IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Skin Tone Based Secret Data Hiding in Images

Miss. Prajakta Deshmane
Electronics Department, RIT, Shivaji University, Maharashtra, India
prajudeshmane@gmail.com

Abstract

Maintaining the secrecy of digital information when being communicated over the internet is presently a challenge. An ideal steganography technique embeds message information into a carrier image with virtually imperceptible modification of the image. Adaptive steganography comes closer to this ideal since it exploits the natural variations in the pixel intensities of a cover image to hide the secret message. The objective of steganography is a method of embedding additional information into the digital contents that is undetectable to listeners.

Proposed method is Biometric Steganography. In this work Biometric feature used to implement Steganography is, Skin tone region of images. Instead of embedding secret data anywhere in image, it will be embedded in only edges of skin tone region. Image Edge detection significantly reduces the amount of data and filters out useless information, while preserving the important structural properties in an image. Edge detection method improves signal to noise ratio, & gives better detection especially in noise conditions.

Keywords: Biometric Steganography, Skin tone detection, edge detection.

Introduction

Steganography means to hide secret information into innocent data. Digital images are ideal for hiding secret information. An image containing a secret message is called a cover image. First, the difference of the cover image and the Stego image should be visually unnoticeable. The embedding itself should draw no extra attention to the Stego image so that no hackers would try to extract the hidden message illegally. Second, the message hiding method should be reliable. It is impossible for someone to extract the hidden message if she/he does not have a special extracting method and a proper secret key. Third, the maximum length of the secret message that can be hidden should be as long as possible.[3] [5]

"Steganography is the art of hiding information in ways that prevent the detection of hidden messages,"

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. This skin region provides excellent secure location for data hiding.[1][2].

Edge detection technique provides better results than earlier techniques because of its capability of carrying large payload with better imperceptibility. This can be achieved by embedding more data in edge areas as compared to smooth areas of the image as human eye cannot detect the distortion at edges easily. The proposed algorithm yields better PSNR values as compared to previous algorithms.

Steganography in History

Steganography comes from Greek and means "covered writing." The ancient Greeks wrote text on wax-covered tablets. To pass a hidden message, a person would scrape off the wax and write the message on the underlying wood. He/she would then once again cover the wood with wax so it appeared unused.

Steganography in the Digital Age

Steganography is the art of secret communication. Its purpose is to hide the very presence of communication as opposed to cryptography whose goal is to make communication unintelligible to those who do not possess the right keys. Digital images, videos, sound files, and other

computer files that contain perceptually irrelevant or redundant information can be used as "covers" or carriers to hide secret messages. After embedding a secret message into the cover-image, a so-called Stego-image is obtained. It is important that the Stego-image does not contain any easily detectable artifacts due to message embedding. A third party could use such artifacts as an indication that a secret message is present. Once this message detection can be reliably achieved, the steganography tool becomes useless.[5]

Obviously, the less information is embedded into the cover-image, the smaller the probability of introducing detectable artifacts by the embedding process. Another important factor is the choice of the cover-image. The selection is at the discretion of the person who sends the message. The sender should avoid using cover-images that would be easy to analyze for presence of secret messages. For example, one should not use computer art, charts, images with large areas of uniform color, images with only a few colors, and images with a unique semantic content, such as fonts. Although computer-generated fractal images may seem as good covers6 because of their complexity and irregularity, they are generated by strict deterministic rules that may be easily violated by message embedding.

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.

Cryptography VS Steganography

Cryptography is the science of encrypting data in such a way that nobody can understand the encrypted message, whereas in steganography the existence of data is conceived means its presence cannot be noticed. The information to be hidden is embedded into the cover object which can be text, image, audio or video so that the appearance of cover object doesn't vary even after the information is hidden.

Information to be hidden + cover object = Stego object.

To add more security the data to be hidden is encrypted with a key before embedding. To extract the hidden information one should have the key. A Stego object is one, which looks exactly same as cover object with an hidden information.

Steganography VS Watermarking

Watermarking is another branch of steganography it is mainly used to restrict the piracy in digital media In steganography the data to be hidden is not at all related to the cover object, here our main intention is secret communication. In watermarking the data to be hidden is related to the cover object it is extended data or attribute of the cover object, here our main intention is to stop piracy of digital data. Steganography is a very powerful tool because, as the stated above, it can be very difficult to detect.

Proposed Framework

As shown in the fig. 3.1, in first stage skin tone detection will be performed on input image i.e. cover image (in which data is to be embedded). After performing skin tone detection, edges of that skin region are found out. After getting edge index secrete data (i.e. image) will be embedded. Proposed work is used for special face or bio-images.

Block diagram of proposed work is shown below:

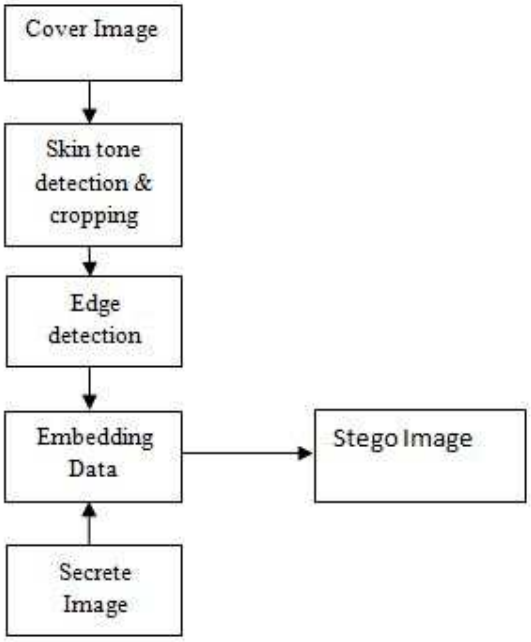

Fig.3.1 Data Embedding Process

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.

RGB Color Space

The RGB color model is an additive color model in which red, green, and blue light are added together in various ways to reproduce a broad array of colors. [6]

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 much stretched skin color cluster in the RGB color cube.

Edge Detection Techniques

Edge detection aims at identifying points in a digital image at which the image brightness changes sharply or more formally has discontinuities. Following edge detectors are handy:

1. Sobels Edge Detector - 3×3 gradient edge detector
2. Prewitt Edge Detector - 3×3 gradient edge detector.
3. Canny Edge Detector - non-maximal suppression of local gradient magnitude.
4. Zero Crossing Detectors - edge detector using the Laplacian of Gaussian operator. In this paper work we are using Zero crossing detector.

[1] Canny Edge Detection

The Canny edge detector is an edge detection operator that uses a multi-stage algorithm to detect a wide range of edges in images.

Some criteria have to improve edge detection. The first and most obvious is low error rate. It is important that edges occurring in images should not be missed and that there be NO responses to non-edges. The second criterion is that the edge points be well localized. In other words, the distance between the edge pixels as found by the detector and the actual edge is to be at a minimum. A third criterion is to have only one response to a single edge. This was implemented because the first 2 were not substantial enough to completely eliminate the possibility of multiple responses to an edge.[4]

Based on these criteria, the canny edge detector first smoothes the image to eliminate and noise. It then finds the image gradient to highlight regions with high spatial derivatives.

Step 1

In order to implement the canny edge detector algorithm, a series of steps must be followed. The first step is to filter out any noise in the original image before trying to locate and detect any edges. . And because the Gaussian filter can be computed using a simple mask, it is used exclusively in the Canny algorithm. Once a suitable mask has been calculated, the Gaussian smoothing can be performed using standard convolution methods. A convolution mask is usually much smaller than the actual image. As a result, the mask is slid over the image, manipulating a square of pixels at a time.

Step 2

After smoothing the image and eliminating the noise, the next step is to find the edge strength by taking the gradient of the image. This gives two gradients, one gradient in the x-direction (columns) and the other gradient in the y-direction (rows).

Step 3

The direction of the edge is computed using the gradient in the x and y directions. However, an error will be generated when sum X is equal to zero. So in the code there has to be a restriction set whenever this takes place. Whenever the gradient in the x direction is equal to zero, the edge direction has to be equal to 90 degrees or 0 degrees, depending on what the value of the gradient in the y-direction is equal to.

Step 4

Once the edge direction is known, the next step is to relate the edge direction to a direction that can be traced in an image. After the edge directions are known, nonmaximum suppression now has to be applied. Finally, hysteresis is used.

Following are the results of proposed framework

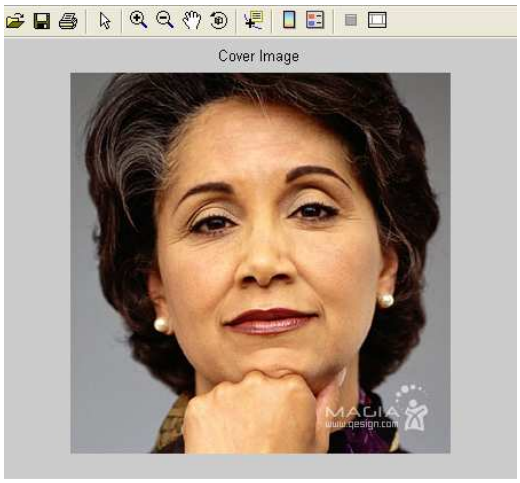

Fig 3.1. Cover Image.

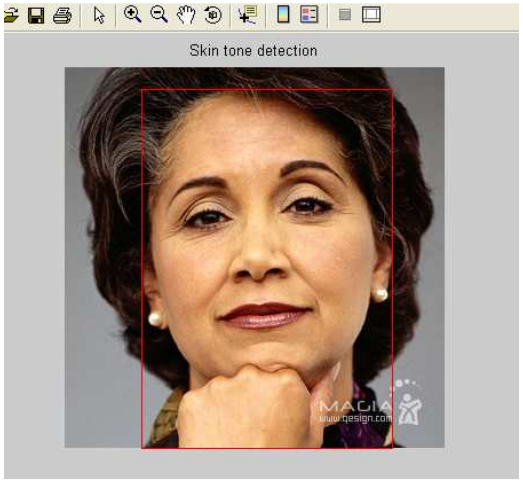

Fig. 3.2. Cropped Skin region.

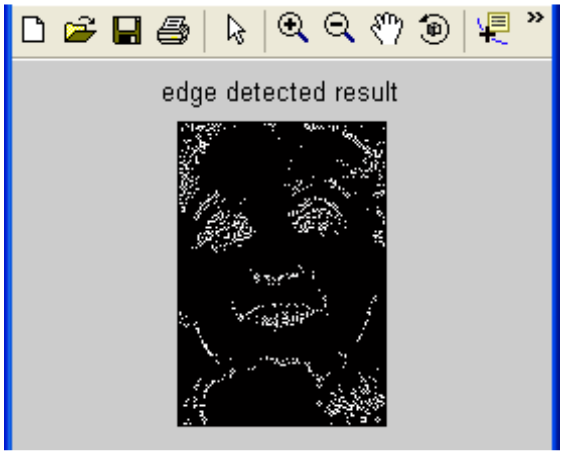

Fig 3.3. Edge detection of cropped skin region.

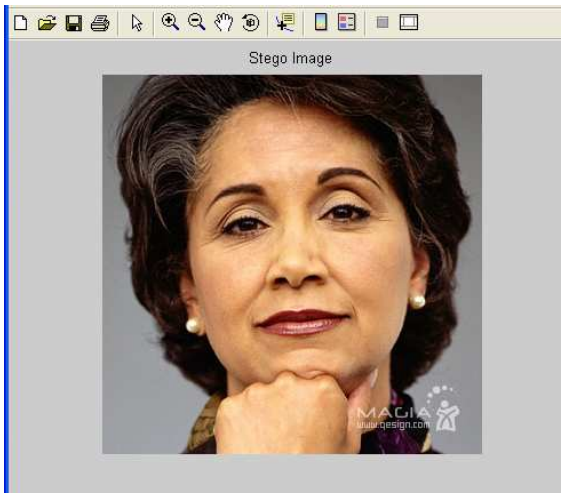

Fig 3.4. Stego Image.

Conclusion

This paper proposes a method for image steganography. According to Human Visual System, any variation in the edges shown in the images has a low probability of being perceived by the human eyes, thus data can be hidden in the pixel of the cover image. In canny edge detection method the gradient of the pixel of the image is determined and the image edges are detected by taking a threshold value of the gradient image. Here we go for multiple edge detection so that more number of pixels around the edge area is detected using the above method. Hence by observing above Fig 3.1. & Fig 3.4. there is less distortion which is not visualized to human eyes.

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] Nitin Jain, Sachin Meshram, Shikha Dubey: "Image Steganography Using LSB and Edge Detection Technique" IJSCE

[5] Provos N, Honeyman P: "Hide and Seek: An Introduction to Steganography", May/June 2003,
[6] Adnan Abdul-Aziz Gutub : " Pixel Indicator Technique for RGB Image Steganography"

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.