ISSN:0975-9646

Robust and Secure Data Hiding in Image Using Biometric Technique

N. Lavanya , V.Manjula, N.V. Krishna Rao
Dept of CSE.
Institute of Aeronautical Engg
Hyderabad, India

***Abstract* --- Steganography method used in this paper is based on biometrics. 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.**

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 outperforms 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.. And also satisfactory PSNR (Peak-Signal-to-Noise Ratio) is obtained.

***Keywords*-Stegoanalysis, PSNR (Peak- Signal-to-Noise Ratio), DWT (Discrete Wavelet Transform), Skin tone detection.**

I. INTRODUCTION

Information hiding is a general term encompassing many sub disciplines. One of the most important subdisciplines is steganography as shown in Figure 1. Steganography,is derived from a work by Johannes Trithemus (1462-1516) entitled ”Steganographia” and comes from the Greek defined as ”covered writing”. It is an ancient art of hiding information in ways a message is hidden in an innocent looking cover media so that will not arouse an eavesdropper’s suspicion[19].

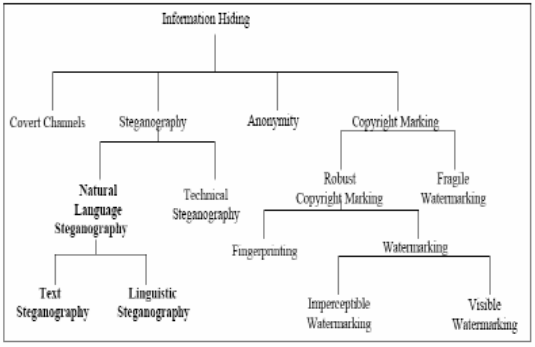


Fig. 1. Types of Information Hiding

A. *Image Steganography System*

A block diagram of a generic image steganographic system is given in Fig. 2.

A message is embedded in a digital image (cover image) through an embedding algorithm, with the help of a secret key. The resulting stego image is transmitted over a channel to the receiver where it is processed by the extraction algorithm using the same key. During transmission the stego image, it can be monitored by unauthenticated viewers who will only notice the transmission of an image without discovering the existence of the hidden message.

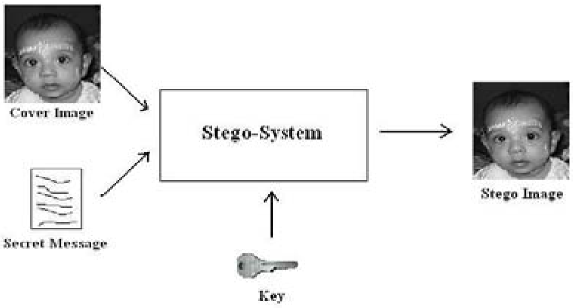


Fig. 2. Generic form of Image Steganography

B. Image Steganographic Techniques

The various image steganographic techniques are: (i) Substitution technique in Spatial Domain: In this technique only the least significant bits of the cover object is replaced without modifying the complete cover object. It is a simplest method for data hiding but it is very weak in resisting even simple attacks such as compression, transforms, etc. (ii)Transform domain technique: The various transform domains techniques are Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Fast Fourier Transform (FFT) are used to hide information in transform coefficients of the cover images that makes much more robust to attacks such as compression, filtering, etc. (iii) Spread spectrum technique: The message is spread over a wide frequency bandwidth than the minimum required bandwidth to send the information. The SNR in every frequency band is small. Hence without destroying the cover image it is very difficult to remove message completely. (iv)Statistical technique: The cover is divided into blocks and the message bits are hidden in each block. The information is encoded by changing various numerical properties of cover image. The cover blocks remain unchanged if message block is zero. (v) Distortion technique: Information is stored by signal distortion. The encoder adds sequence of changes to the cover and the decoder checks for the various differences between the original cover and the distorted cover to recover the secret message.

C. Steganalysis

Steganalysis is the science of detecting hidden information. 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. Mean while active attacks 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.

This paper has been organized as following sections: Section II describes some related works, Section III deals with proposed method. Algorithms are discussed in Section IV and Experimental results are shown in Section V. Section VI contains the analysis of the results and Section VII draws the conclusion.

II. RELATED WORK

An effective data-hiding scheme that embeds data in image using Wavelet-based Steganography. A new idea in the application of wavelets. However, the standard technique of storing in the least significant bits (LSB) of a pixel still applies. The only difference is that the information is stored in the wavelet coefficients of an image, Instead of changing bits of the actual pixels. The idea is that storing in the least important coefficients of each 4 x 4 Haar transformed block will not perceptually degrade the image. While this thought process is inherent in most steganographic techniques, the difference here is that by storing information in the wavelet coefficients, the change in the intensities in images will be imperceptible.

III. PROPOSED METHOD

Steganographic method used in this project is based on biometrics. And the biometric feature used to implement Steganography is skin tone region of images. Here secret data is embedded within cropped skin region of the image which will provide an excellent secure location for data hiding. For this, skin tone detection is performed using HSV (*Hue, Saturation and Value*) color space.

At first skin tone detection is performed on the input image using HSV colour 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 results in greater 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. The secrete image is extracted by using DWT to the stego image.

IV. OVERVIEW OF STEGNOGRAPHY METHOD

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. 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. 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].

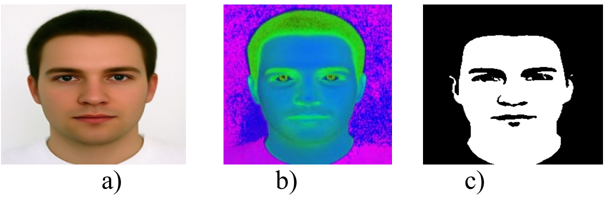


Fig.3. Cover image used in simulation system and its corresponding skin image a) cover image b) HSV image c) skin image

B. Discrete Wavelet Transform (DWT)

DWT applies on entire cropped 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 [12]. 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.

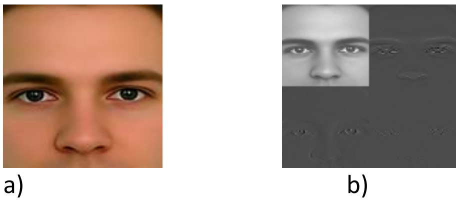


Fig.4. cropped image used in simulation system and its corresponding DWT image a) cropped cover image b) DWT of cropped cover image.

C. Embedding Process

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. Let S is secret data. Here secret data considered is binary image of size a×b. Fig. 5 represents flowchart of embedding process. Different steps of flowchart are given in detail below.

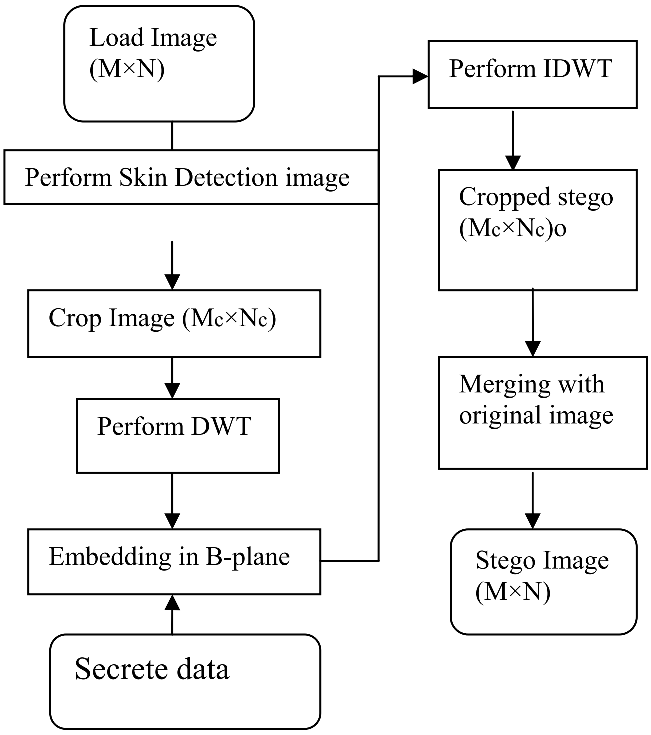


Fig.5. Flowchart of Embedding Process

a) Algorithm for embedding process

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: 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 DWT.

3) Step 3: Apply DWT to only cropped area (Mc×Nc) not whole image (M×N).

4) Step 4: Perform embedding of secret data in one of sub-band we choose high frequency HH sub -band.

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).

a) b)

Fig.6.a) Cover image b) Stego image

D. Extraction Process

Secret data extraction is explained as follows: 24 bit color stego image of size M×N is input to extraction process. We must need value of cropped area to retrieve data. 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. 7

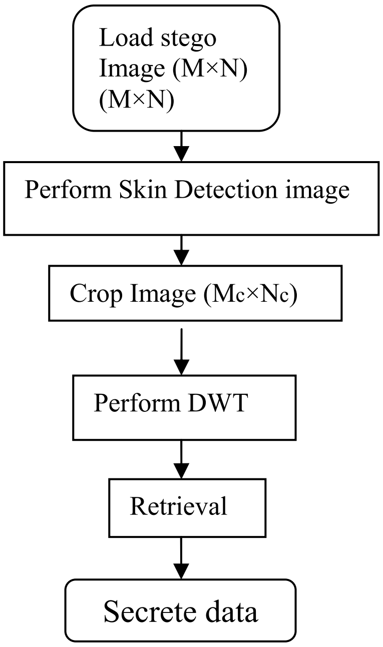
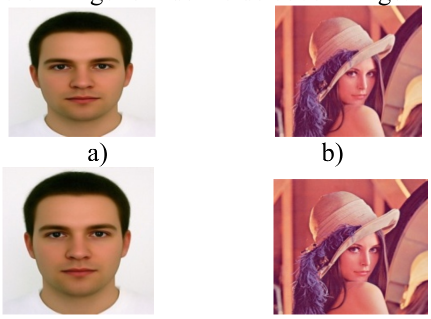


Fig.7. Flowchart of Extraction Process

IV. SIMULATION RESULTS

In this section we demonstrate simulation results for proposed scheme.This have been implemented using MATLAB 7.0. A 24 bit color image is employed as cover-image of size 356×356, shown in Fig. 4. Fig. 5 shows sample secret image to hide inside cover image.



a) b)

c) d)

Fig.8. a) cover image b) secrete image c) stego image d) secrete image

To establish an objective criterion for digital image quality, a parameter named PSNR (Peak Signal to Noise Ratio) is defined as follows:

$$PSNR = 10\log_{10}\frac{255^2}{MSE}$$

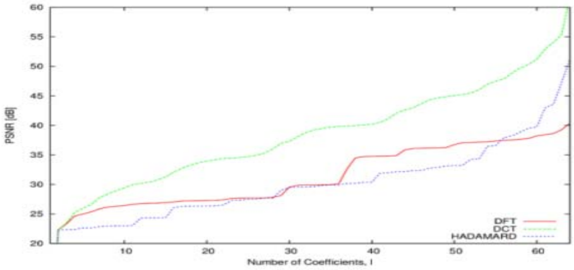


Fig.4 PSNR for Secrete image

MSE (Mean Square Error) stands for the mean-squared difference between the cover-image and the stego-image. The mathematical definition for MSE is:

$$MSE = (\frac{1}{M \times N})\sum_{i=1}^{M}\sum_{j=1}^{N}(a_{ij} - b_{ij})^2$$

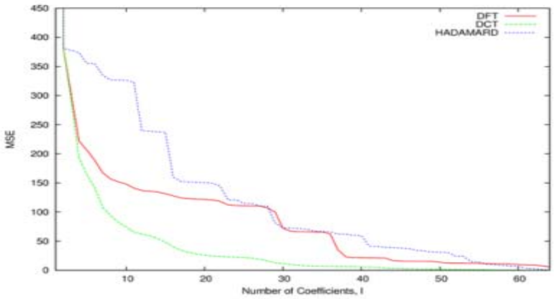


Fig .5 MSE for Secrete image

Where a_{ij} means the pixel value at position (*i*, *j*) in the cover image and b_{ij} means the pixel value at the same position in the corresponding stego-image. The calculated PSNR usually adopts dB value for quality judgment. The larger PSNR is, the higher the image quality is (which means there is only little difference between the cover-image and the stego-image)

CONCLUSION

We have introduced a new high capacity Steganography method in wavelet domain. The embedding process is then performed over the whole block, rather than in its bit-planes. This approach to the embedding ensures that no noisy bit-plane is left unused. Therefore, we achieve a much greater capacity as compared to that offered by previous methods, as confirmed by our analysis and experiments. The proposed approach to the embedding process may also be extended to other transform domains to improve the compromising interrelation between capacity and imperceptibility in image steganography.

ACKNOWLEDGMENT

The authors would like to thank to the earlier work regarding steganography whose guidance significantly contributed to the work made in this paper. All work done, images shown in this paper are for educational purpose and not for commercial purpose.

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

[3] 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

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

[5] Provos,N. and Honeyman, P: "*Hide and Seek: An introduction to steganography".* IEEE security and privacy, 01 (3): 32-44,May-June 2003

[6] Ahmed E., Crystal M. and Dunxu H.: "*Skin Detection-a short Tutorial"*, Encyclopedia of Biometrics by Springer-Verlag Berlin Heidelberg 2009

[7] 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)

[8] Chen,P. Y.and Liao,E.C., :*A new Algorithm for Haar Wavelet Transform,"* 2002 IEEE International Symposium on Intelligent Signal Processing and Communication System, pp.453-457(2002).