# Video Based Steganography in Skin Tone

Reshma R Pillai, Smitha Vas P

**Abstract**— Steganography is the method of concealing a file, message, image or video with in another file, message, image or video.Steganography is the study of invisible communication that deals with the way to hide the existence of the communicated message. It is achieved in such a way that, the message does not attract attention from eavesdroppers and attackers.The information can be hidden in different embedding mediums, known as carriers. The carriers can be images, audio files, video files, and text files. The carriers having messages is called stego.Biometric feature (Skin tone region) is taken to implement steganography. Biometrics is defined as the automatic recognition of individuals based on their behavioural and biological characteristics. The biometrics used here is skin tone. Instead of embedding secret data anywhere in image, it will be embedded within the skin tone of an image. The skin tones are taken from the face images. This skin region provides excellent secure location for data hiding. So, firstly skin tone detection is performed using HSV (Hue, Saturation and Value) colorspace. A region from skin detected area is selected, which is known as the cropped region.Existing system is that it uses image as the carrier file for performing steganography. In the embedding phase, after performing the skin detection and cropping, the secret message which is an image is embedded in the cropped region using DWT (Discrete Wavelet Transform).Secret data embedding is performed in one of the high frequency sub-band by tracing skin pixels in that band. Cropped region works as a key at decoding side so cropping results into more security.Cropped value is stored in one variable for the extraction procedure. This cropped one is then merged to form the original image and it is referred to as the stego image. In the extraction phase the skin detection on stego image is performed using HSV.The cropped value which is stored is used to crop the stego image. Then apply DWT on the image. Then the secret message is extracted. This provides a good PSNR value. The skin tone is different for different images. So it is necessary to change the skin threshold value for different images. This is a complicated task .Also it is not possible to hide large amount of secret messages in one image. To solve this problem instead of using image as the carrier file, video is chosen.Proposed system is that the cover media is changed from image to video. In the embedding phase video is converted in to different frames and stored in a buffer as image. Choose one frame and perform skin detection using HSV (Hue, Saturation and Value) color space. The region from skin detected area is selected, which is known as the cropped region. In this cropped region the secret message which is the image is embedded using DWT (Discrete Wavelet Transform).Secret data embedding is performed in one of the high frequency sub-band by tracing skin pixels in that band. Cropped region works as a key at decoding side. Cropped value and the frame where the message is embedded is stored. The cropped one containing message is then merged to form the original frame and it is referred to as the stego frame. Then it is combined with other frames to form the stego video. In the extraction phase, the stego video is then converted in to frames and stored in the buffer. Choose the frame based on the stored value.The skin detection on that frame is performed using HSV.The cropped region based on the stored value is used to crop the frame. Apply DWT on the frame. Then the secret message is extracted. The idea of using video is that it is possible to hide more messages using different frames. MSE of the proposed system is good compared with the existing system.

**Index Terms**—Steganography, Biometric Steganography, Skin tone Detection, DWT, Video Frames, MSE, PSNR



## 1 Introduction

Steganography is the art of hiding information in ways that prevent the detetion of the hidden messages.Steganography literally means "covered writing" which derived from the Greek words "*Steganos*" means covered and "*Graphein*" means writing.In this digitized internet world steganography plays an important role in providing protection for the confidential document that meant to send to the corresponding receiver from the eavesdropper.In steganography secret message is the data that the sender wishes to remain confidential.The cover or host is the medium in which the message is embedded and serves to hide the presence of the message.

- *Reshma R Pillai,MTech Student,Computer Science and Engineering,LBS Institute of Science and Technology,Poojappura,Trivandrum,India, E-mail: reshmarpillai718@gmail.com*
- *Smitha Vas P,Assistant Professor, Computer Science and Engineering,LBS Institute of Science and Technology,Poojappura,Trivandrum, India, E-mail: smithavas2011@gmail.com*


Fig 1: Steganography Model

The cover medium may be image, text, audio and video.The secret message may be image, audio, video, text. In this paper cover and secret messages are restricted to digital images.The cover-image with the secret data embedding is called stego-image.The stego-image should resemble the cover-image.Fig 1 represents the steganography model. The main objective of steganography is to make the communication securely in such a way that the true message is not made visible to the observer that is the unwanted parties should not be able to distinguish any sense between cover-image and stego-image. Fig 2 represents the steganography model with input as cover image and output as stego image.

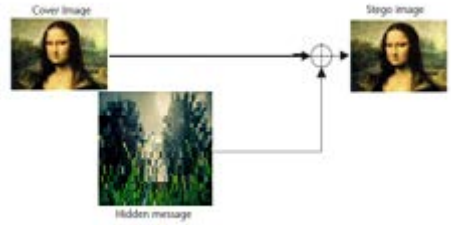


Fig 2: Image Steganography Model

## 2 BIOMETRIC STEGANOGRAPHY

Biometrics is defined as the automatic recognition of individuals based on their behavioral and biological characteristics. It originated from the Greek words "*bios*" and "*metricos*", literally means life to measure. The biometric data is classified as physiological data or behavioral data. The physical biometrics is based on physical characteristics such as fingerprint, iris etc. and the behavioral biometrics is based on behaviour of human such as voice, signature etc. In this highly digitized globe the internet plays an important role in data transmission and sharing of data. Some confidential biometric information and other information may get stolen, copied, modified. To overcome this problem the biometrics is combined with steganography which is called as biometric steganography [1].

### 2.1 Skin Tone Detection

Skin tone detection is the method to detect the skin pixels within an image to hide the information in that region. The biometrics used here is the skin. Instead of embedding the message in whole image, it is embedded in the selected skin region. The goal of skin color detection is to build decision rule that will discriminate between skin and non-skin pixels.
The detection of the skin tone regions requires knowledge in color spaces.
The types of color spaces are [2]:

*RGB*: It is originated from Cathode Ray Tube (CRT) which is a combination of three colored rays; red, green and blue. It is the widely used color spaces.

*RGB Color Value Normalization*: The RGB color representation is obtained from RGB values by a simple normalization procedure.

$$r = \frac{R}{R+G+B}$$

$$g = \frac{G}{R+G+B}$$

$$b = \frac{B}{R+G+B}$$

*HSV, HSL, HIS*: Hue-saturation based color spaces were introduced when there is a need for the user to specify the color spaces properties numerically. Hue defines the dominant color of an area; saturation defines the colourfulness of an area which is proportional to the brightness. The intensity, lightness or value is related to the color luminance.

$$H = arccos \frac{\frac{1}{2}(R-G)+(R-B)}{\sqrt{(R-G)^2+(R-G)(G-B)}}$$

$$S = 1 - 3\frac{min(R,G,B)}{R+G+B}$$

$$V = \frac{1}{3}(R+G+B)$$

*YCbCr Color intensity*: It is an encoded nonlinear RGB signal represented by luma which is constructed as a weighted sum of RGB values and two color difference values *Cb* and *Cr* which is obtained by subtracting luma from RGB red and blue components.

$$Y = 0.299R + 0.587G + 0.114B$$
$$Cr = R - Y$$
$$Cb = B - Y$$

#### 2.1.1 Determine Skin area in HSV color space.

Here for this work HSV color space is used.For this convert RGB image in to HSV color space.Fig 3 represents the RGB and HSV image.

(a) (b)

Fig 3: (a) RGB image; (b) HSV image

#### 2.1.2 Skin detection

A skin detector converts a given pixel into a suitable color space and uses a skin classifier to label the pixel to identify whether it is a skin pixel or non skin pixel. The skin detection algorithm produces a mask, which consist of black and white pixels. The black pixels values are 0 that is false and white pixels values are 1 that is true. The mask of 1 and 0 acts as logic map for skin detection [3].

The simplest way to decide whether a pixel is skin or non skin is to explicitly define the boundary [9].The skin threshold value is different for different image.Here for this image the threshold value choosen is based on the saturation value of the image.The range taken is $S_{min}$=0.16 and $S_{max}$=0.58.Fig 4 represents the skin region after masking using the threshold value.

Fig 4: Skin region

### 2.1.3 Fill image regions and holes

The image that is obtained may contain a set of holes in the outer boundary of some regions.These holes produce unclosed regions.To solve this problems, the advantage of the close morphological operation has been taken which is represented to remove small holes from boundary of face regions to ensure closing it region.

The close operation is implemented by applying dilate operator and then applying erode operator [4].Fig 5b represents the image after filling holes.

(a) (b)

Fig 5: (a) Image with holes; (b) Image after erode and dilate

### 2.2 Cropping

After the skin region is detected it is then cropped to hide the secret message.This is done by using regionprops which measure the properties of the image region.The input for the regionprops is bwlabel that label the connected components which contain the information about the skin region. The aim of the cropping is that it is more secure than using without cropping.The eavesdropper couldnot able to identify the portion where the message is hidden in the image.The cropped value is stored in one variable.This variable is send along with the message to the receiver.With the help of this value the stego image is cropped and extract the message.

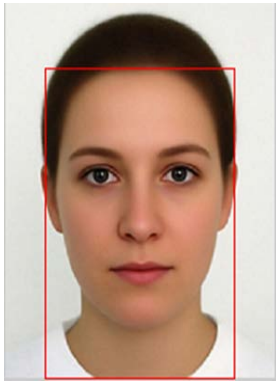

Fig 6: Cropped image

### 2.3 Discrete Wavelet Transform

DWT is the frequency domain that mostly applied for steganography.Wavelets convert the images in to series of wavelets that can be stored more efficiently than pixel blocks.DWT splits the componenets into numerous frequency bands called LL(horizontally and vertically low pass),LH(horizontaly low pass and vertically high pass),HL(horizontally high pass and vertically low pass),HH(horizontally and vertically high pass).

Human eyes are more sensitive to the low frequency part(LL),so it is good to hide the secret image in other three parts which doesnot make any alteration in LL band.Hiding on these bands will not affect the quality of the cover medium.

In this work Haar-DWT is used.This provide better performance in terms of computation time and it is simpler to perform. It performs two steps, row and column transformation.Entire row of the image is taken then do averaging and then differencing is done.After the the entire row is is treated the do the averaging and differencing process for the entire column of image.Using IDWT the image is recovered.Fig 7 represents the DWT form of the cropped image.

Fig 7: DWT representation

After the cropped image is generated it is merged to form the original image and it is used as the stego image.The cropped value is stored in a variable for the process of extaction.

## 3 Related Work

Anjali et al. [5] perform the skin tone detection mechanism, with cropping and without cropping cover image. The skin region is detected using the HSV color space. The cover image is then transformed into frequency domain using Haar- DWT and after that payload is calculated. Then secret data embedding is done in high frequency sub-band by tracing the skin pixels. A comparative study is done on cropping and without cropping case. Both of them uses different embedding algorithm. In cropping case the cover image is cropped and then the above operations are performed. In the decoding side the cropping image acts as the key. In without cropping case, the embedding algorithm tries to preserve the histogram of DWT coefficients even after hiding data. This ensured protection from histogram based first order statistical attacks. It was concluded that both methods provide enough security.

Sunitha et al. [6] perform the skin tone detection by segmenting the skin pixels using masking and filtering mechanism. Masking refers to covering the non skin region with black and filtering refers to replacing the white region with skin color. After performing this, a particular region of the skin is selected to embed the data. The data is embed in the selected region, and then a 2D wavelet transform is performed in the selected region of interest. After this a particular sub band is selected to embed the data. As this method uses two keys and IDWT on the encoder side, it provides a three level robustness. This helps to prevent the steganalysis attacks.

Souvik Bhattacharya et al.[7]used spatial domain ste anographic technique for embedding biometric information in bit stream format.To make the steganalysis more difficult the steganography process has been occurs by using series for embedding space selection and message is embedded with the polynomial function.The secret message not embedded directly.The skin color detection is performed using HSV color space.

Sameer M. Khupse et al.[8] perform the embedding of the data in the skin region of a video frame. They concentrate on the skin detection algorithm to extract the skin region. This acts as the region of interest for embedding the secret message. To perform embedding the video frames are converted to YCbCr color space. The frame having least MSE is selected to embed secret data. The secret data is then inserted into the chrominance component (Cr or Cb) of YCbCr of a frame which has least MSE. After embedding secret data, steganoflage video is created by transforming the data into RGB colour space. Secure transmission of secret message can be achieved through steganoflage video.

## 4 Proposed Work

Proposed method is that instead of using image as the cover medium video is used.The advantage of using is video as cover medium is that it is possible to hide more messages using different frames.Another advantage is that PSNR is good compared to image. In the embedding phase video is converted in to different frames and stored in a buffer as image. Choose one frame and perform skin detection using HSV (Hue, Saturation and Value) color space. The region from skin detected area is selected, which is known as the cropped region. In this cropped region the secret message which is the image is embedded using DWT (Discrete Wavelet Transform).Secret data embedding is performed in one of the high frequency sub-band by tracing skin pixels in that band. Cropped region works as a key at decoding side. Cropped value and the frame where the message is embedded is stored. The cropped one containing message is then merged to form the original frame and it is referred to as the stego frame. Then it is combined with other frames to form the stego video. In the extraction phase, the stego video is then converted in to frames and stored in the buffer. Choose the frame based on the stored value.The skin detection on that frame is performed using HSV.The cropped region based on the stored value is used to crop the frame. Apply DWT on the frame. Then the secret message is extracted.

### 4.1 Encoding Phase

Suppose the cover medium is video of M×N size and secret data is image of size a×b.

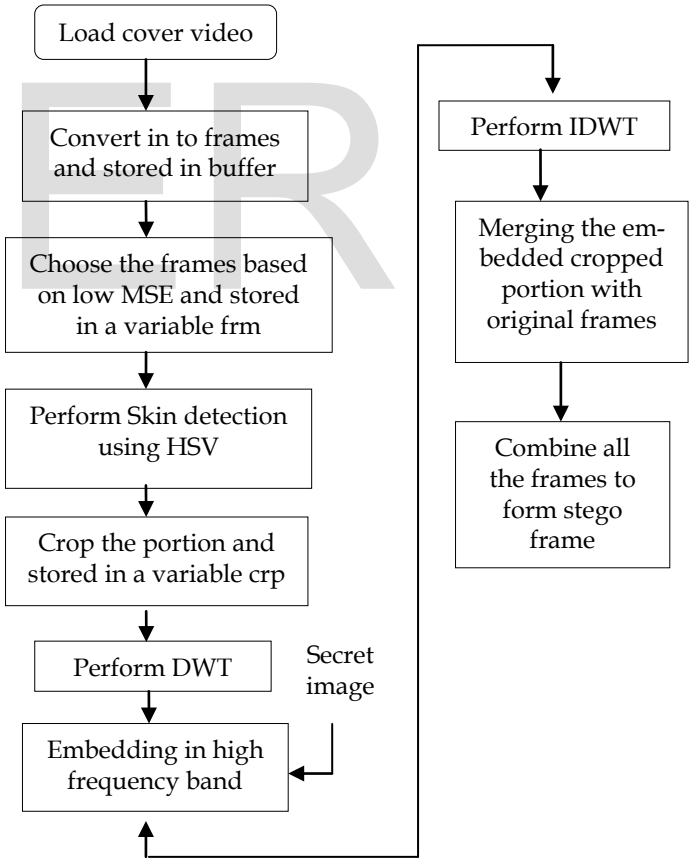


Fig 8: Flowchart of encoding phase

Step 1: Load the cover video which is format .avi
Step 2: Convert the loaded cover video in to different frames and stored in a buffer.

Step 3: Choose the frames based on the low MSE which is the sorted one and stored in a variable to use for extraction procedure.
Step 4: Perform skin detection for the frames that is choosen using HSV color space.
Step 5: After performing skin detection crop the skin portion.
Step 6: Load the secrete image.
Step 7: Perform DWT on the cropped image and embed the secret image in the high frequency band.
Step 8: Perform IDWT.
Step 9: Merge the cropped region having secret data with the original one.
Step 10: Combine all the frames to generate the stego video.

### 4.2 Decoding Phase

Step 1: Load the stego video.
Step 2: Convert the loaded stego video in to different frames and stored in a buffer.
Step 3: Based on the stored value frm choose the frames.
Step 4: Perform skin detection for the frames.
Step 5: Crop the frames based on the stored value crp.
Step 6: Perform DWT.
Step 7: Extract the secret message.

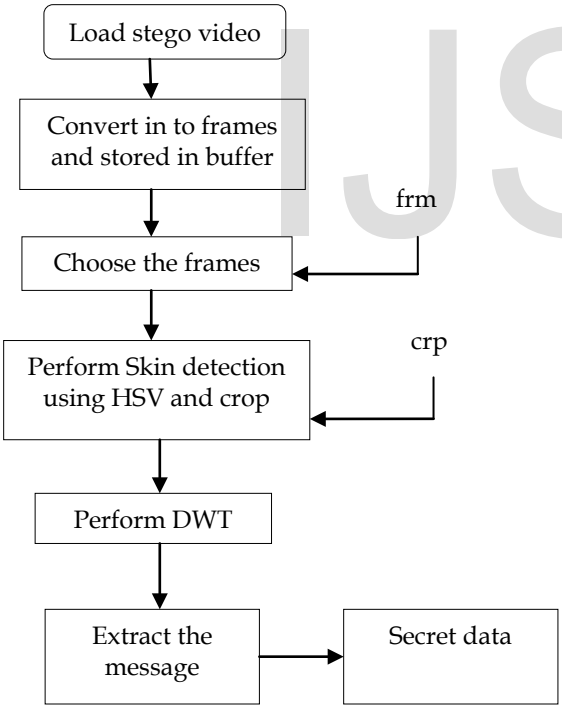


Fig 9: Flowchart of the decoding phase

## 5 Simulation Results

Here the simulation result regarding the proposed method is shown.This is implemented using Matlab 2013a.
Cover video is of size 288 height and 386 width and secret image of different size is taken.
We choose six frames and six secret images.

Fig 10: Cover video

Fig 11: Skin detection of the frames that choose based on low MSE

Fig 12: Cropping the frames

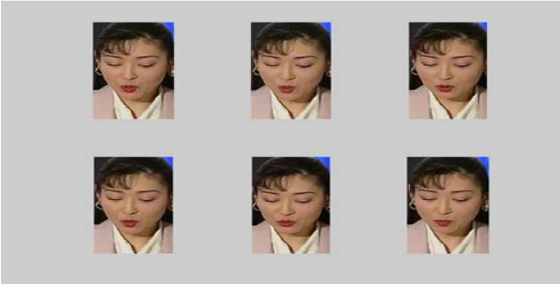

Fig 13: Representing the cropped frames

Fig 14: Secret images

Parameters to determine the performance of steganography are:

*Peak Signal to Noise Ratio (PSNR)*: This is calculated in order to determine the quality of the stego medium after the message is embedded. It is given by equation.

$$PSNR = 10log_{10}{}^{max^2}/_{MSE}$$

*max* is the maximum value of pixels (255 for gray scale images). A greater PSNR value indicates the better quality. It is expressed in decibels (dB).

*Mean Square Error (MSE)*: MSE is the mean square error between the original and stego medium.
It is given by the equation

$$MSE = \frac{1}{MXN}\sum_{i=1}^{M}\sum_{j=1}^{N}\|O(i,j) - D(i,j)\|^2$$

The MSE value for the image=3.3315
The PSNR value for the image=42.9044

The MSE value for the video=3.0048
The PSNR value for the video=43.3527

For the case of video the PSNR is slightly better than the image.

Fig 15: Stego video

Fig 16: Extracted secret images

## 6 Conclusion

Steganography is the interesting method that performs in this digitized world along with the biometrics to embed the message in the cover medium.The existing system is that image is used as the cover medium to hide the secret message by performing skin detection.The problem with this method is that it is not possible to hide more messages. The proposed system is that instead of using image as the cover medium, video is used.The advantage is that it is possible to hide more message using different frames. The quality of the stego video is good compared with the stego image.

## Acknowledgment

We are greatly thankful to our principal,Dr. JAYAMOHAN J, Dr. V GOPAKUMAR, Head of the Department of Computer Science and Engineering, Mr. MANOJ KUMAR G, Associate Professor, Department of Computer Science and Engineering, for their support in the successful completion of this paper.

## References

[1] Christian Rathgeb and Andreas Uhl., "A survey on biometric cryptosystems and cancellable biometrics", EURASIP, 2011. W.-K. Chen, *Linear Networks and Systems*. Belmont, Calif.: Wadsworth, pp. 123-135, 1993. (Book style)

[2] Mr. R.Surendiran and Dr. K. Alagarsamy., "Skin detection based cryptography in steganography", IJCSIT,2010.

[3] Rupa Maan and Lovneesh Bansal,"Comparison and Implementation of Biometric Inspired Digital Image Steganography",IJCST,Vol.3,Dec,2012.

[4] Rafael C. Gonzalez and Richard E. Woods, "Digital Image Processing", Third Edition, Prentice Hall, 2008.

[5] Anjali A Shejul and Umesh L Kulkerni,"A Secure Skin tone based Steganography using wavelet transforms",IJCTE,Vol 3.Feb 2011.

[6] Sunita Barve, Uma Nagaraj and Rohit Gulabani.,"Efficient and Secure Biometric Image Steganography using Discrete Wavelet Transform",IJCSCN,Vol 1,Oct 2011.

[7] Souvik Bhattacharyya, Indradip Banerjee, Anumoy Chakraborty and Gautam Sanyal.,"Biometric Steganography Using Variable Length Embedding",IJCEACIE,Vol.8,2014

[8] Sameer M. Khupse and Sneha K. Deshmukh.,"Video Steganography Technique using Skin Tone based Embedding in Chrominance Component of YCbCr Color Space",MEDHA 2015.