Biometrics based Steganography using Circular Folding in DWT Domain

Santhi K
Department of Electronics and communication
Federal Institute of Science and Technology
(FISAT)

Anil Kumar M N
Department of Electronics and communication
Federal Institute of Science and Technology
(FISAT)

ABSTRACT

Steganography is the art and science of hiding or embedding data in a transmission medium. The goal of steganography is to hide an information message inside a harmless cover medium in such a way that it is not possible even to detect that there is a secret message. In this paper, the object oriented steganography is based on biometrics. Data is embedded into some regions of the skin and not to the whole region. To separate the skin and non-skin regions, skin tone detection is performed using HSV color space. To increase the security, cropping and circular folding is performed on the B plane of the cover image. The secret data is embedded into the high frequency sub-band coefficients of DWT domain. Because human eyes are less sensitive in this sub-band, security is improved. In this paper, we analyze both cropping and non-cropping cases. This results into more security with cropping than without cropping with almost same PSNR.

Keywords

Steganography, Biometrics, Skin tone detection, Cropping, DWT, Circular- folding, PSNR..

1. INTRODUCTION

With advancements in Digital Communication Technology, data hiding plays an important role. The redundancy of digital media, as well as the characteristic of the human visual system makes it possible to hide messages [4]. Steganography is one of the data hiding schemes and is the science of communicating secret data in an appropriate multimedia carrier. It can embed any image, audio and video files. While designing a steganographic system, there are three things should be considered. (1) Security: An eavesdropper's inability to detect hidden information. (2) Capacity: It refers to the amount of information that can be hidden in the cover image. (3) Robustness: An amount of modification the stego - medium can withstand before an opponent can destroy hidden information**.** The cover image with secret data embedded is called Stego-Image.

There are two popular types of hiding methods; spatial domain embedding and transform domain embedding. The Least Significant Bit (LSB) substitution is an example of spatial domain techniques. Till now LSB is the most preferred technique used for data hiding because it is simple to implement offers high hiding capacity, and provides a very easy way to control stego-image quality [2] but it has low robustness to modifications made to the stego-image such as low pass filtering and compression [3] and also low imperceptibility. The other type of hiding method is the transform domain techniques which appeared to overcome the robustness and imperceptibility problems found in the LSB substitution techniques. There are many transforms that can be used in data hiding, the most widely used transforms are; the discrete cosine transforms (DCT), and the discrete wavelet transforms (DWT). DWT outperforms the DCT. DCT is calculated on blocks of independent pixels, a coding error causes discontinuity between blocks resulting in annoying blocking artefact [13]. This drawback of DCT is eliminated using DWT. DWT is applied on the entire image So DWT is used in this proposed method. The advantages of transform domain techniques over spatial domain techniques are their high ability to tolerate noises and handle some signal processing operations but on the other hand they are computationally complex and hence slower. Also they have low hiding capacity. The compatibility of the Human Visual System [10] is the additional advantage in wavelet transforms.

To increase the security, the proposed method uses circular folding. Using this technique, data can be embedded into some regions of the skin portion. To improve the security, the high frequency coefficient of DWT is used for data hiding

The rest of the paper is organized as follows: In section II, a brief introduction to skin tone detection, DWT and circular folding is provided. In section III, the proposed stenographic system is described. In section IV, the achieved results are presented, and in section V, we conclude the paper and suggest future improvements to the system.

2. THE STEGANOGRAPHY METHOD

2.1 Skin Tone Detection

Skin tone detection is the process of finding skin colored pixels and regions in an image. It is performed by using a skin detector. A skin detector transforms a given skin pixel into an appropriate color space and then use a skin classifier to label the pixel whether it is a skin or a non-skin pixel. A skin classifier defines a boundary of the skin color class in the color space based on the skin colored pixels. Detecting skin-colored pixels has proven quite challenging for many reasons. An important challenge in skin detection is to represent the color in a way that is invariant or at least insensitive to changes in illumination [12]. Another challenge is that many objects in the real world might have skin tone colors (eg: wood, leather, skin-colored clothing, hair, sand, etc). This may cause any skin detector to have much false detection in the background if the environment is not controlled [1].

RGB color space does not separate luminance and chrominance and the R, G and B components are highly correlated. The luminance of a given RGB pixel is a linear combination of the R, G and B values. Therefore, changing the luminance of a given skin patch affects all the R, G and B values [3]. The HSV (Hue, Saturation and Value) and YCbCr (Yellow, Chromatic Blue and Chromatic Red) color spaces have their luminance component separated from the chrominance component and they are known to possess higher discriminality between skin pixels and non-skin pixels over various illumination conditions [5]. 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. The skin color boundaries in the H and S subspaces are [11],

S_{min}=0.23, S_{max}=0.68, Hmin=0^0 and Hmax=50^0

2.2 Discrete Wavelet Transform

The frequency domain transform applied in our method is Haar-DWT, the simplest DWT [6]. A 2-dimensional Haar-DWT consists of two operations: one is the horizontal operation and the other is the vertical one. In the first step, 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. Repeat this operation until all the rows are processed. The pixel sums represent the low frequency part (denoted as symbol L) and differences represent the high frequency part of the original image (denoted as symbol H). In the second step, 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. Repeat this operation until all the columns are processed. Finally we will get 4 sub-bands denoted as LL, HL, LH and HH. After each transform is performed the size of the square which contains the most important information is reduced by a factor of 4 [7].

The LL sub-band is the low frequency portion and hence looks very similar to the original image. Human eyes are very sensitive in this sub-band. So we can hide secrete data in the other three sub-bands, because human eyes are less sensitive in these sub-bands. In this work, the frequency coefficients of HH sub-band of Haar-DWT is used for data hiding.

2.3 Circular Folding

Geometrical image processing operations are fundamentally different; instead of modifying the gray values of pixels, they redefine the pixel locations without changing their values. A geometric operation (eg: scaling, rotation, reflection, translation, etc.) maps pixel information, i.e. the intensity values at each pixel location (x1,y1) in an image to another location (x2,y2) in an output image. In this work, for circularly folding the image, reflection of a point in the origin is used. A reflection operator geometrically transforms an image i.e. pixel values, located at position (x1, x2) in an original image axis or image point into a new position (-x1,-x2) in a corresponding output image. This is same thing as a rotation of 180^0.

3. PROPOSED SYSTEM

In the proposed system a new type of data hiding technique is introduced. Data is embedded into some portions of the skin region, instead of embedding in whole portion of skin region. Overview of proposed system as follows: At first skin tone detection of cover image is performed on the HSV space for separating the skin and non-skin portions. This will generate a mask. Then, crop the mask and the cover image. This cropped region will act as the rectangular key at the extraction side. Then, perform circular folding on the cropped B-plane of the cover image and the mask. The contribution of blue color in human skin is less. Then transform this cover image into frequency domain for embedding secret data by using the Haar-DWT. After embedding, it is converted back from the frequency domain to spatial domain. Again circular folding is performed on it and this cropped stego-image is merged with original cover image to get the stego-image. At extraction side, perform skin tone detection on the stego-image for separating skin and non-skin pixels. Then stego- image and the mask are cropped by using rectangular key, which is generated from the embedding side. Then, perform circular folding on the cropped B-plane of the stego image and the mask. The secret data is then extracted from high frequency coefficients of the Haar-DWT.

3.1 Embedding Algorithm

The block diagram of the embedding procedure is shown in Fig. 1. The blocks of the embedding algorithm is explained in the following steps:

Step 1: Load the 24-bit cover image of size AxB.

Step 2: Convert the cover image from RGB plane into HSV plane and generate a mask. The mask is a black and white image of size AxB. The white represents skin pixel and black represents non-skin pixel.

Step 3: First find the total number of ones in the mask. Then crop the mask by taking the middle one as the centre. The size of cropped mask is A_cxB_c. Then also crop the cover image of size A_cxB_c. Cropped area must be in an exact rectangle form i.e. $A_c=B_c$, 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. A_cxB_c should be less than AxB. This cropped rectangle will acts as the key at the extraction side.

Step 4: Take the third plane of the cropped cover image and rotate this by 180^0 using circular folding technique. This will improve the security of the system.

Step 5: Perform DWT on the circularly folded image. Then we get 4 sub-bands denoted as LL, LH, HL, and HH. Payload of image to hold secret data is determined based on number of skin pixels present in one of high frequency sub-band in which data will be hidden. The size of each sub-bands are $A_c/2xB_c/2$.

Step 6: Load a gray scale secret data of size mxn. Its size must be less than $A_c/2xB_c/2$. Embed this secret data into the HH sub-band of cover image, because human eyes are less sensitive in this sub-band. The LL sub-band contains significant information that will affect the image quality greatly. So, the sub-band frequencies other than LL sub-band frequency will be used for embedding. Here, skin pixels are traced using skin mask detected earlier and secret data embedded on it. Secret data embedded into some portions of the skin region. This will improve the security.

Step 7: Perform IDWT for combining 4 sub-bands and we get a single image in spatial domain of size A_cxB_c.

Step 8: Again perform circular folding to rotate the image into 180^0 .

Step 9: The cropped stego image of size A_cxB_c is obtained by placing the B-plane of the circularly folded image back into the cropped cover image.

Step 10: Merge this cropped stego image into the original image and we get the stego image of size AxB. This should be similar to original image after visual inspection.

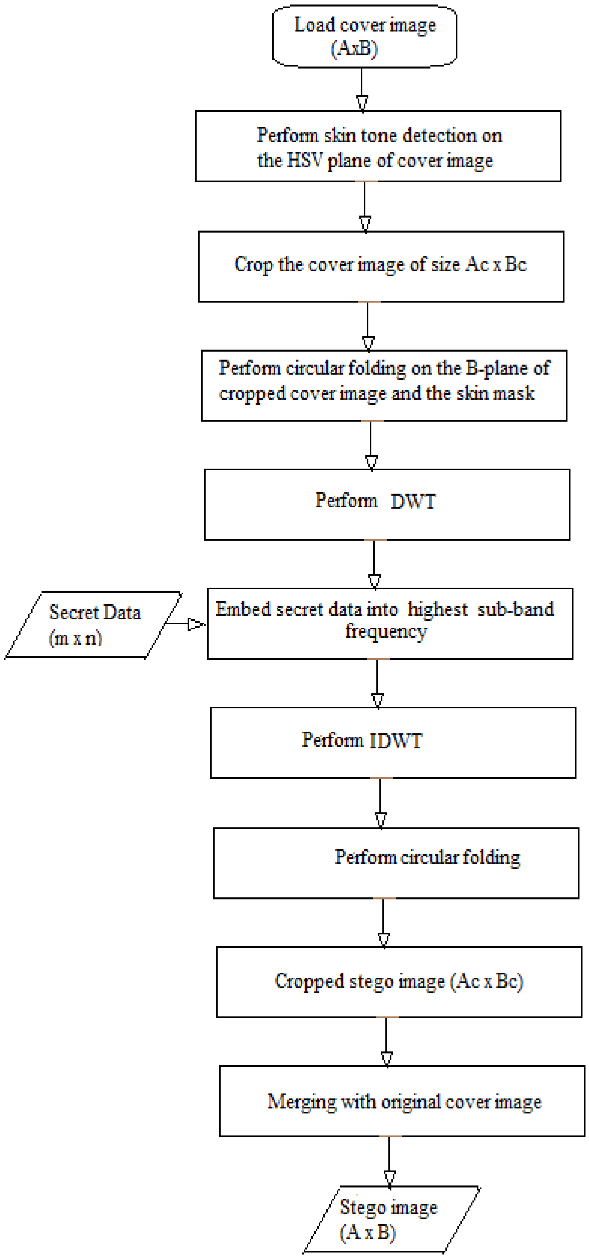
Load cover image (AxB)
Perform skin tone detection on the HSV plane of cover image
Crop the cover image of size Ac x Bc
Perform circular folding on the B-plane of cropped cover image and the skin mask
Perform DWT
Secret Data (m x n)
Embed secret data into highest sub-band frequency
Perform IDWT
Perform circular folding
Cropped stego image (Ac x Bc)
Merging with original cover image
Stego image (A x B)

Fig 1: The Embedding Process

3.2 Extraction Algorithm

At the receiver the extraction algorithm is used to obtain the secret message. The block diagram of the extraction algorithm is shown in Fig. 2. It is also simpler than the embedding procedure.

The blocks of the extraction algorithm is explained in the following steps:

Step 1: Load the 24-bit steo- image of size AxB.

Step 2: Convert this stego-image from RGB plane into HSV plane and generate a mask.

Step 3: Crop the mask and stego- image of size $A_c x B_c$. It is a blind process since it requires only the rectangular key from the sender for cropping the mask and stego image.

Step 4: Take the third plane of the cropped stego image and rotate this by 180^0 using circular folding technique.

Step 5: Perform DWT on the circularly folded image.

Step 6: Extract the secrete data of size mxn.

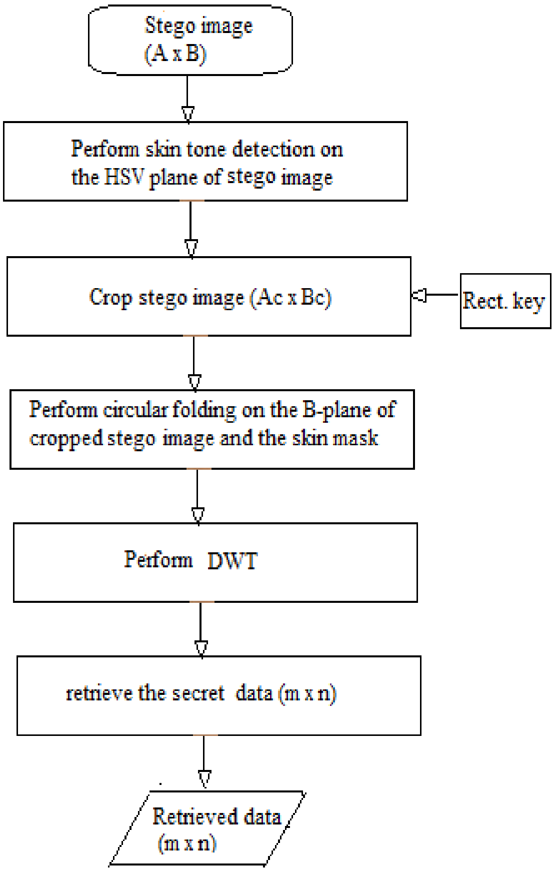
Stego image (A x B)
Perform skin tone detection on the HSV plane of stego image
Crop stego image (Ac x Bc)
Rect. key
Perform circular folding on the B-plane of cropped stego image and the skin mask
Perform DWT
retrieve the secret data (m x n)
Retrieved data (m x n)

Fig 2: The Extraction Process

4. IMPLEMENTATION AND RESULT ANALYSIS

The proposed system was applied to different 24-bit colour images and it achieved satisfactory results. A 24 bit colour image is employed as cover-image of size 350×350 as shown in Fig. 3. The simulation is implemented in Matlab 7.5 or above. The secret message to embed is an 8-bit gray scale image with the same length as the calculated hiding capacity is shown in Fig. 4. Same proposed method is implemented for non-cropping case. In this case secret data is hidden in one of the sub-bands which are obtained by performing the DWT on whole image and not only to cropped region.

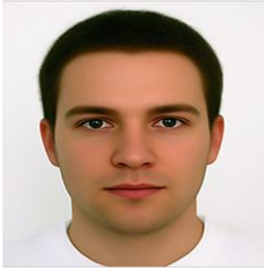

Fig 3: Cover image

Fig 4: Secret data

The performance of the proposed technique is evaluated according to two widely used aspects [8]:

4.1 Imperceptibility/Stego-image quality

This aspect measures how much difference (distortion) was caused by data hiding in the original cover image, where the higher the stego-image quality, the more invisible the hidden message. We can judge the stego-image quality by using Peak Signal to Noise Ratio (PSNR). The PSNR for an image of size AxB is calculated by (1),

$$PSNR=10\log_{10}(255^2/MSE) \qquad (1)$$

Where,

$$MSE = (1/AxB)\sum_{x=1} \sum_{y=1} (P(x,y)-(P'(x,y))^2 \qquad (2)$$

The MSE is the Mean Square Error, P(x,y) stands for the image pixel value in the cover image and P'(x,y) is for the pixel value at position (x,y) in the image after inserting secret data. 'A' represents the height and 'B' represents the width of the cover image [8]. A high value of PSNR means better image quality (less distortion), it is recorded that PSNR goes beyond 50 dB. PSNR values falling below 30dB indicate fairly a low quality. However, high quality strives for 40dB or more [10].

4.2 Payload/Hiding Capacity

The hiding capacity indicates how much data can be hidden within a cover image without making obvious degradation in the cover image quality [9].

The payload/hiding capacity is calculated as follows:

$$C=\frac{(m\times n)\times 8}{(A\times B)\times 8}\times 100\%$$

(3)

Where, m and n are the height and width of the hidden image and A and B represents the height and width of the high frequency sub-band of DWT [11].

After embedding, the resulted cropped stego image is shown in Fig. 5. Fig. 6 shows the stego image of size AxB. It doesn't look like merging is performed into the cover image. The recovered secret data is shown in Fig. 7.

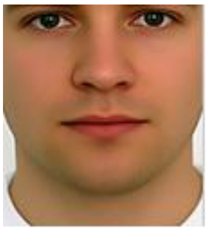

Fig 5: Cropped stego- image

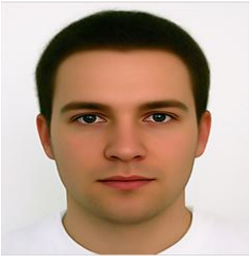

Fig 6: Merged stego- image

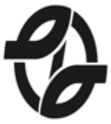

Fig 7: Retrieved secret data

Table 1 summarizes the payload capacity and PSNR for3 sample cover images. With cropping and without cropping cases are analyzed. In both of these two cases, as the size of the cover image increases, the capacity decreases and the PSNR increases. These are done with the fixed size of secret data. In the proposed system, PSNR is almost same for both cropping and without cropping cases.

Table 1. Payload Capacity and PSNR of three stego-images in the proposed system

Size of cover image	Payload Capacity (%)		PSNR (dB)		Size of Logo
	Case A	Case B	Case A	Case B	
(350 x 350)	2.56	8.87	62.185	62.083	(28x28)
(430 x 430)	1.69	5.09	64.074	64.150	
(556 x 556)	1.01	3.10	65.846	66.453	
Average PSNR			64.035	64.228	

Case A: Without Cropping

Case B: With Cropping

The correlation between the input logo and the retrieved logo for case A is 0.995 and for case B is 0.996. As compared to without cropping, with cropping case has its own advantage. The cropping case will ensure more security as we need cropped size at the extraction side. That is cropped region acts as the key at the 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.

To further investigate the imperceptibility of the proposed system we compared the PSNR of our system with other systems and it showed better results. For example, the system in [10] showed an average PSNR value of 48.7 dB with cropping case and without cropping case is 50.7 dB while our system showed a PSNR value of 64.9 dB for with cropping case and 64.4 dB for without cropping case. So, our system provided same PSNR for both cases. Cropping case improved the security with high hiding capacity as compared with without cropping case for the same PSNR value.

5. CONCLUSION

In this paper we proposed a novel data hiding scheme that hides data into the discrete wavelet coefficients of an image. This system used the biometric feature, such as skin tones for hiding the secret data. The proposed system enhanced the security by embedding secret data into some portions of the skin region and not in whole skin region using circular folding technique. Concept of image cropping was also introduced, and this improved the security since no one can extract the secret data without having the value of cropped area. This also increases the quality of stego because data is embedded in high frequency sub-bands which human eyes are less sensitive to. With this proposed system we get good image quality.

The proposed system can be further developed to increase its robustness by changing the transmission medium into audio. This will provide a good, efficient method for hiding the data from hackers and sent to the destination in a safe manner. Also methods must be investigated to increase visual quality of the stego-image with an acceptable level of hiding capacity.

6. REFERENCES

[1] A. Alboil, L. Torres, and E. J. Delp, “Optimum Colour Spaces for Skin Detection”, In Proceedings of the international Conference on Image Processing, vol.1, 122-124, 2001.

[2] S. Barve, U. Nagaraj, and N. Gulabani, “Efficient and secure Biometric Image Steganography using Discrete Wavelet transform,” International Journal of Computer Science & Communication Networks,Vol 1(1),September-October 2011.

[3] Y. Dinesh, A P Ramesh, “Efficient Capacity Image Steganography by using Wavelets,” International Journal of Engineering Research and Applications,Voi.2, pp.251-259,Jan-Feb 2012.

[4] D.Artz, “Digital steganography: hiding data within data,” IEEE Internet Computing, pp.75-80, May-June 2001.

[5] V. Vezhnevets, V. Sazonov, A. Andreeva, “A Survey on Pixel-Based Colour Detection Techniques”, Proc. Graphicon2003, Moscow, Russia, September 2003.

[6] P. Y. Chen and H. J. Lin, “A DWT Based Approach for Image Steganography”, International Journal of Applied Science and Engineering, 4,3: 275-290, 2006.

[7] E Ghasemi, J Shanbehzadeh, and N Fassihi,“High Capacity Image Steganography usingWavelet Transform and Genetic Algorithm”, Proceedings of the International Multi Conference of Engineering and Computer Scientista 2011 Vol I, IMECS 2011, March 16-18,2011.

[8] N. Wu and M. Hwang. "Data Hiding: Current Status and Key Issues," International Journal of Network Security, Vol.4, No.1, pp. 1-9, Jan. 2007.

[9] L. Tawadw, R Mahajan and Chandan Kulthe, “Efficient & Secure Data Hiding Using Secret Reference Matrix,” , International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.1, January 2012.

[10] 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, pp.15916, 2008 .

[11] A. A, Shejul, and U. L. Kulkarni, “A DWT based approach for Steganography Using Biometric”, International Conference on Data Storage and Data Engineering,2010.

[12] 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.

[13] C. C. Chang, T. S. Chan and L. Z. Chung, “A steganographic method based upon JPEG and quantization table modification”, An International Journal on Information Sciences, 123-138, 2012.