ISSN: 2277-9655
Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A Skin Tone Based Stenographic Scheme using Double Density Discrete Wavelet Transforms

Varsha Gupta
Department of ECE, Acropolis Institute of Technology and Research, Indore, Madhya Pradesh, India
varshashree11@gmail.com

Abstract

Steganography is the art of concealing the existence of data in another transmission medium i.e. image, audio, video files to achieve secret communication. It does not replace cryptography but rather boosts the security using its obscurity features. In the proposed method Biometric feature (Skin tone region) is used to implement Steganography[1]. In our proposed method Instead of embedding secret data anywhere in image, it will be embedded in only skin tone region. This skin region provides excellent secure location for data hiding. So, firstly skin detection is performed using, HSV (Hue, Saturation, Value) color space in cover images. Thereafter, a region from skin detected area is selected, which is known as the cropped region. In this cropped region secret message is embedded using DD-DWT (Double Density Discrete Wavelet Transform). DD-DWT overcomes the intertwined shortcomings of DWT (like poor directional selectivity, Shift invariance, oscillations and aliasing)[2].optimal pixel adjustment process (OPA) is used to enhance the image quality of the stego-image. Hence the image obtained after embedding secret message (i.e. Stego image) is far more secure and has an acceptable range of PSNR. The proposed method is much better than the previous works both in terms of PSNR and robustness against various attacks (like Gaussian Noise, salt and pepper Noise, Speckle Noise, rotation, JPEG Compression, Cropping, and Contrast Adjustment etc.)

Keywords: Cropping, DD DWT, HSV, PSNR, Skin tone detection, OPA, Stego Image.

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 known procedure for secured data transmission [3]. Although encryption achieves certain security effects, they make the secret messages unreadable and unnatural. These unnatural messages usually attract some unintended observers' attention and it tells an opponent or enemy that someone is communicating with someone else. This is the reason a new security approach called steganography arises. Steganography takes the opposite approach and attempts to hide all evidence that communication is taking place. In steganography secret message is the data that the sender wishes to keep confidential and that data 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. 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 enhanced security .There are two things that need to be considered while designing the steganographic system (a) Invisibility: human eyes should not distinguish the difference between original and stego image should be considered. (b) Capacity :The more data an image can carry the better it is. However large embedded data may degrade image quality significantly [5]. Rest of the paper is organized as follows. Section II presents Steganographic Scheme and theoretical background. In section III proposed method is described in detail with skin tone detection, DDDWT, OPA and decoding procedure step by step. Section IV

ISSN: 2277-9655
Impact Factor: 1.852

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

Steganoraphic Scheme

In the domain of digital images, many different image file formats exist, most of them for specific applications. For these different image file formats, different steganographic algorithms exist**.** Image steganography scheme can be divided into two groups: those in the Image Domain and those in the Transform Domain.

LSB (Least significant Bit) Substitution based Scheme

Here spatial features of image are used. Image domain techniques encompass bit-wise methods that apply bit insertion and noise manipulation and are sometimes characterized as "simple systems". This is a simplest steganographic scheme 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 [6].

Transform Domain based Scheme

Steganography in the transform domain involves the manipulation of algorithms and image transforms. These methods hide messages in more significant areas of the cover image, making it more robust. Many transform domain methods are independent of the image format and the embedded message may survive conversion between lossy and lossless compression. 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]. 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 using DCT or DWT. We are using DD-DWT.

Proposed Method

Proposed method introduces a new method of embedding secret data within skin and as well as in the edge area, as it is not that much sensitive to HVS (Human Visual System).This method takes advantage of Biometrics features such as skin tone edge detection, instead of embedding data anywhere in Image, data will be embedded in selected regions like skin region. Overview of method is briefly introduced as follows. At first skin tone detection is performed on input image using HSV (Hue, Saturation, Value) color model. Secondly cover image is transformed in Frequency domain. This is performed by applying DD- DWT. 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 enhanced security, since cropped region works as a key at the 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. Then a stego DD-DWT image is produced, so the IDD-DWT is performed on that. Thereafter IDD-DWT image is merged with original image, and we get the final Stego image.

Skin Colour Tone Detection

The 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. 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 .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. 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]. Sobottaka and Pitas [8] defined a face localization based on HSV.
The Skin classifier used for the proposed method is based on the following values of H & S

S_{min}= 0.10, S_{max} =0.68, H_{min} =0^0 and H_{max}=25^0

Methods of Skin Detection are-

***Pixel-Based Methods*:** Classify each pixel as skin or non-skin individually, Independently from its neighbours. Colour Based Methods fall in this category .

Region Based Methods: Try to take the spatial arrangement of skin pixels into account during the detection stage to enhance the methods performance. Additional knowledge (in terms of texture, etc) are required.

Double Density Discrete Wavelet Transform (DD-DWT)

The double-density DWT is an improvement upon the critically sampled DWT with important additional properties: (1) It employs one scaling function

ISSN: 2277-9655
Impact Factor: 1.852

and two distinct wavelets, which are designed to be offset from one another by one half, (2) The double-density DWT is over complete by a factor of two, and (3) It is nearly shift-invariant. In two dimensions, this transform outperforms the standard DWT in terms of denoising; however, there is room for improvement because not all of the wavelets are directional. That is, although the double-density DWT utilizes more wavelets, some lack a dominant spatial orientation, which prevents them from being able to isolate those directions The oversampled dyadic DWT considered, is based on a single scaling function and two distinct wavelets. Having more wavelets than necessary gives a closer spacing between adjacent wavelets within the same scale. Like the dual-tree DWT, the oversampled DWT presented here is redundant by a factor of 2, independent of the number of levels [9].

To implement the double-density DWT, we must first select an appropriate filter bank structure. The filter bank proposed in Figure a illustrates the basic design of the double-density DWT.

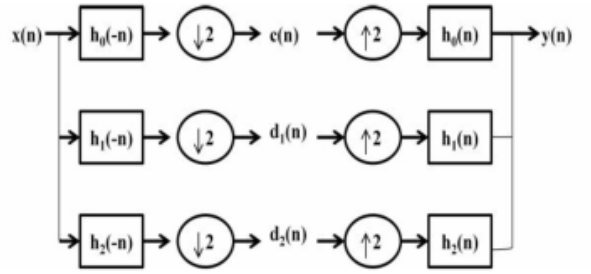

Fig.1 3-Channel Perfect Reconstruction Filter Bank.

The analysis filter bank consists of three analysis filters one lowpass filter denoted by $h_0(-n)$ and two distinct highpass filters denoted by $h_1(-n)$ and $h_2(-n)$. As the input signal x(n),the analysis filter bank decomposes it into three sub-bands, each of which is then down-sampled by 2. From this process we obtain the signals c(n), $d_1(n)$, and $d_2(n)$, which represent the low frequency subband, and the two high frequency sub-bands, respectively. The synthesis filter bank consists of three synthesis filters one lowpass filter denoted by $h_0(n)$ and two distinct highpass filters denoted by h_1 (n) and $h_2(n)$which are essentially the inverse of the analysis filters, they are up-sampled by two, filtered, and then combined to form the output signal y(n). One of the main concerns in filter bank design is to ensure the perfect reconstruction(PR)condition.That is to design $h_0(n)$,$h_1(n)$,and $h_2(n)$ such that y(n)=x(n).

Optimal pixel adjustment process

An optimal pixel adjustment (OPA) process is used to enhance the image quality of the stego-image obtained by the simple LSB substitution method. The basic concept of the OPA is based on the technique proposed in Ref. [10].

Let p_i , p'_i and p''_i be the corresponding pixel values of the i^{th} pixel in the cover-image C, the stego-image C' obtained by the simple LSB substitution method and the refined stego-image obtained after the OPAP. Let $\Delta_i = p'_i - p_i$, be the embedding error between pi and p'_i. According to the embedding process of the simple LSB substitution method [11], p'_i is obtained by the direct replacement of the k least significant bits of pi with k message bits, therefore,
$-2^k < \Delta_i < 2^K$.
The value of Δ_i can be further segmented into three intervals, such that

Interval 1 : $2^{k-1} < \Delta_i < 2^k$,
Interval 2 : $-2^{k-1} <= \Delta_i <= 2^{k-1}$,
Interval 3 : $-2^k < \Delta_i < -2^{k-1}$.

Based on the three intervals, the OPAP, which modifies p'_i to form the stego-pixel p''_i, can be described as follows:

Case 1 ($2^{k-1} < \Delta_i < 2^k$): If $p'_i >= 2^k$, then $p''_i = p'_i - 2^k$; otherwise $p''_i = p'_i$;
Case 2 ($-2^{k-1} <= \Delta_i <= 2^{k-1}$): then $p''_i = p'_i$;
Case 3 ($-2^k < \Delta_i < -2^{k-1}$): If $p'_i < 256-2^k$ then $p''_i = p'_i + 2^k$; otherwise $p''_i = p'_i$

The optimal pixel adjustment process only requires a checking of the embedding error between the original cover-image and the stego-image obtained by the simple LSB substitution method to form the final stego-image. The extra computational cost is very small compared with other Methods.

Encoding Process

1) Initially load the cover Image in which we will hide the secret message (text).
2) Skin Tone Detection: After loading the cover Image, skin tone detection is performed. This enables us to know where and how much data can be hidden.
3) Cropping: From the detected skin portion, cropping is performed. This is done so that within skin pixels data is hidden at only limited pixel positions. This feature of cropping enhances security, as any eavesdropper cannot detect secret message just by detecting the skin pixels.
4) Histogram Modification: This is performed to adjust the contrast of the colors.

ISSN: 2277-9655
Impact Factor: 1.852

5) Key Generation: The encoder 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.
6) Double Density DWT: Double Density Discrete Wavelet Transform is applied to the cropped skin portion.
7) Secret encrypted message is now merged into the transformed skin pixels.
8) Optimal Pixel Adjustment process: OPAP is used to assign secret code values to limited areas of cropped skin portion, so as to have least effect over the HVS (human visual system). The image quality of the stego-image can be greatly improved with low extra computational complexity.
9) Inverse DD-DWT: Now the transformed image has secret code as well, so it is ready to be merged with the original cover Image. To merge this transformed secret message embedded image, with cover Image we first have to inverse transform it.
10) After applying inverse DD-DWT, we get the original cropped image along with secret code. This image is now called stego image. This stego image is now merged with original cover image to get the final reconstructed cover image along with secret data embedded in it.

Decoding Process

1) From the Stego Image skin pixels are detected and cropping of Stego image is performed.
2) Now the DD-DWT is performed to get the transformed cropped image.
3) Secret message is extracted from the transformed cropped stego image.
4) Results of Extraction process are measured in terms of PSNR and MSE. These are discussed below in detail.

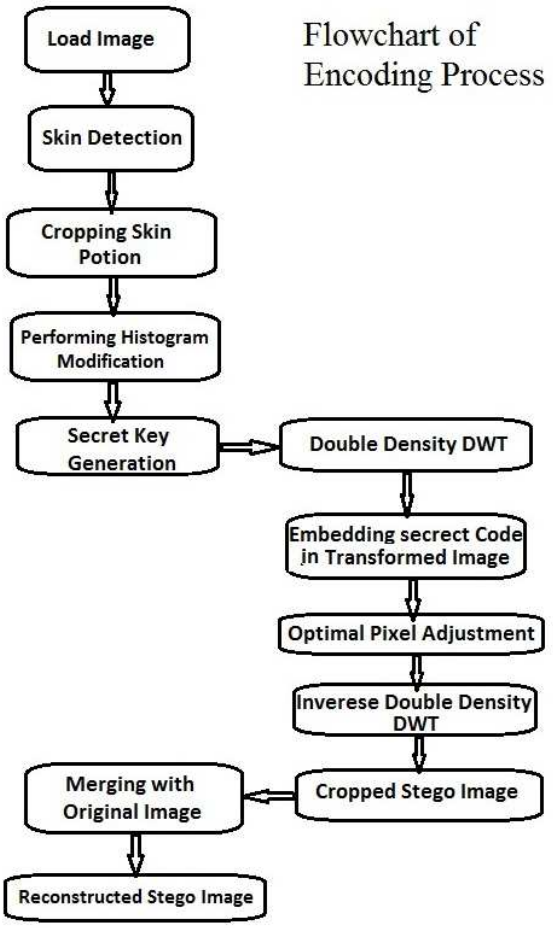

Fig.2 Flowchart of Encoding Process

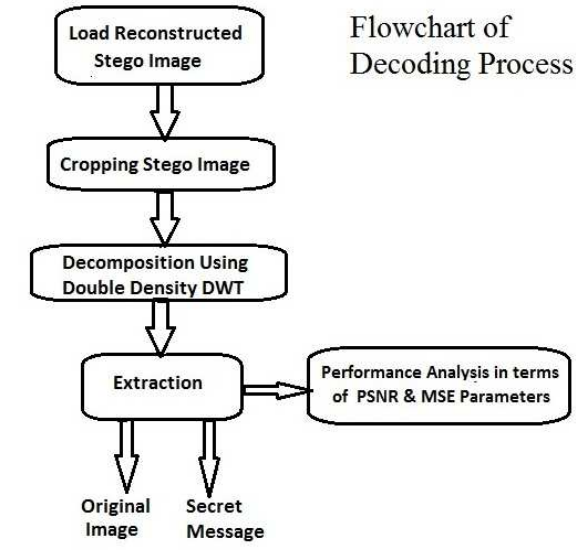

Fig.2 Flowchart of Encoding Process

ISSN: 2277-9655
Impact Factor: 1.852

Results

In this section we demonstrate simulation results for the proposed scheme. These have been implemented using MATLAB 7.8. A 24 bit color image is employed as cover-image of size 256×256,

Fig 4: Cover image

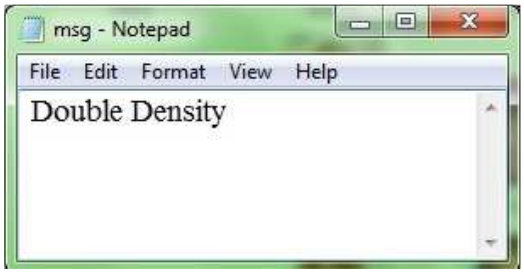

Fig.5 shows sample secret message

Fig. 6: Cropped Stego Image

Fig .7: Merged Stego Image

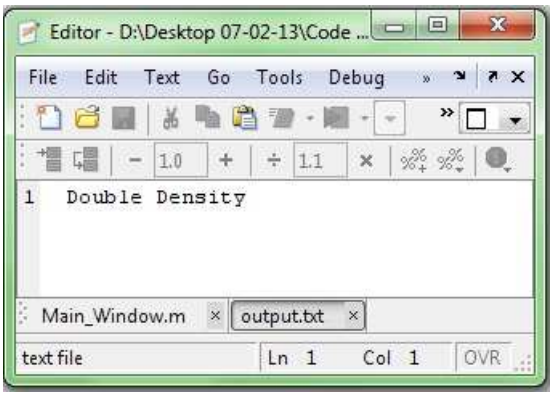

Fig. 8 Output Text File (having the secret message)

Performance in terms of capacity and PSNR (in dB) is demonstrated for the method in the following subsections. PSNR is

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right)$$

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

a_{ij} and b_{ij} represents pixel values of original cover image and stego image respectively as in Equation The calculated PSNR as in Equation 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.

Result Discussion of proposed work

After embedding secret data in cropped image, resulted cropped stego image is shown in Fig. 6. Cover image is now merged with cropped embedded Stego image as is shown in Fig.7. For merging, co-ordinates of first and last pixels of cropped image are calculated and then replaced with the one in original cover image.

Table I
Proposed methods results of PSNR for different images

No.	Images	PSNR values
1	Image 1	70.03
2	Image 2	60.7
3	Image 3	60.1
4	Image 4	58.25
5	Image 5	55.3

ISSN: 2277-9655
Impact Factor: 1.852

TABLE II
PSNR in previous methods and proposed method

Sr. No.	Method	PSNR values
1	Shejul Method	49.3
2	Rekha Nagar Method	51.0
3	Proposed Method	55.3

Conclusion

Digital Steganography is a fascinating scientific area which falls under the umbrella of security systems. Proposed framework is based on steganography that uses Biometric feature i.e. skin tone region. Skin tone detection plays a very important role in Biometrics and can be considered as secure location for data hiding. Secret data embedding is performed in DD-DWT domain than the DWT as DD-DWT outperforms than DWT as well as DCT. Using Biometrics resulting stego image is more tolerant to attacks and more robust than existing methods.

References

[1] 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.

[2] Rekha Nagar, "An Image Hiding Algorithm Using Discrete Wavelet Transform and Skin Tone Detection". In International Journal of Engineering and Social Science, pp 83-94., July 2012

[3] 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.

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

[5] Shejul, A. A., Kulkarni, U.L.,"A DWT Based Approach for Steganography using Biometrics," International Conference on Data Storage and Data Engineering, pp.10-15, 2010.

[6] 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.

[7] Kurak, C. and McHugh, J.: "A Cautionary Note on Image Downgrading" Proceedings of the Eighth Annual Computer Security Applications Conference. pp. 153- 159, 30 Nov-4 Dec 1992.

[8] Sobottka, K. and Pitas, I.:"Extraction of facial regions and features using color and shape information." Proc. IEEE International Conference on Image Processing, pp. 483-486.(1996)

[9] I.W. Selesnick, "The Double Density DWT in Wavelets in Signal and Image Analysis: From Theory to Practice , A. Petrosian and F.G. Meyer, Eds. Boston, MA: Kluwer, 2001

[10] Chi-Kwong Chan, L.M. Cheng, Improved hiding data in images by optimal moderately significant-bit replacement, IEEElectron. Lett. 37 (16) (2001) 1017–1018.

[11] Chi-Kwong Chan, L.M. Cheng, Hiding data in images by simple LSB substitution, Pattern Recognition 37 (2004) 469 – 474