International Journal of Computer Applications in Engineering Sciences
[VOL III, ISSUE III, SEPTMBER 2013] [ISSN: 2231-4946]

Biometric Based Secret Data Hiding in Images Using IWT

Thamaraiselvi M[1], Tina Trueman[2],Rajasoundaran S[3]

Department of Computer Science and Engineering
Anna University, Taramani Campus, Chennai

[1]thamarai.selvim@gmail.com
[2]tinaeaster.jaya@gmail.com

***Abstract*– Steganography is the art of hiding the existence of data in another transmission medium to achieve secret communication. Steganography method used in this paper is based on an IWT algorithm to hide the data into cover image. Here we are using the Biometric feature of the cover image to hide the secret data i.e. the skin region of the image that will provide an excellent secure location for hiding the data. Skin tone detection is performed using YCbCrcolor space and the secret data embedding is performed using frequency domain Approach - IWT (Integer Wavelet Transform).Secret data is hidden in one of the high frequency sub-band of IWT by tracing skin pixels in that sub-band. We are embedding additional information to the embedded Image, so that the decoder can retrieve the loss less secret/hide data, this additional embedded data will give sufficient information of the secret and act as a key for the skin tone area where secret data is hidden. This study shows, that by adopting an object oriented steganography using Image Processing mechanism with some additional information about the encoding message to the decoder, in the sense that, we get a higher security because of cropped image and loss less hidden data at the Decoder. And also satisfactory PSNR (Peak Signal Noise Ratio) is obtained.**

***Keywords*—Biometrics, Skin Tone Detection, IWT, PSNR, YCbCr**

I. 1 INTRODUCTION

Today's internet world is full of data thieves and hackers. There is a strong need for a system that can transfer sensitive data across the internet. Cryptography can achieve this goal. But, cryptography just transforms the sensitive data into another form which could not be understood by everyone, so that only the intended recipients with a key can unlock the data back to the original form. So, the transformed cryptic data is visible to everyone, and thus may create curiosity among cyber criminals to break into the meaning of the cryp-tic data, though it is not that easier.

Steganography is yet another powerful tool that achieves the goal of transferring sensitive data secretly across the web. Steganography, rather than transforming the data into another form, hides the sensitive data inother kinds of data, in such a manner that no one can ever suspect that there are some data bytes hidden in that data. Thus, steganography is the art and science of writing hidden messages in such a way that no one, (apart from the sender and intended recipient), suspects the existence of the message, a form of security through obscurity.

The cover-image with the secret data embedded is called the "Stego-Image". The Stego-Image should resemble the cover image under casual inspection and analysis. In addition, for higher security requirements. We can encrypt the message data before embedding them in the cover-image to provide further protection. For this the encoder usually employs a stego-key which ensures that only recipients who know the corresponding decoding key will be able to extract the message from a stegoimage.

This is a simplest steganographic technique that embeds the bits of secret message directly into the least significant bit (LSB) plane of the cover image. In a gray level image, every pixel consists of 8 bits. The basic concept of LSB substitution is to embed the confidential data at the rightmost bits (bits with the smallest weighting) so embedding procedure does not affect the original pixel value greatly [5].

Hence, a simple permutation of the extracted mi gives us the original confidential data [6]. This method is easy and straightforward but this has low ability to bear some signal processing or noises. And secret data can be easily stolen by extracting whole LSB plane. Robustness of steganography can be improved if properties of the cover image could be exploited. For example it is generally preferable to hide message in noisy regions rather than smoother regions as degradation in smoother regions is more noticeable to human HVS (Human Visual System). Taking these aspects into consideration working in frequency domain becomes more attractive. Here, sender transforms the cover image into frequency domain coefficients before embedding secret messages in it [7].

II. 2RELATED WORKS

*Anjali a.Shejul [2]*Steganography Method used in this paper is based on biometrics. And the biometric feature used to implement steganography is skin tone region of images. Here secret data is embedded within skin region of image that will provide an excellent secure location for data hiding. For this skin tone detection is performed using HSV (Hue, Saturation and Value) color space. Additionally secret data embedding is performed using frequency domain approach - DWT (Discrete Wavelet Transform), DWT outperforms than DCT (Discrete Cosine Transform). Secret data is hidden in one of the high frequency sub-band of DWT by tracing skin pixels in that sub-band. Different steps of data hiding are applied by cropping an image interactively.

*Rl.O.Safy [8]*In this paper, we try to optimize these two main requirements by proposing a novel technique for hiding data in digital images by combining the use of adaptive hiding capacity function that hides secret data in the integer wavelet coefficients of the cover image with the optimum pixel adjustment (OPA) algorithm. The coefficients used are selected according to a pseudorandom function generator to increase the security of the hidden data. The OPA algorithm is applied after embedding secret message to minimize the embedding error. The proposed system showed high hiding rates with reasonable imperceptibility compared to other steganographic systems.

*V.Lokeshwara Reddy [9]*In this paper,SteganPEG is an image steganography application, that operates on JPEG images. It combines the advantages of both cryptography and steganography in a single application. In order to save more data into an image,SteganPEG performs data compression / decompression before actually performing the steganography. In this method used algorithm Rotatocrypt and partial Decoding.

III. 3PROPOSED WORK

An overview of the proposed work contains five phases:

1)Skin Tone Detection
2)Hiding Secret Data Using IWT
3)Header Information
4)Merging with cover Image
5)Data Extraction Process.

3.1 Skin Color Tone Detection

The Cover image is converted from RGB (Red, Green, Blue) color space into YCbCr. A skin detector typically transforms a given pixel into an appropriate color space and then uses a skin classifier to label the pixel whether it is a skin or a non-skin pixel. A skin classifier defines a decision boundary of the skin color class in the color space.

3.2 Hiding Secret Data Using IWT

Using the IWT the selected skin area matrix B-plane is converted into the sub bands and the secret data is embedded in the frequency sub-bands like HH(Horizontally Vertically HighPass), HL(Horizontally highPass& Vertically low Pass), LH(Horizontally Low Pass & Vertically high Pass),LL(Horizontally &Vertically LowPass) where the Human Visual System is less sensitive to these sub-bands using LSB algorithm. After hiding the data IIWT is performed. Hence hidden cropped region is obtained

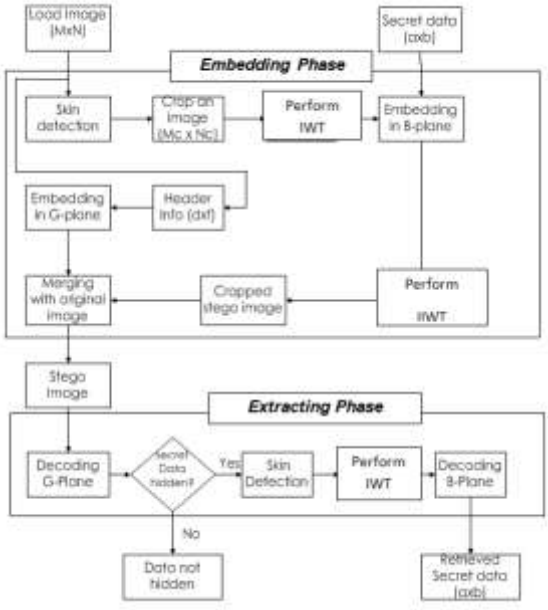

Fig.1 – System Architecture

3.3 Header Information

This is especially for the effective work of decoder while extracting the data. This information is hidden in the G-plane of the Cover Image. For this we used 12byte information like algorithm used(default character MTS), Secret Data type like text or image, Size of the skin/cropped region and the Size of the Image. So, the stego Image itself carries its own information hence no extra key is required.

First three bytes for our Algorithm Use, 3 character which used to make unique set of algorithm.

1. Next one byte for Secret data types(text or Image)
2. Next four bytes for Size of secret data(axb)
3. Next four bytes for cropped size information (McxNc)

3.4 Merging with Cover Image

Data hidden cropped region and the Header information hidden region is combined with the cover image to get the Final Stego Image.

3.5 Data Extraction Process

Our Decoding algorithm has a unique key login to avoid unauthorized access, will decode the G-plane of the Stego Image and look for the algorithm Character(character MTS), if it matches it will further do the extraction process, if not it return with the pop-up message "no data hidden". By extracting the other header information like data type, cropped size and cropped region the encoded data will be retrieved.

IV. 4 Simulation Results

We demonstrated the results here. We implemented this proposed method usingMatlab 7.1

We used Peak noise to signal ration(PSNR) to evaluate the quality of stego Image after embedding the secret data which can be a text or Image . We have taken 156 x 120 gray scale DD logo as a secret data in this simulation. We used the following equation to calculate the PSNR.

PSNR = 10log10 (2552/MSE)

$$MSE = 1/(MxN)\sum_{i=1}^{M} \quad \sum_{i=j}^{N} (Xjj-Yij)2$$

We achieved PSNR : 58.0279 for the text

And achieved PSNR : 57.693 for the grey model

Fig.2 – Cover Image

Fig.3 – Secret Data used to hide in the cover image

Fig.3 – Skin detection

Fig.4 – Stego Image

Fig.5- Retrieved Grey Model

V. 5CONCLUSIONS

In this paper, Digital Steganography is a fascinating scientific area which falls under the umbrella of security systems. Proposed framework is based on steganography that uses Biometric feature i.e. skin tone region. Skin tone detection plays a very important role in Biometrics and can be considered as secure location

for data hiding. Using Biometrics resulting stego image is more tolerant to attacks and more robust than existing methods. By embedding data in only certain region and not in whole image security is enhanced. According to propose approach provides high image quality. Performing Hiding header information and extract the lossless secret data from stego image.

REFERENCES

[1] Simon ClippingdaleMahitoFujii "Skin Region Extraction and Person- independent" NHK (Japan Broadcasting Corporation), Science & Technology Research Labs IEEE 2011.

[2] Anjali A. Shejul Prof. U.L Kulkarni "A DWT based Approach for Steganography Using Biometrics" International Conference on Data Storages &Data engg,IEEE 2010.

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

[4] Provos, N. and Honeyman, P.: Hide and Seek: An Introduction to Steganography. IEEE Security and Privacy, 01 (3): 32-44, May-June 2003.

[5] Moulin, P. and Koetter, R.: Data-hiding codes. Proceedings of the IEEE, 93 (12): 2083- 2126, Dec. 2005.

[6] Sadkhan, S. B.: Cryptography: Current Status and Future Trends. IEEE International Conference on Information & Communication Technologies: From Theory to Applications. Damascus. Syria: April 19 -23, 2004.

[7] R. El SafyH.H.Zayed "An Adaptive Steganographic Technique Based onInteger Wavelet Transform" IEEE 2009.

[8] Hussein A. Aly,"Data Hiding in Motion Vectors ofCompressed VideoBased on Their Associated Prediction Error"IEEE Transaction on Information Security"2011.

[9] Liu Shi, Fengyong Li, Yuejun Chen, Xinpeng Zhang "Steganographic Embedding in JPEG Images with visual criterion"IEEE 2011.

[10] A. I. Trivedi, Member, IEEE "Prominent Boundaries and Foreground Detection Based Technique for Human Face Extraction" Third national conference on graphics.2011

[11] Simmons, G. J.: The Prisoners' Problem and the Subliminal Channel. Proceedings of CRYPTO83- Advances in Cryptology, August 22-24. 1984. pp. 51.67.

[12] Kurak, C. and McHugh, J.: A cautionary note on image downgrading. Proceedings of the Eighth Annual Computer Security Applications Conference.30 Nov-4 Dec 1992 pp. 153-159.

[13] Thomas, T. L.: Al Qaeda and the Internet: The Danger of "Cyberplanning". Parameters, US Army War College Quarterly- Spring 2003.

[14] Lai and L. Chang, "Adaptive Data Hiding for Images Based on Harr Discrete Wavelet transform," Lecture Notes in Computer Science, Volume 4319/2006.

[15] V.LokeshwaraReddy,Dr.A.Subramaniyan, " SteganPEG",International journals of computer Graphics,Vol.No.1,May,2011

[16] M. Ramani, Dr. E. V. Prasad and Dr. S. Varadarajan,"Steganography Using BPCS the Integer Wavelet Transformed Image", UCSNS International Journal of Computer Science and Network Security, VOL. 7 No.7, July 2007.

[17] N. Wu and M. Hwang."Data Hiding: Current Status and Key Issues," International Journal of Network Security, Vol.4, No.1, pp. 1-9, Jan.2007.

[18] W. Chen, "A Comparative Study of Information Hiding Schernes Using Amplitude, frequency and Phase Embedding," PhD Thesis, National Cheng Kung University, Tainan, Taiwan, May 2003.

[19] Changa, C. Changa, P. S. Huangb, and T. Tua, "A Novel Image Steganographic Method Using Tri-way Pixel-Value Differencing,"Journal of Multimedia, Vol. 3, No.2, June 2008.