BIOMETRIC BASED STEGANOGRAPHY USING WAVELET TRANSFORMS

Shruthi Narasimhe Gowda
MERIT MASTERS
UPC
Barcelona, Spain
shruthin88@gmail.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. Here secret data is embedded within skin region of image that will provide an excellent secure location for data hiding. 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 in enhanced security than hiding data without cropping i.e. in whole image. The cropped region works as a key at the 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.

I. INTRODUCTION (HEADING 1)

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. 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.

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 work 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. 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 cannot 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.

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

$$x_{i'} = x_i - x_i \bmod 2^k + m_i$$

In equation , $x_{i'}$ *represents* the i^{th} pixel value of the stego-image and x_i *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.

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. 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.

III. PROPOSED METHODOLOGY

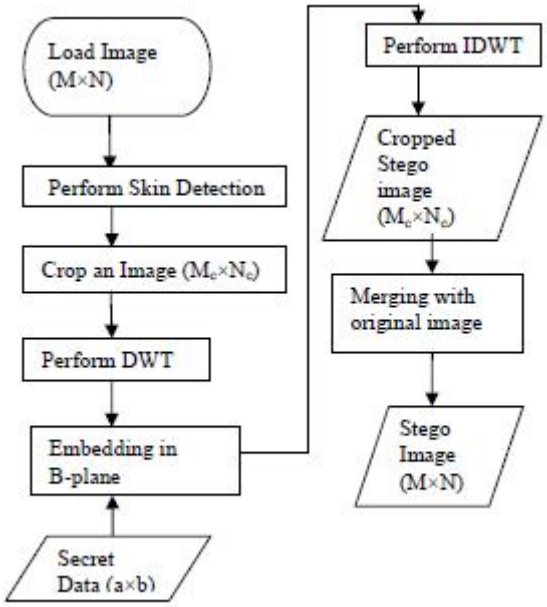
Proposed method introduces a new method of embedding secret data within skin as it is not that much sensitive to HVS (Human Visual System) .This takes advantage of Biometrics features such as skin tone, instead of embedding data anywhere in image, data will be embedded in selected regions. Overview of 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 subbands. Finally secret data embedding is performed in one of the high frequency sub-band by tracing skin pixels in that band.

This is done in 2 methods:

- **With cropping**: Before performing all steps cropping on input image is performed and then in only cropped region embedding is done, not in whole image. Cropping method provides more security than the method 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.
- **Without cropping**: Embedding is done on the image as a whole.

A. *Skin 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. This process has proven quite challenging. Skin detectors can lead to false detection in the background if the environment is not controlled. To decide whether a pixel is of skin color or not, it is necessary 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. Mainly two kinds of color spaces are exploited in the literature of biometrics which are HSV (Hue, Saturation and Value) and YCbCr (Yellow,Chromatic Blue, Chromatic red) spaces.



After detecting the skin region, erosions, dilations and closing operations are performed along with filling to obtain the face image.

- HSV: It is 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

- YCrCb: The range of Cb and Cr most representatives for the skin – color reference map were:

77<=Cb<=127 and 133<=Cr<=173

B. *Discrete Wavelet Transform*

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 effect. 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. 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.

C. *Embedding Procedure*

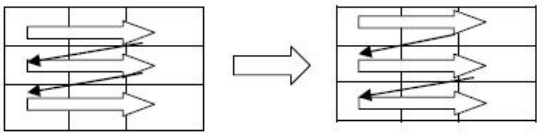
Suppose C is original 24-bit color cover image of M×N size. It is denoted as:

C= {xij, yij, zij |1 ≤ i ≤ M, 1 ≤ j ≤ N, xij, yij, zij Є {0, 1... 255}};

Let S is secret data. Here secret data considered is binary image of size a×b.

Perform embedding of secret data in one of sub-band that we obtained from DWT. 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. While embedding, secret data will not be embedded in all pixels of DWT sub-band but to only those pixels that are skin pixels. The high frequency HH sub-band is chosen. While embedding, secret data will not be embedded in all pixels of DWT subband 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 done as per raster-scan order that embeds secret data coefficient by coefficient in selected sub-band, if coefficient is skin pixel.

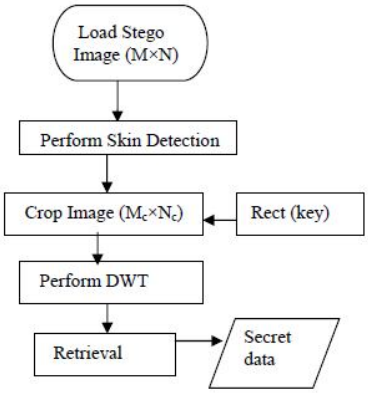


D. *Steps*

- Once image is loaded, apply skin tone detection on cover image. This will produce mask image that contains skin and non skin pixels.
- To perform cropping interactively on mask image. 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.
- Apply DWT to only cropped area (Mc×Nc) not whole image (M×N). This yields 4 sub-bands denoted as HLL, HHL, HLH, and HHH.
- Perform embedding of secret data in one of sub-band that we obtained earlier by tracing skin pixels in that sub-band (HH).
- Perform IDWT to combine 4 sub-bands.
- A cropped stego image of size Mc×Nc is obtained in above step. 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. To perform merging we require coefficients of first and last pixels of cropped area in original image.

E. *Extraction*

From the stego image, the secret image is retrieved back. All steps of Decoder are opposite to Encoder.



IV. RESULTS

A 24 bit color image is employed as cover-image of size MxN. Secret image to hide inside cover image is of size axb.

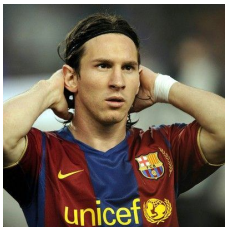
Cover image (400x400) and secret image (32x32)

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

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

$$\text{Where, } MSE = \frac{1}{(MxN)} \sum_{1}^{M} \sum_{1}^{N} \left(x_{ij} - y_{ij}\right)^2$$

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).



Stego image (400x400) and extracted secret image (32x32)

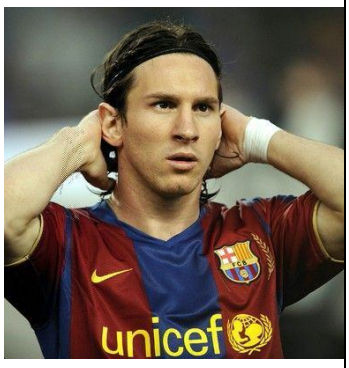
(1) PSNR With cropping and Without cropping

Extracted with cropping

Extracted without cropping

With Cropping	40.5556	26.8630
Without cropping	44.2754	25.2113

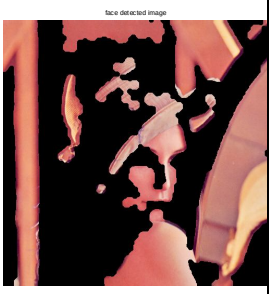
(2) PSNR of 3 different wavelets



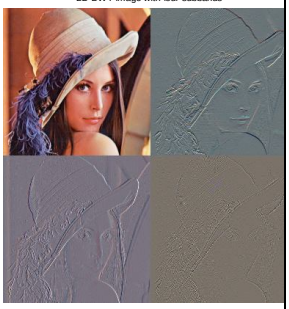
	Cover Psnr	Secret Psnr
Haar	44.6288	31.1287
DB7	43.4616	30.8307
Bior4.4	43.8042	31.2605

(3) Results with a different cover image

Cover image



Skin detected



Extracted secret

	Cover Psnr (512x512)	Secret Psnr (32x32)
Haar	51.1436	40.9361
DB7	49.4364	40.4733
Bior4.4	50.7342	40.6412

(4) Results using different sizes and dynamic ranges for secret images

Cover image	Secret image	PSNR of extracted secret images	
		Haar	Bior
400x400	32x32 (color image)	38.9642	32.6727
	32x32 (grey level)	Mse=0	Mse=0
400x400	50x50	31.0476	30.8004

356x356	64x64	32.0065	31.4806
400x517	32x32	32.7325	27.6372
512x512	32x32	40.9361	40.6412

CONCLUSION

Digital Steganography is a fascinating scientific area which falls under the umbrella of security systems. In this work Biometric Steganography is presented that uses skin region of images in DWT domain for embedding secret data. By embedding data in only certain region (skin region) and not in the whole image, security is enhanced.
Performing biometric steganography with cropping ot without cropping, both are having its own adnatages and disadvantages. But if the method is implemented with cropping then it will ensure more security than without cropping.

REFERENCES

[1] STEFAN KATZENBEISSER & FABIEN A.P.PETITCOLAS, "Information Hiding techniques for steganography and digital watermarking" 2000.

[2] MARC ANTONINI, MICHEL BARLAUD, “Image Coding Using Wavelet Transform”, *IEEE*, Vol.1, No.2, 1992

[3] Mr. R.SURENDIRAN and Dr. K. ALAGARSAMY, "Skin Detection Based Cryptography in Steganography (SDBCS)" , International Journal of Computer Science and Information Technologies, Vol. 1 (4), 2010.