A Robust and Efficient Steganography Using Skin Tone as Biometric for Real Time Images

K.Madhavi[1], D.Manjith Kumar [2], S.Mahitha[3]

[1] Assistant Professor, Electronics and communication engineering (EC), St. martin's Engineering College Secunderabab, India
[2,3]Students, EC Engineering, St.Martin's engineering college, Secunderabad, India

---***---

Abstract: *The steganography is a method used for hiding the confidential or secret information (i.e data etc...) in any type of medium and transferring that information through any of the communication medium without distinguishing the information to other parties. In this paper the steganography is done by using the biometrics features like skin portion of the human beings. We are using the skin portion because it provides the excellent secure location for data hiding and due to this the security will be enhanced. The process involved in the steganography is like this. First we have to select the Skin portion in the human faces ,it is done by using HSV(Hue, Saturation and Value) colour space and after detecting the skin portion we have to crop the image only to that region by doing this the security will be high compared with un cropped image after that by using the DWT (Discrete Wavelet Transform) method we have to find four different frequency sub- bands like HH,HL,LH,LL. In this four sub bands we hide the data only in the HH(Horizontally and vertically high pass) band. Then the data will be embedded into that band and the key will be assigned to the image which will know only to the transmitter and receiver and then the image will be merged back to the original image and the image will be transferred through the communication channel and the data will be extracted by the receiver by using the key.*

Keywords: Steganography, Cropping, DWT, Skin Tone Detection

1. INTRODUCTION

In this world of digitalization the internet has become a great channel in the field for communication and sharing of data, The sharing of information through internet is increasing day by day compared with olden days, because of this exchange of data some unwanted observer are getting this confidential information which is not met for them .So the security has becoming an important factor .The basic purpose of steganography and cryptography is to provide the secret channel of communication. So the both Steganography and cryptography looks somewhat similar. But the advantage of steganography over the cryptography method is that the message hidden does not attract anyone attention to itself due to this the security will be enhanced. This is the reason why steganography came into picture . Steganography means hiding a secret or confidential data which should be disclosed to other people without attracting any attention to it[1].In this steganography method the confidential or secret data will be in the form of text,image,audio,video,etc..,in this paper we take secret data in the form of text. The data will be embedded into skin region of the cover image because the skin region is more efficient for hiding the data. But finding the skin pixels is more challenging. So, to find the skin pixels we use HSV algorithm after this we use the embedding technique like cropping the image ,where the cropped image will act as a key at the receiver side. The image after embedding the data in cover image is called as "stego image".

1.1 The Ancient Steganography:

The word steganography came from the greek word "Steganos",which mean covered or secret and - graphy means writing. Hence, steganography means covered writing. This type of methods are used thousands of years in different forms. In ancient greek the messages were used to tattooed onto the shaved heads of slaves. The slaves are sent to the recipient when the hair of the slaves is grown back. Even at the time of World war II the Nazis invented techniques like invisible ink, null ciphers and microdots. As an example the following messages like this are used at the time of world war I-How is everyone in the home?. Everything is fine here Looking forward to come home. Please take care of your health. In the above sentences by taking the First letter of each sentence leads to the secret data HELP [3].

2. LITERATURE SURVEY

2.1: Steganography in spatial domain:

The spatial domain technique is the simplest one for steganography where the secret data will be embedded directly into the least significant bits(LSB) of the original image. 8 bits will be there in each pixel of every gray level image. The basic concept of Least significant bit is to hide the data in correct bit position (i.e Bits with smallest weighting)[3].The mathematical equation of LSB is:

$X_i'=X_i-X_i mod 2^k+m_{i}$ (1)

In the above equation(1) , X_i' represents the i^{th} pixel value of the stego image(i.e., image after embedding the data) and X_i represents the original image, m_i represents the decimal value of the i^{th} block in the secret data. In the extraction process K-rightmost bits are copied directly. Mathematically the extracted data is represented as:

$M_i=X_i mod 2^k$ (2)

Hence, a simple alteration of the extracted M_i gives the secret data. This method is easy but it's drawback is ,it has very less ability to bear some signal processing pr noises, and also the confidential data can be stolen by extracting the whole LSB plane.

2.2 Steganography in Frequency Domain:

Security of steganography method can be improvised if properties of the cover or original image could be exploited. For example, In a image there are different type of regions smooth and noisy region but to hide the data only noisy regions are preferred than the smoother regions because the smoother region are easily noticeable compared with noisy regions to human eyes. Taking these conditions into consideration this technique is preferred. In this the transmitter transforms the original image into frequency domain coefficients before hiding the secret messages into it [5]. Different sub-bands of this frequency coefficients give information about where smooth and noisy pixels of image resides. This method is more complex and slower compared with spatial domain method; but they are more secure and tolerant to noises. This technique can be applied either in DCT or DWT.

3. SKIN COLOR CLASSIFICATION & PROPOSED MODEL:

The HSV colour model is much better than RGB colour model .HSV is best used when user is selecting colour as he preferred .It is very much easy to select the desired colour using this when compared to the RGB[6][7].As Hue(H) varies from values 0 to 1.0,the colour changes from red, green, blue and magenta, back to red. As Saturation(s) values changes from 0 to 1.0, so the color differ from unsaturated to fully saturated (no white component).As value(v) or brightness, differ from 0 to 1.0 the selected color will get more brighter .The Hue factor in HSV is in the range of 0^o to 360^0 angle in a circle as shown in figure (1).In RGB color model the values are given as (0.5,0.6,0.25),but in HSV color space values will be like(40^o, $\sqrt{1/2}$,0.25).

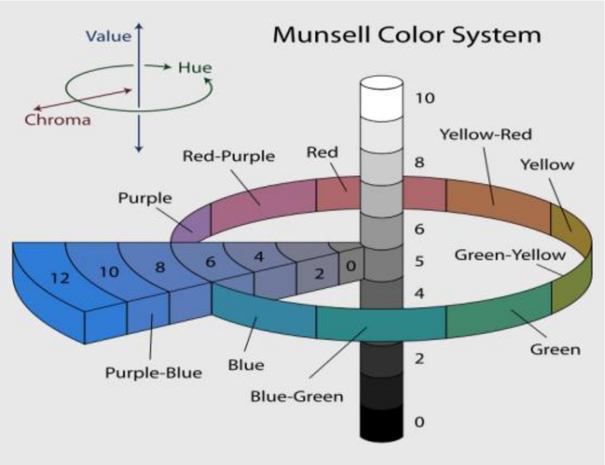

Figure 1: HSV Colour Space

3.1 Skin color tone detection:

Skin color detection is a process which is used to find the pixels and region of an a image that having skin ton colour. Skin tone detection will finds the changes between the skin and non-skin pixels. First it changes the given pixels into appropriate color region and then use the skin classsifers to label whether the pixels are skin colour pixels or not and also by setting some limits it can distinguish whether the pixels are skin or non-skin color. Even though detecting skin region seems a easy task but it is very complex and hard for some reasons. Therefore, important things to care while finding the skin pixels are to represent the skin colour pixels in such a way that the color is invariable or unresponsive to change in bright conditions [8]. In this world many objects might have skin-tone colors. As a result, any of the skin color detector considers the image background as a skin pixels if the environment is not controlled[9].This is also another challenge in skin color detection process. The easy process to check whether region or pixels are skin pixels or not is by define a boundary or limits. RGB matrix of taken color images can be transformed into different color spaces to turnout into a observable regions of skin or near skin tone. Only two kinds of color spaces are exploited in the biometrics they 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 model used for skin detection is HSV. RGB images can be easily transformed into HSV color model. In HSV, responsible values to detect the skin pixels are Hue and Saturation. For detecting the skin region , threshold is chosen as [H1,S1] and [H2,S2] [10] defined a face localization based on HSV color model. It is proves that the threshold value range of human flesh as:

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

3.2: 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 in middle of the blocks resulting in annoying interference of artifact. This drawback of DCT is eliminated using DWT so we use the simplest form of DWT, that is Haar-DWT . DWT is applied on entire cropped image. DWT divides component into four frequency sub-bands they are as follows,

LL – Horizontally Lowpass 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

All the four sub-bands are of same size. In the human face eyes are considered as the most sensitive part to the low frequencies (i.e.LL sub-band) .So we can embedded the confidential or secret message in the remaining three sub-bands without making any changes in the LL sub-band [11]. So the remaining three sub-bands being the high frequency bands they will the contain the insignificant data . Now by embedding the confidential message in the remaining three sub-bands will not decrease the original image quality.

3.3: Embedding process:

Let us consider an original image denoted by C which is of 24-bit and MxN size.Now the image C is given as:

C={ Xij,Yij,Zij |1 ≤ i ≤ M, 1 ≤ j ≤ N, Xij,Yij,Zij € {0,1,….,255}}

Let the size of cropped image is Mc×Nc where Mc≤M and Nc≤N and Mc=Nc. i.e. The region should be a square for applying DWT after cropping the original image. Let S be the secret data. Here we considered secret message as a binary image of size a×b. Fig. 1 is the flowchart of embedding process.

Step1: When the original image is loaded ,we apply HSV on the cover image to detect the skin region. This will give us a mask image which contain both skin and non-skin pixels.

Step 2: Then we have perform cropping on the mask image. Cropped area must be in an exact square form because we have to perform Discrete wavelet transform on this cropped image and this image should contain all the regions where the skin pixels are available so we can embed the data into these regions or pixels or sub-bands of DWT. The size of this cropped image will be taken as (M_cxN_c). Here the cropping is done for the security reasons. As the cropped region will be a key to the receiver. By knowing this key only the data can be extracted by the receiver. Eaves dropper 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.

Step 3: In this step we will apply the DWT only on the cropped region of size (M_cxN_c) but not on the total image. This DWT process will leave the four sub-bands known as LL,HL,LH,HH. The size of this sub-bands will be same (i.e.M_c/2xN_c/2).The total amount of data we can hide in these high frequency sub-bands is given by the no. of skin pixels present in it .

Step 4: The embedding of secret message in any of the sub-band expect LL which was traced in the above step by knowing the available skin pixels. Horizontally and vertically low pass sub-band can't be used for hiding the data because it will contain the significant data ,so by embedding the message into this sub-band we effect the original image quality. In this paper we selected the HH sub-band for embedding the data. The important point is the embedding is done only in Green and Blue plane but not in red-plane because the R-plan is similar to the skin pixels. So by changing the Red –plane pixel values may not give the exact mask image at the receiver side. By this data can't be extracted properly.

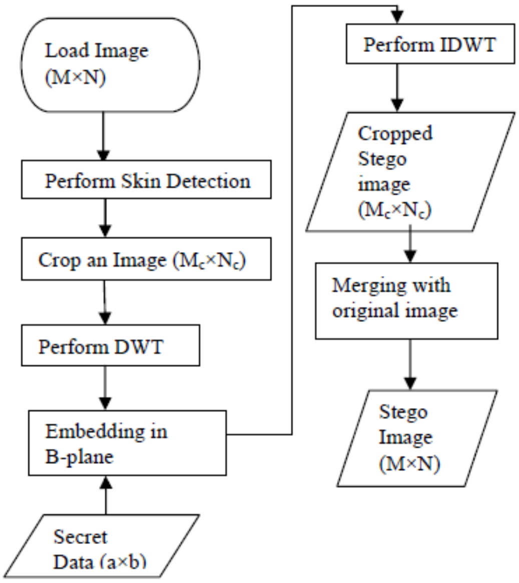

Fig 2: .Flowchart of embedding process

Step 5: In this we Perform inverse Discrete Wavelet Transform to combine all the four sub-bands.

Step6: In this step the stego image which is obtained in the above step of size (M_cxN_c) should be same as the original but it is not .So we have to keep this cropped image into original image which will give us a image of size (MxN).For bringing back this original image we should have the last and first pixels of the cropped image. So now the original image is ready for transmitting.

3.4: Extraction process

The received image which is of 24-bit color image and of size MxN will be given as input to the extraction process. Then for finding the skin pixels and cropping the image we should know the cropped area used by the transmitter side which can be stored in a variable called 'rect' .This is also called as key to the receiver or decoder. Then by knowing the key value the next steps will exact opposite to the transmitter side. But while doing cropping proper care should be taken because same size of square should be taken to get the exact data. Now by detecting the HH sub-band we can extract the secret message. Extraction procedure is represented as:

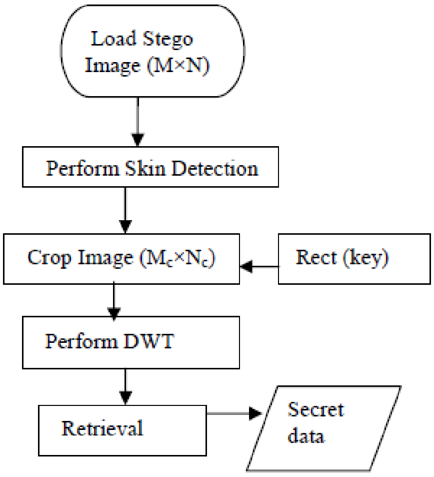

Fig 3:Flowchart of extration process

4. FINAL RESULTS

In this section we have the simulation results for the proposed model. We used MATLAB 2013a version. First we take the Input image of jpg format as in figure(a) then the secret message or data what we embedded is shown in figure(b).Then we perform the skin tone detection and we find the skin pixels followed by cropping which also acts as a key at the receiver side is shown figures (c),(d). Finally the stego image is shown in figure (e).Then the extracted data from stego image is shown in figure (f).

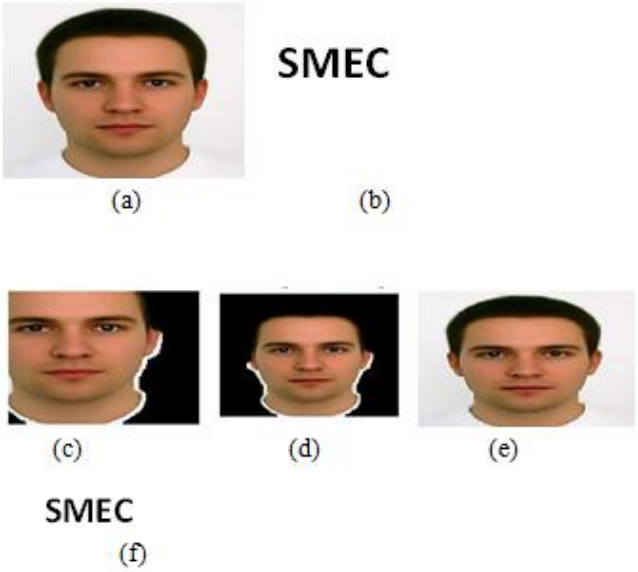

Figure4: a) cover image b) Secret data c) face segmented image d) Cropped image e) stego image f)extracted data

5. CONCLUSION

Steganography is the best part of scientific are which come under the security systems. In this paper steganography is done on the biometric features where the skin region are used for embedding the message which is known by performing DWT. By embedding data in only certain region (here skin region) and not in total image security is enhanced. Due to the cropping technique the security is maintained at a respectable level because no one can extract the message without knowing the value of cropped area. Coefficients obtained from the Discrete Wavelet Transform are used for embedding the secret message. Hence the quality of the image is also increased because we hide data only in the high frequency sub-bands which is unnoticeable to the human eyes. According to simulation results, proposed approach provides fine image quality.

REFERENCES

[1] An Analysis of steganographic system by R.Ropa in 1998.Department of CSE

[2] S.Sadkhan (2004) ,Cryptography in current status and future trends,in IEEE

[3] J.C Judge (2001), Steganography for past, present, future. SANS Publications.

[4] J.Fridrich,Goljan M and Du R in 2001 about the Reilable Detection of least significant bits steganography in Grayscale and colour images

[5] C.Chang,Chen T.S and Chung L,in 2002 about "A steganography based on JPEG ",department of Information Sciences

[6] Phung,S.L.Bouzerodoum and Chai.D about "Skin colour space in Ycbcr and it's application in human face" published in IEEE vol.1,289-292 in 2002

[7] Albiol,A.Torres,L.Delp in 2001 about "colour spaces for skin tone detection" published in ICIP

[8] A.Cheddad,Joan Condell,Kevin Curran and Paul Mc.Kevitt in 2008 about "Biometric digital image stegnaography" published in IEEE conference.

[9] A.Cheddad,Joan condell,Kevin curran and paul Mc kevitt in 2009 about "skin tone detection algorithm for steganography"

[10] K.Sobottka and I.Pitas in 1996 about"Extraction of facial region and feature using colour models " published in IEEE conference

[11] P.Chen and E.C Liao in 2002 about "Haar Wavelet Transform" published in IEEE