technique<br>• Fusion of canny and fuzzy logic edge detection. | • Payload capacity: 0.65 bpp<br>• PSNR: 47.1<br>• High quality of stego image<br>• Offers resistance toward statistical attack analysis | • Applied only at gray scale images |
| Hussain *et al.* [46] | • Canny edge detection with their default threshold parameter | • If threshold value: 16 then PSNR value was 88.23<br>• Low computational complexity<br>• MSE: 9.76 | • Low embedding capacity and used only for horizontal edge detection pixel boundaries |
| Juneja *et al.* [47] | • Adaptive based LSB technique for embedding at non edge pixel<br>• Advanced encryption standard (AES) | • More resistance to steganalysis attacks like chi-square, histogram and RS attacks<br>• Embedding capacity was 60 % for edge area and | |

| | | | |
|---|---|---|---|
| | • Fusion of canny edge detection and advanced Hough transforms used for edge pixel detection | 50% for smooth areas<br>• Utilized 12 bits of RGB color image for embedding | |
| Tseng *et al.* [48] | • Canny and fuzzy block based algorithm<br>• Non-edge pixels based on the least-significant-bit | • PSNR: 38.18 dB<br>• Payload capacity: 2.41(bpp)<br>• Enhancement in imperceptibility | • Some distortion at receiver end when extract cover image form stego image<br>• Grey scale images only used |
| Singla *et al.* [49] | • Fusion of canny edge detection and fuzzy edge detection<br>• 1-4-8 LSB embedding<br>• Advanced encryption standard (AES) | • PSNR: 46.68dB<br>• MSE: 12.45<br>• Payload capacity: 10.26 bits per pixel | • More data was embedded in contrast areas rather than at brighter areas of the image |

## 2.3 Performance parameters

To evaluate the performance of the steganography following parameters are considered:

- **Payload Capacity:** It is defined as the maximum amount of data that is embedded into the image. It is defined as the maximum amount of data that is embedded into the image. It is embedding maximum amount of information into the carrier being used like image file or audio file without causing distortion and without any loss of the original information. Capacity can be measured in terms of bpp which means

what number of bits of a pixel of the cover image has been utilized by the secret information.

$$\text{Capacity} = \frac{\text{Maximum number of embedded bits}}{\text{Cover size}} \quad (1)$$

- **Robustness:** It is the message's ability to persist even after performing the operation like compression, rotation, cropping and filtering etc.
- **Imperceptibility:** It is defined as the quality of the stego-image and which is measured using PSNR and MSE. It is defined as the quality of the stego-image. Imperceptibility is also known as invisibility. It means there is no decay in the quality of image before and after embedding the secret information. It makes difficult for attackers to find the location of secret message. This factor depicts the stego-image's quality and also checks that the number of distortions and irregularities in it are minimum.
- **Peak Signal to Noise Ratio:** It is used to define the quality of image and is measured in decibels (dB). It measures the distortion that occurs during embedding the data in the image. It is mathematically defined as:

$$\text{PSNR} = 10\log\left(\frac{C_{max^2}}{\text{MSE}}\right) \quad (2)$$

where, $C_{max}$ represents the maximum pixel value in the image and its value can either be 1or 255.

- **Mean Square Error:** MSE is defined by comparing the error in data at receiver end with data at sender end before and after processing. It is a mean squared error that represents the mean error occurred in the cover medium and stego medium. Mathematically it is defined as:

$$\text{MSE} = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}(S_{xy} - C_{xy})^2 \quad (3)$$

where, M and N denotes the image dimensions that are the length and breadth and $S_{xy}$ and $C_{xy}$ are the stego image and cover image respectively

- **Bpp:** It depicts the total number of the bits of a single pixel used on an average for embedding the secret file. Bpp is calculated by divided the number of bits used for embedding to total number of pixels in cover image
- **SSIM:** The structural similarity (SSIM) is the parameter to describe the variation in the matrices by analyzing their structural details.

$$\text{SSIM}(x, y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \quad (4)$$

- **Correlation Coefficient:** The correlation coefficient parameter analyzes the overall difference between the two matrices measured by the means of squared distance. The correlation coefficient measures the differences in the non-negative decimal as the final output.

$$r_1 = \frac{\sum_i (x_i - x_m)(y_i - y_m)}{\sqrt{\sum_i (x_i - x_m)^2} - \sqrt{\sum_i (y_i - y_m)^2}} \quad (5)$$

where, $x_i$ is the intensity of the $i^{th}$ pixel of first image, $y_i$ is the intensity of the $i^{th}$ pixel of second image, $x_m$ is the mean intensity of first image, and $y_m$ is the mean intensity of second image.

**GMSD:** The gradient magnitude similarity deviation (GMSD) computes the standard deviation oriented variations between the original and processed image in order to study the distortion in the processed image in comparison with the original image.

$$GMSD = \frac{1}{N}\sum_{i=1}^{N}(GMS(i) - GMSM)^2 \quad (6)$$

where, GMS and GMSM represent the gradient magnitude similarity and Gradient Magnitude Similarity Mean respectively.

## 2.4 Research gaps

- The similarity percentage in the existing model is significantly lower and makes the data embedding easily detectable. The similarity percentage must be increased up to the maximum level in order to realize the robust steganography with minimal chances of detection by improving the overall design for embedding.
- The existing techniques are less imperceptible. The quality of the image after embedding and extraction process is degraded. PSNR must be improved in order to create the highly secure and robust steganographic model.
- The content in the medium is protected but the medium is not protected, this makes it easy to intrude into and makes the content to be exploited easily.

## 2.5 Problem formulation

The existing model is based on the skin-map based pixel selection method combined with the DWT-based embedding mechanism to reduce the embedding evidence. Only blue and red channels have been used for the embedding purposes in the DWT component (3-Level), which has been created with the capability of hiding the secret data more securely than the earlier steganographic models. The skin-map based existing model suffers from the problems associated with lower similarity percentage and PSNR value, which makes it prone to the several steganalysis attacks, which can be overcome by using the highly secure embedding stack selection method in the RGB components according to our study. The further improvement in the existing model will be based upon the embedding in the RGB channel, with pixel selection based upon the improved skin-map model and 3-level DWT for robust steganography, which can be further improved by combining the dynamic 8-pixel floating stack selection for embedding of one secret pixel by using the 1-bit embedding method.

## 2.6 Objectives of the Dissertation

- To study and analyze the existing state of the art steganography techniques.
- To develop a video steganography technique based on 3-Level DWT by employing skin-map selection method on the video frames and 8-pixel float stack selection model with 1-bit embedding mechanism.
- To analyze and compare the proposed model with existing video steganography models on the basis of parameters like PSNR, MSE, Embedding Capacity, SSIM and GMSD etc.

## 2.7 Methodology

In this work, the frequency embedding method has been implemented using Progressive Exponential 8-pixel cover stack selection algorithm. The flowchart of the general principle of this algorithm has been shown in the following flowchart. In this, we will first acquire an image from various sources and will read the required details of an image. After that secret data is read and is converted into integer values. Then it is embedded with the cover image with the use of transform method.

## 2.8 Chapter summary

In this chapter, the work which has already been done in the field of steganography using various techniques is studied. Numerous approaches in spatial domain and frequency domain which are applied for secret information communication are studied. Literature review for discrete wavelet transform and skin-tone detection is also done. Finally, objectives of the dissertation are drawn based upon the gaps in study identified and work methodology is explained for the fulfillment of these objectives.

# Chapter-3

# Data-hiding Approach using Skin-tone Detection

## 3.1 System overview

The proposed scheme hides the secret images within video frames by utilizing human skin regions for adaptive steganography. It targets high imperceptibility and robustness to MPEG-4 compression. The proposed scheme is based upon the DWT based steganography embedded with skin-map extraction for the pixel region selection. The steganographic model required to be efficient and secure, as well as the embedding and extraction time along with error control. A schematic of the proposed technique is shown in figure3.1. The proposed model begins with the selection of the secret image and cover video object. The dimensions of the secret image are obtained from the input image matrix in the form of a number of columns, number of rows and number of planes (defined as image depth, which is usually 2-D or 3-D in our case.) to track the iteration.

The proposed model runs the iteration for each of the secret pixel, with sub-iteration for each of the cover frame in the video object. Skin-map detection algorithm is applied on cover video frames which returns the selective pixel region containing the skin-regions. The skin-mask is utilized to extract the region of interest (ROI) for data hiding. The video frame further undergoes the 3rd level DWT segmentation, which returns the 3rd absolute coefficient, which is used to embed the secret pixel. 8-pixel stacks are extracted one by one for each of the secret pixel. The embedding of the secret pixel is done on the basis of least significant bit (LSB), which has been configured to be 1-bit embedding per gray pixel, which eventually requires the 8-pixel stack from the cover video frame to embed the 8-bits of the secret pixel of the secret image. Afterward, the video frames are clubbed together in the form of output video object, as the stego video object. The reversal model is also designed for the extraction of the secret image from the stego video object using the structural secret image extraction model.

## 3.2 Skin-block-map generation

Skin-tone detection is the process of identifying skin-colored pixels in a video or an image. Various computer vision techniques have been evolved for skin-tone detection. Generally, a skin detector transforms a given pixel into a seemly color space and then utilize a skin classifier to identify the pixel whether it is a skin-colored or non-skin-colored pixel. A skin classifier determines a decision bound of the skin-tone class in the color space. However, this is a direct process and has proven truly challenging. Thus, important challenges in skin-tone detection are to depict the color in such a way that is constant or relatively insensitive to variations in illumination [31]. And other challenge originates from the fact that several objects in the real world may have skin-tone color. Due to this reason, if the environment is uncontrolled, any skin-tone detector have most false detection in the background [32]. The basic way to determine whether a pixel is skin-tone or not is to define a specific boundary. The RGB matrix (of color image) can be transformed to several color spaces to produce distinct regions of skin-tone. There are several color spaces. Primarily YCbCr color space is employed in the literature.

In this context, the skin-tone map is created using the algorithm for adaptive skin-tone detection presented in [33]. Their algorithm acknowledge the skin-tone model according to uprightly detected faces in a target video frame. Initially, face detection is executed on the video frames employing Viola Jones face detector [34]. If it detects multiple faces then each face forms a new skin-tone model, which enables detection of skin having different colors in different light conditions. They exploited the YCbCr color model. The consequent map is a binary matrix, wherein elements analogous to skin-tone pixels have the value one, whereas other elements have the value zero. In the static YCbCr model employed boundary values were set according to [33]. Furthermore, frames which have no faces detected are discarded despite they have other skin regions.

**Algorithm 1: Skin-tone detection algorithm**

1. Acquire the input image matrix
2. Get the size of input image in number of columns and rows
3. Create the binary image equal to number of rows and columns in input image
4. Convert the image matrix to YCbCr space from RGB
5. Run the iteration for each pixel in the image
    a. Acquire the current pixel value on Cb and Cr scale
    b. If the pixel range on Cb scale is between 77 and 127
        i. If the pixel range on Cr scale is between 133 and 173
            - Update the current pixel in binary image to 1
        ii. Otherwise
            - Update the current pixel in binary image to 0
    c. Otherwise
        i. Update the current pixel in binary image to 0
    d. If it's the last pixel
        i. Return the iteration
    e. Otherwise
        i. Repeat 5(a)
6. Return the binary mask

## 3.3 Wavelet-based hiding

Wavelets are significant functions which are used for representing signals as basal functions and are equivalent to sine and cosine in Fourier analysis. Wavelets are generated by dilations and translations of a firm function known as mother wavelet. Wavelet transform offers both spatial and frequency description of an image. Temporal information is preserved in this transformation process unlike conventional Fourier transform. Signal at different frequencies is analyzed by its multi-resolution analysis (MRA) yielding different resolutions. DWT divides the signal into low and high frequency parts. The low frequency parts comprise signal information while high frequency part comprises edge components information. DWT is very suitable to determine the regions in the cover image to embed the secret image effectively. This property permits the utilization of the masking effect of the HVS (human visual system) such that if a coefficient of DWT is altered, it alters only the area correspondent to that

coefficient.

The embedding secret image in the lower frequency sub-band might reduce the image quality as usually most of energy is accumulated in these sub-bands. In wavelets high frequency part comprises information about the edge of image so these frequency sub-bands are generally used for embedding secret image because the human visual system is less sensitive to variations in edges.

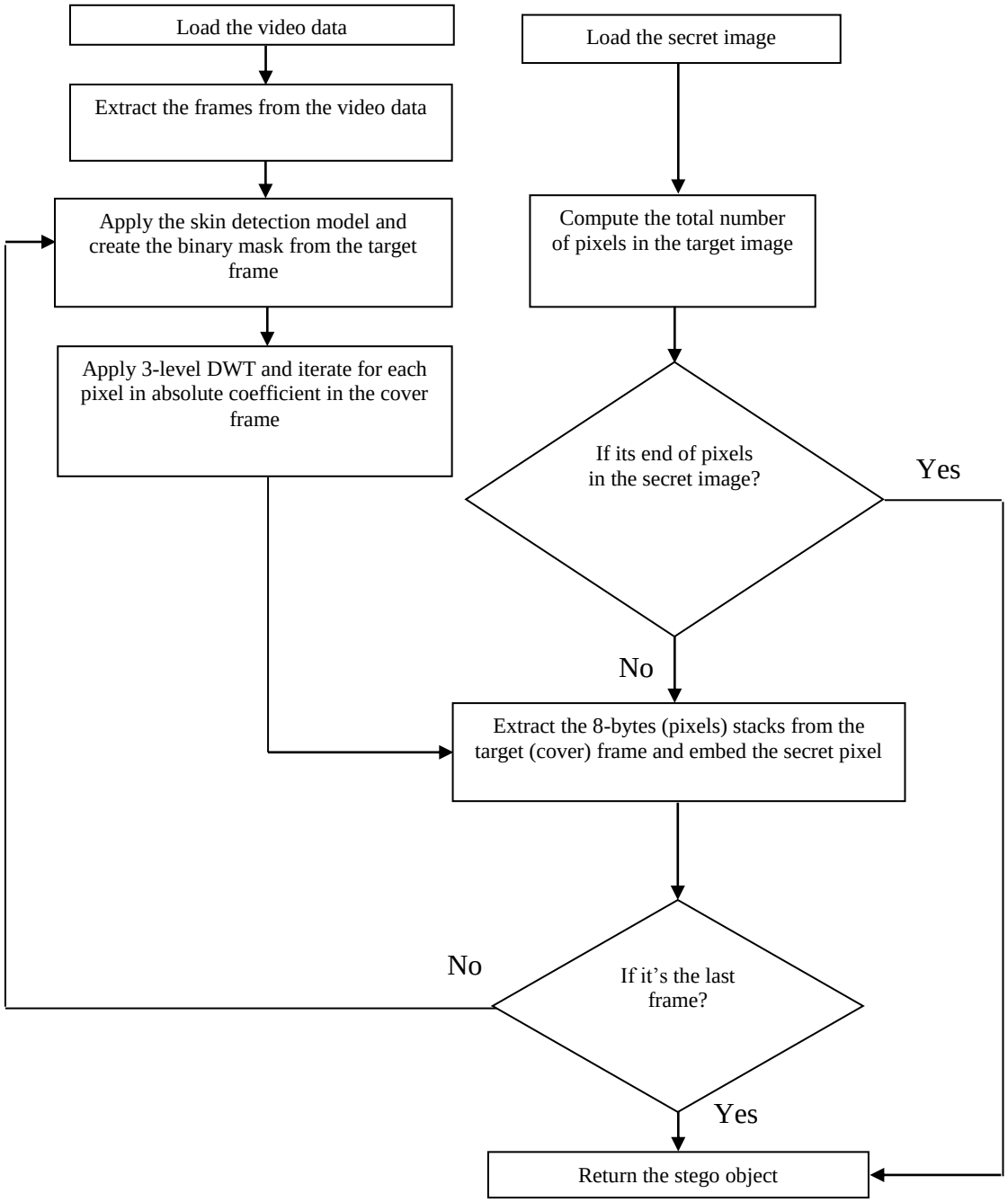



Figure 3.1: Proposed data-hiding scheme for video steganography

## 3.4 Secret-message embedding

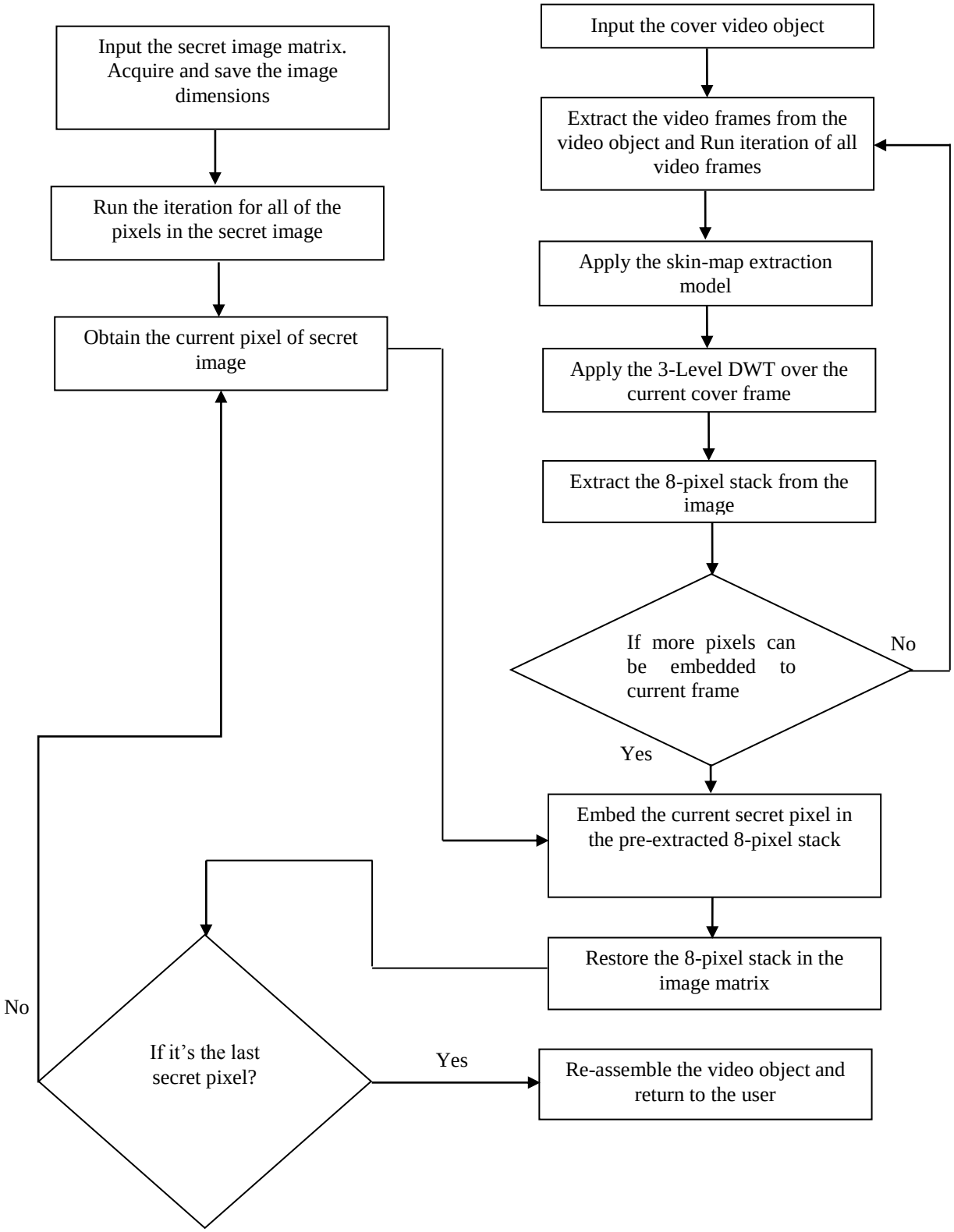



Figure 3.2: Flowchart for embedding the secret image

The embedding procedure has been designed around the combination of a variety of algorithms to create a complex and robust method for data security. The use of low level image decomposition method improvises the higher accuracy achieved by embedding the data in such components. The embedding algorithm has been designed in the layered design, which combines the various steps altogether for the purpose of embedding the secret image in the cover video object. The 1-bit LSB algorithm along with 3rd level DWT and skin-map algorithm has been utilized as the collaborative for the embedding of the secret object in the cover video object. The 1-bit LSB method embeds each bit of hidden or secret object in the pixel with value 1 in the pixel binary. Hence the maximum change would reflect with the value of 1 in the cover frame of the video data. The working methodology of the proposed model has been described in the steps in the following algorithm (Algorithm 2).

**Algorithm 2: Embedding algorithm**

1. Input the cover video object
2. Extract the video frame data
3. Save the video frame data to the temporary folder
4. Input the secret image
5. Obtain the size of secret image in the terms of rows, columns, depth and total number of pixels
6. Covert the secret image to the vectorized data
7. Run the iteration for each of the secret pixel
    a. Run the iteration for each of frame in video object
    b. Apply the skin map detection over the cover frames
    c. Apply the $3^{rd}$ Level DWT over the current frame
    d. Obtain the absolute coefficient component of $3^{rd}$ level DWT
    e. Run the iteration of each pixel in the 3-LC image
        i. Obtain the current pixel in 3-LC
        ii. If the skin map contains 1 for the current pixel in 3-LC
            - Select the Red pixel in the 8-pixel stack
            - Select the Blue pixel in the 8-pixel stack
            - If the length of stack equals 8
                - Embed the current secret pixel into the cover pixel

- Otherwise
    - Repeat 7(e)(i)

iii. Otherwise

- Repeat 7(e)(i)

f. If current pixel is last pixel of the secret image

i. Return the iteration

g. Otherwise

i. Repeat 7(e)(i)

8. Compile the video frames in one video
9. Finalize the video object
10. Return the video object

## 3.5 Data-extraction procedure

The extraction process extracts the embedded hidden pixels from the stego object, which is produced after embedding the secret data to the video frames. The accurate extraction process is always required to enhance the performance of the data security algorithm. The extraction algorithm performs the exact reversal process of the embedding algorithm for the extraction of the stego video object. The stego video object is acquired in the proposed model and the video frames are extracted from the video object. Skin-map extraction is applied on the stego video frames and then 3rd level DWT model is applied to each frame. Afterward, the reverse LSB is applied, which extracts the least significant bit (the bit with maximum value 1), after the 8-pixel stack. The last bit (with value 1) is extracted from each of the pixel in the stego frame, which are marked as skin-region in the skin-binary mask. Finally, the output image is constructed and returned to the user

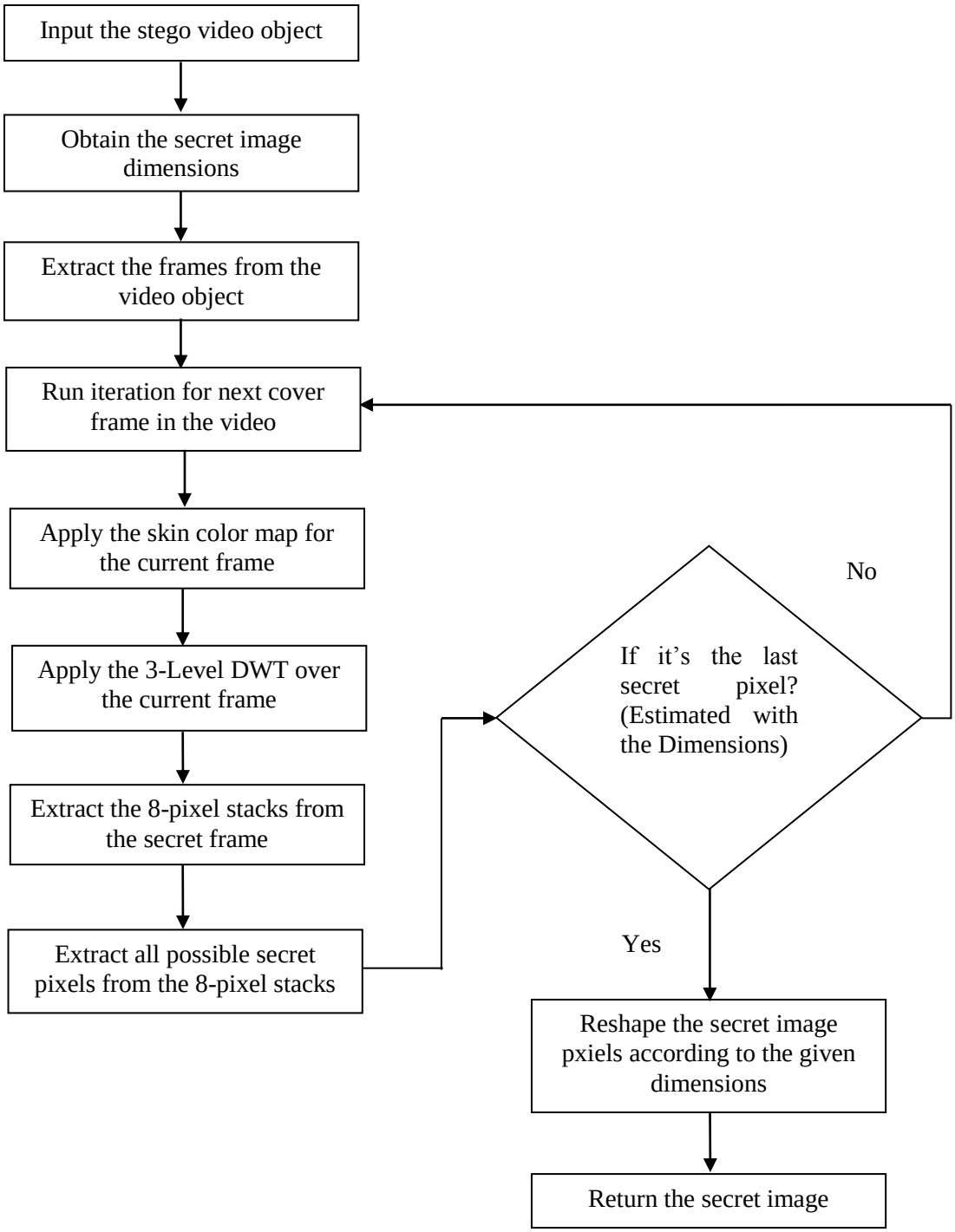



Figure 3.3: Flowchart for data extraction

**Algorithm 3: Extraction algorithm**

1. Input the stego video component
2. Input the dimensions and total number of pixels of the secret image
3. Extract the video frame data
4. Save the video frame data to the temporary folder
5. Run the iteration for each of frame in video object
    a. Obtain the current frame matrix
    b. Apply the skin map detection over the stego video frames
    c. Apply the 3rd Level DWT over the current frame
    d. Obtain the absolute coefficient component of 3rd level DWT
    e. Run the iteration of each pixel in the 3-LC image
        i. Obtain the current pixel in 3-LC
        ii. If the skin map contains 1 for the current pixel in 3-LC
            - Select the Red pixel in the 8-pixel stack
            - Select the Blue pixel in the 8-pixel stack
            - If the length of stack equals 8
                - Extract the secret pixel from the 8-pixel stack
            - Otherwise
                - Repeat 5(e)(i)
        iii. Otherwise
            - Repeat 5(e)(i)
    f. If current pixel is the last pixel of the secret image
        i. Return the iteration
    g. Otherwise
        i. Repeat 5 (e)(i)
6. Compile the secret image
7. Reshape the secret image in the particular dimensions as per input
8. Return the secret image

## 3.6 Chapter summary

This chapter explains the proposed methodology applied in this work for the video steganography using skin-tone detection. It comprises of pre-processing, skin-block-

map generation, wavelet based hiding, secret message embedding and data extraction procedure. Pre-processing includes normalization of secret image size and cover videos. Each step is explained one by one in separate sections and with relevant theory wherever required.

# Chapter-4
# Results and Discussions

## 4.1 Overview

The steganography models are image oriented security models for the creation of the covert channels over the internet. The secret data sharing is practiced through the watermarking or steganographic techniques, which utilizes the various pixel selection models for the embedding of the data into the images. The steganography model requires the secret data (the data which is being embedded) and the cover data (where the secret data is being embedded) in order to complete the steganography process. The pixel selection methods are designed to become as strong as possible in order to realize the non-detectable steganography traces in the cover data. There are color or appearance based pixel selection, random pixel sequence selection, etc. methods are utilized for the embedding of the secret data pixels in the cover data pixels.

## 4.2 Simulation scenario

In this simulation, the proposed model is based upon the image based steganography in the video frames using the skin-tone detection model. The skin-tone detection model is being utilized for the selection of the pixels, where the secret data is being embedded. The skin-tone detection model utilizes the color pixel ranges in the 3-D pixel format to make the skin-tone region selection. The proposed model utilizes the third level DWT model to decompose the image matrix in order to strengthen the steganographic model. The one-bit embedding is realized in the proposed to minimize the bit error rate, where one bit of the secret pixel is embedded within one pixel of the cover frame.

## 4.3 Result evaluation

The result evaluation has been done based upon the seven cover videos for the embedding one standard secret image. The dataset includes the videos of Foreman (352×288), Suzie (176×144), Car phone (176×144), Tennis (320×240), Akiyo (320×240), Trevor (320×240) and Salesman (176×144) of 25 frames per second each

represented by V1,V2,V3,V4,V5,V6 and V7 respectively taken from [50]. The skin-tone detection model has been realized in this technique for the pixel selection, which is based upon the 3-D pixel ranges for the selection of the target pixels in order to embed one secret pixel. The stack of eight pixels is selected in one round for the embedding of every secret pixel undergoes round by round iterations.

Figure 4.1: Secret image used in experiment

The following figure represents the first frame of the foreman video, which contains the plentiful of the skin pixel in the face region. The shadow of the safety helmet contains the probability to reduce the overall pixel selection using the skin region model, which eventually reduces the embedding capacity.

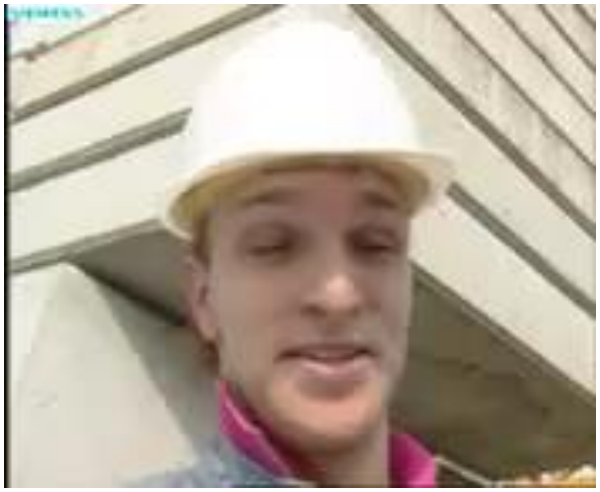


Figure 4.2: First frame of foreman video

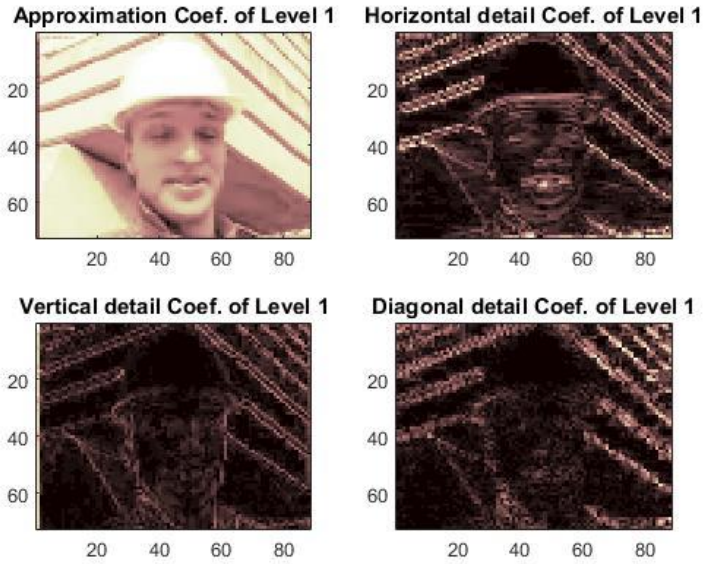



Figure 4.3: First level DWT application over first frame

The proposed model utilizes the third level DWT model, figure 4.3 shows the first-level DWT showing the absolute coefficient in the first place holder, detail coefficient, horizontal coefficient and vertical coefficient returned by the DWT algorithm over the submission of input image.

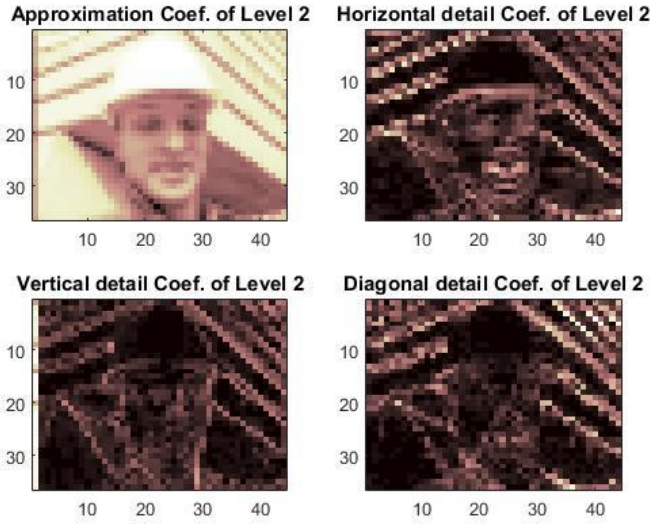



Figure 4.4: Second level DWT application over first frame

Figure 4.4 shows the second level DWT showing the absolute coefficient in the first place holder, detail coefficient, horizontal coefficient and vertical coefficient returned by

the DWT algorithm over the submission of input image. The overall quality seems to be degraded in comparison to the first level DWT.

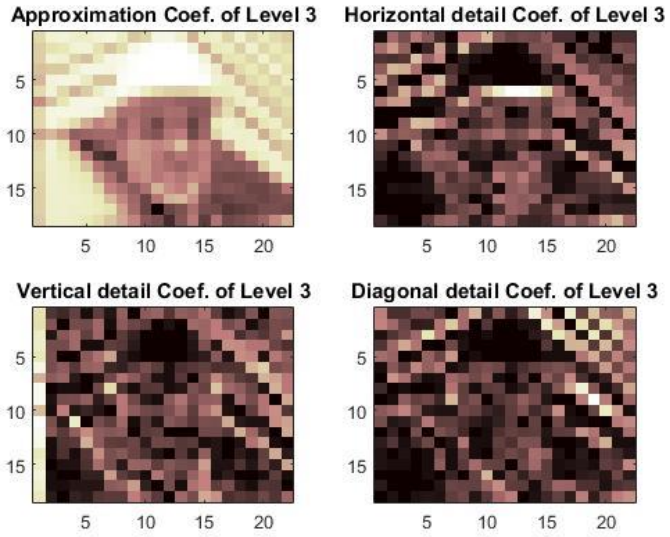
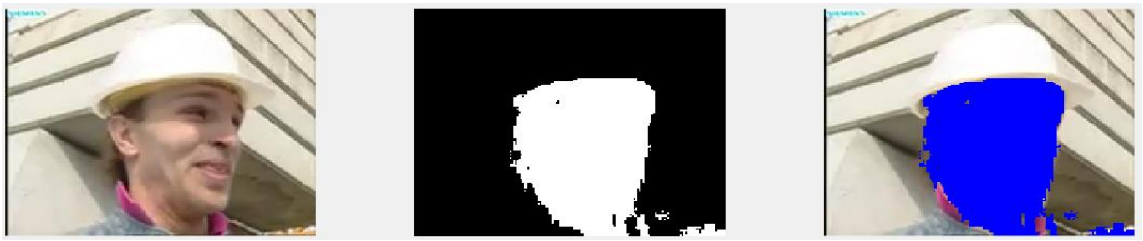
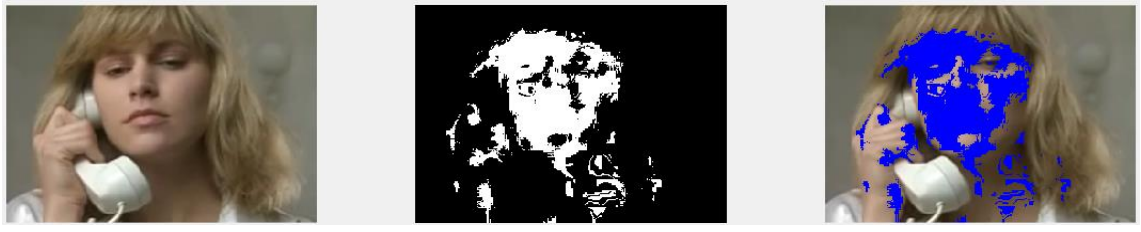



Figure 4.5: Third level DWT application over first frame

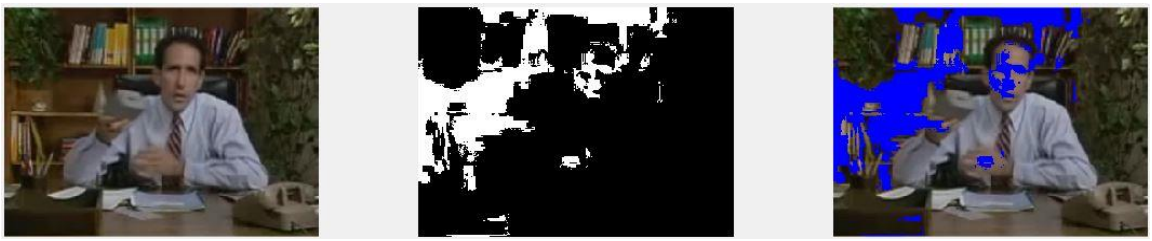
Figure 4.5 shows the third level DWT showing the absolute coefficient in the first place holder, detail coefficient, horizontal coefficient and vertical coefficient returned by the DWT algorithm over the submission of input image. The overall quality seems to be further degraded in comparison to the second level DWT (absolute coefficient) in the second decomposition level.



**(a)**



**(b)**



**(c)**

**(d)**

Figure 4.6: Skin detection upon the first frame of **(a)** Foreman, **(b)** Suzie, **(c)** Salesman and **(d)** Car phone videos

Figure 4.6 shows the results obtained after the skin pixel detection in the target frame. The skin region has been described in the form of binary mask in the second image shown in figure 4.6 and third image shows the skin pixel region marked on the target image (first image).

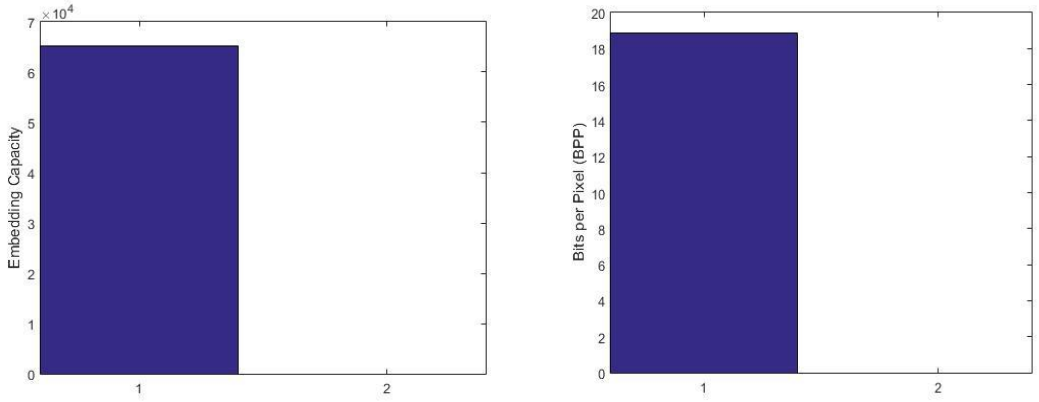



Figure 4.7: Embedding capacity and bits per pixel for Foreman video

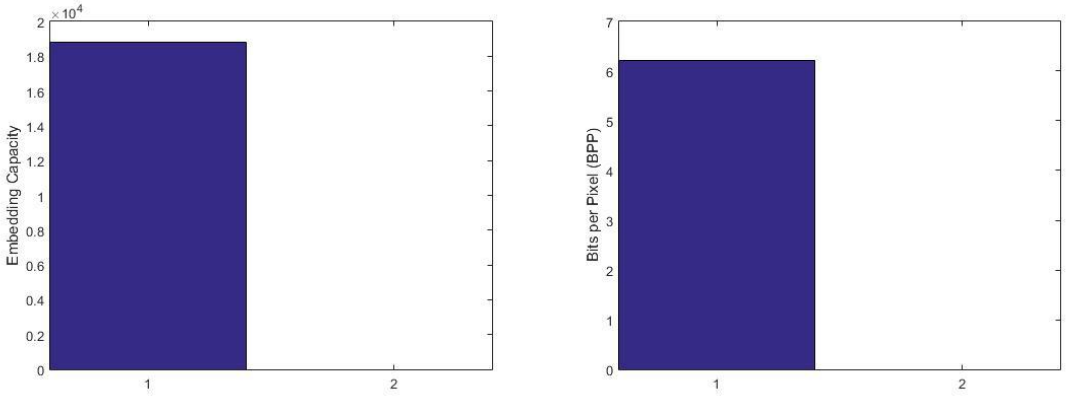



Figure 4.8: Embedding capacity and bits per pixel for Suzie video

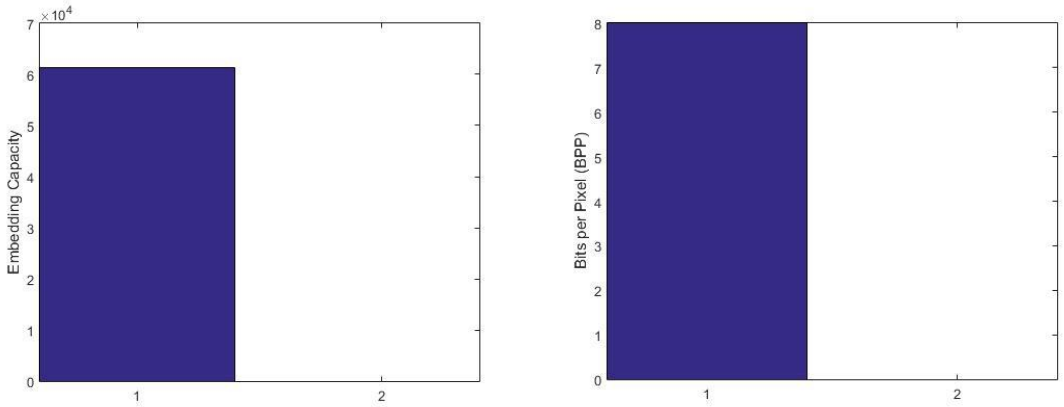



Figure 4.9: Embedding capacity and bits per pixel for Car phone video

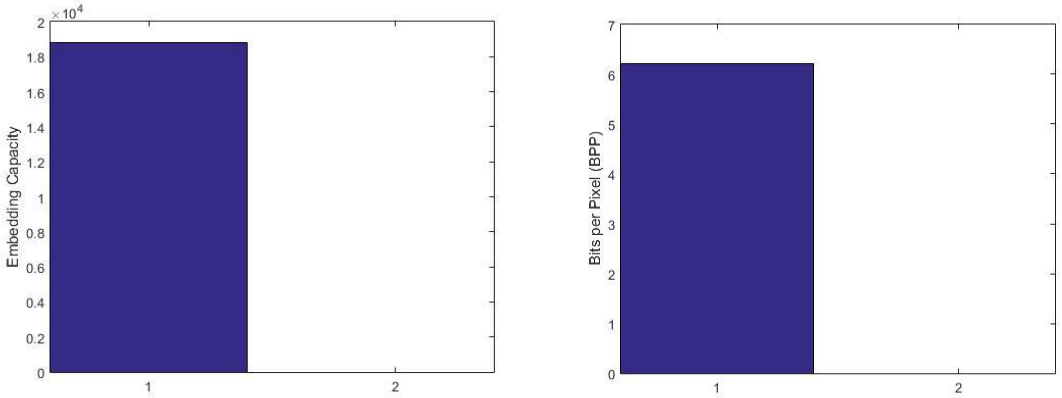



Figure 4.10: Embedding capacity and bits per pixel (BPP) for Tennis video

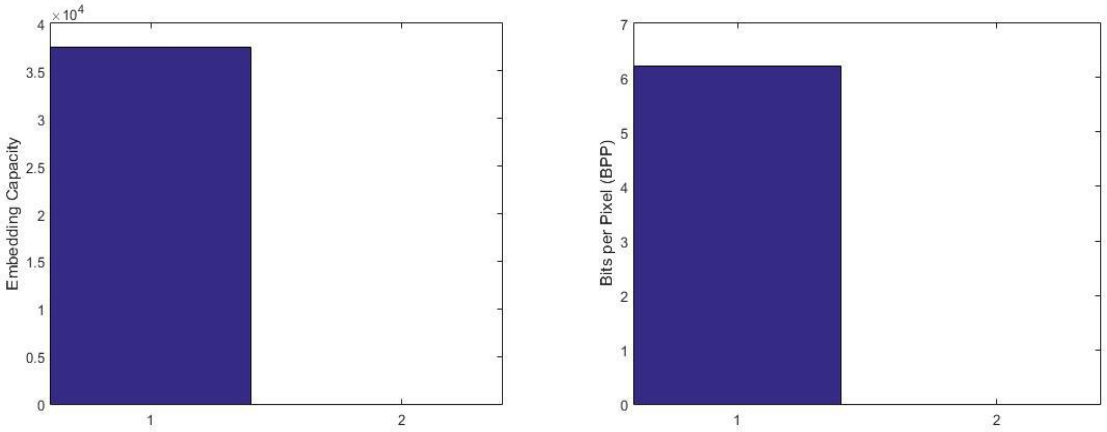



Figure 4.11: Embedding capacity and bits per pixel (BPP) for Akiyo video

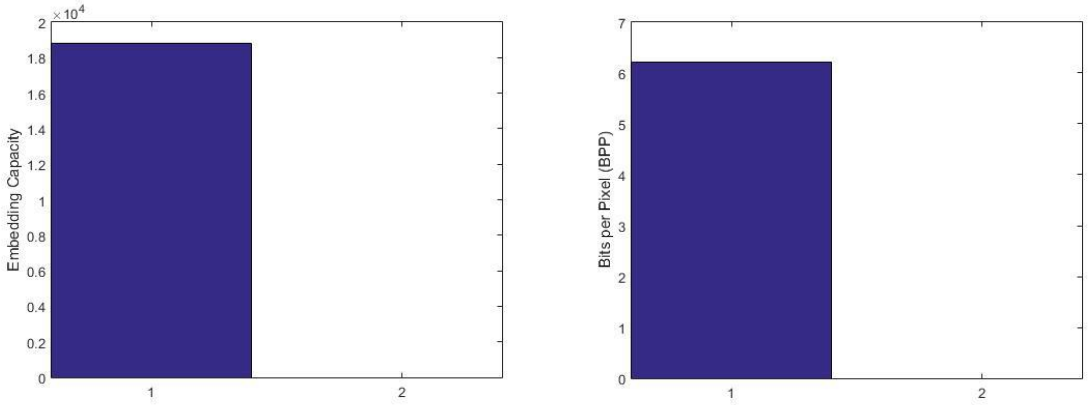



Figure 4.12: Embedding capacity and bits per pixel (BPP) for Trevor video

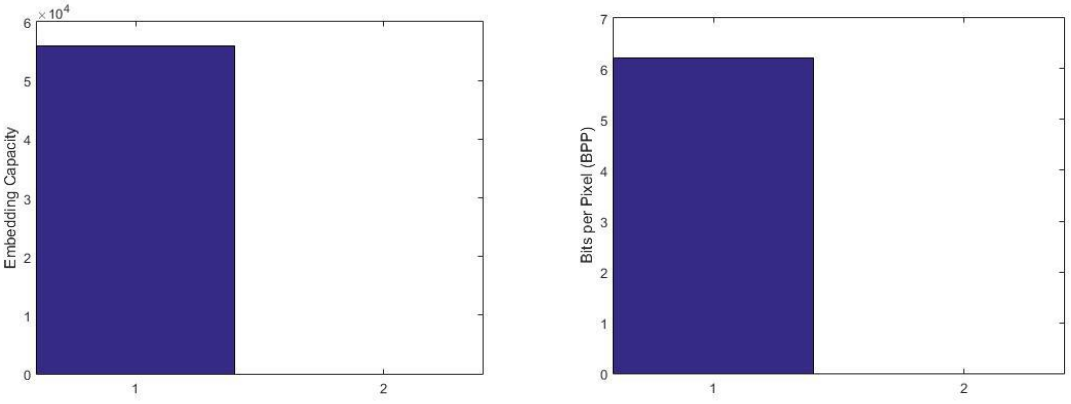



Figure 4.13: Embedding capacity and bits per pixel (BPP) for Salesman video

The embedding capacity of 18805.50 (Suzie, Tennis and Trevor), 65127.27 (Foreman), 61248.00 (Car phone), 37461.75 (Akiyo) and 55968.75 (Salesman) have been recorded from the proposed model with 18.84 bits per pixel (Foreman), 8.00 bits per pixel (Car phone) and 6.22 bits per pixel (Suzie, Tennis, Akiyo, Trevor and salesman) while embedding the secret image in the target video.

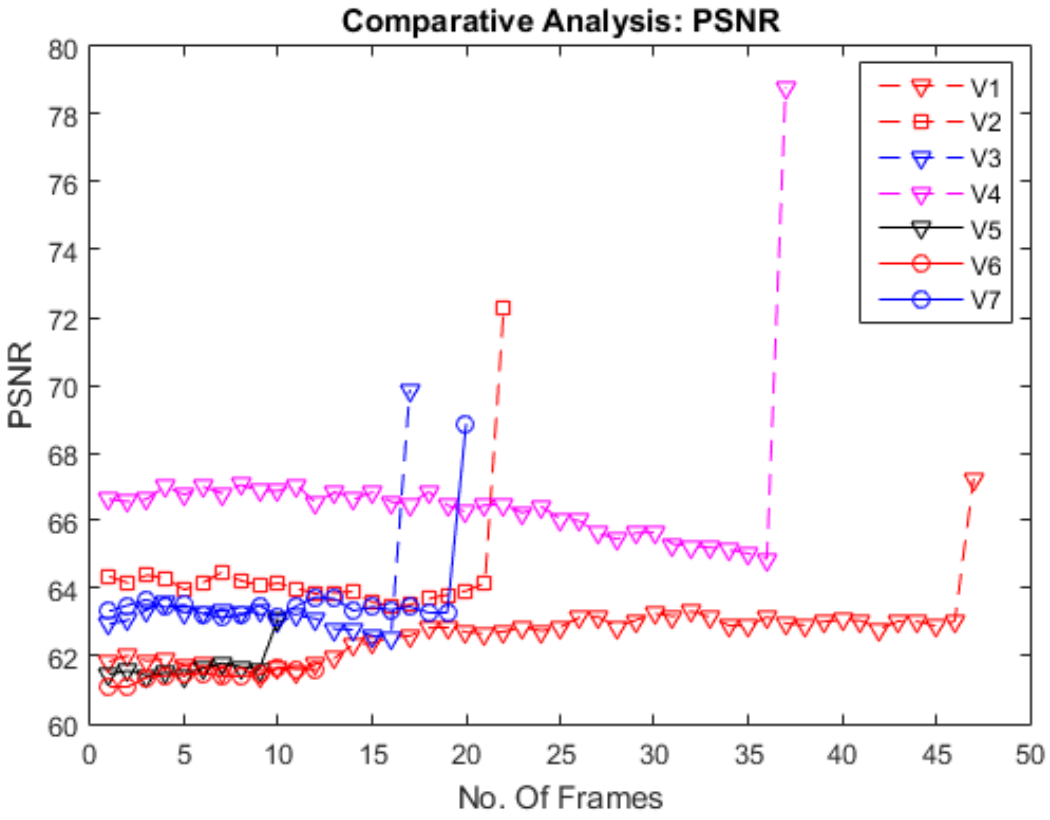



Figure 4.14: PSNR comparison of test videos

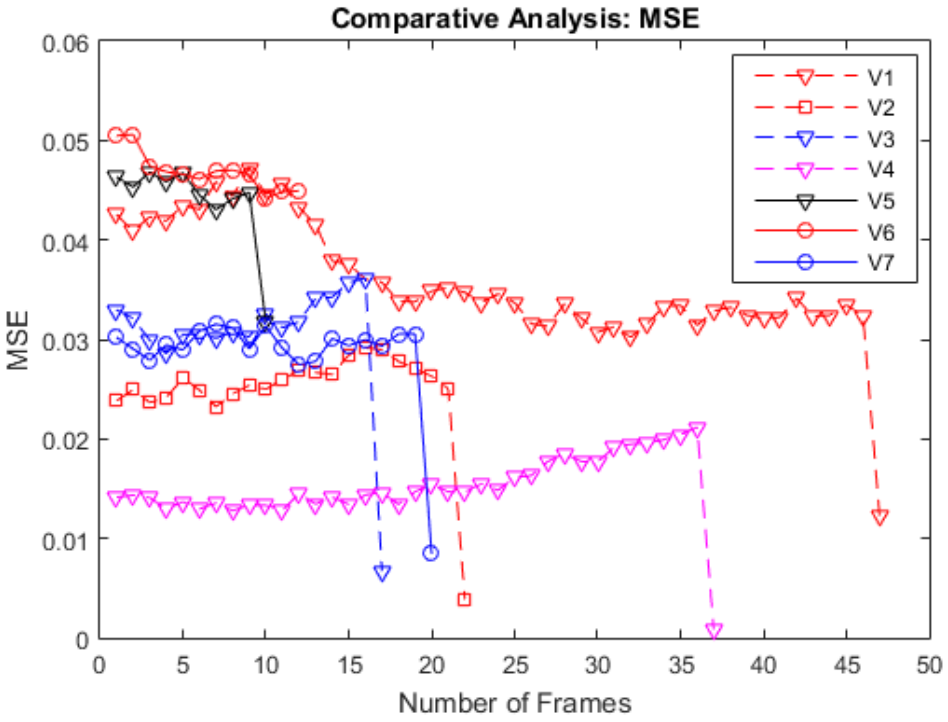



Figure 4.15: MSE comparison of test videos

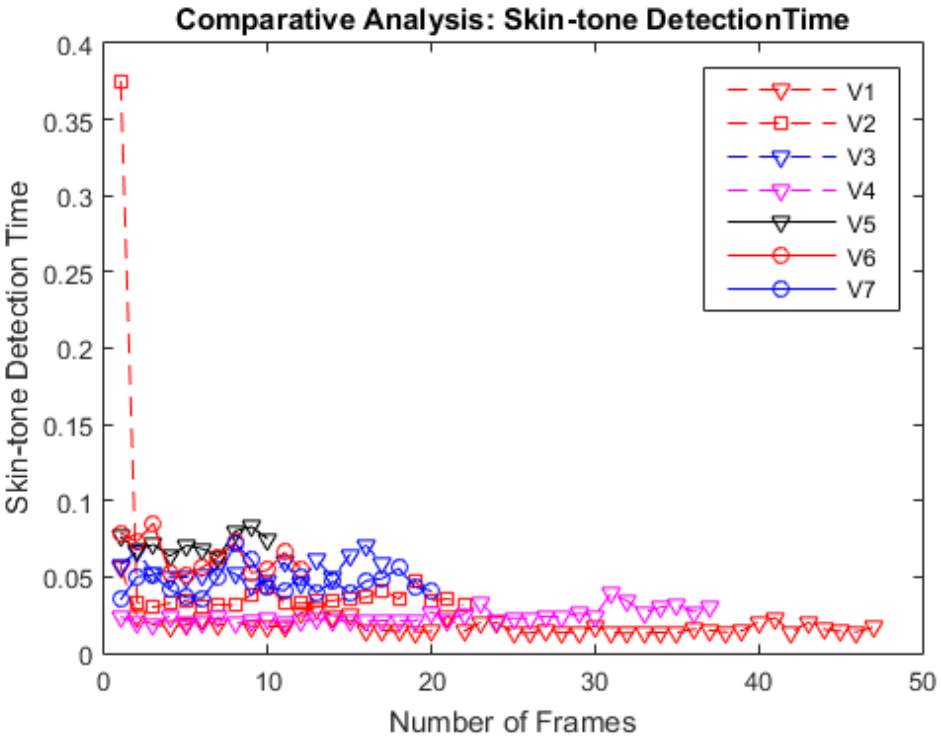



Figure 4.16: Skin-tone detection time for test videos

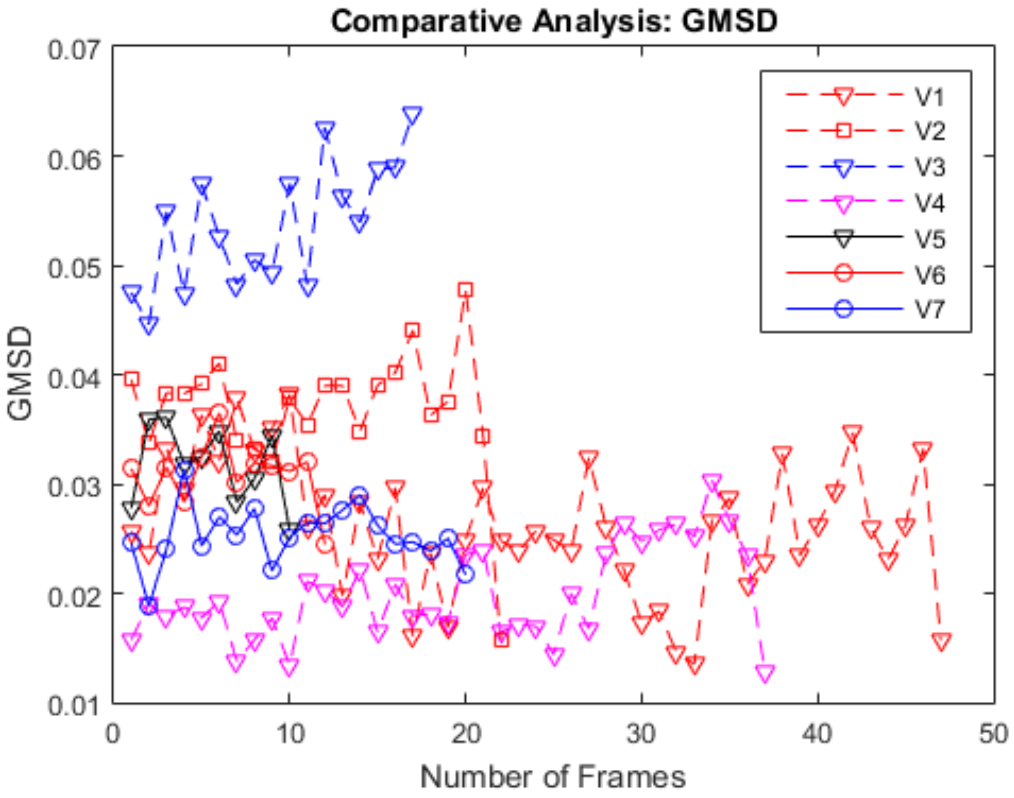



Figure 4.17: GMSD comparison of test videos

The video foreman has been analyzed in the first round of result assessment. The results obtained from the video conclude the parameters of MSE value of 0.037240, which show the low existence of error bits among the cover image. The PSNR value has been recorded at 62.47 decibels, SSIM value of 0.99, Correlation coefficient at 0.99 and GMSD value at 0.025, which are the qualitative parameters and shows the significance of embedding quality, which remains very high according to these parameters. The total run time of 0.85 seconds has been recorded for the embedding of the secret image into the target cover image as shown in Table 4.1.

Table 4.1: Result analysis for test videos

| | MSE | PSNR (dB) | SSIM | Correlation Coefficient | GMSD | BPP | Capacity (bits) | Total Run Time (sec) |
|---|---|---|---|---|---|---|---|---|
| **V1** | 0.03724 | 62.46749 | 0.999837 | 0.999995 | 0.025082 | 18.84 | 65127.27 | 0.85365 |
| **V2** | 0.03040 | 63.33739 | 0.999742 | 0.999989 | 0.036974 | 6.22 | 18805.50 | 0.83896 |
| **V3** | 0.03168 | 63.15191 | 0.999745 | 0.999996 | 0.053522 | 8.00 | 61248.00 | 1.02 |
| **V4** | 0.01801 | 65.60134 | 0.999873 | 0.999996 | 0.020579 | 6.22 | 18805.50 | 0.96064 |
| **V5** | 0.04376 | 61.74082 | 0.999760 | 0.999993 | 0.031473 | 6.22 | 37461.75 | 0.85665 |
| **V6** | 0.04685 | 61.46292 | 0.999811 | 0.999988 | 0.031873 | 6.22 | 18805.50 | 0.8551 |
| **V7** | 0.03171 | 63.12101 | 0.999779 | 0.999989 | 0.027264 | 6.22 | 55968.75 | 1.7237 |

## 4.4 Comparison of performance with other approaches

The imperceptibility and capacity of the proposed approach are evaluated in comparison with other similar approaches. These approaches are designed to be robust techniques and standard test videos salesman and car phone have been used for experimental results. The proposed model has been designed as the high security embedding (steganography) model based on the discrete wavelet transform (DWT), skin-map extraction and least significant bit (LSB). In the proposed model, the embedding capacity of 55968 and 61248 bits, as well as the PSNR value of 63.12 and 63.15 dB in the video of Salesman and Car phone videos respectively. In comparison to the existing models, the proposed model has been found improved by nearly 2-times on the basis of embedding capacity from nearly all of the existing models, except the underperformance than the Cheddad's [52] model. The proposed model has been found consistently better than the existing models by 2 to 5 decibels from the existing highest performer Cheddad's [52] model for both videos of Salesman and Car phone respectively. The following table (Table 4.2) further explains the comparison of the proposed model with the existing models.

Table 4.2: Comparison of performance with other approaches

| Techniques | Salesman | | Car phone | |
|---|---|---|---|---|
| | Capacity(bits) | PSNR(dB) | Capacity(bits) | PSNR(dB) |
| Proposed Method | 55,968 | 63.12 | 61,248 | 63.15 |
| Sadek et al. [51] | 25,914 | 54.64 | 18,620 | 52.47 |
| Cheddad et al. [52] | 77,587 | 61.22 | 156,426 | 58.04 |
| Ma et al. [53] | 936 | 38.58 | 806 | 42.9 |
| Gong et al. [54] | 750 | 39.57 | 500 | 41.24 |
| Noorkami et al. [55] | 736 | 36.69 | 507 | 38.32 |

The proposed model has been assessed on the basis of robustness, and compared with the existing models with higher efficiency. The proposed model has been tested over the standard video data set, which includes the video of Suzie, Foreman, Salesman and Car phone. The proposed model has been consistently recorded with the robustness higher than 99 on all of the videos, which is consistently higher than the existing model by nearly 11-21% from the highest performing existing model. The following table (Table 4.3) further explains the performance of the proposed model on the basis of robustness on the standard video data set.

Table 4.3: Comparison of robustness with other approaches based on SSIM

| Test videos | Sadek [51] | Cheddad [52] | Proposed Method | Improvement (%) from Sadek [51] | Improvement (%) from Cheddad [52] |
|---|---|---|---|---|---|
| Suzie | 87% | 80.55% | 99.98% | 12.93% | 19.43% |
| Foreman | 86.32% | 77.17% | 99.96% | 13.64% | 22.79% |
| Salesman | 85.88% | 80.78% | 99.87% | 13.99% | 19.09% |
| Car phone | 88.1% | 78.72% | 99.98% | 11.88% | 21.26% |

## 4.5 Chapter summary

In this chapter, results attained based on the proposed methodology explained in chapter 3 are given. A detailed description of results is provided in form of graphs and tables for various performance parameters. Comparative analysis of the results obtained is also done with the previous approaches used in video steganography. It is concluded that proposed technique for video steganography using skin tone detection is more robust and imperceptible than previous techniques

# Chapter-5

# Conclusions and Future Scope

## 5.1 Conclusion

The proposed model is based upon the steganography model involving the layered approach based upon the multiple models. The DWT based image decomposition along with skin-map extraction and least significant bit (LSB) has been amalgamated in the layered approach to realize the steganography model. The proposed model has been analyzed in the experimental procedure and based upon the performance parameters of PSNR, Embedding capacity and robustness. The proposed approach has been recorded with the 55968 bits of embedding capacity in comparison with the Sadek's [51] 25914 and Cheddad's [52] 77587 bits for the salesman video. Also, the embedding capacity of proposed model at 61248 bit of embedding capacity, which again outperformed the Sadek's 18620, and underperformed than the 156426 by Cheddad's [52] scheme. Further, the imperceptibility in proposed scheme has been enhanced with the PSNR value of greater than 63 dB in the case of Salesman and Car phone, and has been found higher than the all other models by minimum 1-2%. The robustness of the proposed model has been recorded with the value of 99%, which is higher than the maximum value of 88.1% per robustness of the existing model (Sadek's scheme) for the Car phone video.

## 5.2 Future scope

In future, the proposed scheme can be further improved by combining the data encryption of the secret pixels in order to achieve the higher level of security. The proposed scheme can be also improved by using the fuzzy rule based embedding, which can match the cover data segments effectively in order to minimize the probability of detection. The application of travelling salesman algorithm can be also utilized to align up the non-continuous pixel based embedding with higher accuracy with minimized error bits during the secret data recovery. The pseudo-random pixel selection mechanism can empower the proposed model with high security level by embedding the pixels in the random pixels of the cover image.

# REFERENCES


[1] F. P. Petitcolas, R. J. Anderson and M. G. Kuhn, "Information hiding-a survey," in Proceedings of the IEEE, pp. 1062-1078, 1999.

[2] K. S. Poonam, A. B. Singh, "A session based multiple image hiding technique using DWT and DCT," International Journal of Computer Applications, pp.18-21, 2012.

[3] N. D. Thepade and P. R. Rothe, "Data Hiding Technique for Security by using Image Steganography," International Journal of Computer Science and Information Security (IJCSIS), pp 33-36, 2014.

[4] T. Samidha and J. Mani, "Steganography using the technique of orderly changing pixel componenet," International Journal of Computer Applications, 2014.

[5] J. P. Anderson and C. E. Irvine, "Embeddeed Information, Information Hiding," Scientific American, pp.142-46, 1996.

[6] J. Mani, N. Memon and B. Sankur, "Steganalysis Using Image Quality Metrics", IEEE Transactions on Image Processing, pp. 221- 229, 2003.

[7] G. Prabhakran and R. Bhavani, "A Modified Secure Digital Image Steganography Based on Discrete Wavelet Transform," International Conference on Computing, Electronics and Electrical Technologies (ICCEET), pp.1096-1100, 2012.

[8] A. Tamer, J. Condell, K. Curran and P. M. Kevitt, "Digital image steganography: survey and analysis of current methods," IEEE Signal Processing letters, pp.27-34, 2012.

[9] H. Zaidooon and R. Naoum, "A Novel Method for Steganography in Spatial Domain," International Journal of Advanced Research in Computer Science and Software Engineering, pp. 208-14, 2010.

[10] L. Cheng, M. Y. Kiang, "Hybrid domain in LSB steganography",International Journal of Computer Applications. PP. 35-40, 2008.

[11] H. O. Alanazi, B. B. Zaidan, A. A. Zaiden, H. A. Jalab, M. Shabbir and Y. A. Nabhani, " New comparative study between DES, 3DES and ASE within Nine factor," Journal of computing, pp. 152-157, 2010.

[12] A. Shadded, J. Condell, K. Curran, and P. Mckevtt, "Biometric inspried digital image stegnography," Proceedings of the 15th Annual IEEE International Conference and workshop on the Engineering of Computer based system, pp. 159-168, 2008.

[13] P. Sallee, “Model based watermarking,” proceeding of the 2nd International Workshop on Digital watermarking, lecture Notes in Computer science springer, pp. 254-260, 2004.

[14] P. Kruus, C. Scace, M Heyman, and M. Mundy, “A survey of watermarking techniques for image files,” advanced security Research Journal, pp. 41-52, 2003.

[15] N. F. Johnson and S. Jajodia, “Exploring Steganography: Seeing the Unseen,” Computer, pp. 26-34, 1998.

[16] M. A. Bajura, Y. Boulghassoul, R. Naseer, S. D. Gupta, A. F. Witulski, J. Sondeen, S. D. Stansberry, J. Draper, L. W. Massengill, and J. N. Damoulakis, “Models and algorithmic limits for an ECC-based approach to hardening sub-100-nm SRAMs,” IEEE Trans. Nucl. Sci., pp. 935–945, 2007.

[17] C. Cachin, “An information-theoretic model for steganography,” in Information Hiding, ser. Lecture Notes Comput. Sci.. Berlin, Germany: Springer, pp. 306–318, 1998.

[18] E. Koch, J. Rindfrey, and J. Zhao, “Copyright Protection for Multimedia Data,” Proc. Int’l Conf. Digital Media and Electronic Publishing, Leeds, UK, 1994.

[19] K. Matsui and K. Tanaka, “Video-steganography: How to secretly embed a signature in a picture," Journal of the Inter-active Multimedia Association Intellectual Property Project, pp. 187, 1994.

[20] H. V. Desai, “Watermarking, Cryptography, Watermarking: A comparative study,” Journal of Global Research in Computing science, pp. 33-35, 2012.

[21] L. Guo, J. Ni, and Y. Q. Shi, “An efficient JPEG steganographic scheme using uniform embedding,” in Proc. 4th IEEE Int. Workshop Inf. Forensics Secur., Tenerife, Spain, pp. 169–174, 2012.

[22] L. Guo, J. Ni, and Y. Q. Shi, “Uniform embedding for efficient JPEG steganography,” IEEE Trans. Inf. Forensics Security, pp. 814–825, 2014.

[23] C. Kurak and J. McHugh, “A Cautionary Note On Image Downgrading,” Proc. IEEE Eighth Ann. Computer Security Applications Conf., IEEE Press, Piscataway, pp. 153-159, 1992.

[24] B. Chen and G. W. Worwell, “Quantization index modulation: A class of proveably good methods for digital watermarking and information embedding,” IEEE Transaction Information Theory, pp. 1423-1443, 2001.

[25] N. Hamid, A. Yahya, R. B. Ahmad and O. M. Qershi, " Image watermarking Techniques: An Overview," International Journal of Computer Science and security, pp. 168-187, 2012.

[26] G. Kaur and A. Kochhar, "A Steganography Implementation based on LSB & DCT," International Journal for Science and Emerging Technologies with Latest Trends, pp.35-41, 2012.

[27] J. Fridich and M. Goljan, "Practical Steganalysis – State of the Art," proceedings of SPIE, pp. 1-13, 2002.

[28] P. Y. Chen and H. J. Lin, "A DWT based approach for image steganography," International Journal of Applied Science and Engineering, pp. 275–290, 2006.

[29] S. J. You and N. I. Cho, "An adaptive bandwidth nonlocal means image de-noising in wavelet domain," EURASIP J Image Video Process, 2013.

[30] T. Bhattacharya, N. Dey, and S. R. Chaudhuri. "A session based multiple image hiding technique using DWT and DCT," Int J Comput Appl, pp. 18–21, 2012.

[31] S. Bhattacharyya, and G. Sanyal, "A robust image steganography using DWT difference modulation (DWTDM)," International Journal of Computer Network and Information Security, pp. 27–40, 2012.

[32] M. Sheikhan, K. Asadollahi, and R. Shahnazi, "Improvement of embedding capacity and quality of DWT-based audio steganography systems," World Applied Sciences Journal, pp. 507–16, 2011.

[33] S. Barve, U. Nagara and R. Gulabani, "Efficient and secure biometric image stegnography using discrete wavelet transform," Int J Comput Sci Commun Netw, pp. 96–9, 2011.

[34] H. Jalab, A. A. Zaidan, and B. B. Zaidan, "Frame selected approach for hiding data within MPEG video using bit plane complexity segmentation." J Comput, pp. 108–13, 2009.

[35] D. C. Wu and W. H. Tsai, "A watermarking method for images by pixel-value differencing," Pattern Recognit Lett, 2003, pp. 1613–1626, 2003.

[36] A. Ali and A. Fawzi, "Modified high capacity image steganography technique based on wavelet transform," The Int Arab J Inform Technol, pp. 358–64, 2010.

[37] M. Eltahir, L. M. Kiah, B. B. Zaidan, and A. A. Zaidan, "High rate video streaming steganography," In:International Conference on Future Computer and Communication, pp. 672–675, 2009.

[38] S. K. Kapotas and A. N. Skodras, "A new data hiding scheme for scene change

detection in H.264 encoded video sequences," 2008 IEEE International Conference on Multimedia and Expo, Hannover, 2008, pp. 277-280.

[39] Z. Li, J. Jiang, G. Xiao and H. Fang, “An effective and fast scene change detection algorithm for MPEG compressed videos,” Springer-Verlag, pp. 206–214, 2006.

[40] H. C. Wu, N. I. Wu, C. S. Tsai, and M. S. Hwang, “Image watermarking scheme based on pixel-value differencing and LSB replacement methods,” Proceedings of 2005 Instrument Electric Engineering, Vis. Images Signal Process, pp. 611–615, 2005.

[41] M. Singh, B. Singh, S. S. Singh, “Hiding Encrypted Message in the Features of Images,” IJCSNS, VOL. 7, No.4. April, 2007.

[42] C. H. Yang, C. Y. Weng, S. J. Wang and H. M. Sun, "Adaptive Data Hiding in Edge Areas of Images With Spatial LSB Domain Systems," in IEEE Transactions on Information Forensics and Security, vol. 3, no. 3, pp. 488-497, Sept. 2008.

[43] C. H. Yang and M. H. Tsai, “Improving Histogram-based Reversible Data Hiding by Interleaving Predictions,” IET Image Processing, Vol.4. Iss. 4 pp. 223-234, 2010.

[44] W. Luo, F. Huang and J. Huang, "Edge Adaptive Image Steganography Based on LSB Matching Revisited," In IEEE Transactions on Information Forensics and Security, pp. 201-214, 2010.

[45] W. J. Chen, C. C. Chang, and T. H. N. Le, “High payload watermarking mechanism using hybrid edge detector,” Expert Systems with Applications, pp. 3292–3301, 2010.

[46] M. Hussain and M. Hussain, “Embedding data in edge boundaries with high PSNR”, Proceedings of 7th International Conference on Emerging Technologies (ICET 2011), pp.1-6, Sept 2011.

[47] M. Juneja and P. S. Sandhu, “A New Approach for Information Security using an Improved Watermarking Technique,” J Inf Process Syst, 2013.

[48] H. W. Tseng and H. S. Leng, “High-payload block-based data hiding scheme using hybrid edge detector with minimal distortion,” IET Image Process, pp. 647–654, 2014.

[49] D. Singla and M. Juneja, ‘‘Hybrid Edge Detection-Based Image Watermarking Technique for Color Images,” Intelligent Computing, Communication and Devices, Advances in Intelligent Systems and Computing, Springer India, 2015.

[50] Dataset: http://see.xidian.edu.cn/vipsl/database_Video.html.

[51] M. Sadek, A Khalifa and M. G. M. Mostafa, “Robust video steganography algorithm

using adaptive skin-tone detection," Multimed Tools Appl, 2016.

[52] A. Cheddad, J. Condell, K. Curran and P. Kevitt, "A skin tone detection algorithm for an adaptive approach to steganography," Signal Process 89(12), pp. 2465–2478, 2009.

[53] X. Ma, Z. Li, H. Tu and B. Zhang, "A data hiding algorithm for H.264/AVC video streams without intraframe distortion drift," In: IEEE transactions on circuits and systems for video technology pp. 1-20, 2010.

[54] X. Gong and H. M. Lu, "Towards fast and robust watermarking scheme for H.264 video," In Proc. 10th IEEE ISM, pp. 649–653, 2008.

[55] M. Noorkami and R. M. Mersereau, "A Framework for Robust Watermarking of H.264-Encoded Video With Controllable Detection Performance," IEEE Transactions on Information Forensics and Security, pp. 14-23, 2007.

# LIST OF PUBLICATIONS

P. Kumar and K. Singh, “An Improved Data-hiding Approach using Skin-tone Detection for Video Steganography,” in Multimedia tools and applications (Communicated).