ISSN: 2277-9655
Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

SKIN TONE BASED IMAGE STEGANOGRAPHY USING PARTICLE SWARM OPTIMIZATION

Vaddadi Swetha*, Dr. V.S.R.Kumari
* B.Tech Student of SMCE, ECE Department, SMCE,Tummalapalem
M.Tech, PH.D. Professor, HOD, ECE, SMCE,Tummalapalem

DOI: 10.5281/zenodo.52499

ABSTRACT

In data communication field, security problems become an essential issue. Steganography is the art of hiding the actual data in another transmission medium to obtain secret communication. It does not replace the cryptography but rather boosts the security using its features. In this paper, Biometric feature is implemented for skin tone region of images. Data hiding is done at detected skin tone regions. A novel steganography method is proposed which is based on particle swarm optimization for data hiding. It assures high security, good invisibility and robustness. The secret information is hided in the image to improve the security of stego images by means of PSO algorithm.

KEYWORDS: Communication, Stenography, Biometric, Data hiding, Skin tone, Particle swarm optimization.

INTRODUCTION

Steganography is defined as science or art of hiding (embedding) the secret and confidential data in another transmission medium. Its ultimate objectives, are un-detectable, robustness and capacity of the hidden data (i.e., how much data we can hide in carrier file), are the main elements that distinguish it from other techniques, namely watermarking and cryptography.

In contrast to Cryptography, the enemy is allowed to detect, intercept and modify messages without being able to offend certain security premises assured by a cryptosystem, the main goal of Steganography is to hide messages inside other messages in such a way that any enemy does not allow to even detect that there is a second message situated. In a digital world, Steganography and Cryptography are both intended to protect information and are accomplished, but neither technology individual one is perfect and both can be broken. For this reason most experts would suggest that using both to add multiple layers of security. Steganography is used in a bulk amount of data formats in today's digital world .

In this work Biometric feature is used to implement for skin tone stenography in images. A new method of embedding secret data within edges of skin images is proposed and it is not sensitive to Human Visual System (HVS). The crucial role is to detect the skin tone region and there are different algorithms for detecting skin tone regions.

Steganography is used in wide range of applications like in defense organizations for safe transmission of secret messages, military and intelligence agencies, smart identity cards where personal details are embedded in the photograph etc. There are mainly two things that need to be considered while constructing the steganographic system:

(a) Invisibility: Human eyes can't distinguish the difference between original image and stego image.
(b) Capacity: The secret data capacity which is to be embedded in the cover image doesn't degrade an image quality significantly.

LITERATURE SURVEY

The existing methods for image steganography are

- LSB(Least Significant Bit) Substitution based.
- Transform domain based.
- Adaptive method.

LSB (LEAST SIGNIFICANT BIT) SUBSTITUTION

In the spatial domain approach, the least significant pixels are embedded by secret messages in cover images. Least Significant Bit Substitution (LSB) is the most commonly used stenographic technique. In the gray level image, each pixel consists of 8 bits. The basic concept of LSB is to embed the secret data at the bits which is having minimum weight (rightmost bits) so that the embedded process wont affect much more the original pixel value. Modulating the least significant bit does not result in human distinguishable because the amplitude of this change is small. For example to hide the character 'A'into an 8-bit color cover image, an eight consecutive pixels are taken from top left corner of the image. The equivalent binary bit pattern of those pixels be:- 00100111 11101001 11001000 00100111 11001000 11101001 11001000 00100111.After that the binary equivalence of letter 'A' i.e. 01100101 is copied one by one (from the left hand side) to the LSB's binary pattern of pixels and the resulting bit pattern will be 00100110 11101001 11001001 00100110 11001000 11101001 11001000 00100111.

TRANSFORM DOMAIN

Robustness of steganography can also be improved if properties of the cover image could be exploited. For example it is preferable to hide message in noisy regions rather than smooth regions as the degradation in smooth regions are more noticeable to human HVS (Human Visual System). When working in frequency domain, by considering these aspects it becomes more attractive. Before embedding the secret messages, the frequency domain approach transforms the cover image into the frequency domain coefficients. This transformation can be either Discrete Cosine transform (DCT) or Discrete Wavelet Transform (DWT). Though these methods are more difficult and slower than spatial domain, they have an advantage of being more secure and noise tolerant.

ADAPTIVE STEGANOGRAPHY

Adaptive steganography is a special case of above two methods. It is also called as Statistics aware embedding. This method captures the statistical global features of the image before embedding the secret data in DCT or DWT coefficients. These statistics will help to know, where to make the necessary changes. A random adaptive selection of pixels is characterized by the selection of pixels and on the cover image with large local STD (Standard Deviation).

EXISTING METHOD

- First the Skin tone detection is implemented on input image using HSV (Hue, saturation, value).
- Then the Cover image is transformed into frequency domain using Haar-DWT and the payload number is calculated.
- Finally one of the high frequency sub band is occupied by secret message by tracing the appropriate skin pixels in that band.
- Embedding steps are applied :
  - With cropping.
  - Without cropping.

With cropping

Input image is first cropped and only in that cropped region data hiding is performed. Cropped region works as a key at decoding side and it is more secure**.**

Without cropping

In whole skin region, Data is embedded in image. Embedding algorithm attempts to store the histogram of DWT coefficients after embedding.

Data Embedding Process:

The below diagram shows the data embedding process of the steganography:

ISSN: 2277-9655
Impact Factor: 3.785

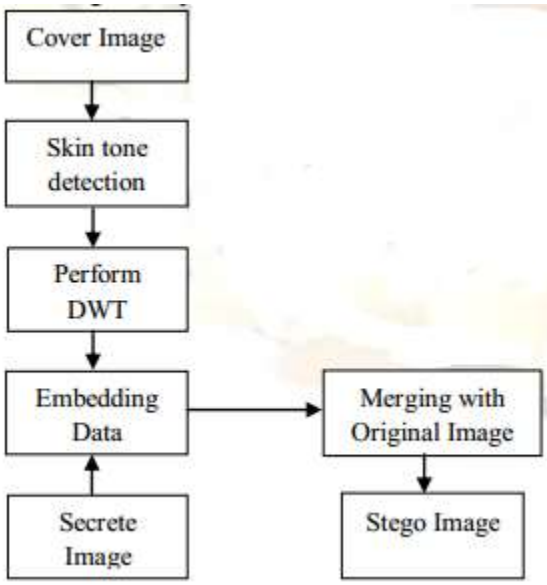

Fig 1: Data Embedded Process

SKIN TONE COLOR DETECTION:

Skin tone detection means identifying the image pixels and area that contain skin tone color. In images, skin color is a sign of human and its existence. Research has been focused on skin tone detection in images and advantages involved in detecting face and non-face like features. Skin detection using color information is a challenging task, as the appearance of skin in images is affected by various factors such as illumination, background, camera characteristics etc. Numerous techniques are presented in literature for skin detection using color. In visible spectrum, skin-color detection can be a challenging task as the skin color in an image is sensitive to various factors such as:

1) Color constancy problem i.e. in indoor, in outdoor, shadows, highlight produces a change in the skin color of images. So, it is the main problem which seriously affects the performance of skin detection task.

2) From person to person also skin tone changes, belonging to different ethnic groups and from persons across different regions.

3) For the same person, the skin-color distribution varies from one camera to another depending on the camera sensor characteristics.

4) Individual features such as age, sex and body parts also affect the skin-color appearance.

5) Different factors such as appearances like makeup, hairstyle and glasses, background colors, shadows and motion also influence skin-color appearance.

Skin detection also produces a mask – black and white.

- White pixel = 1 →Skin pixel.
- Black pixel = 0 → Non-Skin pixel.

RGB matrix of the given colour image is converted into different colour spaces to get distinguishable regions of skin. Mainly there are two kinds of colour spaces are possible. They are HSV (Hue, Saturation and Value) and YCbCr(Yellow, Chromatic blue, Chromatic red) spaces. It is experimentally found that the distribution of human skin colour constantly persists in a certain range within the colour space. The HSV colour space is chosen in this paper and the RGB image is converted into HSV colour space. In HSV, responsible values for skin detection are Hue & Saturation. Hue & Saturation dimensions are extracted and separate them into new variables (H & S).

- The threshold is chosen for Skin detection as [H1, S1] & [H2, S2].
- Sobottaka & Pitas gives a face localization based on HSV.The threshold range of human flesh are obtained as:

S_{min}= 0.23, S_{max} =0.68, H_{min} =0° & H_{max}=50°.

2D HAAR DWT

DWT is the frequency domain in which the biometric steganography is implemented. The frequency domain transform applied is Haar-DWT, i.e. the simplest DWT. DWT splits component into numerous frequency sub bands as:

- Horizontally and vertically low pass - LL
- Horizontally low pass and vertically high pass - LH
- Horizontally high pass and vertically low pass -HL
- Horizontally and vertically high pass -HH

Human eyes are more sensitive to the low frequency part (LL sub-band). Hence, the secret messages are hidden in other 3 parts.

Advantages:

- High Computation Speed, Simplicity.
- It performs row and column transformation of Image matrix.

EMBEDDING PROCESS

In this process, embedding is done on the cropped image and secret data is hidden in it..

Let the dimension of cropped image i.e. cropped region must be exact square, as to apply DWT later on this region. Let 'S' is secret data. Here the secret data is as considered as an binary image of size. Below figure represent flowchart of embedding process.

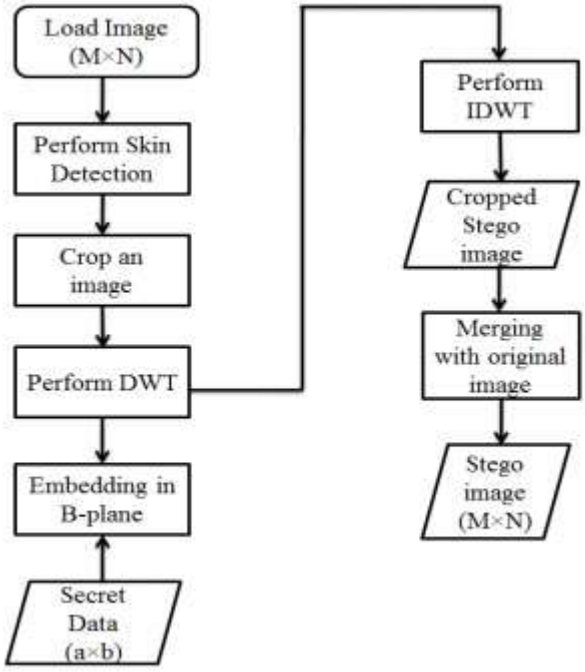

Fig 2: Flowchart of embedding process

EXTRACTION PROCESS

A 24 bit color stego image of size is loaded as input to extraction process. Then perform the skin detection to this stego image & obtain the cropped image of size . Suppose cropped area value is stored in 'rect'variable that is same as in encoder. So this 'rect'acts as a key at decoder or receiver side. The steps of Decoder are opposite to Encoder. While cropping, care must be taken to crop same size of square as per Encoder. Secret data is retrieved by tracing skin pixels in frequency sub-band of DWT. The flowchart of extraction process is given below in Fig

ISSN: 2277-9655
Impact Factor: 3.785

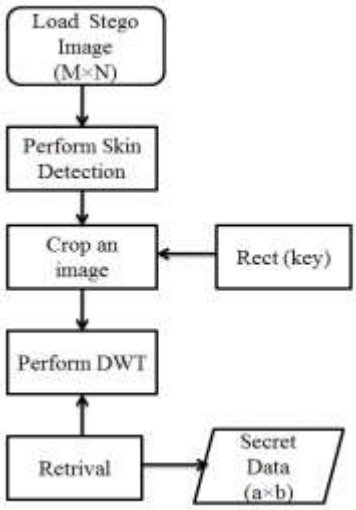

Fig 3: Flowchart of extraction process

PROPOSED METHOD

Particle swarm optimization technique is based on the particles (i.e. swarm of individuals). In PSO, the particles fly across the space by the current optimum particles. Each particle is associated with the best position in its neighborhood. When smaller neighborhoods are used, the algorithm is generally referred to as a lbest PSO. The performance of each particle is measured using a fitness function that varies depending on the optimization.
Each particle in the swarm is represented by the following characteristics:

x id : The current position of the particle.
v id : The current velocity of the particle.
P id : The personal best position of the particle.

The new velocity and position of each particle can be calculated using the current velocity and the distance from i p to g p as shown in the following formulas:

$$v_{id}^{k+1} = w \times v_{id}^{k} + c_1 \times rand() \times (p_{id} - x_{id}^{k}) + c_2 \times rand() \times (p_{gd} - x_{id}^{k})$$

$$x_{id}^{k+1} = x_{id}^{k} + v_{id}^{k+1}$$

where i = 1,2,...n, d =1,2, ….m. w,c1,c2 > 0,n is the number of particles in a group, m is the number of members in a particle, w is the inertia weight factor, c1 and c2 are acceleration constants, rand are random numbers with the range [0,1].

CONCLUSION

Digital Steganography is a scientific area which falls under the category of security systems. In this paper Biometric Steganography is discussed that uses skin region of images. For data embedding, with cropping is considered. It is observed that it offers enough security. A hybrid technique is proposed which providing high security. Image steganography using PSO algorithm is implemented which shows the better results than other techniques.

REFERENCES

[1] Cheddad, J. Condell, K. Curran and P. Mc Kevitt, “Biometric inspired digital image Steganography”, in: Proceedings of the 15th Annual IEEE International Conference and workshops on the Engg.of Computer-Based Systems (ECBS’08) Belfast, 2008, pp. 159-168.

[2] Petitcolas, F.A.P.: "Introduction to Information Hiding". In Katzenbeisser, S and Petitcolas, F.A.P (ed.) (2000) Information hiding Techniques for Steganography and Digital Watermarking. Norwood: Artech House, INC.
[3] Johnson, N. F. and Jajodia, S.: "Exploring Steganography: Seeing the Unseen." IEEE Computer, 31 (2): 26-34, Feb 1998. [4] Chris Shoemaker, "Hidden Bits: A Survey of Techniques for Digital Watermarking" Independent Study EER- 290 Prof Rudko Spring 2002
[4] 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.
[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] Provos,N. and Honeyman, P: "Hide and Seek: An introduction to steganography". IEEE security and privacy, 01 (3): 32- 44,May-June 2003
[8] Ahmed E., Crystal M. and Dunxu H.: "Skin Detection-a short Tutorial", Encyclopedia of Biometrics by SpringerVerlag Berlin Heidelberg 2009
[9] Yang, J., & Waibel, a. (1996). A realtime face tracker. Proceedings of the 3th IEEE Workshop on Applications of Computer Vision, Sarasota, Florida, 142- 147
[10] Sobottka, K. and Pitas, I.:"Extraction of facial regions and features using color and shape information." Proc. IEEE International Conference on Image Processing, pp. 483-486.(1996)
[11] Chen,P. Y.and Liao,E.C., :A new Algorithem for Haar Wavelet Transform," 2002 IEEE International Symposium on Intelligent Signal Processing and Communication System, pp.453-457(2002).