ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Skin Tone Based Steganography: A Review

Reshma.R.Pillai[1], Smitha Vas.P[2]

M.Tech Student, Dept. of CSE., LBS Institute of Technology for Women, Thiruvananthapuram, Kerala, India[1]

Assistant Professor, Dept. of CSE, LBS Institute of Technology for Women, Thiruvananthapuram, Kerala, India[2]

ABSTRACT: Steganography is the method to hide the data in another transmission medium to perform a secure secret communication. The secret information may be text or image or audio. The transmission medium is known as the cover medium which is the image or audio. Biometrics is the science to measure and analyse the characteristics like skin, fingerprints, face etc. It has the ability to identify individuals with high degree of confidence. It is difficult to ensure the security and integrity of storage and transmission of biometric templates and confidential messages. So they need to transmit with more security. The combination of cryptography with steganography adds a good level of security and can be used to exchange biometric data. It is possible to combine biometrics with steganography for transmission of encrypted biometric data and other confidential data to boost security. In the last decades a significant amount of approaches on this technology have been introduced. Here a comprehensive survey on skin tone based steganography is presented.

KEYWORDS: Image steganography; Biometric Image Steganography; Skin tone detection; colorspace; cropping; PSNR; MSE

I. INTRODUCTION

In this extremely digitized globe, the internet provides an important role for the data transmission and sharing. So a safe and secure communication system is necessary. Encryption is a well-known procedure for secured data transmission [1].Frequently used encryption methods include RSA; DES. Encryption achieves certain security aspects like they make the secret messages unreadable and unnatural or meaningless. This unnatural message usually attracts the attention of some unintended observers. Due to this reason it is necessary to introduce a new security mechanism called steganography. Steganography is the mechanism to hide the existence of data in another transmission medium to perform secret communication. It doesn't replace the cryptography .It boosts the security using its own features. Steganography is originated from the Greek words,"*steganos* and *graphein*", which means"covered writing". In steganography the secret message is the data in which the sender wishes to remain confidential. The cover is the medium where the message is embedded and helps to hide the presence of the message.

Fig.1. Steganography Model

The secret message is embedded inside the cover object and then it is called stego. To ensure high security the secret message should be encrypted before embedding in the cover. Fig.1 describes the steganography model. During the extraction process the message is retrieved from stego without causing any distortion in cover. The combination of cryptography and steganography provides more security for the data which is transmitted. Main objectives of steganography are:

- Embedding capacity: The amount of information that can be hidden relative to the size of the cover object without deteriorating the quality of cover object.
- Robustness: It is the ability of the stego to avoid manipulations such as filtering, cropping, rotation, compression etc.
- Invisibility: It is the ability to be unnoticed by the human.
- Security: It is the ability to be undetected by the attacker. The security of the image is calculated using PSNR.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

The other quantitative parameters are:

Peak Signal to Noise Ratio (PSNR): This is calculated in order to determine the quality of the stego medium after the message is embedded. It is given by equation.

$$PSNR = 10log_{10} {}^{max^2}/_{MSE}$$

max is the maximum value of pixels (255 for gray scale images). A greater PSNR value indicates the better quality. It is expressed in decibels (dB).

Mean Square Error (MSE): MSE is the mean square error between the original and stego medium.
It is given by the equation

$$MSE = \frac{1}{MXN}\sum_{i=1}^{M}\sum_{j=1}^{N}\|O(i,j) - D(i,j)\|^2$$

where*O (i , j)* is the original pixel and *D (i, j)* is the stego pixel.

The main purpose of energy efficient algorithm is to maximize the network lifetime. These algorithms are not just related to maximize the total energy consumption of the route but also to maximize the life time of each node in the network to increase the network lifetime. Energy efficient algorithms can be based on the two metrics: i) Minimizing total transmission energy ii) maximizing network lifetime. The first metric focuses on the total transmission energy used to send the packets from source to destination by selecting the large number of hops criteria. Second metric focuses on the residual batter energy level of entire network or individual battery energy of a node [1].

II. IMAGE STEGANOGRAPHY

In image steganography the secret message is embedded within the digital image called cover image. The cover image carrying embedded data is called stego image. The steganography equation is defined as stego_image = cover_image + message+ stego_key. Fig.2 describes the image steganography model. The hidden data is the message which the people wish to send secretly. It is hidden in a cover image and then forming stego image. The message is hidden in the redundant bits. A stego key is used to control the hiding process to restrict the detection of the embedded data to another party. At the receiver side during the extraction process the secret key that is used to embed the data is taken to remove the data. The secret key is known only by the sender and the receiver.

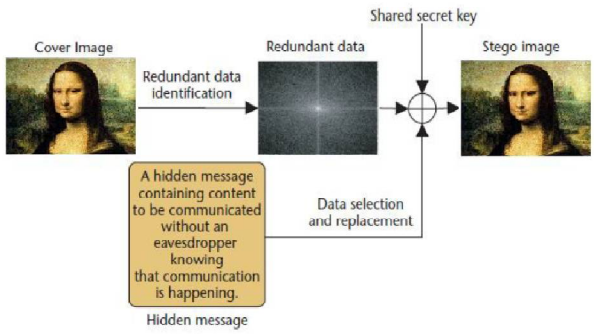

Fig.2. Image Steganography Model

A. Classification of Image Steganographic System

The image steganographic system can be classified in to two types: Spatial domain and the transform domain. In the spatial domain the messages are directly embedded in the pixels and in the transform domain the image is transformed and then hides the message.

Spatial Domain Techniques: This technique is based on the physical location of the pixels in an image. This technique provides some changes in the pixel of the cover image before embedding the message. The types of spatial domain techniques are [2]:

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

LSB Replacement: This is a well-known technique to hide the message. Here the least significant bit of the cover image is overwritten with the secret message using pseudo random number generator.
LSB matching: This technique provides a minor change to the LSB Replacement. Here if the secret bit doesn't match the LSB of the cover image then +1 or -1 is added to the corresponding pixel value.
Bit Plane Complexity Segmentation: In this technique higher bits are used for embedding information. Here each block is divided in two domains: informative domain and the noise domain. The message is made to embed in the noise region. This makes the image to escape from degradation. Large amount of data can be hiding using this technique.

Transform Domain Techniques: This technique is based on encoding the message in the transform domain coefficients of the cover image. A high quality embedded image is obtained by transforming the original image in to the frequency domain. This technique provides more security than spatial domain technique. The types transform domain techniques are [2]:

Discrete Cosine Transform (DCT): This technique allows the image to be broken into different frequency bands and make it to embed the message in the middle frequency band. The middle frequency band is chosen because it minimizes the most visual part of the image. The transformed image consists of AC and DC coefficient. The left corner element is called DC coefficient which is perceptually significant and remaining portions are called AC coefficients which is perceptually insignificant.
Discrete Wavelet Transform (DWT): This technique divides the image into high frequency and low frequency. The low frequency is again divided into two parts as high and low frequency. The message is embedded in the high frequency.
Discrete Fourier Transform (DFT): This technique divides the image into two matrices called amplitude and phase. The message is embedded in the phase part which contains the quality part of the image.

III. BIOMETRIC STEGANOGRAPHY

Biometrics is defined as the automatic recognition of individuals based on their behavioral and biological characteristics. It originated from the Greek words"*bios* and *metricos*", literally means life to measure. The biometric data is classified as physiological data or behavioral data. The physical biometrics is based on physical characteristics such as fingerprint, iris etc. and the behavioral biometrics is based on behaviour of human such as voice, signature etc. In this highly digitized globe the internet plays an important role in data transmission and sharing of data. Some confidential biometric information and other information may get stolen, copied, modified. To overcome this problem the biometrics is combined with steganography which is called as biometric steganography [3].

IV. SKIN TONE DETECTION

Skin tone detection is the method to detect the skin pixels with in an image to hide the information in that region. The biometrics used here is the skin. Instead of embedding the message in whole image, it is embedded in the selected skin region. The goal of skin color detection is to build decision rule that will discriminate between skin and non-skin pixels. A skin detector converts a given pixel into a suitable color space and uses a skin classifier to label the pixel to identify whether it is a skin pixel or non-skin pixel. The skin detection algorithm produces a mask, which simply a black and white pixels. The black pixels values are 0 that is false and white pixels values are 1 that is true. The mask of I and 0 act as logic map for skin detection. The simplest way to decide whether a pixel is skin or non-skin is to explicitly define the boundary [9]. The detection of the skin tone regions requires knowledge in color spaces.

The types of color spaces are [4]:

RGB: It is originated from Cathode Ray Tube (CRT) which is a combination of three colored rays; red, green and blue. It is the widely used color spaces.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

(a) (b) (c)

Fig.3. (a) Cover image, (b) Skin region of image represented in white pixels, (c) Masked image (skin pixels white and non-skin pixels black)

RGB Color Value Normalization: The RGB color representation is obtained from RGB values by a simple normalization procedure.

$$r = \frac{R}{R+G+B} g = \frac{G}{R+G+B} b = \frac{B}{R+G+B}$$

HSV, HSL, HIS: Hue-saturation based color spaces were introduced when there is a need for the user to specify the color spaces properties numerically. Hue defines the dominant color of an area; saturation defines the colourfulness of an area which is proportional to the brightness. The intensity, lightness or value is related to the color luminance.

$$H = \arccos \frac{\frac{1}{2}(R-G)+(R-B)}{\sqrt{(R-G)^2+(R-G)(G-B)}} \qquad S = 1 - 3\frac{\min(R,G,B)}{R+G+B} V = \frac{1}{3}(R+G+B)$$

YCbCrColor intensity: It is an encoded nonlinear RGB signal represented by luma which is constructed as a weighted sum of RGB values and two color difference values *Cb* and *Cr* which is obtained by subtracting luma from RGB red and blue components.

$$Y = 0.299R + 0.587G + 0.114BCr = R - YCb = B - Y$$

The RGB matrix of the given color image can be converted in to different color spaces in order to distinguish skin region and non skin region. It is experimentally proved that the distribution of human skin color constantly resides in a certain region within the color space [9].

V. RELATED WORK

Many research works have been done based on the skin tone detection techniques.

Abbas Chetad et al. [5] perform the skin tone detection using a novel color space method in which human clusters is well classified with carefully selected boundaries. The payload to embed is encrypted by exploiting the strength of ID encryption algorithm named SHA-1 and extended to handle 2D data. An object oriented embedding is performed to embed the encrypted payload in the cover image.

Anjali et al. [6] perform the skin tone detection mechanism, with cropping and without cropping cover image. The skin region is detected using the HSV color space. The cover image is then transformed into frequency domain using Haar- DWT and after that payload is calculated. Then secret data embedding is done in high frequency sub-band by tracing the skin pixels. A comparative study is done on cropping and without cropping case. She concluded that both provide enough security.

Sunitha et al. [7] perform the skin tone detection by segmenting the skin pixels using masking and filtering mechanism. This means that masks the black region and filters the white region. After performing this, a particular region of the skin is selected to embed the data. The data is embed in the selected region, before a 2D wavelet transform is performed in the selected region of interest. After this a particular sub band is selected to embed the data. Here this paper encompasses the three tier robustness with the existence of two keys and IDWT on the decoder side. This helps to prevent the steganalysis.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Lavanya et al. [8] perform the skin tone detection on the input image using the HSV color space. Then the cover image is cropped and this cropped one is transformed in to frequency domain which Haar-DWT. This generates four subbands. This paper find out that cropping results in more security than without cropping. This cropping image will act as the key in the decoder side. The embedding process is only in the selected region not in the whole part of the image.

Rupa et al. [9] perform the skin tone detection using HSV color space. The embedding is performed in G-plane and B-plane but not in R-plane. This is because in skin color the contribution of R-plane is more than the G-plane and B-plane. This embedding algorithm attempts to preserve histogram of DWT after the embedding the message. It protects from histogram based first order statistics attacks. The image is then cropped and then transformed in to frequency domain which is Haar-DWT. The secret data is embedded in any one of the subbands.

Snehal et al. [10] perform the skin tone detection using the HSV color space. The cover image is cropped and is transformed into frequency domain which is Haar-DWT. The secret data is embedded in any of the frequency band. It is observed that cropping results in more security than without cropping. This cropping image will act as the key in the decoder side. The embedding process is only in the selected region not in the whole part of the image.

Vemula et al. [11] perform a skin tone detection using HSV color space. After the skin is detected the cover image is cropped. Then the cropped cover image is remodeled in frequency domain by applying Haar-DWT. Then payload is calculated. Before embedding process a secret key is generated. The secret key and the cropped region works as two keys. The embedding method affects only the region of interest not whole image.

VI. CONCLUSION AND FUTURE WORK

Steganography becomes a fascinating mechanism in this digitized globe to hide the secret data in the image. Instead of hiding the message in whole part of the image, it is hidden in the skin tone region of the image to ensure more security. Many researches are done based on the skin tone detection mechanism. A comparative study is done based on the related work. By the analysis it is find out that most researchers try to hide the message before cropping the image. The cropped image ensures more security. Some of them try to encrypting the image and messages that needed to hide in the cover medium. Most of them concentrated on image. Further research can be done in video also.

REFERENCES

1. Fabien A. P. Petitcolas., Ross J. Anderson .,and Markus G. Kuhn.,"Introduction to Information Hiding",Proceedings of the IEEE, special issue on protection of multimedia content,Vol.87,Issue.7,pp.1062-1078,1999.
2. Kirti D. Nagpal.,and Prof.Dabhade.D.S,"A Survey on Image steganography and its techniques in Spatial and Frequency domain",International Journal on Recent and Innovation Trends in Computing and Communication,Vol. 3, Issue.2,pp.776-779,2015.
3. Christian Rathgeb and Andreas Uhl,"A survey on biometric cryptosystems and cancellable biometrics",EURASIP Journal on Information Security,Vol.2011,Issue.3,pp.1-25,2011.
4. Surendiran.R and Dr.Alagarsamy.K, "Skin detection based cryptography in steganography", International Journal of Computer Science and Information Technologies,Vol.1,Issue.4,pp.221-225,2010.
5. Abbas Cheddad.., Joan Condell., Kevin Curran., and Paul Mc Kevitt.,"Steganoflage-A Novel Approach to image Steganography",pp.191-194.
6. Anjali A Shejul .,and Umesh L Kulkerni.,"A Secure Skin tone based Steganography using wavelet transforms",International Journal of Computer Theory and Engineering,Vol.3,Issue.1,pp.16-25,2011.
7. Sunita Barve., Uma Nagaraj., and Rohit Gulabani.,"Efficient and Secure Biometric Image Steganography using Discrete Wavelet Transform", International Journal of Computer Science & Communication Networks,Vol.1,Issue.1,pp.96-99,2011.
8. Lavanya.N., Manjula.V., and Krishna Rao.N.V.,"Robust and Secure Data Hiding inImage Using Biometric Technique", International Journal of Computer Science and Information Technologies,Vol.3,Issue.5,pp.5133-5136,2012.
9. Rupa Maan .,and Lovneesh Bansal.,"Comparison and Implementation of Biometric Inspired Digital Image Steganography", International Journal of Computer Science And Technology,Vol.3,Issue.4,pp.848-853,2012.
10. Snehal Manjare., and Chougule.S.R.,"Steganography using concept of Skin tone Detection",International Journal of Scientific Research Engineering & Technology,Vol.2,Issue.4,pp.189-193,2013.
11. Vermula Harini., and Jeevan Kishor G.,"Skin Tone Base Secret Data Hiding in images Using Wavelet Transform",International Journal of Computer Applications Technology and Research,Vol.2,Issue.6,pp.666-670,2013.