# A Security Enhanced Approach For Digital Image Steganography Using DWT And RC4 Encryption

Amritha.G[#1], Meethu Varkey[*2]

[#]*CSE Department,KMCT College Of Engg,Calicut University*
*Calicut,Kerala*

***Abstract*—Steganography is the art of hiding the existence of data in another transmission medium to achieve secret communication . Steganography method used in this paper is based on biometrics, 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 applied 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 satisfactory PSNR obtained**

***Keywords*—Biometrics,Skin detection,DWT,cropping,PSNR,RC4**

## I. Introduction

Internet is a worldwide and publicized medium that serves as an important role in data transmission and sharing.Message transmission over the internet still having many data security problems.ie some confidential data might be stolen,modified,copied or destroyed by intruders.This has driven the interest among computer security researchers to overcome the serious threats for secured data transmission. An approach to secured communication is cryptography,which deals with the data encryption at the sender side and data decryption at the receiver side.Another method of providing more security to data is information hiding.ie, Steganography.Steganography is the art of hiding the existence of data in another transmission medium. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words "*stegos*" meaning "cover" and "*grafia*" meaning "writing" defining it as "covered writing". In image steganography the information is hidden exclusively in images. The idea and practice of hiding information has a long history. it doesnot replaces the cryptography

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.

The different requirements that need to be considered while designing a steganographic system are invisibility,payload capacity,independent of the file format,robustness aganist statistical attack

## II. Literature Survey

. There is Steganography In Spatial Domain and steganography in frequency domain.In first case 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.Steganography In Frequency Domain 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 the round-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.

## III. Image Steganography

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.

## IV. Biometric Steganography

Instead of embedding the secret data anywhere in the cover image data is going to embedd only on some selected regions.This project takes the advantage of Biometric features such as skin tone.Because skin region is not much sensitive to HVS(Human Visual System).That is secret data is embedded within the skin region of the image such as facial regions,hand etc.Hence the name biometric.Biometrics or biometric authentication refer to the identification of humans by their traits or characteristics.Biometrics in computer science is the form of identification

## V. Proposed Method

This paper propose a biometric steganographic technique using DWT and encryption.It is based on the concept that before embedding the secret data in cover image,secret data is needed to be encrypted.It provide high degree of security.ie,two keys are used.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 stream cipher encryption,RC4.ie, a key is given to a key generator produces a key stream.By using that key stream binary secret image is encrypted by doing an XOR operation produces encrypted image.Encryption is performed as pixel by pixel.Then that encrypted image is embedded on the number of skin pixels in that high frequency subband.Then data is extracted at the decoder side by using two keys.ie, value of cropped region will act as a key1 .Key2 is those that is used to encrypt the secret image.So it is saying that it provide two layers of security.So this two keys are used at the decoder side in order to extract the 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. 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.

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

### *B. 2D Haar DWT*

DWT is the frequency domain in which this biometric steganography is implemented.DCT is not preferred.This is because of the following disadvantages.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. It offers better energy compaction than DCT

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). 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:

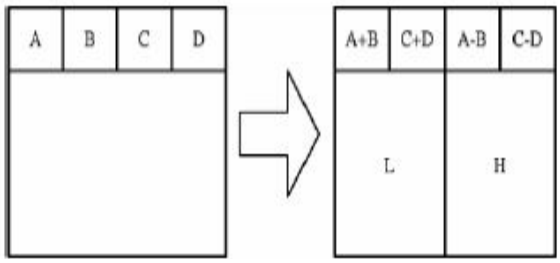


Fig.1 Horizontal Operation on the first row

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

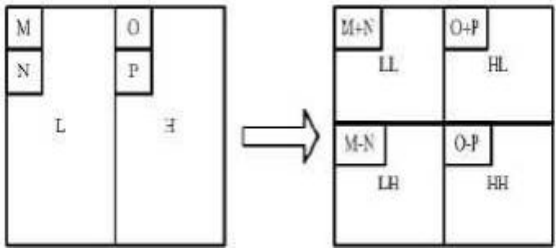


Fig.2 Vertical Operation

The whole procedure which has been described above is called the first-order 2-D Haar-DWT. The figure below shows the four frequency subbands that is formed

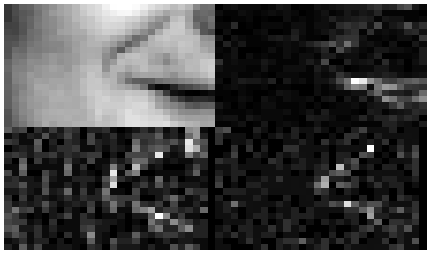

Fig.3 Image after performing 2D Haar

### 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 Figure. 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.

$$C_i = P_i \oplus K_i$$

RC4 system consists of two main parts [5]:

1- Algorithm to generate keystream.
2- XOR gate

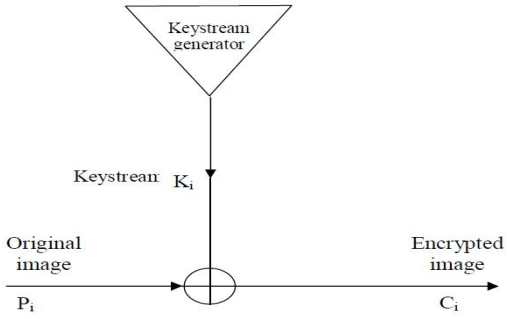


Fig 4. Image Hiding Process

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. The RC4 algorithm is remarkably simply and quite easy to explain. A variable-length keyof from 1 to 256 bytes (8 to 2048 bits) is used to initialize a 256-byte state vector S, withelements S[0], S[1], …, S[255]. At all times, S contains a permutation of all 8-bit numbers from 0 through 255. For encryption and decryption, a byte *k* is generated from S byselecting one of the 255 entries in a systematic fashion. As each value of *k* is generated, the entries in S are once again permuted.

### 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.Cropped region need not be a rectangle.It can be set based on the size of the secret data that is going to be embed. DWT is then going to be performed on the particular cropped area ie,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.After selecting the particular ROI secret data is embed only on skin pixel region by comparing the pixels in the cropped region with the image after ski tone detection

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.

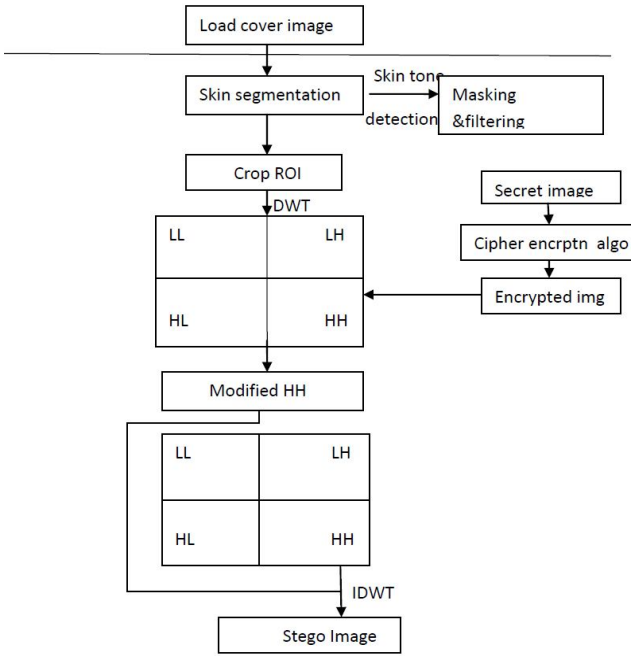


Fig.5 Image Hiding Process

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*

Embedded data is going to be extracted by using the size of the image,ie by using the value of cropped region will act as a key1 and the key that is used for encryption is needed to be known for the extraction of secret data.it will act as key2.RC4 stream cipher encryption is used.So the same key that is used for the secret dataencryption is used for the decryption of secret data

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

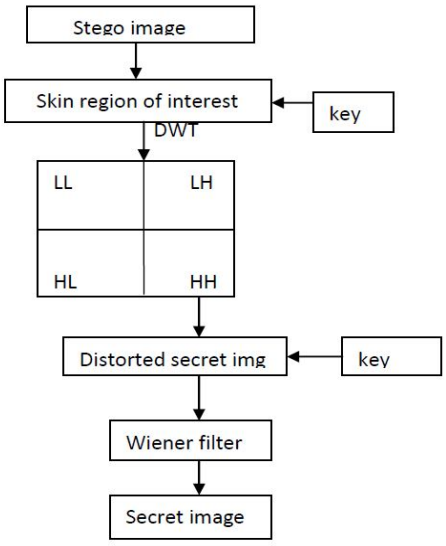


Fig.6 Image Extraction Process

## VI. 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

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

## VII. EXPERIMENTAL RESULTS

The cover image is color image which is of size m*n.The secret image is the binary image.

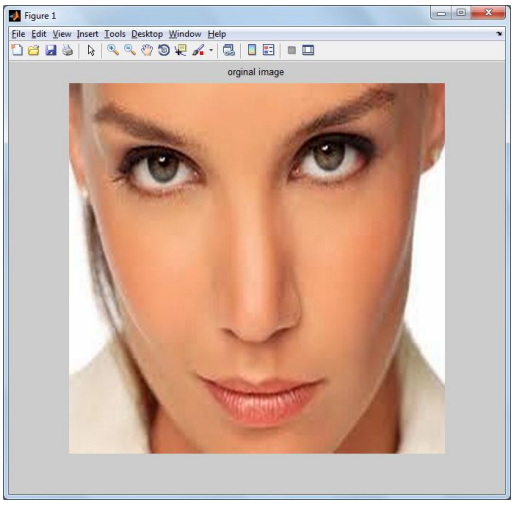


fig.7 Orginal cover image


fig.8 secret image


fig.9 Encrypted Secret Image

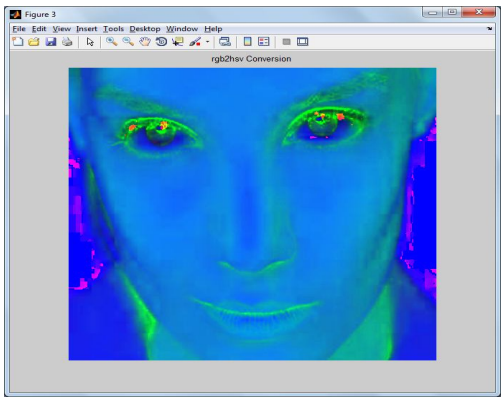


fig.10 Image after rgb2hsv conversion

Figure10 shows the image after rgb2hsv conversion.Figure 11 shows the image after skin tone detection.Then figure 12 shows the cropped stego image.Then embedding is performed on the high frequency subband..Inverse dwt is performed after embedding.Then stego image is obtained and then secret

image is reconstructed after removing noise in the distorted stego image

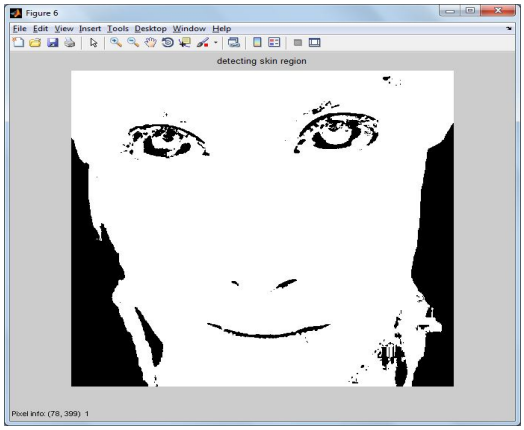


Fig.11 Image after skin tone detection

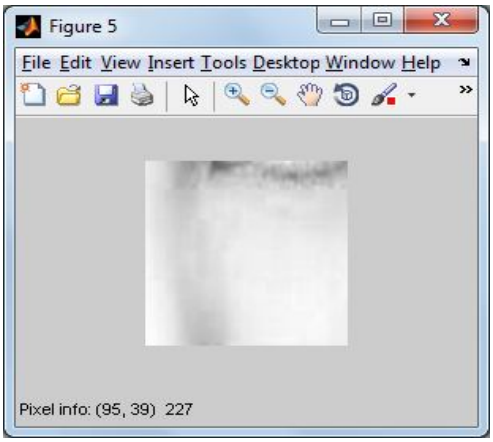


Fig.12 cropped skin region

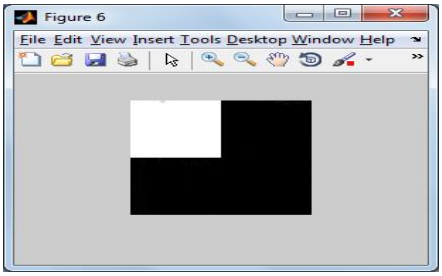


fig.13 DWT applied on cropped region

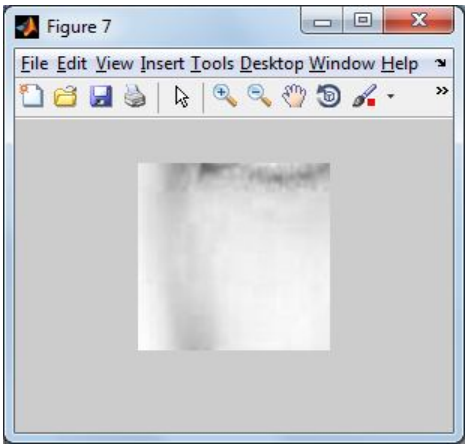


fig.14 cropped stego image

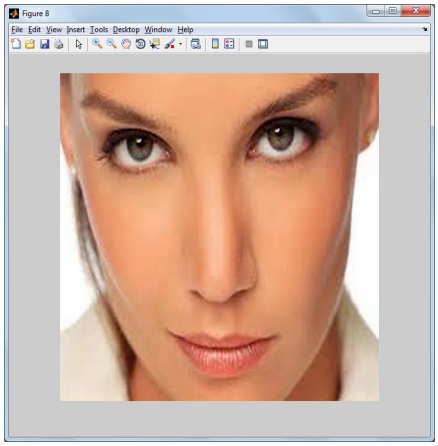

fig.15 Stego Image

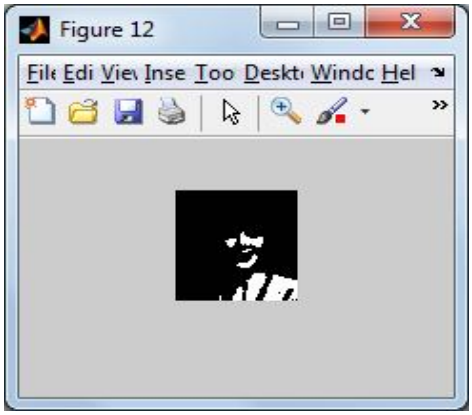


fig.16 Reconstructed Stego Image

## VIII. 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 the 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.

## 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