A DWT based Approach for Steganography Using Biometrics

Anjali A. Shejul
Computer Engineering Department,
MGM College of Engineering & Technology,
Navi Mumbai, Maharashtra, India.
anjalishejul@yahoo.co.in

Prof. U.L Kulkarni
Computer Engineering Department,
Konkan Gyanpeeth College of Engineering,
Karjat, Maharashtra, India.
kumeshl@rediffmail.com

Abstract-

Steganography is the art of hiding the existence of data in another transmission medium to achieve secret communication. It does not replace cryptography but rather boosts the security using its obscurity features. 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]. 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. 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.

Keywords: Biometrics; Skin tone detection; DWT; DCT; Cropping; Security; PSNR.

I. INTRODUCTION

In this highly digitalized world, the Internet serves as an important role for data transmission and sharing. However, since it is a worldwide and publicized medium, some confidential data might be stolen, copied, modified, or destroyed by an unintended observer. Therefore, security problems become an essential issue. Encryption is a well-know procedure for secured data transmission [2]. Frequently used encryption methods include RSA, DES (Data encryption standard). Although encryption achieves certain security effects, they make the secret messages unreadable and unnatural or meaningless. These unnatural messages usually attract some unintended observers' attention. This is the reason a new security approach called "steganography" arises.

As an example, the cover text [3]:

"I'm feeling really stuffy. Emily's medicine wasn't strong enough without another febrifuge." Hides the sentence "Meet me at nine"

If the reader retains the second letter of each word in sequence.

In steganography secret message is the data that the sender wishes to remain confidential and can be text, images, audio, video, or any other data that can be represented by a stream of bits. The cover or host is the medium in which the message is embedded and serves to hide the presence of the message. The message embedding technique is strongly dependent on the structure of the cover, and in this paper covers and secret messages are restricted to being digital images. The cover-image with the secret data embedded is called the "Stego-Image". The Stego-Image should resemble the cover image under casual inspection and analysis. In addition, for higher security requirements, we can encrypt the message data before embedding them in the cover-image to provide further protection [4]. For this the encoder usually employs a stego-key which ensures that only recipients who know the corresponding decoding key will be able to extract the message from a stego-image. For proposed method cover image is cropped interactively and that cropped region works as a key at decoding side yielding improved security.

There are two things that need to be considered while designing the steganographic system: (a) Invisibility: Human eyes can not distinguish the difference between original and stego image. (b) Capacity: The more data an image can carry better it is. However large embedded data may degrade image quality significantly.

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. Section IV demonstrated the experimental results. Finally conclusions are provided in section V.

II. LITERATURE SURVEY

A. 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

978-0-7695-3958-4/10 $26.00 © 2010 IEEE
DOI 10.1109/DSDE.2010.10

embedding procedure does not affect the original pixel value greatly [5]. The mathematical representation for LSB is:

$x_i' = x_i - x_i \bmod 2^k + m_i$ (1)

In equation (1), *x_i' represents* the *i* th pixel value of the stego-image and *xi represents* that of the original cover-image. *m_i represents* the decimal value of the *i* th block in the confidential data. The number of LSBs to be substituted is k. The extraction process is to copy the k-rightmost bits directly. Mathematically the extracted message is represented as:

$m_i = x_i \bmod 2^k$ (2)

Hence, a simple permutation of the extracted *m_i gives* us the original confidential data [6]. 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.

B. 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 [7]. 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.

C Adaptive Steganography

Adaptive steganography is special case of two former methods. It is also known as "Statistics aware embedding" [8] and "Masking" [4]. 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.

III. PROPOSED METHOD

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 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 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. Here 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 [1]. Next sub-sections briefly introduce skin tone detection and DWT.

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. 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:

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

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 causes 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 subband) we can hide secret message in other three parts without making any alteration in LL subband [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.

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 $M_c \times N_c$ where $M_c \leq M$ and $Nc \leq N$ and $M_c = N_c$ 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.

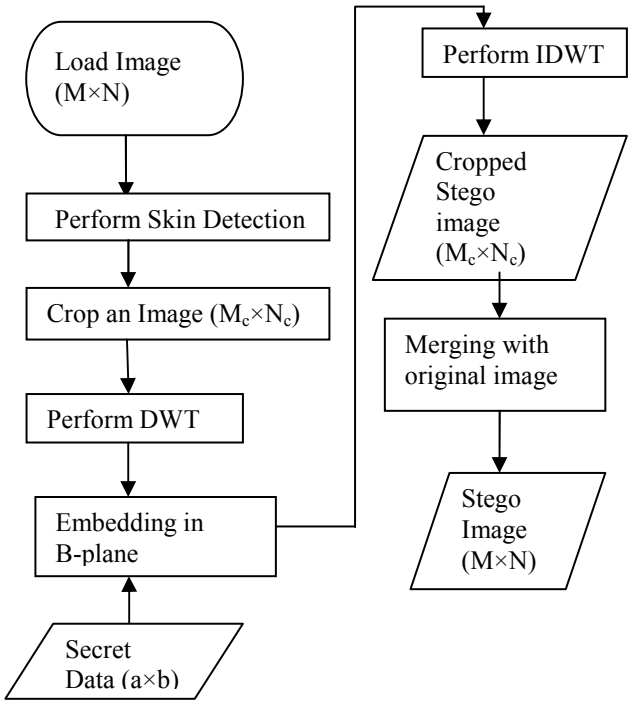

Figure 1. Flowchart of Embedding Process

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: Ask user to perform cropping interactively on mask image ($M_c \times N_c$). 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 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 ($M_c \times N_c$) not whole image (M×N). This yields 4 sub-bands denoted as $H_{LL}, H_{HL}, H_{LH}, H_{HH}$. (All 4 sub-band are of same size of $M_c/2, N_c/2$). 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. 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 (as shown in Fig.2) that embeds secret data coefficient by coefficient in selected sub-band [6], if coefficient is skin pixel.

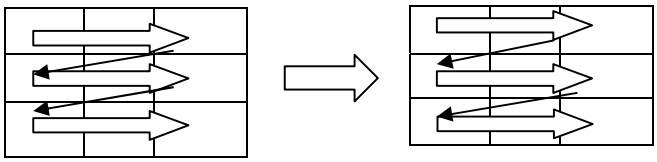

Figure 2. Raster Scan Order

5) Step 5: Perform IDWT to combine 4 sub-bands.

6) Step 6: A cropped stego image of size $M_c \times N_c$ 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 $M_c \times N_c$, So we need to merge the cropped stego image

with original image to get the stego image of size M×N. 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 H_{HH} sub-band of DWT secret data is retrieved. Extraction procedure is represented using Flowchart in Fig. 3

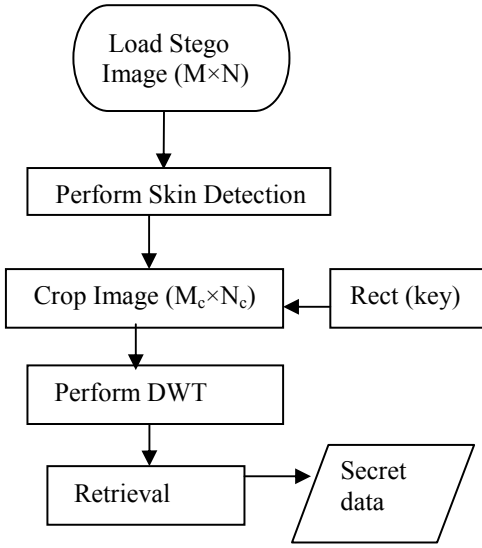

Figure 3. Flowchart of Extraction Process

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.

Figure 4. Cover Image

Figure 5. Image to hide

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.

$$PSNR = 10 \log_{10} (255^2/MSE), \quad (3)$$

$$\text{Where, } MSE = (1/(M \times N)) \sum_{i=1}^{M} \sum_{j=1}^{N} (x_{ij} - y_{ij})^2 \quad (4)$$

x_{ij} and y_{ij} 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. 6. (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. 7. (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 process retrieved image is shown in figure 8. Above method uses cropping. Same proposed method is implemented for without cropping case. In without cropping case secret data is hidden in one of the sub-band which is obtained by performing the DWT on whole image and not only to cropped region. PSNR is calculated for four different final stego images resulted from a considered image and three more sample images. This PSNR for different cases is shown in table 1. Average PSNR of proposed method is calculated based on the obtained PSNR.

Performing biometric steganography with cropping or without cropping, both are having its own advantages and disadvantages. 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 without cropping case is more than with cropping case. So, this is trade off that occurs if we need more security.

Fig.ure 6 Cropped Stego Image after step 5 of embedding process

Fig.ure 7 Final. Stego Image after step 6 of embedding process

Figure 8. Retrieved image

TABLE 1. CAPACITY AND PSNR OF 4 FINAL STEGO IMAGES IN PROPOSED METHOD

Cover Image (356× 356)	Capacity of Cover Image		PSNR		Size of Logo
	Case A	*Case B*	*Case A*	*Case B*	
Image 1	7173	5294	53.0	50.5	64×70
Image 2	1067	1056	51.9	49.7	32×32
Image 3	1452	1354	51.2	49.2	32×32
Image 4	4850	2572	46.4	45.4	32×32
Average PSNR			50.7	48.7	

Case A- Without Cropping
Case B- With Cropping

V. CONCLUSION

Digital Steganography is a fascinating scientific area which falls under the umbrella of security systems. In this paper biometric steganography is presented that uses skin region of images in DWT domain for embedding secret data. By embedding data in only certain region (here skin region) and not in whole image security is enhanced. Also image cropping concept introduced, maintains security at respectable level since no one can extract message without having value of cropped region. Features obtained from DWT coefficients are utilized for secret data embedding. This also increases the quality of stego because secret messages are embedded in high frequency sub-bands which human eyes are less sensitive to. According to simulation results, proposed approach provides fine image quality.

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] Petitcolas, F.A.P.: "Introduction to Information Hiding". In: Katzenbeisser, S and Petitcolas, F.A.P (ed.) (2000) Information hiding Techniques for Steganography and Digital Watermarking. Norwood: Artech House, INC.

[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] 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).

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

[9] Abbas Chedda, Joan Condell, Kevin Curran and Paul Mc Kevitt "A Skin Tone Detection Algorithm for an Adaptive Approach to Steganography" , School of Computing and Intelligent Systems, Faculty of Computing and Engineering, University of Ulster, BT48 7JL, Londonderry, Northern Ireland, UK,2008

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

[11] 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)

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