Skin Tone Steganography for Real Time Images

1. Miss. Prajakta Deshmane, 2. Prof. S.R. Jagtap.
1. (Electronics Department, RIT,Shivaji University,Maharashtra)
2.(Electronics Department, RIT,Shivaji University,Maharashtra)

Abstract

Steganography is the science of concealing the existence of data in another transmission medium. It does not replace cryptography but rather boosts the security using its obscurity features. As Proposed method is Biometric Steganography. In this work Biometric feature used to implement Steganography is Skin tone region of images.

Proposed method introduces a new method of embedding secret data within edges of skin of image, as it is not that much sensitive to HVS (Human Visual System). 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 in cover images and then Secret data embedding will be performed in DWT(Discrete Wavelet Transform) domain as DWT gives better performance than DCT(Discrete Cosine Transform) while compression.. This biometric method of Steganography enhances robustness than existing methods.

Keywords:- Steganography, Skin tone detection, HSV,DWT

1. INTRODUCTION

Steganography is defined as science or art of hiding (embedding) data in transmission medium . Its ultimate objectives, which are undetectibility, robustness (i.e., against image processing and other attacks) and capacity of the hidden data (i.e., how much data we can hide in the carrier file), are the main factors that distinguish it from other 'sisters-in science' techniques, namely watermarking and Cryptography. [2]

In this work Biometric feature used to implement Steganography is Skin tone region of images. Proposed method introduces a new method of embedding secret data within edges of skin of image, as it is not that much sensitive to HVS (Human Visual System). Instead of embedding secret data anywhere in image, it will be embedded in only selected ROI (Region of Interest) not in whole image. Here ROI is skin region. Most important stage is skin tone detection. Skin detection means detecting image pixels and regions that contain skin-tone color. A skin classifier defines a decision boundary of the skin color class in the color space based on a training database of skin-colored pixels. [1]

Different algorithms are present for detecting skin region. Most of them put luminance part in non useful zone and uses only chrominance part but algorithm used here considers luminance part and detects skin. Choosing color space is main task. Color space used is new color space that contains error signal derived from differentiating gray color scale map and non red gray scale version. Here gray scale map is only luminance part of image. As most skin region resides in red channel non red gray scale version is considered that deliberately discarded red channel. So error signal is obtained by eliminating non red gray scale from luminance part. This performs skin detection. This skin region provides excellent secure location for data hiding.[1][2]. In the first phase of the work skin detection is performed. In the second phase of the work DWT (Discrete Wavelet Transform) will be performed that decomposes whole image into different sub bands. Secret data will be embedded in that sub band. [1]

1.1 The Ancient Steganography

The word Steganography is originally made up of two Greek words which mean "Covered Writing". It has been used in various forms for thousands of years. In the 5th century BC Histaiacus shaved a slave's head, tattooed a message on his skull and was dispatched with the message after his hair grew back. In Saudi Arabia at the king Abdulaziz City of Science and Technology, a project was initiated to translate into English some ancient Arabic manuscripts on secret writing which are believed to have been written 1200 years ago. 500 years ago, the Italian mathematician Jerome Cardan reinvented a Chinese ancient method of secret writing, its scenario goes as follows:- A paper mask with holes is shared among two parties, this mask is placed over a blank paper and the sender writes his secret message through the holes then takes the mask off and fills the blanks so that the letter appears as an innocuous text. This method is credited to Cardan and is called Cardan Grille. In more recent history, the Nazis invented several Steganographic methods during WWII such as Microdots, invisible ink and null ciphers.[1]

1.2 The Digital area of Steganography

As computer power, the internet and with the development of Digital Signal Processing (DSP), Information Theory and Coding Theory, Steganography goes in 'Digital'. Steganography does not exist merely in still images. Embedding hidden messages in videos and audios is also possible and even in a simpler form such as in Hyper Text Markup Language (HTML), executable files (.EXE) and Extensible Markup Language (XML).[1]

Steganography has various interesting applications of the science. e.g., copyright control of materials, enhancing robustness of image search engines and Smart IDs where individuals' details are embedded in their photographs. Other applications are Video-audio synchronization, companies' safe circulation of secret data, TV broadcasting, Transmission Control Protocol and Internet Protocol packets (TCP/IP) - for instance a unique ID can be embedded into an image to analyze the network traffic of particular users, embedding Checksum.[1]

1.3 Steganalysis

Steganalysis is the science of attacking Steganography in a battle that never ends. It mimics the already established science of Cryptanalysis. Steganalysis is achieved through applying different image processing techniques e.g., image filtering, rotating, cropping, translating, etc, or more deliberately by coding a program that examines the stego-image structure and measures its statistical properties e.g., first order statistics (histograms), second order statistics (correlations between pixels, distance, direction).Apart from many other advantages higher order statistics, if taken into account before embedding, can improve the signal-to-noise ratio when dealing with Gaussian additive noise. Some virus creators can exploit Steganography.

2. PRESENT THEORIES & PRACTICES

Different algorithms have been proposed to implement Steganography in digital images. They can be categorized in three major categories. New algorithms keep emerging by the rapid development of information technology and by the need for an enhanced security system. The discovery of the LSB embedding mechanism is actually a big achievement. An algorithm in spatial domain uses LSB (Least Significant bit) approach. LSB is simplest technique that embeds bits of secret data into LSB plane of cover image. The logic behind this work is to divide the cover image into sub-images and compress and encrypt the secret data. But this is not robust method.[1]

Another algorithm uses transfer domain technique that divides image into different frequency band and embeds secret data inside high frequency band. Unlike the space domain approaches, secret messages are embedded in the high frequency coefficients resulted from Discrete Wavelet Transform. Last type of algorithm is Adaptive algorithm that is generally combined with one of the former algorithms. Most of the existing methods suffer from intolerance to any kind of geometric distortions.[1]

As per above discussion the emerging techniques such as DCT (Discrete Cosine Transform), DWT and Adaptive Steganography are not an easy target for attacks, especially when the hidden message is small. That is because they alter bits in the transform domain, thus image distortion is kept to a minimum.

2.1 Steganography Methods

Different methods have been proposed to implement Steganography in digital images.

2.1.1 Steganography Exploiting Image Format

Steganography can be accomplished by simply feeding into a Microsoft XP command window the following half line of code:

```
C:\> Copy Cover. jpg /b + Message.txt /b
   Stego.jpg
```

This code appends the secret message found in the text file 'Message.txt' into the JPEG image file 'Cover. jpg' and produces the stego-image 'Stego.jpg'. The idea behind this is to abuse the recognition of EOF (End of file).In other words, the message is packed and inserted after the EOF tag. When Stego.jpg is viewed using any photo editing application, the latter will just display the picture and will ignore any data coming after the EOF tag. However, when opened in Notepad for example, our message reveals itself after displaying some data. The embedded message does not impair the image quality. Neither the image histograms nor the visual perception can detect any difference between the two images due to the secret message being hidden after the EOF tag. This simple technique would not resist any kind of editing to the Stego image nor does any attack by Steganalysis experts.[1][2]

2.1.2 Steganography in the Spatial Domain

In spatial domain methods a we modifies the secret data and the cover medium in the spatial domain, which is the encoding at the level of the LSBs. This method has the largest impact compared to the other two methods even though it is known for its simplicity. Embedding in the 4th LSB generates more visual distortion to the cover image as the hidden information is seen as 'non-natural'. The logic behind this work is to divide the cover image into sub-images and compress and encrypt the secret data. The resulting data is then sub-divided in turn and embedded into those images portions. [1]

2.1.3 Steganography in the Frequency Domain

New algorithms are coming, by the rapid development of information technology and by the need for an enhanced security system. The discovery of the LSB embedding mechanism is actually a big achievement. DCT is used extensively in Video and image (i.e., JPEG) lossy compression. Each block DCT coefficients obtained is quantized using a specific Quantization.[1]

Wavelet transform is used to convert a spatial domain into frequency domain. The use of wavelet in image stenographic model lies in the fact that the wavelet transform clearly separates the high frequency and low frequency information on a pixel by pixel basis. Discrete Wavelet Transform (DWT) is preferred over Discrete Cosine Transforms (DCT) because image in low frequency at various levels can offer corresponding resolution needed.[5][4]

The Haar Wavelet Transform is the simplest of all wavelet transform. In this the low frequency wavelet coefficient are generated by averaging the two pixel values and high frequency coefficients are generated by taking half of the difference of the same two pixels. The four bands obtained are approximate band (LL), Vertical Band (LH), Horizontal band (HL), and diagonal detail band (HH). The approximation band consists of low frequency wavelet coefficients, which contain significant part of the spatial domain image. The other bands also called as detail bands consists of high frequency coefficients, which contain the edge details of the spatial domain image.[5]

Embedding in the DWT domain shows promising results and outperforms the DCT domain especially in surviving compression. We should be cautious when embedding in the transformation domains in general. However, DWT tends to be more tolerant to embedding than DCT.[1]

3. PROPOSED FRAMEWORK

Block diagram of proposed work is shown below.

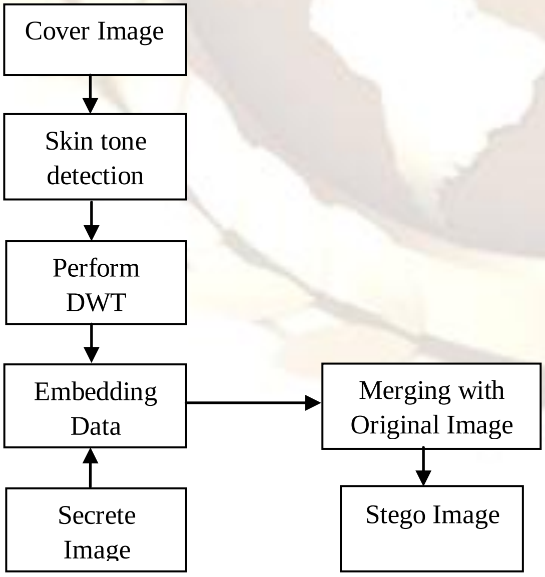

Fig.3.1 Data Embedding Process

3.1 Skin Color Tone Detection

Skin detection means detecting image pixels and regions that contain skin-tone color. We can use colour space transformations to detect and track any presence of human skin tone. We can also adjust the human skin tone values, within the permissible value ranges, to embed secret data without introducing artifacts on the carrier image. We perform skin tone detection to embed secret data in videos for the reason- When the embedding is spread on the entire image (or frame), scaling, rotation or cropping will result in the destruction of the embedded data because any reference point that can reconstruct the image will be lost. However, skin tone detection in the transformed colour space ensures immunity to geometric transforms.

3.1.1 RGB & YCbCr (Yellow, Chromatic Blue, Chromatic red) Color Space

RGB color space is the most commonly used color space in digital images. It encodes colors as an additive combination of three primary colors: red(R), green (G) and blue (B). One main advantage of the RGB space is its simplicity. However, it is not perceptually uniform, which means distances in the RGB space do not linearly correspond to human perception. In addition, 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 components. In other words, the location of a given skin patch in the RGB color cube will change based on the intensity of the illumination under which such patch was imaged! This results in a very stretched skin color cluster in the RGB color cube.

3.1.2 HSV COLOR SPACE

Color space used for skin detection in this work is HSV. (Hue Saturation Value)

- Hue: It is that quality by which we distinguish one colour family from another, as red from yellow, or green from blue or purple.
- Saturation : It is that quality of colour by which we distinguish a strong colour from a weak one; the degree of departure of a colour sensation from that of a white or gray; the intensity of a distinctive hue; colour intensity.
- Value: It is that quality by which we distinguish a light colour from a dark one.

Any color image of RGB color space can be easily converted into HSV color space.

I = imread(CoverImage);

HSV=rgb2hsv(I);

We 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 =0 and Hmax=50 *(HSV image is shown in fig.3.2)*

3.1.3 DWT (Discrete Wavelet Transform)

The wavelet transform describes a multi-resolution decomposition process in terms of expansion of an image onto a set of wavelet basis functions. Discrete Wavelet Transformation has its own excellent space frequency localization property. Applying DWT in 2D images corresponds to 2D filter image processing in each dimension. The input image is divided into 4 non-overlapping multi-resolution sub-bands by the filters, namely LL1 (Approximation coefficients), LH1 (vertical details), HL1 (horizontal details) and HH1 (diagonal details).

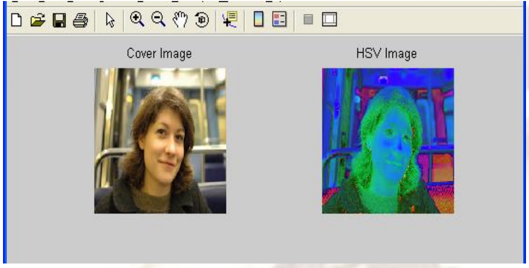

Fig 3.2 Original Image and HSV Image.

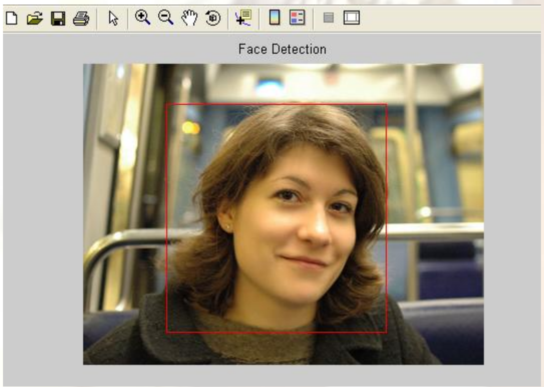

Fig 3.3 Face detection.

4. Conclusion

Skin tone steganography is secured way of data hiding in the real time images. The proposed framework is based on color spaces and DWT techniques for a data hiding. The data merging techniques like LSB or DWT are not easy to attacks especially when the hidden image/data is small. According to proposed method distortion after the data hiding is minimum.

REFERENCES

Technical Paper References:

[1] Abbas Chedda, Joan Condell, Kevin Curran and Paul Mc Kevitt 'Biometric Inspired Digital Image Steganography' ,School of Computing and Intelligent Systems, Faculty of Computing and Engineering, University of Ulster. Londonderry, Northern Ireland, United Kingdom.

[2] Abbas Cheddad, 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, United Kingdom.

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

[4] Po-Yueh Chen* and Hung-Ju Lin 'A DWT Based Approach for Image Steganography' National Changhua University of Education

[5] H S Manjunatha Reddy and K B Raja "High capacity and security steganography using discrete wavelet transform"

Text References:

[1] R.C.Gonzalez, Digital Image Processing, Second edition, Pearson Education.

[2] Anil K.Jain, Fundamentals of Digital Image Processing, Prentice-Hall(PHI).

[3] Digital Image Processing, Using MATLAB by Gonzalez, Woods and Eddins,Prentice Hall.