INPRESSCO
International Press Corporation

International Journal of Current Engineering and Technology
ISSN 2277 - 4106

Available at http://inpressco.com/category/ijcet

Research Article

Skin Tone Based Secret Data Hiding in Images

Dipika Nehete[A*] and Anant Bhide[A]

[A]E & C (Communication) Engineering Department, SSGBCOET Bhusawal, North Maharashtra University-India

Accepted 11 March 2014, Available online 01 April 2014, **Special Issue-3, (April 2014)**

Abstract

Steganography is the art of hiding the secret and confidential data in another transmission medium to achieve secret communication. In this paper steganography method used is based on biometrics. And the biometric feature used to implement steganography is skin portion of images where secret data is embedded within skin region of image. This skin region provides excellent secure location for data hiding, so security is enhanced. For this, firstly skin tone detection is performed on a cover image using HSV (Hue, Saturation and Value) color space and then secret data embedding will be performed by using frequency domain approach - DWT (Discrete Wavelet Transform). DWT consist of four frequency sub bands and secret data is hidden in one of the high frequency sub band. This is done by tracking skin pixels in that sub band. Various steps of data hiding are applied by cropping an image interactively. Cropping provides an enhanced security than without cropping i.e. in whole image, so cropped region works as a key at receiving side. Thus hiding the secret data in skin portion of images provides higher security and satisfactory PSNR (Peak Signal to Noise Ratio).

Keywords: *Biometrics, Cropping, DWT, PSNR, Skin tone detection.*

1. Introduction

In this era of digitalization the internet occupies a conspicuous position for transmitting and sharing the data. The exchange of information is greater today than at any other time in history. Some confidential data might be stolen, copied, altered or destroyed by an unwanted observer. So, security problems become an essential issue. Basically, the purpose of steganography and cryptography is same to provide secret communication. So they are closely related. The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages—no matter how unbreakable—will arouse interest, and may in themselves be incriminating in countries where encryption is illegal. Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message. Cryptography protects the contents of a secret message from a malicious people, also in this; structure of a message is scrambled to make it meaningless, unreadable, unnatural and unintelligible unless the decryption key is available. But these unnatural messages usually attract some unintended observer's attention. This is the reason a newly security approach called "Steganography" arises.

Steganography is the art and science of hiding information such that its presence cannot be detected and a communication is happening (Popa, et al, 1998). Steganography does not scramble the structure of the secret message, but hides it inside a cover-image so it cannot be seen. In steganography, it is not to keep others from knowing the hidden information but it is to keep others from thinking that the information even exists.
As an example, the cover text (Lin and Delp, 1999);
"I'm feeling really stuffy. Emily's medicine wasn't strong enough without another febrifuge". Hides the sentence "Meet me at nine".
If the reader retains the second letter of each word in sequence.

In steganography, sender wishes to remain secret data confidential. The secret data can be images, audio, video or any other that can be represented in the form of stream of bits. The cover image is nothing but one type of medium in which the secret data is embedded to conceal the presence of the data. The techniques of embedding message or data strongly depends on the structure of the cover image and in this paper covers and secret messages are restricted to being digital images. The cover-image containing the secret data is called the "Stego-Image". Additionally, before embedding the secret data in cover image, we can encrypt the message for higher security and protection of image (Johnson and Jajodia, 1998). For this, the encoder usually employs a stego-key which ensures only those recipients, who know the decoding key will be able to get the message from a stego-image. In this

*Corresponding author: Dipika Nehete

proposed method, cropped region of an image is used as a key at receiving side and thus gives enhanced security. Thus steganography is used in wide range of applications like in defense organizations for safe transmission of secret message, in military and intelligence agencies, in smart identity cards where personal details are embedded in the photograph itself for copyright control of materials, etc.

There are mainly two things that need to be considered while framing the steganographic system: Invisibility: Human eyes can't distinguish the difference between original image and stego image. (b) Capacity: The capacity of the secret data which is to be embedded in the cover image doesn't degrade an image quality significantly.

1.1 The ancient steganography

The word steganography derived from the Greek word *Steganos*, which mean covered or secret and *–graphy* mean writing. Hence, steganography means, literally, covered writing or concealed writing. It has been used in various forms for thousands of years. An ancient Greek historian Herodotus reports that messages were tattooed onto the shaved heads of slaves. Once the hair grew back, the slaves were sent to the recipient, with the message hidden "in plain sight". In Saudi Arabia at the king Abdulaziz City of Science and Technology, a project was initiated to translate into English, some ancient Arabic manuscripts on secret writing which are believed to have been written 1200 years ago. Some of these manuscripts were found in Turkey and Germany [Sadkhan, et al, 2004).

In more recent history, the Nazis invented several Steganographic methods during WWII such as invisible ink, null ciphers and Microdots. As an example the message below was sent by the German embassy in World War I.

"*President's embargo ruling should have immediate notice. Grave situation affecting international law. Statement foreshadows ruin of many neutrals. Yellow journals unifying national excitement immensely".*
Taking the first letter in each word of message reveals the hidden text: "*Pershing sails from NY June 1"* (Judge, et al, 2001).

1.2 The digital era of steganography

With the boost of computer power, the internet and with the development of Digital Signal Processing (DSP), Information Theory and Coding Theory, steganography went "*Digital*". Steganography does not exist merely in still images. Embedding hidden messages in videos and audios is also possible and even in a simpler form such as in Hyper Text Markup Language (HTML), executable files (.EXE) and Extensible Markup Language (XML) (Hernandez-Castro, Blasco-Lopez and Estevez-Tapiador, 2006). Steganography is employed in various useful applications e.g., Copyright control of materials, enhancing robustness of image search engines and Smart IDs where individuals' details are embedded in their photographs.

Other applications are Video-audio synchronization, companies' safe circulation of secret data, TV broadcasting, Transmission Control Protocol and Internet Protocol packets (TCP/IP) - for instance a unique ID can be embedded into an image to analyze the network traffic of particular users (Johnson and Jajodia, 1998) embedding Checksum, etc. In a very interesting way Petitcolas demonstrated some contemporary applications; one of which was in Medical Imaging Systems where a separation is considered necessary for confidentiality between patients' image data or DNA sequences and their captions e.g., Physician, Patient's name, address and other particulars. A link however, must be maintained between the two. Thus, embedding the patient's information in the image could be a useful safety measure and helps in solving such problems.

1.3 Steganalysis

Steganalysis is the science of detecting hidden information (Lavanya, Manjula and Krishna Rao, 2012). The main objective of Steganalysis is to break steganography and the detection of stego image is the goal of steganalysis. Almost all steganalysis algorithms rely on the steganographic algorithms introducing statistical differences between cover and stego image. Steganalysis deals with three important categories: (a) Visual attacks: In these types of attacks with a assistance of a computer or through inspection with a naked eye it reveal the presence of hidden information, which helps to separate the image into bit planes for further more analysis. (b) Statistical attacks: These types of attacks are more powerful and successful, because they reveal the smallest alterations in an images statistical behavior. Statistical attacks can be further divided into (i) Passive attack and (ii) Active attack. Passive attacks involves with identifying presence or absence of a covert message or embedding algorithm used etc. On the other hand, active attack is used to investigate embedded message length or hidden message location or secret key used in embedding. (c) Structural attacks: The format of the data files changes as the data to be hidden is embedded; identifying this characteristic structure changes can help us to find the presence of image.

Rest of the paper is organized as follows. Section 2 presents literature survey and theoretical background. In Section 3, color models for skin color classification are described. Section 4 deals with proposed method containing skin tone detection, DWT, embedding and extraction procedure step by step. Experimental results are shown in Section 5. Finally conclusions are provided.

2. Literature survey

2.1 Steganography in spatial domain

In the spatial domain approach, the secret messages are embedded into least significant pixels of cover images.

Least Significant Bit Substitution (LSB) is the most frequently used stenographic technique. In a gray level image, every pixel consists of 8 bits. The basic concept of LSB is to embed the secret data at the bits which having minimum weighting (rightmost bits) so that the embedding process will not significantly affect the original pixel value greatly (Fridrich, Goljan and Du. R., 2001). Modulating the least significant bit does not result in human-perceptible difference because the amplitude of the change is small. For example we will try to hide the character 'A' into an 8-bit color cover image. We are taking eight consecutive pixels from top left corner of the image. The equivalent binary bit pattern of those pixels may be like this: -
00100111 11101001 11001000 00100111
11001000 11101001 11001000 00100111
Then each bit of binary equivalence of letter 'A' i.e. **01100101** are copied serially (from the left hand side) to the LSB's of equivalent binary pattern of pixels, resulting bit pattern will become like this: -
0010011**0** 1110100**1** 1100100**1** 0010011**0**
1100100**0** 1110100**1** 1100100**0** 0010011**1**
The mathematical representation for LSB is:

$$x_i' = x_i - x_i mod 2^k + m_i \quad (1)$$

In equation (1), x_i' represents the i 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 th block in the confidential data (Po-Yueh Chen and Hung-Ju Lin, 2006). K is number of LSBs to be substituted. The extraction process is to copy the k-rightmost bits directly. Mathematically the extracted message is represented as:

$$m_i = x_i mod 2^k \quad (2)$$

Hence, a simple permutation of the extracted m_i gives us the original confidential data (Po-Yueh Chen and Hung-Ju Lin, 2006). The only problem with this technique is that it is very vulnerable to attacks such as image compression and formatting. 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.

2.2 Steganography in frequency domain

Robustness of steganography can be improved if properties of the cover image could be exploited. For example it is generally preferable to hide message in noisy regions rather than smoother regions as degradation in smoother regions is more noticeable to human HVS (Human Visual System). Taking these aspects into consideration working in frequency domain becomes more attractive. The frequency domain approach transforms the cover image into the frequency domain coefficients before embedding secret messages in it (Chang, Chen and Chung, 2002). The transformation can be either Discrete Cosine transform (DCT) or Discrete Wavelet Transform (DWT). Though these methods are more difficult and slower than spatial domain, yet they have an advantage of being more secure and noise tolerant.

2.3 Adaptive steganography

Adaptive steganography is special case of two former methods. It is also known as "Statistics aware embedding" (Provos and Honeyman, 2003) and "Masking" (Johnson and Jajodia, 1998). This method takes statistical global features of the image before attempting to embed secret data in DCT or DWT coefficients. The statistics will find where to make changes. This method is characterized by a random adaptive selection of pixels depending on the cover image and the selection of pixels in a block with large local STD (Standard Deviation).

3. Color models for skin color classification

The study on skin color classification has gained increasing attention in recent years due to the active research in content-based image representation. For instance, the ability to locate image object as a face can be exploited for image coding, editing, indexing or other user interactivity purposes. Moreover, face localization also provides a good stepping stone in facial expression studies. It would be fair to say that the most popular algorithm to face localization is the use of color information, whereby estimating areas with skin color is often the first vital step of such strategy. Hence, skin color classification has become an important task. Much of the research in skin color based face localization and detection is based on RGB (Red-Green-Blue), YCbCr (Yellow-Chromatic blue-Chromatic red) and HSV color models. In this section these color spaces are being described.

3. 1 RGB color space

The RGB color model is composed of three primary colors: red, green and blue. This system defines the color model that is used in most color CRT monitors and color raster graphics. They are considered the "additive primaries" since these colors are added together to produce the desired color (Ashok Kumar Balijepalli and L.Srinivas, 2012). The RGB model uses the Cartesian coordinate system. The color subspace of interest is the cube as shown in fig in which values are at three corners. Cyan, magenta and yellow are at three other corners. Black is at the origin and white is at the corner farthest from the origin. The diagonal from (0, 0, 0) black to (1, 1, 1) white represents the grey-scale. With 8 bits per color channel, red is (255, 0, and 0) in a 24-bit color graphics system. On the color cube, red is (1, 0, and 0).

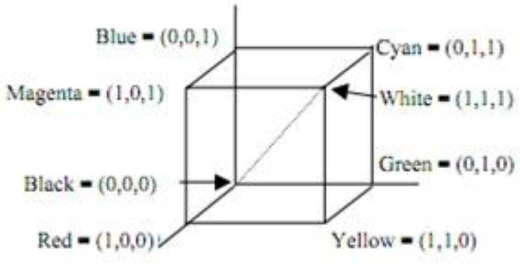


Fig. 1.RGB co-ordinates system

RGB color space is the most commonly used color space in digital images. One of the main advantage of the RGB space is its simplicity. The RGB model simplifies the design of computer graphics systems. Also RGB color space doesn’t separate luminance and chrominance and R, G & B components are highly correlated.

3. 2 YCbCr color space

YCbCr color space has been defined in response to increasing demands for digital algorithms in handling video information, and has since become a widely used model in a digital video. YCbCr color space belongs to the family of television transmission color spaces. This family includes other spaces such as YUV and YIQ. YCbCr space is used in JPEG image compression and MPEG video compression while YIQ is used in NTSC TV broadcasting. YCbCr is a digital color system.

3. 3 HSV color space

The HSV stands for the Hue, Saturation, and Value based on the artists (Tint, Shade, and Tone). The value represents intensity of a color. Since hue, saturation and value are three properties used to describe color, it seems logical that there be a corresponding color model, HSV. While using the HSV color model, we don't need to know what percentage of blue or green is required to produce a color. We simply adjust the hue to get the color we wish. To change a deep red to pink, adjust the saturation. To make it darker or lighter, alter the intensity.

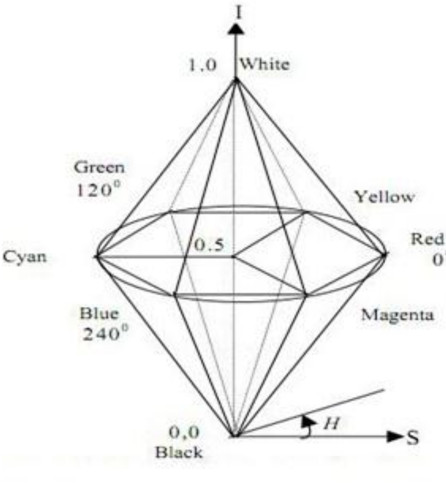


Fig. 2. Double cone model of HSV color space

Many applications use the HSV color model. Machine vision uses HSV color space in identifying the color of different objects. Image processing applications such as histogram operations, intensity transformations and convolutions operate only on an intensity image. These operations are performed with much ease on an image in the HSV color space. For the HSV being modeled with cylindrical coordinates, see Fig. 2. The hue (H) is represented as the angle 0, varying from 0^0 to 〖360〗^0. Saturation (S) corresponds to the radius, varying from 0 to 1. Value (V) varies along the z axis with 0 being black and 1 being white. When S = 0, color is a gray value of intensity 1. When S = 1, color is on the boundary of top cone base. The greater the saturation, the farther the color is from white/gray/black (depending on the intensity).

4. Proposed method

Proposed method introduces a new method of embedding secret data within skin as it is not that much sensitive to HVS (Cheddad, Condell, Curran and Mc Kevitt, 2008). This takes advantage of biometrics features such as skin tone region. Secret data will be embedded in selected regions, instead of embedding data anywhere in image. The proposed method is briefly introduced as follows. Firstly, skin tone detection is performed on the cover image using HSV 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. Before performing all steps cropping on secrete image is performed and then only in cropped region embedding is done, not in the whole image. Cropping provides greater security than without cropping, since cropped region works as a key at receiving side. Here embedding process affects only certain Regions of Interest (ROI) rather than the whole image. The secrete image is extracted by using DWT to the stego image.

4.1 Skin color tone detection

Skin detection is the process of detecting image pixels and regions that contain skin tone color. The main aim of skin tone detection is to discriminate between skin and non-skin pixels. Skin tone detector transforms a given pixels into an appropriate color space and then uses skin classifier to label whether the pixels are skin pixels or non-skin pixels. By defining a boundary it can be easily identified that the pixel is of skin color or not. Detecting skin colored pixels, although seems a straightforward easy task, has proven quite challenging for many reasons. Therefore, important challenges in skin detection are to represent the color in such a way that the color is invariant or at least insensitive to changes in illumination conditions (Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt, 2008). In the real world many objects might have skin-tone colors. As a result, any skin detector detects much false detection in the background if the environment is not controlled (Ahmed, Crystal and Dunxu, 2009).This is also another challenge in skin detection process.

The simplest way to check whether a pixel is skin color or not is to explicitly define a boundary. RGB matrix of 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 exploited in the literature of biometrics which are the HSV and YCbCr spaces. It is experimentally found that the distribution of human skin color constantly resides in a certain range within those two spaces as different people differ in their skin color (e. g., European, African, Asian, Middle Eastern, etc.).

In this work, color space used for skin detection is HSV. RGB image can be easily converted into HSV color space. In HSV, responsible values for skin detection are Hue and Saturation. For skin detection threshold is chosen as [H1,S1] and [H2,S2]. Sobottaka and Pitas (Sobottka and Pitas, 1996) defined a face localization based on HSV color space. They found that the threshold range of human flesh as:

$$S_{min} = 0.23, S_{max} = 0.68, H_{min} = 0^0 \ and \ H_{max} = 50^0$$

4.2 Discrete wavelet transform (DWT)

Here, we are using DWT instead of DCT as DCT calculated on independent pixels block. As a result, a coding error causes discontinuity between the blocks resulting in annoying interference of artifact. This drawback of DCT is eliminated using DWT. The simplest DWT, Haar-DWT is used in this work. DWT applies on entire cropped image. DWT divides component into four frequency bands called sub bands known as,

LL – Horizontally and vertically low pass
LH – Horizontally low pass and vertically high
HL - Horizontally high pass and vertically low
HH - Horizontally and vertically high pass

All the four sub-bands are of same size. Since Human eyes are much more sensitive to the low frequency part (LL sub band) we can hide secret message in other three bands without making any alteration in LL sub band (Chen and Liao, 2002). As other three sub-bands are high frequency sub-band they contain insignificant data. Hiding secret data in these high frequency sub-bands doesn't degrade image quality that much. DWT used in this paper is Haar-DWT, the simplest DWT.

4.3 Embedding process

In this process, embedding is performed on the cropped image and it results into hiding of secret data. Suppose C is original 24-bit color cover image of M×N size.
It is denoted as:

$$\mathrm{C} = \{\mathrm{xij}, \mathrm{yij}, \mathrm{zij} | 1 \le \mathrm{i} \le \mathrm{M}, 1 \le \mathrm{j} \le \mathrm{N}, \mathrm{xij}, \mathrm{yij}, \mathrm{zij} \in \{0,1..,255\}\}$$

Let dimension of cropped image is $M_c \times N_c$ where $M_c \le M$ and $N_c \le N$ and $M_c = N_c$ i.e. cropped region must be exact square as we have to apply DWT later on this region. Let S is secret data. Here secret data considered is binary image of size$a \times b$. Fig. 3 represent flowchart of embedding process.

The description of the embedding process is given below.
Step 1. First load the cover image and apply skin tone detection on that image. This will produce mask image that contains skin and non-skin pixels.
Step 2. Perform cropping on mask image$(M_c \times N_c)$. After this, original image is also cropped of same area. Cropped area must be in an exact square as we have performed DWT later and this should contain skin region like face, hand, etc. The data will hide in skin pixels of one of the high frequency sub band of DWT. Here Cropping is performed for security reasons. Cropped region acts as a key at the receiver side. Only by using this key data retrieval is possible. In short no one can extract secret message without having value of cropped region.

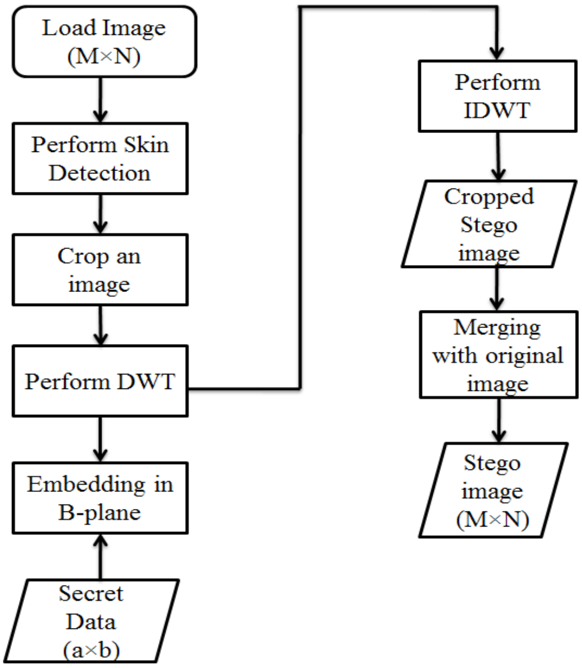


Fig. 3. Flowchart of embedding process

Step 3. Apply DWT to only cropped area $(M_c \times N_c)$ not to whole image$(M \times N)$. This yields 4 frequency sub-bands denoted as $H_{LL}, H_{HL}, H_{LH}, H_{HH}$. All 4 sub-bands are of same size of $M_c/2, N_c/2$. Determine the payload of image to hold the secret data that based on the no. of skin pixels present in one of the high frequency sub band in which data will be hidden.
Step 4. Embedding of secret data is performed in high frequency sub band that we obtained by tracing skin pixels in that sub bands. Skin pixels are traced using skin mask detector and the secret data is embedded. Embedding is performed in G-plane and B-plane of RGB color space but strictly not in R-plane as contribution of R plane in skin color is more than the G-plane and B-plane. As the pixel value of R plane changes, receiver side does not find data at all as skin detection at decoder side give different mask than encoder side.

Embedding is done as per raster-scan order (as shown below in Fig. 4) that embeds secret data coefficient by coefficient in selected sub band (Po-Yueh Chen and Hung-Ju Lin, 2006), if coefficient is skin pixel.

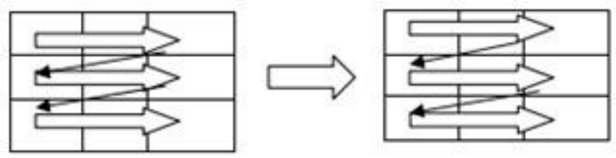


Fig. 4. Raster scan order

Step 5. Perform IDWT (Inverse Discrete Wavelet Transform) to combine 4 frequency sub-bands.
Step 6. After combination of sub bands, a cropped stego image of size $(M_c \times N_c)$ is obtained. Then merge the cropped stego image with original image to get the stego image of size$M \times N$. For merging, coefficients of first and last pixels of cropped area in original image are required so that R is calculated. Finally, stego image is ready for secret communications.

4.4 Extraction process

A 24 bit color stego image of size $M \times N$ is loaded as input to extraction process. Then perform the skin detection to this stego image & obtain the cropped image of size $M_c \times N_c$. Suppose cropped area value is stored in 'rect' variable that is same as in encoder. So this 'rect' acts as a key at decoder or receiver side. The steps of Decoder are opposite to Encoder. While cropping, care must be taken to crop same size of square as per Encoder. Secret data is retrieved by tracing skin pixels in H_{HH} frequency sub-band of DWT.
The flowchart of extraction process is given below in Fig. 5.

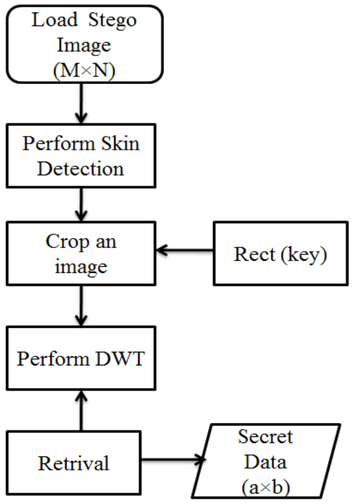


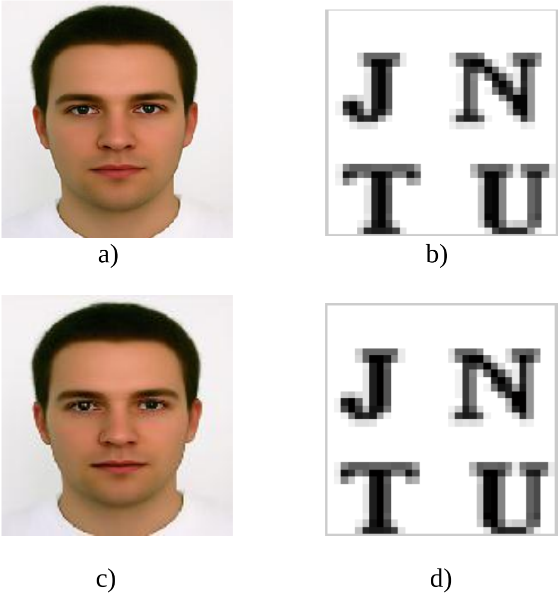
Fig. 5. Flowchart of extraction process

5. Simulation results

This section contains simulation results for the proposed method. It has been implemented using MATLAB 7.5.

A 24 bit color image is taken as input image 1 or cover image 1 of size 356×356 as shown in Fig. 6 a).

Fig. 6 b), c) and d) below shows sample secret image to hide inside the input image, stego image and retrieved image respectively.



a) b)

c) d)

Fig. 6. Cover Image 1 b) Secret image to hide c) Stego Image d) Retrieved Image

The secret message S is gray image of size 32×32. Peak signal to noise ratio (PSNR) is used to evaluate quality of stego image after embedding the secret image. The performance in terms of capacity and PSNR (in dB) is demonstrated for the method in the following subsection.
PSNR is defined as per Eq.3 and Eq.4.

$$\mathrm{PSNR} = 10\log_{10}(255^2/\mathrm{MSE}) \quad (3)$$

Where, MSE (Mean Square Error) stands for the mean squared difference between original cover image and the stego image.
MSE is defined as,

$$\mathrm{MSE} = \left(1/(\mathrm{M} \times \mathrm{N})\right) \sum_{\mathrm{i}=1}^{\mathrm{M}} \sum_{\mathrm{j}=1}^{\mathrm{N}} \left(\mathrm{X}_{\mathrm{ij}} - \mathrm{Y}_{\mathrm{ij}}\right)^2 \quad (4)$$

xij and yij represents pixel values of original cover image and stego image respectively. The calculated PSNR usually adopts dB value for quality judgment, larger the PSNR, higher is 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 below 30dB indicate fairly a low quality. However, high quality strives for 40dB or more (Cheddad, Condell, Curran and Kevitt, 2008).

5.1 Performance of the proposed method

After embedding secret message in cropped image, resulted cropped stego image doesn't look like cover image so merging is performed to get final stego image that is shown in Fig. 6 c). For merging step, co-ordinates of first and last pixels of cropped image in original image are calculated.

After performing extraction process retrieved image is obtained as shown in Fig. 6 d). Above method uses cropping case. Same proposed method is implemented for without cropping case. In without cropping case secret data is hidden in one of the frequency sub-band which is obtained by performing DWT on entire image and not only to cropped region. PSNR is calculated for two different final stego images resulted from a considered image and one more sample image. This PSNR for different cases is shown in table 1. Average PSNR of proposed method is calculated from the obtained PSNR.

Performing biometric based steganography with cropping or without cropping, both are having its own advantages and disadvantages. But if method is implemented with cropping then it will provide more security than without cropping case. As with cropping case we need cropped region at the decoder side then only secret data retrieval is possible. So cropped region works as a key at receiver side. While in case of without cropping method intruder may try to perform DWT randomly and can hack secret data from sub-band with trial and error method.

Table 1 shows that PSNR of without cropping case is more than with cropping case. So, this is trade off that occurs if we need more security.

Table 1. Capacity and PSNR Of 2 Final Stego Images In Proposed Method

Cover Image (356×356)	Capacity of the Cover image		PSNR		Size of Logo
	Case A	*Case B*	*Case A*	*Case B*	
Image 1	16348	7396	69.52	67.95	32×32
Image 2	16348	13924	72.49	69.51	32×32
Average PSNR			71.01	68.73	

Case A- Without Cropping
Case B- With Cropping

Conclusions

Digital Steganography is a fascinating scientific area which falls under the umbrella of security systems. Proposed framework is based on steganography that uses biometric feature i.e. skin tone region. Skin tone detection plays a very important role in biometrics and can be considered as secure location for data hiding. Secret data embedding is performed in DWT domain. By embedding data in only skin portion and not in whole image security is enhanced. Also image cropping concept provides security at respectable level since secret data retrieval is not possible without having value of cropped region. Features obtained from DWT coefficients are utilized for embedding secret data. This also increases the quality of stego image because secret messages are embedded in high frequency sub-bands which are less sensitive to human eyes. According to performance measure results, proposed approach provides fine image quality.

Acknowledgement

The authors would like to thank to the earlier work regarding steganography whose guidance significantly contributed to the work made in this paper.

References

E.T. Lin and Delp, E. J, (1999), "A Review of Data Hiding in Digital Images", *Computer Forensics, Cyber crime and Steganography Resources, Digital Watermarking Links and Whitepapers.*

A.Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt, (2008), "Biometric inspired digital image steganography", *15th Annual IEEE International Conference and Workshops on the Engineering of Computer-Based System*, 159-168.

Anjali A. Shejul, Prof. U.L Kulkarni, (2010), "A DWT based Approach for Steganography Using Biometrics", *International conference on data storage and data Engineering*, 39-43.

N.F Johnson and Jajodia S. (1998), "Exploring Steganography: Seeing the Unseen", *IEEE Computer*, 31(2), 26-34.

J.Fridrich, Goljan M. and Du R., (2001), "Reliable Detection of LSB Steganography in Grayscale and Color Images", *Proceeding of ACM, Special Session on Multimedia Security and Watermarking*, 8, 22-28.

Po-Yueh Chen and Hung-Ju Lin, (2006), "A DWT Based Approach for Image Steganography", *International Journal of Applied Science and Engineering*, 4, 275-290.

N.Lavanya , V. Manjula, N.V. Krishna Rao, (2012)," Robust and Secure Data Hiding in Image Using Biometric Technique", *International Journal of Computer Science and Information Technologies*, Vol. No.3 (5), Page No.5133 – 5136.

J.C Judge, (2001), "Steganography: Past, Present, Future", *SANS Institute Publication* http://www.sans.org/reading_room/whitepapers/steganography/552.php.

N.Provas and Honeyman P., (2003), "Hide and Seek: An Introduction to Steganography", *IEEE Security and Privacy*, 01(3), 32-44.

P.Moulin and R. Koetter, (2005), "Data Hiding Codes", *Proceeding of the IEEE*, 93(12), 2083-2126.

S.Sadkhan, (2004), "Cryptography: Current Status and Future Trends", *IEEE International Conference on Information and Communication Technologies: From Theory to Applications*, 417-418.

J.C Hernandez-Castro, Blasco-Lopez I. and Estevez-Tapiador J. M, (2006), "Steganography in Games", *A general methodology and its application to the game of Go. Computers and Security*, 25, 64-71.

C.Chang, Chen T. S and Chung L. Z, (2002), "A Steganographic method based upon JPEG and quantization table modification", *Information Sciences*, 4, 123-138.

Ashok Kumar Balijepalli and L. Srinivas, (2012), "Steganography Based Secret Communication Using DWT", *International Journal of Engineering Research and Technology (IJERT*), 1(5).

R.Popa, (1998), "An Analysis of Steganographic System", *The Politechnica University of Timisoara, Faculty of Automatics and computers, Department of Computer Science and Software Engineering.*

A.Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt, (2009), "A Skin Tone Detection Algorithm for an Adaptive Approach to Steganography", *School of Computing and Intelligent Systems, Faculty of Computing and Engineering, University of Ulster.*

E.Ahmed, Crystal M. and Dunxu H, (2009), "Skin Detection-A Short Tutorial", *Encyclopedia of Biometrics by Springer-Verlag Berlin Heidelberg.*

K.Sobottka and I. Pitas, (1996), "Extraction of facial regions and features using color shape information", *IEEE International Conference on Image Processing*, 3, 421-425.

P.Chen and E C. Liao, (2002), "A new Algorithm for Harr Wavelet Transform", *2002 IEEE International Symposium on Intelligent Signal Processing and Communication System*, 453-457.