Implementation of Skin Tone Based *Steganography* in Biometric Applications

1. S.Swarnalatha, 2.T.Harikala

1. Associate Professor of ECE, Department of ECE, S. V. University, Tirupati – 517 502.
2. M.Tech, Communication Systems, Dept. of ECE, SVUCE, Tirupati-517502

Abstract

Steganography is the art of hiding the existence of data in another transmission medium to achieve secret communication. It does not replace cryptography but rather boosts the security using its obscurity features. 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 provides 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 out performs 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. Different steps of data hiding are applied by cropping an image interactively. Cropping results into an enhanced security than hiding data without cropping i.e. in whole image, so cropped

region works as a key at decoding side. This study of project shows that by
adopting an object oriented Steganography mechanism, in the sense that, we track skin tone objects in image, to get a higher security.
Keywords: Biometrics; Skin tone detection; DWT; DCT; Cropping; Security.

1. 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-known procedure for secured data transmission [2]. Frequently used encryption methods include RSA, DES (Data encryption standard). Although encryption achieves certain security effects, they make the secret messages unreadable and unnatural or meaningless. These unnatural messages usually attract some unintended observers' attention. This is the reason a new security approach called "Steganography" arises. As an example, the cover text [3]: "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 secret message is the data that the sender wishes to remain confidential and can be text, images, audio, video, or any other data that can be represented by a stream of bits. The cover or host is the medium in which the message is embedded and serves to hide the presence of the message. The message embedding technique is strongly dependent on the structure of the cover, and 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 [4]. For this the encoder

S.Swarnalatha,T.Harikala/ International Journal of Engineering Research and Applications (IJERA)   **ISSN: 2248-9622**   **www.ijera.com**

Vol. 1, Issue 4, pp.1696-1701

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.

There are two things that need to be considered while designing the steganographic system:

(a)Invisibility: Human eyes can not distinguish the difference between original and stego image.

(b) Capacity: The more data an image can carry better it is.

2. Steganographic Techniques:

A. *Steganography in Spatial Domain*

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 graylevel 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:

$$x_i' = x_i - x_i \bmod 2^k + m_i \quad \ldots\ldots.. (1)$$

In equation (1), x_i' *represents* the i th pixel value of the stego-image and x_i *represents* that of the original coverimage. m_i *represents* the decimal value of the i 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:

$$m_i = x_i \bmod 2^k \quad \ldots\ldots (2)$$

Hence, a simple permutation of the extracted m_i *gives* us the original confidential data. 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. *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. Here, sender transforms the cover image into frequency domain coefficients before embedding secret messages in it. Different sub-bands of frequency domain coefficients give significant information about where vital and non vital pixels of image resides. 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.

3. PROPOSED METHOD:

Proposed method introduces a new method of embedding secret data within skin 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. Before performing all steps cropping on input image is performed and then in only cropped region embedding is done, not in whole image. Cropping results into more security than without cropping. Since cropped region works as a key at decoding side. Here 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 briefly introduce skin tone detection and DWT.

A. Skin Color Tone Detection

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. A skin classifier defines a decision boundary of the skin color class in the color space. Although this is a straightforward process has proven quite challenging. Therefore, important challenges in skin detection are to represent the color in a way that is invariant or at least insensitive to changes in illumination and another challenge comes from the fact that many objects in the real world might have skin-tone colors. This causes any skin detector to have much false detection in the background if the environment is not controlled. The simplest way to decide whether a pixel is skin color or not is to explicitly define a boundary. RGB matrix of the given color image can be converted into different color spaces to yield distinguishable regions of skin or near skin tone. There exists several color spaces. Mainly two kinds of color spaces are exploited in the literature of biometrics which are HSV (Hue, Saturation and Value) and YCbCr (Yellow, Chromatic Blue, Chromatic red) spaces it is experimentally found and theoretically proven that the distribution of human skin color constantly resides in a certain range within those two color spaces [1]. Color space used for skin detection in this work is HSV. Any color image of RGB color space can be easily converted into HSV color space. Sobottaka and Pitas 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:

Smin= 0.23, Smax =0.68, Hmin =00 and Hmax=500

.

B. Discrete Wavelet Transform (DWT)

This is another frequency domain in which Steganography can be implemented. 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. 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.DWT used in this work is Haar-DWT, the simplest DWT.

C. Embedding Process

Suppose C is original 24-bit color cover image of M×N Size. It is denoted as:

C= {x_{ij}, y_{ij}, z_{ij} |$1 \le i \le M$, $1 \le j \le N$, x_{ij}, y_{ij}, z_{ij} Є {0, 1,.., 255}}

Let size of cropped image is Mc×Nc where Mc≤M andNc≤N and Mc=Nc. i.e. Cropped region must be exact squares we have to apply DWT later on this region.

Let S is secret data. Here secret data considered is binary image of size a×b. Fig. 1 represents flowchart of embedding process. Different steps of flowchart are given in detail below.

1) 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.

2) Step 2: Ask user to perform cropping interactively unmask image (Mc×Nc). After this 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.
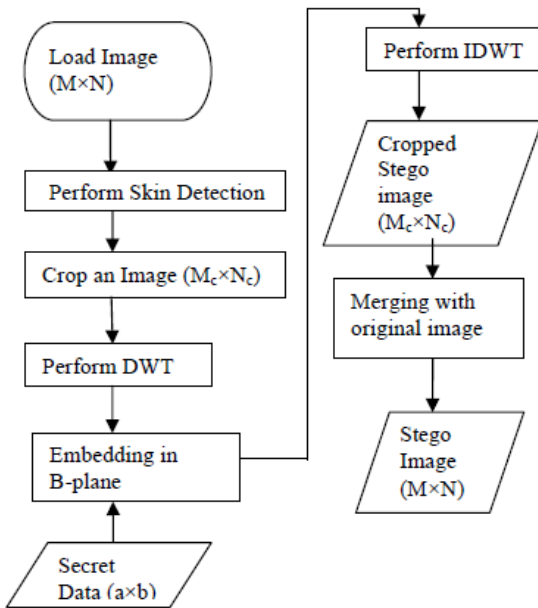

Figure 1. Flowchart of Embedding Process

3) Step 3: Apply DWT to only cropped area (Mc×Nc) not whole image (M×N). This yields 4 sub-bands denoted as HLL, HHL, HLH, HHH . (All 4 sub-band are of same size of (Mc/2,Nc/2). Payload of image to hold secret data is determined based on no. of skin pixels present in one of high frequency sub-band in which data will be hidden.

4) 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 LL, low frequency sub-band any high frequency sub-band can be selected for embeddings 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.2) that embeds secret data coefficient by coefficient in selected sub-band [6], if coefficient is skin pixel.
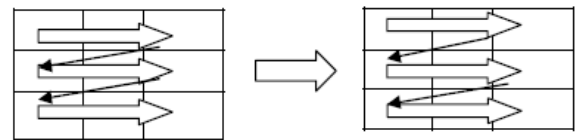

Figure 2. Raster Scan Order

5) Step 5: Perform IDWT to combine 4 sub-bands.

6) Step 6: A cropped stego image of size Mc×Nc 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 Mc× Nc, So we need to merge the cropped stego image Load Image (M×N) Perform Skin Detection Crop an Image (Mc×Nc) Perform DWT Embedding in B-plane Secret Data (a×b) Cropped Stego image(Mc×Nc) Merging with original image Stego Image (M×N)Perform IDWT

D. Extraction Process:

Secret data extraction is explained as follows: 24 bit color stego image of size M×N is input to extraction process. The process must need 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. All steps of Decoder are opposite to Encoder. Care must be taken to crop same size of square as per Encoder. By tracing skin pixels in HHH sub-band of DWT secret data is retrieved. Extraction procedure is represented using Flowchart in Fig. 3
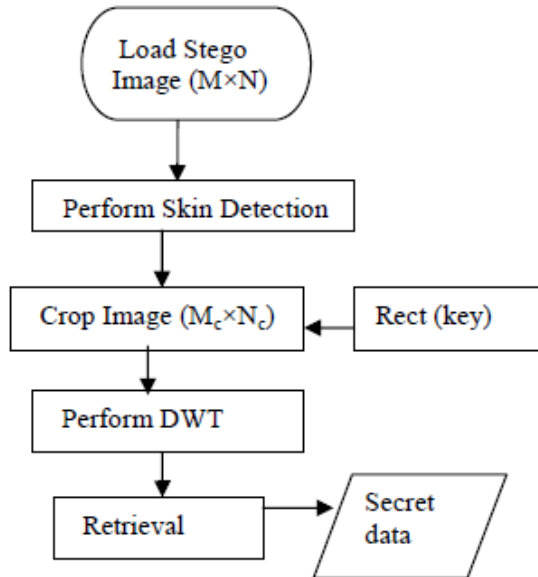
Figure 3. Flowchart of Extraction Process

4. Results and Conclusions:

A. Performance of the proposed method

After embedding secret data in cropped image, resulted cropped stego image is shown in Fig. 4. As this doesn't look like cover image merging is performed to obtain final stego image that is shown in Fig. 5. For merging co-ordinates of first and last pixels of cropped image in original image are calculated. After performing extraction process retrieved image is shown in figure 6. Above method uses cropping. 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.

Figure. (4) and Figure. (5)

Figure. (6)

Performing biometric Steganography with cropping or without cropping, both are having its own advantages and disadvantages. But if method is implemented with cropping then it ensures more security than without cropping case. As with cropping case the need of cropped region at the decoder side then only secret data extraction is

possible. So cropped region works as a key at decoder side. For without cropping method intruder may try to perform DWT randomly and can hack secret data from sub-band with trial and error method.

5.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 Engineering 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] Lin, E. T. and Delp, E. J.:"A Review of Data Hiding in Digital Images". Retrieved on 1.Dec.2006 from Computer Forensics, Cyber crime and Steganography Resources, Digital Watermarking Links and Whitepapers, Apr 1999

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

[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.