International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-3 Issue-5, June 2014

Secret Data Hiding in Images by using DWT Technique's

Swapnali Zagade, Smita Bhosale

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 [1]. Communication of data by maintaining confidentiality is a major issue everywhere, so to increase the security a non – conventional approach called steganography is proposed. "Steganography" is an art of "hiding data within data" [1, 2]. In general, Stego means "covering" and graphic means "writing". Combining these two terms gives the meaning of steganography, i.e. "covered writing" [2]. 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). In DWT Different techniques are used. 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 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 (Peak- Signal-to-Noise Ratio) is obtained and MSE.

Index Terms*— Skin tone detection, B-Panel, Cropping, DWT Security, PSNR, MSE.

I. INTRODUCTION

Steganography is a technique of hiding information in digital media. Steganography is the art of hiding the existence of data in another transmission medium to achieve secret communication. One method of providing more security to data is information hiding. The approach to secured communication is cryptography, which deals with the data encryption at the sender side and data decryption at the receiver side. The main difference between steganography and cryptography is the suspicion factor. The steganography and cryptography implemented together, the amount of security increases.It does not replace cryptography but rather boosts the security using its obscurity features.Steganography
is the art of inconspicuously hiding data within data. Steganography goal in general is to hide data well enough that unintended recipients do not suspect the steganography medium of containing hidden data. 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.

Manuscript published on 30 June 2014.
***** Correspondence Author (s)
Swapnali Zagade, Electronics and Telecommunication, Pune University, Pune, India.
Smita Bhosale, Electronics and Telecommunication, Pune University, Pune, India.

In steganography the secret image is embedded in the cover image and transmitted in such a way that the existence of information is undetectable. The digital images, videos, sound files and other computer files can be used as carrier to embed the information. The object in which the secret information is hidden is called covert object. Stego image is referred as an image that is obtained by embedding secret image into covert image. The hidden message may be plain text, cipher text or images etc.Steganography, copyright protection for digital media and data embedding are the data hiding techniques. Steganography is a method of hiding secret information using cover images. The various steganography techniques are: (i) Substitution technique: 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. The main aspect of steganography is to achieve high capacity, security and robustness.

- Cover Image: It is defined as the original image into which the required secret message is embedded. It is also termed as innocent image or host image. The secret message should be embedded in such a manner that there are no significant changes in the statistical properties of the cover image. Good cover images range from gray scale image to colored image in uncompressed format.
- Stego image: It is the final image obtained after embedded the payload into a given cover image. It should have similar statistical properties to that of the cover image.

- Hiding Capacity: The size of information that can be hidden relative to the size of the cover without deteriorating the quality of the cover image.
- Robustness: The ability of the embedded data to remain intact if the stego image undergoes transformation due to intelligent stego attacks.
- Security: This refers to eavesdropper's inability to detect the hidden information.
- Mean Square Error (MSE): It is the measure used to quantify the difference between the initial and the distorted or noisy image.

Rest of the paper is organized as follows. Section II presents literature survey and theoretical background. In section III proposed method is described in detail with skin tone detection, DWT, embedding and extraction procedure step by step & Detail Block Diagram. Section IV demonstrated the experimental results. Finally conclusion.

II. LITERATURE SURVEY

The earliest recordings of Steganography were by the Greek historian Herodotus in his chronicles known as "Histories" and date back to around 440 BC. In the 15th and 16th century, Romans used invisible inks, which were based on natural substances such as fruit juices and milk. During the times of WWI and WWII, significant advances in Steganography took place. Concepts such as null ciphers (taking the 3rd letter from each word in a harmless message to create a hidden message, etc), image substitution and microdot (taking data such as pictures and reducing it to the size of a large period Piece of paper) were introduced and embraced as great Steganographic techniques.

A) *Wavelet Transform*

Wavelet transform is used to convert a spatial domain into frequency domain. The use of wavelet in image stenographic model lies in the fact that the wavelet transform clearly separates the high frequency and low frequency information on a pixel by pixel basis. Discrete Wavelet Transform (DWT) is preferred over Discrete Cosine Transforms (DCT) because image in low frequency at various levels can offer corresponding resolution needed.

B) Haar Wavelet

It is a piecewise wavelet that provides orthogonal decomposition given as Wavelet Transform: It converts an image from time or spatial domain to frequency domain. It provides a time frequency representation. The Wavelet Transform is obtained by repeated filtering of the coefficients of the image row-by-row and column-by-column. The Haar Wavelet Transform is the simplest of all wavelet transform. In this the low frequency wavelet coefficient are generated by averaging the two pixel values and high frequency coefficients are generated by taking half of the difference of the same two pixels. The four bands obtained are approximate band (LL), Vertical Band (LH), Horizontal band (HL), and diagonal detail band (HH). The approximation band consists of low frequency wavelet coefficients, which contain significant part of the spatial domain image. The other bands also called as detail bands consists of high frequency coefficients, which contain the edge details of the spatial domain image.

C) 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 gray- level 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. 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.

D) 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.

E) Adaptive Steganography

Adaptive Steganography is special case of two former methods. It is also known as "Statistics aware embedding" and "Masking". This method takes statistical global features of the image before attempting to embed secret data in DCT or DWT coefficients. The statistics will dictate where to make changes.

F) Haar Discrete Wavelet Transform

Wavelet transform has the capability to offer some information on frequency-time domain simultaneously. In this transform, time domain is passed through low-pass and high-pass filters to extract low and high frequencies respectively. This process is repeated for several times and each time a section of the signal is drawn out. DWT analysis divides signal into two classes (i.e. Approximation and Detail) by signal decomposition for various frequency bands and scales. DWT utilizes two function sets: scaling and wavelet which associate with low and high pass filters orderly. Such a decomposition manner bisects time reparability. Haar wavelet operates on data by calculating the sums and differences of adjacent elements. This wavelet operates first on adjacent horizontal elements and then on adjacent vertical elements. One nice feature of the Haar wavelet transform is that the transform is equal to its inverse. Each transform computes the data energy in relocated to the top left hand corner. Figure 1 shows the image Lena after one Haar wavelet transform.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

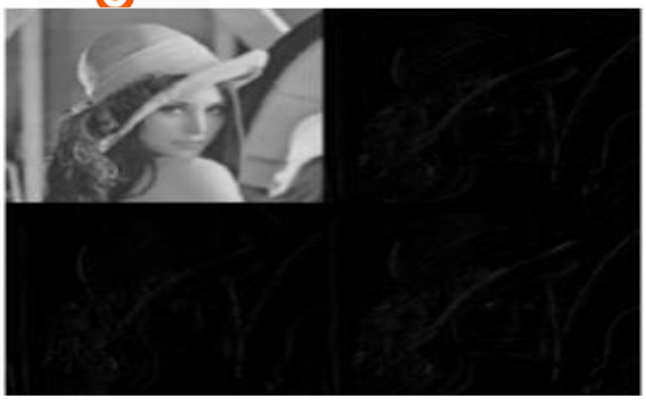

Fig. 1 The Image Lena After One Haar Wavelet Transforms

After each transform is performed the size of the square which contains the most important information is reduced by a factor of 4.

III. PROPOSED METHOD

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 image 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. Steganography in the transform domain involves the manipulation of algorithms and image transforms. These methods hide secret image in more significant areas of the cover image, making it more robust.

HSV (Hue, Saturation, and Value) Hue-saturation based colorspaces were introduced when there was a need for the user to specify color properties numerically. They describe color with intuitive values, based on the artist's idea of tint, saturation and tone. Hue defines the dominant color (such as red, green, purple and yellow) of an area; saturation measures the colourfulness' of an area in proportion to its brightness. The "intensity", "lightness" or "value" is related to the color luminance. The intuitiveness of the color space components and explicit discrimination between luminance and chrominance properties made these colorspaces popular in the works on skin color segmentation.

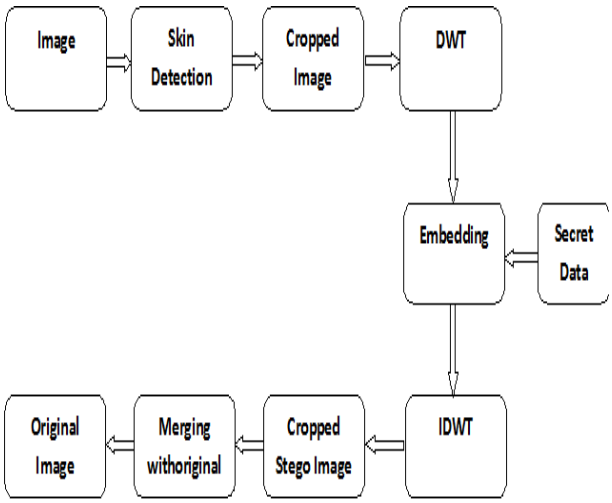

Fig. 2 Block Diagram of Embedding Process

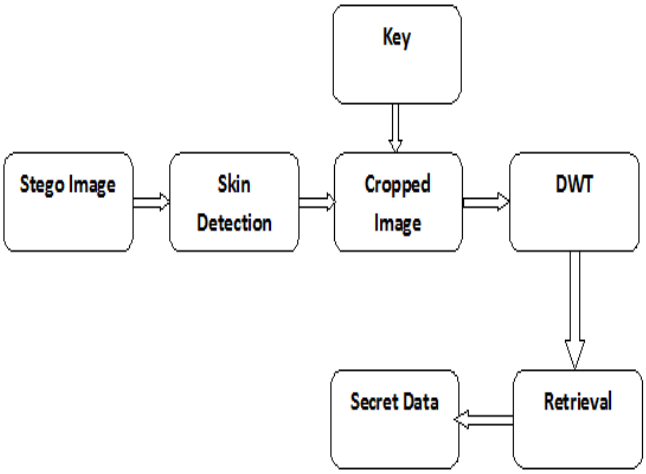

Fig. 3 Block Diagram of Extraction Process

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 subands. 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.

Advantages of Proposed Method:

1. By embedding data in only certain region (here skin region) and not in whole image security is enhanced.
2. Also image cropping concept introduced, maintains security at respectable level since no one can extract message without having value of cropped region.
3. It increases the quality of stego because secret messages are embedded in high frequency sub-bands which human eyes are less sensitive to.
4. The proposed approach provides fine image quality.

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.[9] and Another challenge comes from the fact that many objects in the real world might have skin-tone colors.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

This causes any skin detector to have much false detection in the background if the environment is not controlled [10]. 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.Mainely 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 [11] 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 cause's 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 bands. 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= {xij, yij, zij |1 ≤ i ≤ M, 1 ≤ j ≤ N, xij, yij, zij Є {0, 1... 255}}

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. 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 on mask 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 Haar 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.

3) Step 3: Apply DWT to only cropped area (Mc×Nc) not hole image (M×N). This yields 4 sub-bands denoted as HLL, HHL, HLH, and 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 embedding as 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. Here using only 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 that embeds secret data coefficient by coefficient in selected sub-band [6], if coefficient is skin pixel.

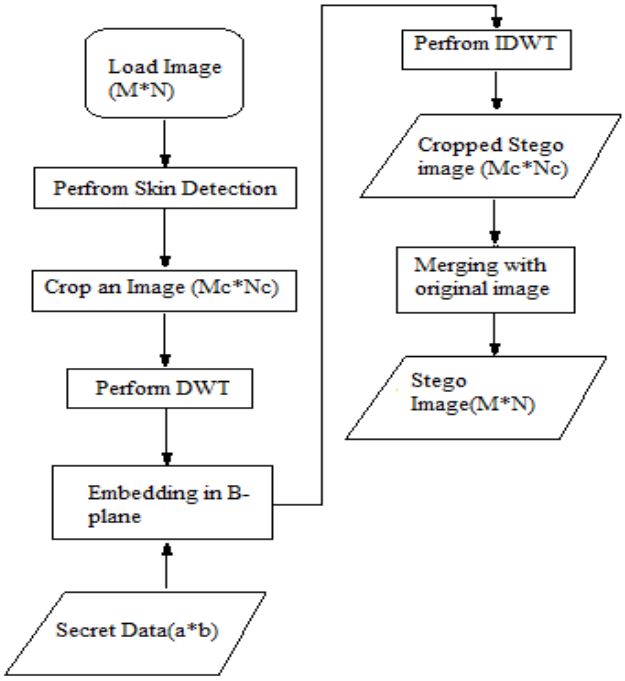

Fig. 4 Flowchart of Embedding Process

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 with original image to get the stego image of size M×N.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

To perform merging we require coefficients of first and last pixels of cropped area in original image so that r calculated. Thus a stego image is ready for quality evaluation.

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. 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. 2

IV. SIMULATION RESULTS

In this section we demonstrate simulation results for proposed scheme. These have been implemented using MATLAB 7.8. A 24 bit color image is employed as cover-image of size 256×256, shown in Fig. 6. Fig. 7 shows sample secret image to hide inside cover image.

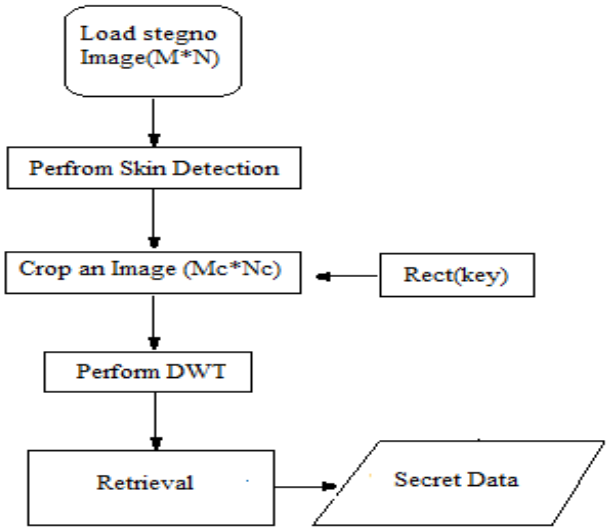

Fig. 5 Flowchart of Extraction Process

Fig. 6 Cover Image

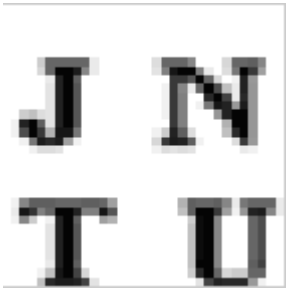

Fig. 7 Logo Image

The secret message S is gray image of size 32×32. We use Peak signal to noise ratio (PSNR) to evaluate quality of stego image after embedding the secret message. The performance in terms of capacity and PSNR (in dB) is demonstrated for the method in the following subsections.PSNR is defined as per Eq.3 and Eq.4.

$$PSNR = 10 \log_{10} (2552/MSE) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots (3)$$

$$MSE = (1/(M \times N)) \sum_{i=1}^{M} \sum_{j=1}^{N} (xij - yij)^2 \quad \ldots\ldots (4)$$

Xij and yij represents pixel values of original cover image and stego image respectively. The calculated PSNR usually adopts dB value for quality judgement, the larger PSNR is, higher the image quality (which means there is a little difference between cover image and stego image).On the contrary smaller dB value means there is a more distortion. PSNR values falling below 30dB indicate fairly a low quality. However, high quality strives for 40dB or more [1].

A. Performance of the proposed method

After embedding secret data in cropped image, resulted cropped stego image is shown in Fig. 8. (Result of step 5 of embedding process). As this doesn't look like cover image merging is performed to obtain final stego image that is shown in Fig. 9. (Result of step 6 of embedding process).For merging co-ordinates of first and last pixels of cropped image in original image are calculated. After performing extraction cess retrieved image is shown in figure 10.This PSNR for different cases is shown in table 1. Is calculated PSNR.

Fig.8. Embedded Image

Fig.9. Reconstructed Image

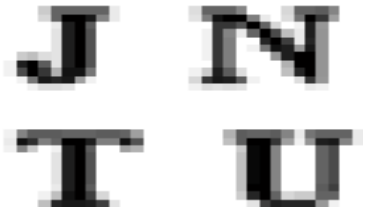

Figure10. Extracted Logo Image

TABLE I
EXTRACTED QUALITY, PSNR AND MSE OF FINAL STEGNO IMAGE IN PROPOSED METHODE

Cover Image: 1.bmp
Logo Image: logo.bmp

Sr. No.	*Wavelet types*	*PSNR of stego image*	*MSE of stego image*	*Extraction quality*
1.	Haar	69.5104	0.00727844	1
2.	db2	70.3077	0.00605774	0.5
3.	bior 1.3	69.8809	0.00668335	0.3
4.	rbio 1.3	70.7205	0.00550842	0.1

Performing biometric steganography with cropping or without cropping, both are having its own advantages and disadvantages.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

But if method is implemented with cropping then it will ensure more security than without cropping case.As with cropping case we need 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.From the table 1 it is obvious that PSNR of is more than in cropping case. So, this is trade off that occurs if we need more security.

V. CONCLUSION

In this paper Skin Tone based Secret Data hiding in Images by Using DWT Technique's is proposed which is perceptually invisible. As shown in table 1, the MSE should be as low as possible to have less error and the PSNR should be as high as possible to have better quality of reconstructed Image.

VI. ACKNOWLEDGMENT

I would like to express my gratitude to my guide **Prof. S. A. Bhosale** for her able guidance and constant encouragement. I have been greatly benefited by her valuable suggestion and ideas. I am externally grateful to, **Prof. Dr. G. M. Malwatkar**, Head of the Department of Electronics and telecommunication and **Prof. V. B. Shere** for their guidance and wholehearted support. Furthermore I would also like to thank all the staff members of the E & TC Department at D.C.O.E.R, who has always been ready with a helping hand.

REFERENCES

[1] Anjali A.Ahejul And U.L.Kulkarni, "A DWT based Approach for Steganography Using Biometrics",International Conference on Data Storage and Data Engineering,2010

[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 Engineering of Computer-Based Systems (ECBS'08), Belfast, 2008, pp. 159-168.

[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

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

Swapnali Zagade, Studying Master Degree in VLSI design and embedded systems from Pune University, Pune, India. Currently she is working as an Assistant Professor in Electronics Department of the Navshyadri College of engineering, Pune, India.she has published many research papers in reputed journals.

Smita Bhosale, Received Master Degree in Digital System from University Pune, India. Currently she is working as an Assistant Professor in Electronics Department of the Dnyanganga College of engineering, Pune, India. She has published many research papers in reputed journals.