PRIVATE CONFIDENTIAL DATA HIDING BY USING WAVELET APPROACH

Shilparani Noubade[1], Hemavathi.N.V[2]

[1]*Dept.ECE, EPCET Bangalore*
[2]*Asst.prof. Dept.ECE, EPCET Bangalore*

Abstract

This paper introduces a secret data hiding method which is based on the biometric features. In this rapid technically developing world sharing multimedia on an internet has become a trend, digital media like audio, video and images are being shared through social networks. Also there is a possibility of threatening these digital media whichever sent through internet so to address this issue one need to take security measure to get strong communication system which should be able to withstand against hackers. Steganography by using discrete wavelet transform (DWT). Here in this context skin region particularly face area is opted out. Because, compared to all other skin area like hand, neck etc., face region will be brighter. Skin classifier Adaboost is used. In this paper graphic manipulation process called cropping is introduced, also cropped value helps in extraction process. Here, data is embedded by tracing skin pixel in frequency band and strictly speaking data is embedded in G and B plane. Simulation is carried out by using MATLAB software.

Keywords- *Steganography, Biometric, DWT, skin classifier, cropping, G and B plane, MATLAB, peak signal to noise ratio and mean square error.*

----------***----------

1. INTRODUCTION

In this digitalized world sharing or passing of data from one place to other takes place through internet, providing security to the confidential data which is passing on internet becomes a major concern. Now a day's security measures have grown rapidly all over the world. Cryptography, steganography and watermarking are widely used techniques for securing data. In cryptography original message itself made unreadable so that which cannot be easily understood by any other third party except authorized party. Steganograpy is also one of the methods which provide security to the data communication system. In this method secrete original data is hidden in cover image without altering original data, multimedia signals like audio, video and images are used as carrier for original message. The image or text in which object is hidden is called cover image, hidden confidential data may be plain text, encrypted text or an image, stego image means the image procured after embedding process i.e., it is a combination of original data and cover image. Against harmful threats an additional assurance or barrier is provided before embedding process for this encoder provides a security key this key ensures that only advised identity will be able to access confidential data.

A perfect steganography method should have following features:

1. **Capacity:** How much amount of confidential data can embed without worsening the quality of the cover image.
2. **Robustness:** Indicates that how stego image is immune to possible attacks.
3. **Invisibility:** Third party or attacker should not figure out the existence of secret data in cover image except intended person.
4. **Mean square error:** It indicates the difference between quality of stego image and cover image.

All data hiding techniques are divided into two classes those are:

1. **Spatial domain:** In this data is hidden in the cover image pixels as it is. In this pixel value changes with respect to intensity of image.
2. **Transform domain:** Here image is transformed from time domain to frequency domain using mathematical operators called transforms there are so many transforms are there like DWT Fourier transform, Discrete cosine transform, Z-transform etc., out of them using DWT. But what do this frequency domain actually mean, which contains high frequency bands, consists of only edge information of a particular image Low frequency band consists of smooth region of an image it contains more information of an image compared to high frequency band.

Rest of the paper contains following parts. Literature survey, proposed method with block diagram, details about embedding process, extraction process and experimental results. Finally conclusion.

2. LITERATURE SURVEY

Any data hiding method will be done in two domains either in spatial domain or in frequency domain. Spatial domain

has many techniques like LSB replacement, LSB matching, matrix embedding and pixel value difference (PVD). In frequency domain or transform domain also many steganography techniques are there some of them are steganography by using DCT, steganography by using Z-transform, based on DWT etc.,

2.1 Steganography in Spatial Method

LSB replacement method: Data hiding scheme by using simple LSB replacement method, in this LSB bit of the cover image is replaced with bit of the message this data hiding scheme is most common and easy method. But, hackers can hack the data easily by extracting whole least significant bit plane.

LSB matching method: In this method rather than simply replacing the LSB with message bit, the pixel value is either incremented or decremented there by removing asymmetry of odd and even pixel. Even valued pixel will be incremented by one, and odd valued pixel decremented by one. i.e., if secret data bit does not matches with LSB of cover image then one will be added or subtracted from the cover image pixel value. But, this technique is limited by artificial noises these noises greatly affect the visual quality of the stego image.

Pixel value differencing: In this method, cover image is divided into non overlapping two pixel blocks each block is categorized according to the difference value of two pixels; a small difference indicates that pixels are from smooth region and large difference indicates that pixels are from edge region, edge pixels bear larger changes in pixel value than the smooth region pixels hence, more data is embedded in edge region. Some downsides of this technique are time consuming, complex and can b attacked.

2.2 Steganography in Frequency Domain

In this transforms are used to convert spatial domain image into its frequency domain these methods are slow and not so simple but these are more secure and tolerant to noises.

Steganography based on DCT co-efficient: In this method, DCT converts the cover image from spatial domain to frequency domain. It separates the image into spectral sub bands based on its visual quality. The secret data is embedded in the cover image for DCT co-efficient lower than the threshold value, strictly data embedding in DCT coefficient 0 is avoided. But from this perfect robustness is not achieved hence, it is less secure.

Steganography by using Z-transform: In this Z-transform is applied on a 2*2 mask of a source image in a row major order to transform original sub image mask to its frequency domain. One bit of secret message is hidden in each mask's transformed co-efficient.

Steganography by using wavelet transform: This transform separates the high frequency component from low frequency component. Discrete wavelet transform divides image into four sub bands those are approximate band, vertical band, horizontal band and diagonal band (LL, LH, HL, and HH respectively) where LL band contains low frequency components, as it contains smooth region of image hence, these low frequency components are visible to eyes, where as all other three bands (LH, HL, HH) contains only edge information. DWT is preferred over DCT because it provides better resolution than DCT. This is all about the existing system.

2.3 Proposed Method

This section deals with the details about the proposed method. This secure method for exchanging confidential data uses the biometric feature. Here skin region of face is selected for hiding confidential data because; it provides more security to other region of skin. Wavelets are used to transform image which is used just like vehicle for the hiding and passing that from one place to other is converted from time domain to frequency domain. Here, Db2 wavelet is used. The phase which corresponds to hiding of data is given in below figure, at the same time it is necessary to extract the hidden data back which is depicted in next column of this page.

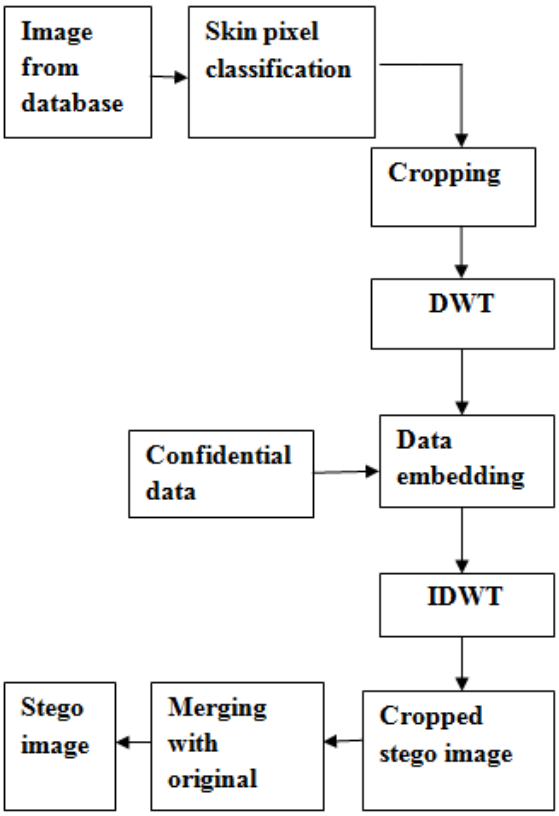

Fig1: Block diagram of embedding process.

Embedding phase is briefly explained as follows. First cover image is taken from the database; skin pixel classification is performed by using adaboost classifier for the cover image. Next, cropped skin region of the cover image is transformed from spatial domain into frequency domain; this task is done by using Db2 wavelet transformation. At the last embedding is done in skin region of face by using LSB substitution

method. After applying inverse DWT, cropped stego image is obtained, this is merged with original to get stego image. Below shown figure is block diagram of extraction process.

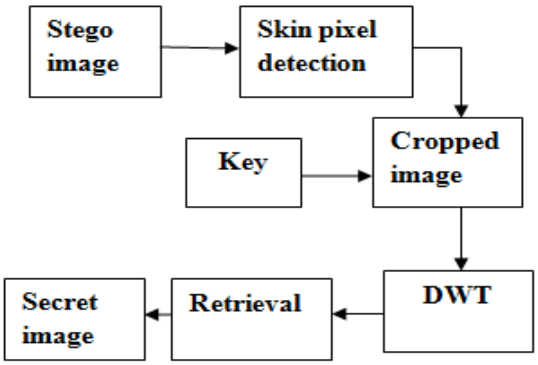

Fig2: Block diagram to reconstruct original image and Extraction Of Hidden Message

In Extraction process skin pixel detection is done on stego image, and then cropped region is detected by using key. Finally DWT is applied to retrieve confidential data.

2.4 Steps Used In Embedding Process

Let us consider a cover image of size P*Q and cropped image size is Pc*Qc. The size of the confidential data is A*B. So steps included in embedding and extraction phase are given below.
Step1: Load cover image of size P*Q from the data set.
Step2: Perform skin pixel classification by using Adaboost algorithm.
Step3: Cropping is done in order to get skin region in a square form so that it becomes easy to apply DWT. Size of the cropped image is Pc*Qc.
Step4: Apply DWT to get four sub bands of frequency like LL, LH, HL, and HH (approximate band, vertical band, horizontal band and diagonal detail band).
Step5: Perform embedding of confidential data of size A*B, by using LSB substitution method by tracing skin pixels in frequency bands.
Step6: Apply IDWT to merge all four sub bands of frequency. A cropped stego image of size Pc*Qc is obtained.
Step7: Cropped stego image (Pc*Qc) is merged with original image. Here, stego image of size P*Q is obtained.
Extraction process is carried out in a reverse way. But, cropped value acts as a key to extract secrete data.

2.5 Discrete Wavelet Transform

DWT splits the frequency component into four sub bands they are, LL(Low pass in both Horizontally and vertically it is also called as approximate band), LH(Horizontally low pass and vertically high pass it is also called as horizontal band), HL(Horizontally high pass and vertically low pass it is also called as vertical band) and HH(horizontally and vertically high pass it is also called as diagonal detail band).DWT outperforms than DCT because, time consumption in DCT is more and also complex compared to DWT . In this paper db2 wavelet is used.

2.6 Adaboost Classifier

As skin tone classifier is applicable only to the uniform skin region, it does not classify the skin region of non uniform type so to avoid this drawback, Adaboost algorithm is used which works for both uniform and non uniform type skin regions.

LSB substitution method: A message bit is hidden in a least significant bit of the skin pixel by tracing skin pixels in higher frequency band. Security to the data will be given before embedding process. Cropped value acts as key at the decoder or receiver.

2.7 Advantages of Proposed Method

1. By hiding data only in a certain region increases security level.
2. Cropping is done on cover image which keeps the security at a respectable level.
3. No one can extract the data until and unless they get the value of cropped region.
4. Since data is hidden in a higher frequency band rather than lower frequency band. Higher frequency components are less sensitive to human eye hence; good stego image quality is obtained.

2.8 Applications of Proposed Method

1. Health department: Some time for further treatment it needs to send patient's confidential medical details from one place to other place, in such situation, one can opt this proposed method.
2. Banking sector: It is used in banking to prevent user's password hacking in net banking.
3. Defense organization: For safe circulation of secret data from one place to other in military department.
4. Copy right protection: It gives protection to the creator of an original work by embedding details about of art.

4. SIMULATION RESULTS

Simulation is carried by using MATLAB software of version 7.10. The simulation results are shown below. Cover image of size 256*256 is taken and secret image is of 64*64.

Fig3: Cover image

This is the cover image in this the below shown secret image is hidden

Fig4: Secret image

This is the secret image which is used to hide in above shown cover image.

Fig5: embedded image

This image is obtained after embedding process

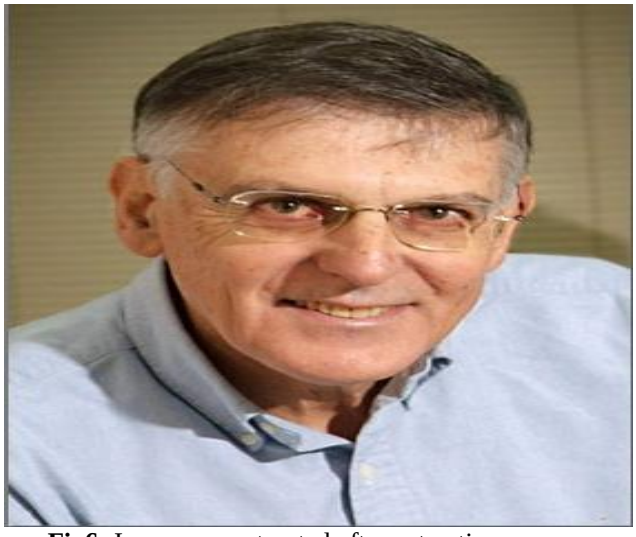

Fig6: Image reconstructed after extraction process

This image is obtained after extraction process

5. CONCLUSION

In this paper Biometric feature based private data hiding method by using DWT is proposed. a adaboost algorithm helps to detect uniform type skin as well as non uniform type skin of face And obtained a perfect stego image quality, stego image quality is assessed by using performance parameters like peak signal to noise ratio and mean square error. Embedded image is absolutely invisible to human eye hence achieved a good stego image quality, and also reconstructed a original image back and retrieved secret data successfully with the help of cropped value as a key by intended personality only at the receiver.

REFERENCES

[1] Swapnali zagade and smita bhosale, "Secret data hiding by using DWT", International journal of engineering and advanced technology 2014.

[2] Vemula Harini and Jeevan kishor.G, "skin tone based secret data hiding in image using wavelet transform", International journal of computer applications technology and research 2013.

[3] Suchi Sharma and Uma kumara,"High capacity data hiding technique using steganography", International journal of emerging trends and technology in computer science 2013.

[4] S.premkumar and A.E. Narayan, "New visual steganography scheme for secure banking application", International conference in computing, electronics and electrical technology 2012.

[5] Po-Yueh Chen and Hung-ju Lin,"DWT Based approach for image steganography", International journal of applied science and engineering 2006.

[6] Cheddad.j, Condell, K.curran and P. Mc Kevitt, "Biometric inspired digital image inspired digital image steganography", IEEE International conference and workshops on engineering of computer based system.

[7] P.Maheshkumar and Dr.K .L shunmugnathan,

[8] "A reversible high embedding capacity data hiding technique for hiding secret data in images, International journal of computer science and information security 2010.

[9] G.S.Sravanthi, B.SunithDevi, S.M.Riyazoddin And M.Janga Reddy,"A spatial domain image steganography technique based on plane bit substitution method", Global journal of computer science and technology graphic and vision 2012.

[10] Dr.Maheshkumar and Munesh yadav,"Image steganography using frequency domain", International journal of scientific an technology research 2014.