# A Secure Skin Tone based Steganography Using Wavelet Transform 

Anjali A. Shejul, Umesh L. Kulkarni


#### Abstract

Steganography is the art of hiding the existence of data in another transmission medium to achieve secret communication. Steganography method used in this paper is based on biometrics. And the biometric feature used to implement Steganography is skin tone region of images [1]. Here secret data is embedded within skin region of image that will provide an excellent secure location for data hiding. For this skin tone detection is performed using HSV (Hue, Saturation and Value) color space. Additionally secret data embedding is performed using frequency domain approach DWT (Discrete Wavelet Transform), DWT outperforms than DCT (Discrete Cosine Transform). Secret data is hidden in one of the high frequency sub-band of DWT by tracing skin pixels in that sub-band. For data hiding two cases are considered, first is with cropping and other is without cropping. In both the cases different steps of data hiding are applied either by cropping an image interactively or without cropping i.e. on whole image. Both cases are compared and analyzed from different aspects. This is concluded that both cases offer enough security. Main feature of with cropping case is that this results into an enhanced security because cropped region works as a key at decoding side. Where as without cropping case uses embedding algorithm that preserves histogram of DWT coefficient after data embedding also by preventing histogram based attacks and leading to a more security. This study shows that by adopting an object oriented steganography mechanism, in the sense that, we track skin tone objects in image, we get a higher security. And simulation result shows that satisfactory PSNR (Peak-Signal-to-Noise Ratio) is also obtained.


Index Terms—Biometrics, DCT, DWT, PSNR, Security, Skin tone detection, With Cropping, Without Cropping.

## I. INTRODUCTION

In this highly digitalized world, the Internet serves as an important role for data transmission and sharing. However, since it is a worldwide and publicized medium, some confidential data might be stolen, copied, modified, or destroyed by an unintended observer. Therefore, security problems become an essential issue. Encryption is a well-know procedure for secured data transmission [2]. Although encryption achieves certain security effects, they make the secret messages unreadable and unnatural.

Manuscript received April 11, 2010.
Anjali A. Shejul is with the Department of Computer Engineering, University of Mumbai, Maharashtra, India. (e-mail: anjalishejul123@gmail.com)

Umesh L. Kulkarni is with the Department of Computer Engineering, University of Mumbai, Maharashtra, India. (e-mail:kumeshl@rediffmail.com)

These unnatural messages usually attract some unintended observers' attention. This is the reason a new security approach called "steganography" arises.

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. In this paper covers and secret messages are restricted to being digital images. The cover-image with the secret data embedded is called the "Stego-Image". The Stego-Image should resemble the cover image under casual inspection and analysis. In addition, for higher security requirements, we can encrypt the message data before embedding them in the cover-image to provide further protection [3]. For this the encoder usually employs a stego-key which ensures that only recipients who know the corresponding decoding key will be able to extract the message from a stego-image. For proposed method cover image is cropped interactively and that cropped region works as a key at decoding side yielding improved security.

While designing the steganographic system, invisibility factor i.e. human eyes should not distinguish the difference between original and stego image should be considered. Next subsection gives difference between two data hiding branches, Steganography and Watermarking.

## A. Steganography and Watermarking

Steganography and Watermarking both are branches of data hiding but they are used for different purposes. Watermarking is very similar to Steganography in a number of respects. Both seek to embed information inside a cover message with little to no degradation of the cover-object. Digital watermarking is the technique of embedding digital marks inside a container so that there is a logical way of extracting the data embedded, while not harming the container in any perceived way. Steganography uses cover files to deliver its messages. On the other hand watermarking considers the cover file as the important data that is to be preserved. In Steganography purpose of embedded data is to deliver secret communication. In watermarking, purpose of embedded data is to supply some additional information about the cover image such as image owner to verify image's ownership to achieve control over the copy process of digital data. In Steganography, the object of communication is the hidden message. In digital water-marks, the object of communication is the cover. In short, Steganography pay attention to the degree of invisibility while Watermarking pay most of its attribute to the robustness of the message and its ability to withstand attacks of removal, such as image operations(rotation, cropping, filtering) [4].

A compromise between the embedding capacity,
robustness and undetectability exists and can be decided before carrying out the communication. Fig. 1 shows trade off between capacity, robustness, undetectability and shows where Steganography and Watermarking resides.


Figure 1. Trade off between Embedding capacity, Robustness and Undetectability in Data Hiding

This paper focuses on method of Steganography and not Watermarking.

Rest of the paper is organized as follows. Section II presents related work and theoretical background. In section III proposed method is described in detail with encoding, skin tone detection, DWT and decoding procedure step by step for both cases with and without cropping. Section IV demonstrated the experimental results. Finally conclusions are provided in section V .

## II. Related Work

## A. LSB(Least significant Bit) Substitution based Steganography

Here spatial features of image are used. This is a simplest steganographic technique that embeds the bits of secret message directly into the least significant bit (LSB) plane of the cover image. In a gray-level image, every pixel consists of 8 bits. The basic concept of LSB substitution is to embed the confidential data at the rightmost bits (bits with the smallest weighting) so that the embedding procedure does not affect the original pixel value greatly [5]. The mathematical representation for LSB is:

$$
\begin{equation*}
\mathrm{x}_{\mathrm{i}}^{\prime}=\mathrm{x}_{\mathrm{i}}-\mathrm{x}_{\mathrm{i}} \bmod 2^{\mathrm{k}}+\mathrm{m}_{\mathrm{i}} \tag{1}
\end{equation*}
$$

In Equation (1), $x_{i}{ }^{\prime}$ represents the $i^{\text {th }}$ pixel value of the stego-image and $x_{i}$ represents that of the original cover-image. $m_{i}$ represents the decimal value of the $i^{\text {th }}$ block in the confidential data. The number of LSBs to be substituted is k . The extraction process is to copy the k-rightmost bits directly. Mathematically the extracted message is represented as in Equation (2).

$$
\begin{equation*}
\mathrm{m}_{\mathrm{i}}=\mathrm{x}_{\mathrm{i}} \bmod 2^{\mathrm{k}} \tag{2}
\end{equation*}
$$

Hence, a simple permutation of the extracted $m_{i}$ gives us the original confidential data [6]. This method is easy and straightforward but this has low ability to bear some signal processing or noises. And secret data can be easily stolen by extracting whole LSB plane.

## B. Transform Domain based Steganography

Robustness of steganography can be improved if properties of the cover image could be exploited. Taking these aspects into consideration working in frequency domain becomes more attractive. Here, sender transforms the cover image into frequency domain coefficients before embedding secret messages in it [7]. Different sub-bands of frequency domain coefficients give significant information about where vital and non vital pixels of image resides. Using
transform-domain techniques it is possible to embed a secret message in different frequency bands of the cover. Embedding in the high frequencies creates less impact on the perceivability of the media but provide low robustness to different attacks. In contrast, embedding in the lower frequencies helps to withstand many attacks but creates perceptible impact on the media. So, middle frequency bands offers excellent location for data hiding. These methods are more complex and slower than spatial domain methods; however they are more secure and tolerant to noises. Frequency domain transformation can be applied either in DCT or DWT.

## C. Adaptive Steganography

Adaptive steganography is special case of two former
methods. It is also known as "Statistics aware embedding"
[8] and "Masking" [3]. This method takes statistical global features of the image before attempting to embed secret data in DCT or DWT coefficients. The statistics will dictate where to make changes.

## III. Proposed Method

Proposed method introduces a new method of embedding secret data within skin region as it is not that much sensitive to HVS (Human Visual System) [1]. This takes advantage of biometrics features such as skin tone, instead of embedding data anywhere in image, data will be embedded in selected regions. Overview of method is briefly introduced as follows. At first skin tone detection is performed on input image using HSV (Hue, saturation, value) color space. Secondly, cover image is transformed in frequency domain. This is performed by applying

Haar-DWT, the simplest DWT on image leading to four sub-bands. Then payload (number of bits in which we can hide data) is calculated. Finally, secret data embedding is performed in one of the high frequency sub-band by tracing skin pixels in that band. All these embedding steps are applied to two cases: a] With Cropping b] Without Cropping. Comparison and analysis of both cases is done. For the with cropping case before performing all above mentioned embedding steps cropping on input image is performed and then in only cropped region data hiding is performed, not in whole image. Cropped region works as a key at decoding side so cropping results into more security. Both cases uses different embedding algorithm. In without cropping case, embedding algorithm attempts to preserve histogram of DWT coefficients after embedding also. This protects from histogram based first order statistics attacks. Ultimately it is observed that both the cases provide enough security. In both cases embedding process affects only certain Regions of Interest (ROI) rather than the entire image. So utilizing objects within images can be more advantageous. This is also called as Object Oriented steganography [1]. Next sub-sections describe encoding, decoding process in detail and briefly introduce skin tone detection and DWT.

## A. Encoding Process

Suppose C is original 24-bit color cover image of $M \times N$ size. It is denoted as:
$\mathrm{C}=\{x i j$, yij, zij $\mid 1 \leq \mathrm{i} \leq \mathrm{M}, 1 \leq \mathrm{j} \leq \mathrm{N}, \mathrm{xij}$, yij, zij $\in\{0,1, . .$, 255\} \}

Let S is secret data. Here secret data considered is binary image of size $\mathrm{a} \times \mathrm{b}$. As encoding process considers two cases, with cropping and without cropping, both cases are described in detail below.

## 1) Case 1-With Cropping:

Flowchart for this case is shown in Fig. 2 and different steps are discussed in detail. Let size of cropped image is $M_{c} \times N_{c}$ where $M_{c} \leq M$ and $N_{c} \leq N$ and $M_{c}=N_{c}$. i.e. Cropped region must be exact square as we have to apply DWT later on this region.


Figure 2. Flowchart of With Cropping case of Embedding Process
a) Step 1: Once image is loaded, apply skin tone detection on cover image. This will produce mask image that contains skin and non skin pixels. Skin tone detection is discussed in coming subsection.
b) Step 2: Ask user to perform cropping interactively on mask image $\left(\mathrm{M}_{\mathrm{c}} \times \mathrm{N}_{\mathrm{c}}\right)$. Then original image is also cropped of same area. Cropped area must be in an exact square form as we have to perform DWT later and cropped area should contain skin region such as face, hand etc since we will hide data in skin pixels of one of the sub-band of DWT. Here cropping is performed for security reasons. Cropped rectangle will act as key at receiving side. If it knows then only data retrieval is possible. Eavesdropper may try to perform DWT on whole image; in such a case attack will fail as we are applying DWT on specific cropped region only.
c) Step 3: Apply DWT to only cropped area $\left(\mathrm{M}_{\mathrm{c}} \times \mathrm{N}_{\mathrm{c}}\right)$ not whole image $(\mathrm{M} \times \mathrm{N})$. This yields 4 sub-bands denoted as $\mathrm{H}_{\mathrm{LL}}, \mathrm{H}_{\mathrm{HL}}, \mathrm{H}_{\mathrm{LH}}, \mathrm{H}_{\mathrm{HH}}$. (All 4 sub-bands are of same size of $\mathrm{M}_{\mathrm{c}} / 2$, $\mathrm{N}_{\mathrm{c}} / 2$ ). Payload of image to hold secret data is determined based on number of skin pixels present in one of high frequency sub-band in which data will be hidden.
d) Step 4: Perform embedding of secret data in one of sub-band that we obtained earlier by tracing skin pixels in that sub-band. Other than the low frequency sub-band (LL) any high frequency sub-band can be selected for embedding as LL sub-band contains significant information. Embedding
in LL sub-band affects image quality greatly. We have chosen high frequency HH sub-band. While embedding, secret data will not be embedded in all pixels of DWT sub-band but to only those pixels that are skin pixels. So here skin pixels are traced using skin mask detected earlier and secret data is embedded. Embedding is performed in G-plane and B-plane but strictly not in R-plane as contribution of R plane in skin color is more than $G$ or $B$ plane. So if we are modifying R plane pixel values, decoder side doesn't retrieve data at all as skin detection at decoder side gives different mask than encoder side.

Embedding is done as per raster-scan order (as shown in Fig.3) that embeds secret data coefficient by coefficient in selected sub-band [6], if coefficient is skin pixel. While embedding bits of one of the sub-band are replaced with bits of secret data.


Figure 3. Raster Scan Order
e) Step 5: Perform IDWT to combine 4 sub-bands.
f) Step 6: A cropped stego image of size $\mathrm{M}_{\mathrm{c}} \times \mathrm{N}_{\mathrm{c}}$ is obtained in above step (step 5). This should be similar to original image after visual inspection but at this stage it is of size $\mathrm{M}_{\mathrm{c}} \times$ $\mathrm{N}_{\mathrm{c}}$, So we need to merge the cropped stego image with original image to get the stego image of size $M \times N$. To perform merging we require coefficients of first and last pixels of cropped area in original image so that $r$ calculated.

Thus a stego image is ready for quality evaluation.
Case 2- Without Cropping:
Most of embedding steps of this case are same as per with cropping case. Major difference in this case is that all the steps of embedding are not performed on cropped region but performed to whole image without applying any cropping. And other major difference is that actual embedding algorithm i.e. the way in which we are replacing bits of cover image to bits of secret image (data) is different in this case. The main intention of using this different embedding algorithm is to hide data such that the histogram of the cover image shouldn't not get modified after embedding, in other words first order statistics of the DWT coefficients should be preserved. This requires an embedding procedure which does not modify the pixel values such that the corresponding bin value in the histogram is changed. We used a simple yet effective algorithm in which message bits are embedded into the cover image without making any modifications to the image histogram. All the steps of encoding using this case are listed below:
a) Step 1: Apply skin tone detection.
b) Step 2: Separate R, G, B planes and apply DWT to B plane, this leads into 4 sub-bands denoted as $H_{L L}, H_{H L}, H_{L H}$, $\mathrm{H}_{\mathrm{HH}}$. As embedding is performed in one of the obtained high frequency sub-band let it HH , skin pixels from this sub-band are retrieved and stored in one matrix.
c) Step 3: Apply embedding algorithm to retrieved matrix containing only skin pixels. In this matrix of skin pixels, start
from first pixel and using pseudorandom sequence its corresponding pixel for pair is found. In the same way other skin pixel pairs are formed. To create a pseudo random sequence Lehmer's Congruential generator is used that generates non overlapping random sequence. Lehmer invented the multiplicative congruential algorithm, which is the basis for many of the random number generators in use today. Lehmer's generators involve three integer parameters, $a, c$, and $m$, and an initial value, $x 0$, called the seed. A sequence of integers is shown in Equation (3).

$$
\begin{equation*}
\mathrm{x}_{\mathrm{k}+1}=\mathrm{ax}_{\mathrm{k}}+\mathrm{c} \bmod \mathrm{~m} \tag{3}
\end{equation*}
$$

Once pairs are formed secret message bits are embedded based on values of pixel pairs. Each message bit is related with one pair. For embedding 0 , check if the first pixel of pair is less than other pixel, if it is then don't change anything otherwise swap gray level values. Similarly pixel value of 1 can be embedded by making the value of first pixel greater than the second pixel. All skin pixels pairs chosen are skin pixels as we have to hide data in only skin pixels. Note that values of pixels are altered but in this way that total count of gray vales in image should remain same. As pixel gray values are not modified, count will remain same leading to an unchanged histogram. This embedding algorithm is described below:
Input- matrix of only skin pixels, let it is S and secret message bits of size M

Output- Modified matrix of only skin pixels
Begin
1] Select non-overlapping, random pair from S . Let it is p 1 , p2.

If count (message bits) $=\mathrm{M}$ then
goto End
Else
goto step 2
2] if $\mathrm{p} 1=\mathrm{p} 2$ then
goto step 1 (choose other pair.)
3] if $\mathrm{p} 1 \neq \mathrm{p} 2$ then
goto step 4.
4] if message bit $=0$ then
if $\mathrm{p} 1>\mathrm{p} 2$ then
swap (p1,p2).
Choose next message bit.
Else Choose next message bit.
goto step 1.
5] if message bit=1 then
if $\mathrm{p} 1<\mathrm{p} 2$ then
swap(p1,p2)
Choose next message bit.
else Choose next message bit.
goto step 1.
End
This embedding algorithm is not used in with cropping case as its main drawback is that is reduces payload by half and because of cropping already we have less region to hide data in with cropping case.
d) Step 4: This modified matrix of only skin pixels is restored in HH sub-band. So HH sub-band that contains hidden data is obtained. Finally, all sub-bands are merged by applying IDWT and all planes are also merged leading to a stego image for quality evaluation.

Next section gives introduction of skin tone detection and DWT performed in encoding process.

## B. Skin Color Tone Detection using HSV

The goal of skin color detection is to build decision rule that will discriminate between skin and non-skin pixels. A skin detector typically transforms a given pixel into an appropriate color space and then uses a skin classifier to label the pixel whether it is a skin or a non-skin pixel [9].

The skin detection algorithm produces a mask, which is simply a black and white image. The black pixel values are 0 (false) and the white pixel values are 1 (true). This mask of ones and zeros acts as a logic map for skin detection (i.e., if a pixel is 1 this pixel location is likely skin). The simplest way to decide whether a pixel is skin color or not is to explicitly define a boundary. RGB (Red, Green, Blue) matrix of the given color image can be converted into different color spaces to yield distinguishable regions of skin or near skin tone. Mainly two kinds of color spaces are available HSV (Hue, Saturation and Value) and YCbCr (Yellow, Chromatic Blue, Chromatic red) spaces. For this work HSV color space is chosen. It is experimentally found and theoretically proven that the distribution of human skin color constantly resides in a certain range within the color space [1]. Yang and Waibel [10] are able to achieve skin tracking by dimensional reduction of the available color space.
In this work, skin detection is performed using HSV color space. For this convert RGB image into HSV color space. In HSV, responsible vales for skin detection are Hue \& Saturation so extract the Hue and Saturation dimensions into separate new variables (H \& S). For skin detection threshold should be chosen as [H1, S1] \& [H2, S2]. A pixel is classified as skin pixel if the values $[\mathrm{H}, \mathrm{S}]$ fall within the threshold. Threshold is predefined range associated with the target skin pixel values. Most of the researchers determined threshold as h_range $=[0,0.11]$ and s_range $=[0.2,0.7]$. Sobottaka and Pitas [11] defined a face localization based on HSV. They found that human flesh can be an approximation from a sector out of a hexagon with the constraints:
$\mathrm{S}_{\text {min }}=0.23, \operatorname{Smax}=0.68, \mathrm{H}_{\min }=0^{\circ}$ and $\mathrm{H}_{\max }=50^{\circ}$.

## C. Discrete Wavelet Transform (DWT) and Haar-DWT

This is one of the frequency domain in which Steganography can be implemented. In this work DWT is used as it performs better than the DCT. DCT is calculated on blocks of independent pixels, a coding error causes discontinuity between blocks resulting in annoying blocking artifact. This drawback of DCT is eliminated using DWT. DWT applies on entire image. DWT offers better energy compaction than DCT without any blocking artifact. DWT splits component into numerous frequency bands called sub bands known as
LL - Horizontally and vertically low pass
LH - Horizontally low pass and vertically high pass
HL - Horizontally high pass and vertically low pass
HH - Horizontally and vertically high pass
Since Human eyes are much more sensitive to the low frequency part (LL sub-band) we can hide secret message in other three parts without making any alteration in LL sub-band [12]. As other three sub-bands are high frequency
sub-band they contain insignificant data. Hiding secret data in these sub-bands doesn't degrade image quality that much. In this work, we use simplest DWT, Haar-DWT, to transform images into frequency domain.

1) Advantages of Haar Wavelet transform as follows:

- Best performance in terms of computation time.
- Computation speed is high.
- Simplicity.

It performs two steps, row and column transformation respectively. Entire row of an image matrix is taken, then do the averaging, differencing is done. After we treated entire row of an image matrix, then do the averaging and differencing process for the entire each column of images.
2) Procedure for Haar Wavelet Transform: To calculate the Haar transform of an array, procedure is given below [13].

- Find the average of each pair of samples.
- Find the difference between each average and the samples it was calculated from.
- Fill the first half of the array with averages.
- Fill the second half of the array with differences.
- Repeat the process on the first half of the array.

Haar-DWT can be performed using matrix multiplication. If $A$ is matrix on which we want to perform Haar-DWT, row transformation is performed using $\mathrm{Q}=\mathrm{A} \times \mathrm{P}$. Where $\mathrm{P}=\left[\begin{array}{llllllllllll}1 & 0 & 1 & 0 & 1 & 0 & -1 & 0 & 0 & 1 & 0 & 1 ;\end{array} 010-1\right]$. Output of row transformation becomes input at column transformation. Column transformation is obtained using $R=P^{\prime} \times Q$ where $P^{\prime}$ is transpose of P . Matrix P performs averaging and differencing operation. After completing all the steps we obtain four sub-bands.

Example of Haar-DWT: Numerical example of Haar-DWT is shown in Fig. 4

| 20 | 15 | 30 | 20 |
| :--- | :--- | :--- | :--- |
| 17 | 16 | 31 | 22 |
| 15 | 18 | 17 | 25 |
| 21 | 22 | 19 | 18 |
| (a) |  |  |  |$\hookrightarrow$| 68 | 103 | 6 | 19 |
| :--- | :--- | :--- | :--- |
| 76 | 79 | -4 | -7 |
| 2 | -3 | 4 | 1 |
| -10 | 5 | -2 | -9 |

Figure 4. (a) Original Matrix (b) Resulted sub-bands after Haar-DWT

## D. Decoding Process

All steps of Decoder are opposite to Encoder. 24 bit color stego image of size $\mathrm{M} \times \mathrm{N}$ is input to decoding process. Decoding process for with and without cropping case is explained below. Flowchart shows different steps for both cases. This is shown in Fig. 5

1) Case 1-With Cropping:

In this case we must need a value of cropped area to retrieve data. Suppose cropped area value is stored in 'rect' variable that is same as in encoder. So this 'rect' will act as a key at decoder side. Care must be taken to crop same size of square as per Encoder. By tracing skin pixels in $\mathrm{H}_{\mathrm{HH}}$ sub-band of DWT secret data is retrieved.
2) Case 2- Without Cropping:

In this case without performing cropping extraction of secret data is performed. As encoder uses different
embedding algorithm than with cropping case, same logic of embedding algorithm is used for decoding. This requires finding skin pixel pairs that are used for embedding. These pixel pairs are found by generating non-overlapping, random sequence using Lehmer's Congruential generator. Once correct pixel pairs are found, based on their values either one or zero of secret data is decided.


Figure 5. Flowchart of Decoding Process

## IV. Simulation Results

In this section we demonstrate simulation results for proposed scheme.This have been implemented using MATLAB 7.0.

A 24 bit color image is employed as cover-image of size $356 \times 356$, shown in Fig. 6. Fig. 7 and Fig. 8 shows sample secret images to hide inside cover image for with cropping and without cropping case respectively.


Figure 6. Cover Image


Figure 7. Image to hide for case with cropping


Figure 8. Image to hide for case without cropping

The secret images are of size $32 \times 32$.
We use Peak signal to noise ratio (PSNR) to evaluate quality of stego image after embedding the secret message. The performance in terms of capacity and PSNR (in dB) is demonstrated for the method in the following subsections. PSNR is defined as per Equation (4) and Equation (5).

$$
\begin{align*}
& \text { PSNR }=10 \log _{10}\left(255^{2} / \mathrm{MSE}\right),  \tag{4}\\
& \mathrm{M} \\
& \text { Where, } \mathrm{MSE}=(1 /(\mathrm{M} \times \mathrm{N})) \sum \sum\left(\mathrm{x}_{\mathrm{ij}}-\mathrm{y}_{\mathrm{ij}}\right)^{2} \tag{5}
\end{align*}
$$

$$
\mathrm{i}=1 \quad \mathrm{j}=1
$$

$\mathrm{x}_{\mathrm{ij}}$ and $\mathrm{y}_{\mathrm{ij}}$ represents pixel values of original cover image and stego image respectively. The calculated PSNR usually adopts dB value for quality judgement, the larger PSNR is, higher the image quality (which means there is a little difference between cover image and stego image). On the contrary smaller dB value means there is a more distortion. PSNR values falling below 30 dB indicate fairly a low quality. However, high quality strives for 40 dB or more [1].

## A. Performance of the proposed method

For with cropping case, after embedding secret data in cropped image, resulted cropped stego image is shown in Fig. 9(a). (Result of step 5 of encoding process of with cropping case). As this doesn't look like cover image merging is performed to obtain final stego image that is shown in Fig. 9(b). (Result of step 6 of encoding process of with cropping case). For merging co-ordinates of first and last pixels of cropped image in original image are calculated. After performing decoding process on stego image obtained in with cropping case, retrieved image is shown in Fig. 9(c). Same proposed method is implemented for without cropping case. In without cropping case secret data is hidden in one of the sub-band which is obtained by performing the DWT on whole image and not only to cropped region and by applying new embedding algorithm described earlier for preservation of histogram. Resultant stego image obtained in without cropping case is shown in Fig. 10(a). It is observed that this preserves histogram of DWT coefficients after embedding also. After performing decoding on this stego image, retrieved secret image is shown in Fig. 10(b). PSNR is calculated for four different final stego images resulted from a considered image and three more sample images, here secret image used for embedding is shown in Fig. 8. PSNR for with and without cropping case is shown in table 1. Average PSNR of proposed method is calculated based on the obtained PSNR.

Performing biometric steganography with cropping or without cropping, both offer respectable level of security. With cropping case ensures security as decoder requires cropped region for secret data extraction, so cropped region works as a key at decoder side. By adopting embedding algorithm that preserves histogram of DWT coefficients after embedding, without cropping prevents histogram based attacks. Reason for not using this embedding algorithm in with cropping case is that as algorithm reduces payload by half and with cropping case already reduces skin region because of cropping. After using this embedding algorithm in with cropping case there is higher possibility that this may not fulfill real time requirements. It is observed that PSNR of without cropping case is more than with cropping case.


(c)

Figure 9 (a) Cropped Stego Image (b) Final Stego Image (c) Retrieved Image for Case- With Cropping

(a)

(b)

Figure 10 (a) Stego Image (b) Retrieved Image for Case - Without Cropping
TABLE 1. CAPACITY AND PSNR OF 4 FINAL STEGO IMAGES IN PROPOSED METHOD.
Case A- Without Cropping, Case B- With Cropping

| Cover <br> Image <br> (356 $\times$ <br> 356) | Capacity of <br> Cover <br> Image |  | PSNR |  |
| :---: | :--- | :--- | :--- | :--- |
|  | Case B | Case A | Case B |  |
| Image 1 | 7173 | 6006 | 64.92 | 55.68 |
| Image 2 | 2407 | 2244 | 53.75 | 48.19 |
| Image 3 | 1452 | 1310 | 52.65 | 48.15 |
| Image 4 | 4850 | 2572 | 54.38 | 45.4 |
| Average PSNR | 56.42 | 49.35 |  |  |

## V. Conclusion

Digital Steganography is a fascinating scientific area which falls under the umbrella of security systems. In this paper Biometric Steganography is presented that uses skin region of images in DWT domain for embedding secret data. By embedding data in only certain region (here skin region) and not in whole image security is enhanced. Two cases for data embedding are considered, with cropping and without cropping. It is ob served that both offer enough security. In with cropping case no one can extract message without having value of cropped region. Where as without cropping case uses embedding algorithm that preserves histogram of DWT coefficients after embedding also and prevents histogram based attacks. According to simulation results, proposed approach provides fine image quality.

## Acknowledgment

The authors would like to thank to the earlier work regarding Steganography whose guidance significantly contributed to the work made in this paper. All work done, images shown in this paper are for educational purpose and not for commercial purpose.

## References

[1] A. Cheddad, J. Condell, K. Curran and P. Mc Kevitt, "Biometric inspired digital image Steganography", in: Proceedings of the 15th Annual IEEE International Conference and Workshops on the Engg.of Computer-Based Systems (ECBS’08), Belfast, 2008, pp. 159-168.
[2] Petitcolas, F.A.P.: "Introduction to Information Hiding". In: Katzenbeisser, S and Petitcolas, F.A.P (ed.) (2000) Information hiding Techniques for Steganography and Digital Watermarking. Norwood: Artech House, INC.
[3] Johnson, N. F. and Jajodia, S.: "Exploring Steganography: Seeing the Unseen." IEEE Computer, 31 (2): 26-34, Feb 1998.
[4] Chris Shoemaker, "Hidden Bits: A Survey of Techniques for Digital Watermarking" Independent Study EER-290 Prof Rudko Spring 2002
[5] Fridrich, J., Goljan, M. and Du, R.., (2001). "Reliable Detection of LSB Steganography in Grayscale and Color Images." Proceedings of ACM, Special Session on Multimedia Security and Watermarking, Ottawa, Canada, October 5, 2001, pp. 27-30.
[6] Po-Yueh Chen and Hung-Ju Lin "A DWT Based Approach for Image Steganography", International Journal of Applied Science and Engineering, 2006. 4, 3: 275-290
[7] Chang, C. C., Chen, T.S and Chung, L. Z., "A steganographic method based upon JPEG and quantization table modification," Information Sciences, vol.[4], pp. 123-138(2002).
[8] Provos,N. and Honeyman, P: "Hide and Seek: An introduction to steganography". IEEE security and privacy, 01 (3): 32-44,May-June 2003
[9] Ahmed E., Crystal M. and Dunxu H.: "Skin Detection-a short Tutorial", Encyclopedia of Biometrics by Springer-Verlag Berlin Heidelberg 2009
[10] Yang, J., \& Waibel, a. (1996). A real-time face tracker. Proceedings of the 3th IEEE Workshop on Applications of Computer Vision, Sarasota, Florida, 142-147
[11] Sobottka, K. and Pitas, I.:"Extraction of facial regionsand features using color and shape information." Proc. IEEE International Conference on Image Processing, pp. 483-486.(1996)
[12] Chen,P. Y.and Liao,E.C., :A new Algorithem for Haar Wavelet Transform," 2002 IEEE International Symposium on Intelligent Signal Processing and Communication System, pp.453-457(2002).
[13] P. Raviraj and M.Y. Sanavullah,"The Modified 2D-Haar Wavelet Transformation in Image Compression," Middle-East Journal of Scientific Research 2 (2): 73-78, 2007 ISSN 1990-9233 © IDOSI Publications, 2007

