Volume 3, Issue 3, March 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Biometric Steganographic Technique Using DWT and Encryption

Amritha.G
Department Of CSE
Calicut University, India

Meethu Varkey
Department Of CSE
Calicut university, India

Abstract— Steganography is the art of hiding the existence of data inanother transmission medium to achieve secret communication . Steganography method used in this paper is based on biometrics, ie biometric steganography. And the biometric feature used to implement steganography is skin tone region of images. Here secret data is embedded within skin region of image that will provide an excellent secure location for data hiding. Before embedding secret data is needed to be encrypted using stream cipher encryption scheme RC4.Skin color tone detection is performed by using HSV color space.DWT is the frequency domain in which this biometric steganography is implemented.Secret data is embedded in one of the high frequency subband by tracing the number of skin pixels in that band. Different embedding steps are embedded on the cropped region of the image.ie value of this cropped region will act as a key at the decoder side. 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 also satisfactory PSNR (PeakSignal-to-Noise Ratio) is obtained

Keywords— Biometrics,Skin tone detection,DWT, cropping,PSNR,RC4.

I. INTRODUCTION

Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography.

Steganography, derived from Greek, literally means "covered writing." It includes a vast array of secret communications methods that conceal the message's very existence. These methods include invisible inks, microdots, character arrangement, digital signatures, covert channels, and spread spectrum communications. Steganography and cryptography are cousins in the spycraft family. Cryptography scrambles a message so it cannot be understood. Steganography hides the message so it cannot be seen. A message in ciphertext, forinstance, might arouse suspicion on the part of the recipient while an "invisible" message created with steganographic methods will not. Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels.

Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret . Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect a nd can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated . The strength of steganography can thus be amplified by combining it with cryptography.

Two other technologies that are closely related to steganography are watermarking and fingerprinting. The kind of information hidden in objects when using watermarking is usually a signature to signify origin or ownership for the purpose of copyright protection . With fingerprinting on the other hand, different, unique marks are embedded in distinct copies of the carrier object that are supplied to different customers. This enables the intellectual property owner to identify customers who break their licensing agreement by supplying the
property to third parties .

In steganography secret data is the data that the sender wishes to send to the receiver. it can be audio,video,image,text file,or other data.They are represented as the stream of bits.This secret data is hidden on the medium or cover or host.Medium of communication is also the image.In this paper secret data is restricted to digital images.Cover image with secret data embedded is called Stego-Image.

II. LITERATURE SURVEY

To a computer, an image is a collection of numbers that constitute different light intensities in different areas of the image. This numeric representation forms a grid and the individual points are referred to as pixels. Digital color images are typically stored in 24-bit files and use the RGB color model, also known as true color.Image steganography

techniques can be divided into two groups: those in the Image Domain and those in the Transform Domain . Image – also known as spatial – domain techniques. embed messages in the intensity of the pixels directly, while for transform – also known as frequency – domain, images are first transformed and then the message is embedded in the image.

A. Steganography In Spatial Domain

In this method secret data is embedded directly into the least significant bit (LSB)plane of the cover image.This method is also called LSB substitution.Example of such LSB embedding system developed is steganos ie, developed in Germany.

B. Steganography In Frequency Domain

This method is also called transform domain based steganography.In this method before embedding the secret data into the cover image,it is needed to be transformed into frequency domain coefficients.It is done by using DCT or DWT. Different sub-bands of freq domain coeff gives significant information about where the vital and non vital pixels of image resides.it is very complex method and take more time than spatial domain techniques. An example of a transform-basedsteganographic system is the "Jpeg-Jsteg" software ,which embeds the message by modulating DCT coefficientsof the stego-image based upon bits of the message and theround-off error during quantization . Transform-based steganography also typically offer increased robustness toscaling and rotations or cropping, depending on the invariant properties of a particular transform.

C. Adaptive Steganography

This method is also called "*statistics aware embedding*" or *"masking*".

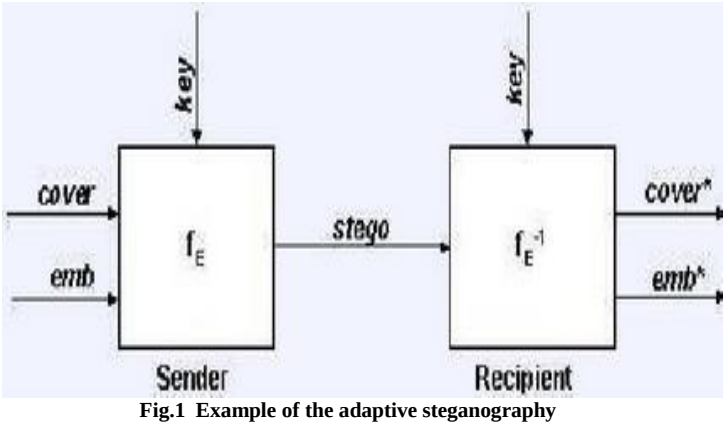

Fig.1 Example of the adaptive steganography

fE - steganographic function "embedding"

fE -1- steganographic function "extraction".emb is the messege to be hidden.cover is the cover data in which secret data is hidden.stego is the cover data with secret data embedded.Key is the parameter of fE.

III. PROPOSED METHOD

This paper propose a dual biometric steganographic technique using DWT and spread spectrum.Dual in the sense that before embedding the secret data in cover image secret data is needed to be encrypted.In this method secret data is embedded in the skin region of the image.for that skin color tone detection is needed to be performed.it is by using HSV color space.Then cropping is needed to be performed.DWT is needed to be applied on that cropped region of the image.Then one of the high frequency sub band is selected to embed the secret data.Before embedding the secret data it is needed to be encrypted using spread spectrum technique[9] .ie,generating pseudo random noise sequence by using a session based key.Then that encrypted data is embedded on the number of skin pixels in that high frequency subband.Then data is extracted at the decoder side by using the session key and size of the secret data

A. Skin Color Tone Detection

Instead of embedding data anywhere in the image secret data is needed to be embedded in the skin region of the image.For that input image is converted into an appropriate color space[1].Mainly two kinds of color spaces are suitable for biometric operations. HSV (Hue, Saturation and Value) and YCbCr(Yellow, Chromatic Blue, Chromatic red) spaces.

For the skin color tone detection [7] a skin detector and a skin classifier was there.Skin detector convert the cover image of RGB color space into appropriate color space.Skin classifier will classify pixels in the cover image to skin and non skin pixels by defining a boundary. 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).

For this paper HSV color space is choosen.For that first, the image in RGB was converted to HSV color space, because it is more related to human color perception. Hue-saturation based colorspaces were introduced when there was a need for the user to specify color properties numerically. 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 [H, 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].

Fig. 2 Orginal cover image

Fig 2 shows the orginal cover image.while converting it to HSV color space is shown in figure 3.Skin detector performs this job. considering now each channel HSV represented on the R, G and B channels.Hue means dominant color of the particular area.Saturation mean brightness in proportion to colorness.Value means intensity,ie the value associated with each of the pixel.

Fig. 3 Image in HSV

Skin pixels are marked as white and all other pixels as black.

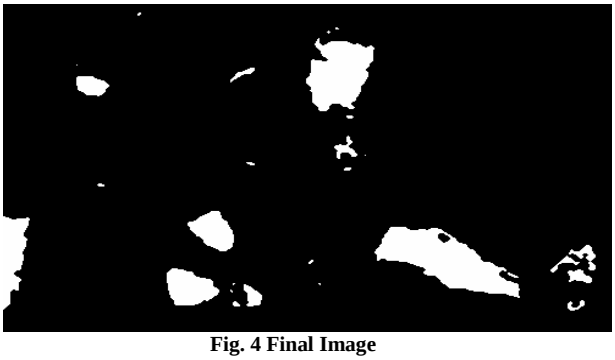

Fig. 4 Final Image

Skin pixels are marked as white and all other pixels as black.Figure 4 represent the final image after removing noise by using a morphological filter performing two operations such as dilation and erosion.Dilation means expand the skin regions to detect the imperfections Erosion operation will remove the imperfections.

B. 2D Haar DWT

DWT is the frequency domain in which this biometric steganography is implemented.The frequency domain transform we applied in this research is Haar-DWT, the simplest DWT. A 2-dimensional Haar- DWT consists of two operations: One is the horizontal operation and the other is the vertical one. Detailed procedures of a 2-D Haar-DWT are described as follows:

Step 1: At first, scan the pixels from left to right in horizontal direction. Then, perform the addition and subtraction operations on neighboring pixels. Store the sum on the left and the difference on the right as illustrated in Figure 4. Repeat this operation until all the rows are processed. The pixel sums represent the low frequency part (denoted as symbol L) while the pixel differences represent the high frequency part of the original image (denoted as symbol H).

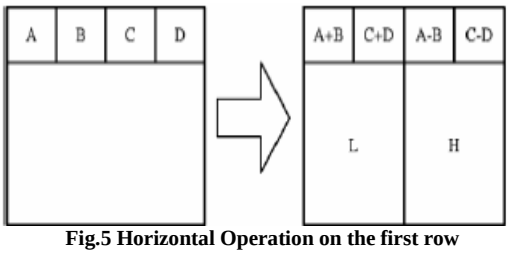

Fig.5 Horizontal Operation on the first row

Step 2: Secondly, scan the pixels from top to bottom in vertical direction. Perform the addition and subtraction operations on neighboring pixels and then store the sum on the top and the difference on the bottom as illustrated in Fig 5.

Repeat this operation until all the columns are processed. Finally we will obtain 4 sub-bands denoted as LL, HL, LH, and HH respectively. The LL sub-band is the low frequency portion and hence looks very similar to the original image

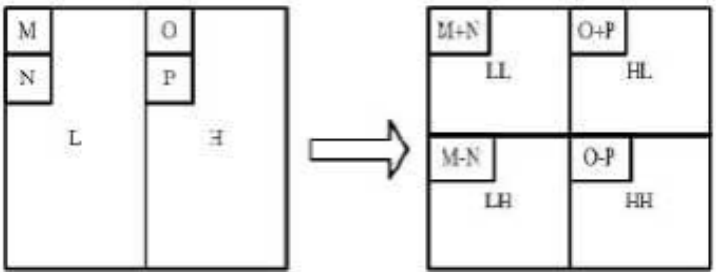

Fig. 6 Vertical Operation

The whole procedure which has been described above is called the first-order 2-D Haar-DWT. The first-order 2-D Haar- DWT applied on the image "Lena" is illustrated in Fig 7.

Fig. 7 (a) Original image-Lena, (b) Result after the first-order 2-D Haar-DWT

C. RC4 Image Encryption

A secret key cryptosystem encrypt image pixel by pixel, with the RC4 algorithm. RC4 convert original image to encrypted image one bit at a time. The simplest implementation of a RC4 is shown in Figure8.In this structure a key is input to the keystream generator.A keystream generator (sometimes called a running-key generator) outputs a stream of bits: K1, K2, K3,……, Ki. This keystream is XORed with a stream of plaintext bits, P1, P2, P3,….,Pi to produce the stream of ciphertext bits C1, C2,……Ci.Key stream generator is also called pseudo random generator.

$$C_i = P_i \oplus K_i$$

RC4 system consists of two main parts [5]:

1- Algorithm to generate keystream. 2- XOR gate

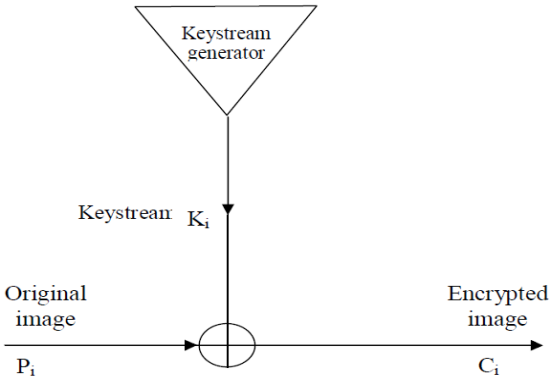

Fig 8. RC4 Encryption Process

Orginal image pixels are encrypted by using a keystream to generate encrypted image.so a user defined key is given to a keystream generator to produce an encrypted image pixel stream Ci.For example when five character ASCII code given to a keystream generator is translated to 40 character binary equivalent or key stream which is used to encrypt the binary image.output of the key stream generator depend on the value of input key and the keystream generated will have the properties of true random number stream.ie,there should be an equal number of 0's and 1's.So RC4 is a well established stream cipher. RC4 was kept as a trade secret by RSASecurity.

D. Embedding Process

Before performing all steps of embedding process 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. Cropping provides enough security. 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.

Suppose C is original 24-bit color cover image of M×N size. It is denoted as: C= {xij, yij, zij |1 ≤ i ≤ M, 1 ≤ j ≤ N, xij, yij, zij Є {0, 1,.., 255}} Let S is secret data. Here secret data considered is binary image of size a×b.Let size of cropped image is Mc×Nc where Mc≤M and Nc≤N and Mc=Nc. i.e. Cropped region must be exact square as we have to apply DWT later on this region.

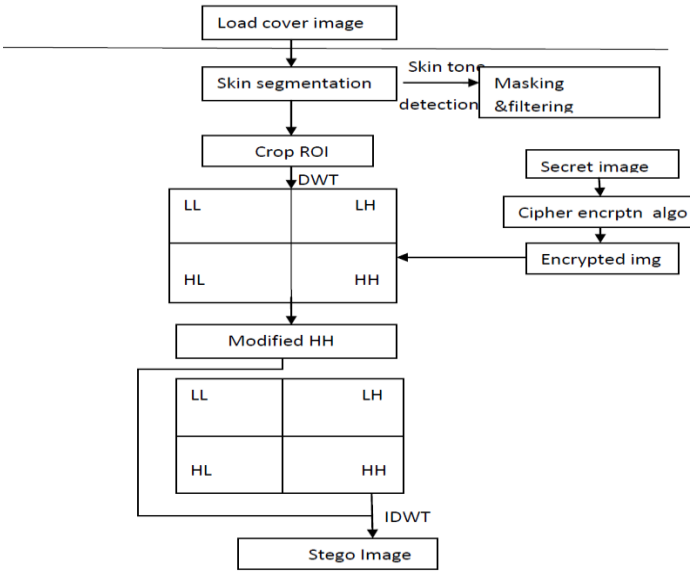

Fig.9 Image Hiding Process

Step 1: Cover image is loaded & skin color detection is performed using HSV
Step 2:. Segment out skin pixels by performing masking and filtering
Step 3:Crop the particular ROI
Step 4: Load secret image and encrypt it using the cipher encryption algorithm RC4
Step 5: Calculate the payload
Step 6:Encrypted secret image is embedded in only the skin pixel region of high frequency sub-band of cover image
Step 7:Perform IDWT to combine four frequency subbands
Step8:Merge it with orginal cover image to form stego image

Using DWT the Cover image is decomposed into four sub bands (LL, LH, HL and HH). Binary images ie, Secrete Image is taken and encrypted using stream cipher algorithm RC4. RC4 is a well-established stream cipher and its security has been investigated in depth. Thus the homomorphic cipher scheme applied here is secure and thus the encrypted secret image is obtained and it is needed to embed in the skin pixel region of HH subband by calculating the payload.payload is calculated .ie number of skin pixels find in the high frequency subband is calculated . Embedding is done as per raster-scan order that embeds secret data coefficient by coefficient in selected sub-band , if coefficient is skin pixel.Taking all the sub bands including the modified HH and LH sub bands, stego image is obtained applying IDWT (Inverse Discrete Wavelet Transformation)

E. Extraction Process

Step1 :Load stego image of size m x n
Step2: .Perform skin detection
Step3: Retrive the cropped region of the image by using the key
Step4: Perform DWT on the cropped region of the image
Step5: Recover the secret image using secret key used for encryption
Step6:Retrive the distorted secret image
Step7:Reduce noise components in the image using wiener filter
Step8: Result is the orginal hidden image

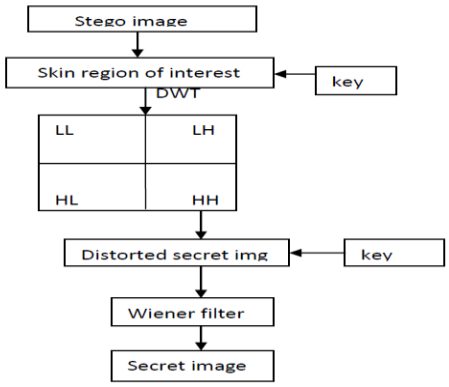

Fig.10 Image Extraction Process

IV. PERFORMANCE EVALUATION

Peak Signal to Noise Ratio (PSNR). Performance measurement for image distortion is well known as peak signal to noise ratio (PSNR) which is classified under the difference distortion metrics can be applied on stego images. We use Peak signal to noise ratio (PSNR) to evaluate quality of stego image after embedding the secret message .This is basically a performance metric and use to determine perceptual transparency of the stego image with respect to cover image.It is measured in terms of decibel(db).Higher the PSNR higher the quality of the image(which means there is a little difference between cover image and stego image)..Quality of the image is more when it is greater than 40db and less when PSNR is 30db or low.ie PSNR is measured in terms of MSE(Mean Square Error).Thus performance can be measured. PSNR is defined by using the following equation.

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

Where MSE is defined as follows

$$MSE = (1/(M \times N))\sum_{i=1}^{M}\sum_{j=1}^{N}(X_{ij}Y_{ij})^2$$

V. ATTACKS ON STEGO IMAGE

When stego image is transmitted it may be corrupted due to noise. Besides noise this image may undergo attack like rotation, scaling, cropping etc. Here two attacks (i) addition of salt and pepper noise-ie random introduction of black and white pixels on to the color image (ii) rotation of stego image have been taken.

VI . Expected Results

Here the Figure 11 shows the secret image and its encrypted form.Figure 12 shows orginal cover image to which we are going to hide the secret image.Figure 13 shows the cropped skin region ie, the ROI.Figure14 shows DWT applied on the cropped region of interest(ROI).Then the secret image is hidden on the high frequency (HH)subband by calculating the payload.ie identyfing the number of skin pixels in the HH subband.ie,hiding the encrypted secret image in the skin pixels of the high frequency subband.Figure 15 shows the cropped stego image.ie the cropped region to which the secret image is hide.Figure 16 shows the reconstructed stego image ie obtained by combining the cropped stego image with the orginal cover image by performing an IDWT

Fig.11 a)secret image b) its encrypted form

fig.12 Orginal cover image

VII.CONCLUSION

The goal of steganography is to avoid drawing suspicion to the transmission of a hidden message. In this paper approach for steganography is object oriented i.e. it is based on one of the feature of image. Here the feature used is skin region of image i.e. biometric approach. Instead of using whole image, embedding data only within the skin regions

provide an excellent secure location for data hiding. Encrypt secret image using RC4 stream cipher algorithm before embedding enhances the security level. The quality of recovered message is not degraded even if the stego-image is attacked after transmission. The proposed approach provides invisibility and fine image quality of the stego image, higher security and satisfactory PSNR.

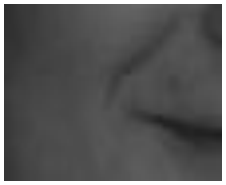

Fig.13 cropped skin region

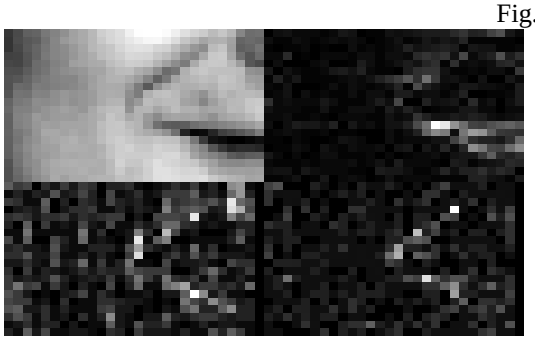

fig.14 DWT applied on cropped region

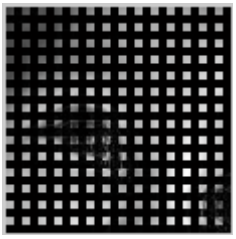

fig.15 cropped stego image

fig.16 Reconstructed Stego Image

.

REFERENCES

[1] A Secure Skin Tone based Steganography Using Wavelet Transform Anjali A. Shejul, Umesh L. Kulkarni, International Journal of Computer Theory and Engineering, Vol.3, No.1, February, 2011 1793-8201

[2] 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.

[3] A Novel Session Based Dual Steganographic Technique Using DWT and Spread Spectrum. International Journal of Modern Engineering Research (IJMER). Vol.1, Issue1, pp-157-161

[4] Schneier B.,"Applied Cryptography**,** Second Edition: Protocols, Algorithms andSource Code in C",John Wiley & Sons, Inc., USA, 1996

[5] Exploring Steganography:Seeing the Unseen

[6] Methodology of Spread-Spectrum Image Steganography,army research laboratory

[7] Object Oriented steganography Based On Biomertic And spread Spectrum. International Journal of Scientific & Engineering Research Volume 3, Issue 6, June-2012

[8] 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)

[9] Skin Detection using HSV color spaceV. A. Oliveira,A. Conci Computation Institute – Universidade Federal Fluminense – UFF – Niter • i, Brazil. {victor_oliveira , aconci}@ic.uff.br

[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

