International Journal of Electronics and Communication Engineering (IJECE)
ISSN 2278-9901
Vol. 2, Issue 4, Sep 2013, 105-112

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

DATA HIDING IN SKIN TONE OF IMAGES USING STEGANOGRAPHY

RAKHI[1] & VIJAY PRAKASH SINGH[2]

[1]Department of E. C, Bhabha Engineering Research Institute, Bhopal, Madhya Pradesh, India

[2]H.O.D. Department of E. C, Bhabha Engineering Research Institute, Bhopal, Madhya Pradesh, India

ABSTRACT

Steganography is a method of data hiding from its existence to another transmission medium for secret data communication [1]. This paper is based on the skin tone region of the images [2]. Here, hiding of the data is done in skin tone region of the image that will provide an excellence in data hiding. This skin tone detection is performed using HSV (Hue, Saturation and Value) color space. The embedding of secret data is done by using frequency domain approach of DWT (Discrete Wavelet Transform). The DWT having four sub bands of frequency in which high frequency sub band is used for secret data hiding by tracking skin pixels in that sub band. We shall use digital images as the cover object in this paper in which we embed the hidden information.

The challenge of using steganography in cover images is to hide as much data as possible with the least noticeable difference in the stego-image. Steganographic algorithms operate on basically three types of images: Raw images (i.e., bmp format), Palette based images (i.e., GIF images) and JPEG images. JPEG images are routinely used in steganographic algorithms due to the most popular lossy image compression method. Here, another feature used in data hiding i.e. cropping of image. The cropped image is used in different steps of data hiding. This cropping feature increased the security than the use of whole image. So, this cropped region used as the key at decoding side. This shows that the mechanism of hiding the information in skin tone region of images gives higher security and satisfactory PSNR.

KEYWORDS: Cropping, DWT, PSNR, Skin Tone Detection

INTRODUTION

In this era of digitalization the Internet occupies a conspicuous position for data transmission and sharing. Some secret data might be stolen, copied, modified or destroyed by an unwanted observer. It is used in internet security, authentication, copyright protection and information assurance etc**.** Hence, security problems could have dire consequences and thus it has become an important issue. Encryption procedure is used for secure data transmission [3]. It makes the secret data undecipherable and unnatural or meaningless. This unnaturality in data entices some unintended observer's attention. This reason gives rise to new method of data security known as steganography.

In Steganography, sender wishes to remain secret data confidential and data can be images, audio, video or other that can be in the form of stream of bits. The cover is the medium in which the message is embedded to conceal the presence of the message. The embedding is dependent on the structure of the cover and in this paper covers and secret messages are confined to being digital images. The cover-image with the secret data is called the "Stego-Image".

Additionally, we can encrypt the message before embedding of secret data in cover image for high security and protection of image [4]. For this the encoder usually employs a stego-key which ensures only those recipients, who know the decoding key will be able to overt, the message from a stego-image. For this proposed method, cropped region of image used as a key at decoding side and thus achieve invigorating security.

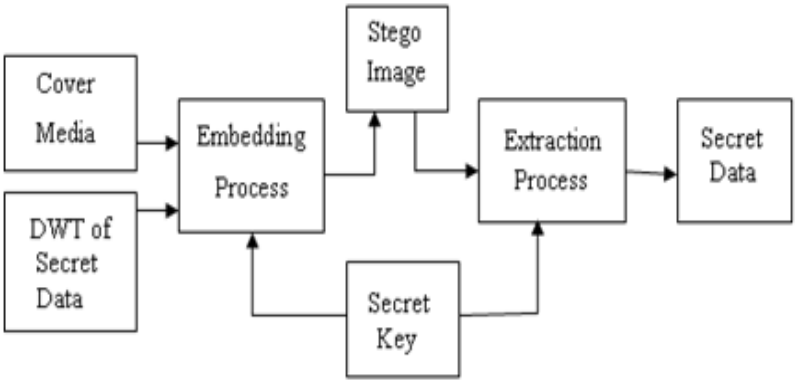

Figure 1: Modern Stego System

There are two things that need to be considered while framing the steganographic system: Invisibility: Human eyes cannot distinguish the difference between original and stego image. (b) Capacity: The capacity of data in image should be in a manner that during embedding, it doesn't degrade image quality significantly.

LITERATURE SURVEY

Steganography in Spatial Domain

This is the simplest steganographic technique that is most frequently used. In this technique, the bits of a secret message embedded directly into the Least Significant Bit (LSB) plane of the cover image so that the embedding procedure does not affect the original pixel value to a large extent [9]. The mathematical representation for LSB is :

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

In equation (1), x_i' represents the i th pixel value of the stego-image and x_i represents the original cover image. m_i represents the decimal value of the i th block in the secret data and k is the number of LSBs to be substituted. The extraction process is done by coping the k-rightmost bits directly. Mathematical representation of extracted message is:

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

Hence, a simple permutation of the extracted m_i gives us the original secret data [5]. This method is easy but it has low ability to bear some signal processing or noises. Thus, secret data can be easily stolen by breaching whole LSB plane.

Steganography in Frequency Domain

Robustness of steganography can be substantiated if properties of the cover image could be exploited. it is generally preferable to hide message in noisy regions rather than smoother regions as degradation in smoother regions is more noticeable to HVS (Human Visual System) [1]. Taking these aspects into consideration, working in frequency domain becomes more tempting. In this frequency domain approach, sender transforms cover image into frequency sub bands before embedding secret messages in it [6]. These sub bands give significant information about space occupy by vital and non-vital pixels in image. This frequency domain transform can applied to cover images either in DCT or DWT.

PROPOSED METHOD

This proposed method introduces hiding of secret data in skin tone region of images which is not much sensitive to Human Visual System (HVS) [1]. The embedding of data is done only in skin tone region. This method introduce following steps. At first, the detection of skin tone region in images is done by using HSV (Hue, Saturation, Value) color space. In the next step, the transformation of the cover image is taken in frequency domain. The Haar-DWT, simple DWT

is performed on image by using four sub bands of frequency. Finally, the secret data is embedded into high frequency sub band by tracing skin pixel in that band. The embedding is done only in cropped region instead of whole image. The cropping results high security. This cropped region works as secret key at decoding side. The embedding will affect only cropped region instead of whole image and it is not detectable by human visual system. In the next sub-sections skin tone detection and DWT are introduced.

Skin Tone Region Detection

Here, skin tone detector transforms given pixels into its color space value and the uses skin classifier to assign the pixel that it is skin pixel or non-skin pixel. By defining a boundary it can be easily decided that the pixel is of skin color or not. RGB matrix of given color can be converted into different color spaces to differentiate the region of skin or near skin tone. There are two color spaces in literature of the skin tone i.e. HSV (Hue, Saturation, Value) and YCbCr (Yellow, Chromatic Blue, Chromatic Red).

The human skin color is distributed within these two color spaces [2]. In this proposed method, HSV is used as any color image can be easily converted into HSV color space. Sobottaka and Pitas [7] 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:

$S_{min} = 0.23$, $S_{max} = 0.68$, $H_{min} = 0°$ and $H_{max} = 50°$

Discrete Wavelet Transform

This is one of the frequency domain in which steganography can be implemented. Here, we are using DWT instead if DCT as DCT calculated on independent pixels block. Due to this, a coding error causes discontinuity between the blocks resulting in annoying interference of artifact. The simplest DWT, Haar-DWT is used in this work. DWT applies on whole image. DWT splits component into frequency bands called sub bands. These are

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 eye are much more sensitive to LL, so secret data must be hide in other three sub bands without any change in LL sub band [8]. Hiding in high frequency sub band doesn't degrade the image quality that much.

Embedding of Secret Data

In this process, embedding is performed on the cropped image and it results into hiding of secret data. Take a 24 bit cover image C of dimension M×N.

It is denoted as:

$C = \{xij, yij, zij \mid 1 \leq i \leq M, 1 \leq j \leq N, xij, yij, zij \in \{0,1,..,255\}\}$

Let dimension 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. The secret data considered is binary image of size a×b. Figure 2 represent flowchart of embedding process.

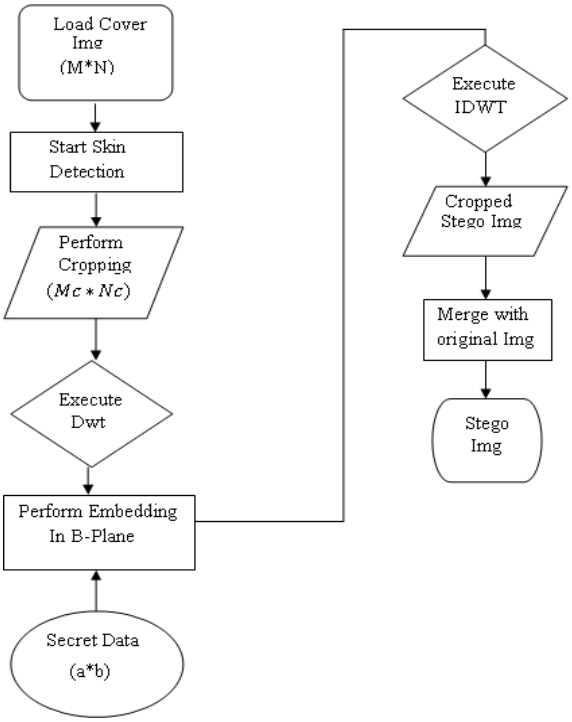

Figure 2: Flowchart of Embedding Process

The description of the process is given below.

- **Step 1:** First image is loaded and apply the skin tone detection on cover image. It results into mask image that contains skin and non skin pixels.
- **Step 2:** Perform cropping on mask image (Mc×Nc). After this original image is also cropped of same area. Cropped area must be in an exact square as we have performed DWT later and this should contain skin region. The data will hide in skin pixels of one of the high frequency sub band of DWT. Cropped region act as key at the receiver side. Only by using this key data retrieval is possible.
- **Step 3:** Apply DWT to cropped region only not to whole image. This gives 4 sub bands denoted as H_{LL} H_{HL} H_{LH} H_{HH}. Determine the payload of image to hold the secret data that based on the no. of skin pixels present in one of the high frequency sub band in which data will be hidden.
- **Step 4:** Perform embedding of secret data in high frequency sub band that we obtained by tracing skin pixels in that sub bands. Secret data is embedded in skin pixels that are traced by using skin mask detector. Embedding is done in G-plane and B-plane but strictly not in R-plane. Contribution of R plane is more in skin color than the B and G plane. As the pixel value of R plane changes decoder side doesn't find data at all. Skin detection at decoder side give different mask than encoder side.
- Perform IDWT to combine 4 sub bands.
- After combination of sub bands, a cropped stego image of size Mc×Nc is obtained. Then merge the cropped stego image with original image of size M×N. The coefficients of first and last pixels of cropped image required for merging. Thus, a stego image obtained.

Extraction of Secret Data

Load a 24 bit color stego image of size M×N. Then perform the skin detection to this stego image and obtain the

cropped image of size Mc×Nc as we have the value of cropped region that stored in 'rect' Variable. This will act as the key. Then perform the DWT on cropped image and retrieve the secret data by tracing skin pixels in high frequency sub band.

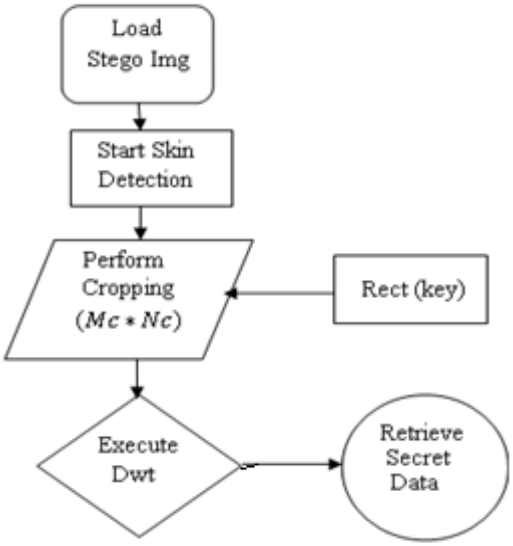

Figure 3: Flowchart of Extraction Process

SIMULATION RESULTS

In this section we talk about the simulation results for proposed method. This has been implemented by using MATLAB 7.10.0.

A 24 bit color image is used as cover image of size 256×256 shows in Figure 4 in which we hide secret data.

Figure 4: Cover Image

We use Peak Signal to Noise Ratio (PSNR) to determine quality of stego image after embedding the secret data. The performance in terms of PSNR (in dB) is shown in following subsections.

PSNR is defined by Eq. 3 and Eq. 4.

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

Where,

MSE = (1/(M×N)) $\sum_{i=1}^{M} \sum_{j=1}^{N} (x_{ij} - y_{ij})^2$ (4)

x_{ij} and y_{ij} represents pixel value of original cover image and stego image respectively. The calculated PSNR usually implement db value for quality judgments, the larger PSNR is, higher the image quality. On the contrary smaller dB value means there is a more distortion. PSNR values below 30dB indicate fairly a low quality.

Performance of the Proposed Method

After embedding secret data in cropped image, cropped stego image is obtained shown in Figure 5. This is not same as the cover image, so to obtain final stego image merging is performed that shown in Figure 6. The co-ordinates of the first and last pixels of cropped image in original image are calculated for merging. After extraction, the secret data retrieved. PSNR is calculated for four different final stego images resulted from a considered image and three more samples shown in table 1. Performing Steganography in skin tone of images with cropping ensure more security than without cropping. But both the cases have its own advantages and disadvantages. As the proposed method using cropping and this cropping region use as key at the decoder side then only extraction of secret data possible. PSNR of proposed method shows that data hiding in natural images with cropping concept giving more security and improve quality of images.

Figure 5: Histogram Cropped Stego Image

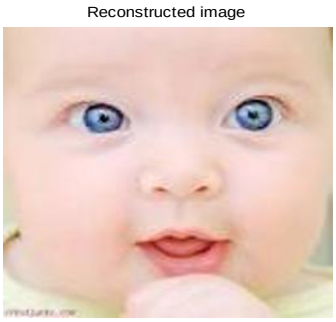

Figure 6: Final Stego Image after Embedding Process

Table 1: PSNR and MSE of 4 Final Stego Images In Proposed Method

Cover Image (256×256)	PSNR (Peak Signal To Noise Ratio)	MSE (Mean Square Error)
Image 1	47.4609	37.3674
Image 2	33.2008	32.9193
Image 3	35.8314	32.5882
Image 4	27.4253	33.7493

CONCLUSIONS

Digital Steganography is a engrossing scientific area which comes under the security system. In this paper Steganography uses skin region of images and embed the secret data in cropped region (only skin) of images by using DWT. This cropping concept enhances the security level since no one can extract secret data without having value of cropped region. The use of high frequency sub band of DWT in embedding gives high security as this is less sensitive to human eyes and also improves the quality of stego image. According to simulation results proposed method provides fine image quality.

ACKNOWLEDGEMENTS

The authors feel extreme gratitude to the existing work in steganography that has played a crucial role and has made immense contribution to the work done in this paper. All work done and images shown in this paper are for educational purpose.

REFERENCES

1. Anjali A. Shejul, Prof. U.L Kulkarni " A DWT based Approach for Steganography Using Biometrics", in: Proceedings of the 2010 International conference on data storage and data Engineering.

2. A. Cheddad, J. Condell, K. Curran and P. Mc Kevitt, "Biometric inspired digital image Stganography", 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. Petitcolas, F. A. P.: "Introduction to Information Hiding". In: Katzenbeisser, S and Petitcoals, F. A. P (ed.) (2000) Information Hiding Techniques for Steganography and Digital Watermarking. Norwood: Artech House, INC.

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

5. 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

6. 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).

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

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

9. 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.