.

A Secure Video Steganographic Method Using Enhanced Ant Colony Optimization (EACO) Algorithm

S.Anitha[1], K.Rajalakshmi[2] ,Dr.K.Mahesh[3]

[1] M.Phil Research Scholar, Department of Computer Applications, Alagappa University, Karaikudi.
[2] PhD Research Scholar, Department of Computer Applications, Alagappa University, Karaikudi.
[3] Professor, Department of Computer Applications, Alagappa University, Karaikudi.

ABSTRACT

In the development of the network field, the necessity for hiding the information is more important for protecting the information from the third party in an open network. In order to overcome this video Steganography technique is used. It is the profession of hiding the information which helps to conceal the sensitive data than other medium. In Steganography different cover objects are used for video, it can be separate into images and audio and accommodate massive amount of secret information. In this proposed work, introduce the new method for hiding the secret data into a video file using video Steganography technique. In this technique, IWT and Enhanced Ant Colony Optimization Algorithm to get a Stego video. And obtain extraction procedure is similar to embedding procedure vice versa. So that this proposed method is convenient and extracting data easily from stego video.

Keyword: *- Integer Wavelet Transform(IWT),Enhanced Ant Colony Optimization Algorithm(EACO) , Steganography.*

1. INTRODUCTION

The Steganography is of Greek word which is hiding secret information within cover media such as image, text, audio or video so that imposters can't detect what data is hidden in it. In the cryptography, render message unintelligible but in Steganography cover the existence of the message. Video steganography means video file is use as a cover medium for hiding secret information. Among all the steganography, video steganography beaten some restrictions because it has capability to embed massive amount of secret data inside the carrier and also it is difficult to detect by third person. This steganography use H.264, Mp4, MPEG, AVI, etc., file formats.

In practice, Video steganography technique can be classified into two types which are temporal and spatial domain. In temporal domain, transforming cover data by using DCT, DWT etc., and on this transformed coefficients, secret information can be embedded. In spatial domain, data bits are embedded in LSBs positions. If SNR and PSNR value is large means small difference between original image and stego image [1]. The data is hidden in sub bands which address the robustness and good visual quality. It is mapping an integer to integer data. With usage of Integer wavelet transform for floating point values of the wavelet filters can be avoided. Use of Lifting schemes, Integer wavelet transform is perform in which transforms from integer pixel values of an image into the integer wavelet coefficients[2]. One of the Wavelet transform a families known as "Integer Wavelet Transform" has been implemented work. It converts an image from spatial domain to the frequency domain by applying horizontal and vertical operations, respectively. The IWT is used in the proposed Steganography technique to convert the cover image into four sub-bands are approximation, vertical, horizontal, diagonal coefficients, which represent low-low, high-low, low-high and high-high frequencies respectively. Approximation coefficients will not be used to conceal secret information since human eyes are very sensitive to small changes low-low frequency. However, the rest of the coefficients contain high frequencies, thus secret data will be corrected and concealed within these bands by the use of both least significant bit and pseudo random number techniques. Once the embedding process is completed, the inverse IWT is applied in order to form the stego-image.

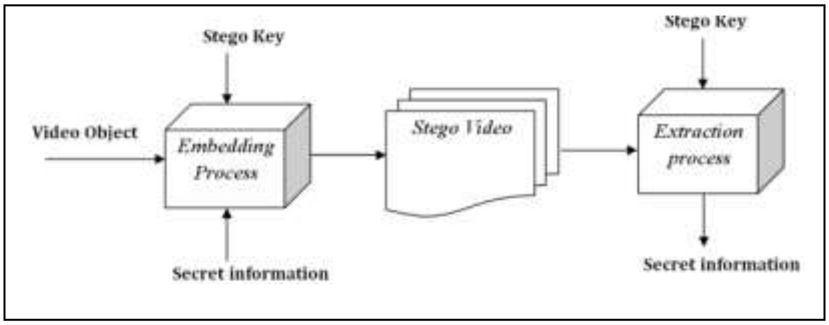

Fig.1 Basic structure of video steganography

2. RELATED WORK

Varying methods are proved that secret data is hidden without change the quality of visuals, structure of video file.

Mritha Ramalingam et al [5] have proposed Haar Integer Wavelet Transforms based steganography for transfer data with highest level of security. In embedding process, cover video is partitioned into RGB frames and apply Haar DWT on this frames to get wavelet coefficients. Then, read the secret message and convert into bits. Embed this binary formed message into LSBs of IWT coefficients of RGB frames. To extract the data from these coefficients, inverse process of embedding data procedure is used. In this work, AVI Video file is used for hide and extract the data. This algorithm has less complexity.

Avinash K. Gulve et al [6] use Integer Wavelet Transform with PVD technique to improve security of secret data which is cover by image. 2D Haar integer wavelet transform is employed to transform the image into four subbands. Then PVD technique is used to embed the secret data into wavelet coefficients of four subbands. This proposed method enhancing the security by calculating the difference between the two IWT coefficients in the pair and modify these difference values. This modified value is used to hide the secret data. This method gives PSNR values are near 39.5 which demonstrates that the stego images are good in quality and resist to RS attack.

Seyyed Amin Seyyedi et al [7] use integer Haar wavelet transform to achieve high both in data capacity and security of secret data. In this method, the cover image is split into 8× 8 blocks and these blocks are transformed in to two subsets by using two levels integer Haar wavelet transform. Then, secret data is embedded into suitable subset. To improve higher secure, one level integer Haar wavelet transform is applied to secret data before embedding.

Tanmay Bhattacharya et al [8] use DWT and spread spectrum method for embedding secret image into a cover image. In this proposed algorithm, the cover image is split into 4 sub bands by using DWT. On each band, the secret image is embedded with the help of pseudo random sequence and session key. This algorithm can be applicable to color image and also audio steganography.

Lisa M. Marvel et al [9] have introduced new method for data is hidden in the digital image by inherent noise. A binary signal is embedded within samples of a low-power white Gaussian noise sequence consisting of real numbers. To obtain the stego image, this signal is combined with the cover image. The Power of the embedded signal is less than cover image that so it is difficult to detect by an observer.

3. PROPOSED WORK

The main idea behind the proposed work is hide sensitive data inside input video sequences of frames using IWT and EACO which is named as Enhanced Ant Colony Optimization algorithm. In this method, text file and video clip as a cover video which is multimedia elements are read as input, input text is converted into ASCII values and other input video is extracted into red, green and blue frames and those frames are divided into 8x8 blocks. Then IWT technique is applied on these blocks to obtain wavelet coefficients. On these transformed coefficients, EACO Algorithm is utilized to find the best pixel values and embed the information at those optimal points. Afterwards embedded process has been completed; inverse IWT method is employed to get the stego video at the sender side. Authorized recipient can extract the secret data from stego video by performing the embedding process reversely. The entire process of proposed method is illustrated as in figure 2.

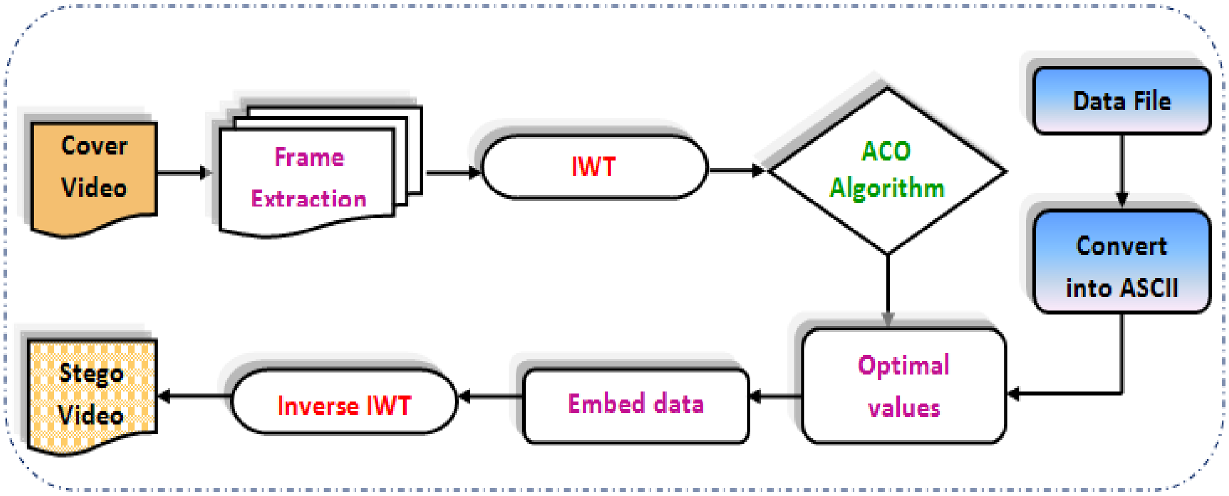

Figure 2. Block diagram of proposed method

3.1 Algorithm for Embedding Procedure

Step 1: Input: cover video and secret data.
Step 2: Cover video is partitioned into three frames (R, G, and B)
Step 3: Divide these frames into 8x8 blocks
Step 4: Each frame are transformed by using one level IWT.
Step 5: Input video is break into R, G, B color components and then IWT is applied on each color band separately.
Step 6: Another input secret data is converted in to ASCII values.
Step 7: Ant Colony Optimization (ACO) algorithm is used to find the optimal points where the data to be hide.
Step 8: Secret data could be hide at that optimal points.
Step 9: After that, Inverse IWT is applied to obtain stego video.

3.2 Algorithm for Extracting Procedure

The following steps are used to extracting the sensitive data from stego video.

Step 1: Input: stego video
Step 2: Stego video is partitioned into three frames (R, G, and B)
Step 3: Divide these frames into 8x8 blocks
Step 4: Each frame are transformed by using one level IWT
Step 5: Use EACO Algorithm on RGB frame.
Step 6: Extracting Hidden data bits.
Step 7: Data is extract by applying reverse procedure of embedding process.
Step 8: Apply inverse IWT to get video object
Step 9: Output: Cover video and Original Data.

4. CONCLUSION

In this thesis, the proposed Video Steganographic methodology is a Information Hiding technique for provides high Information Hiding strength and robustness against the attacks such as compression and tampering. It provides high capacity and imperceptible stego-video for human vision of the hidden secret information. The performance of the proposed method is studied and experimental results shows that this scheme can be applied on videos with no noticeable degradation in its quality. This method extracts the data as identically, *without any loss in quality and size of the original video. This algorithm is to achieve high capacity, security, low time consuming and certain robustness.* The Conclusion of this thesis presents video Steganography using enhanced ant colony algorithm and IWT techniques as an efficient and robust tool for protection.

6. REFERENCES

[1] F.A.P. Petitcolas, R.J. Anderson and M.G. Kuhn: Information Hiding-A Survey, Proc. IEEE, 1999

[2] N. Provos and P. Honeyman, Hide and Seek: An introduction to steganography, IEEE Security and Privacy, 1(3), 2003, 32-44.

[3] K.G.Paterson, Cryptography from Painings: A snapshot of Current Research, Information Security Technical Report, 7(3), September 2002, 41-54.

[4] M. Bachrach, F.Y. Shih, Image Steganography and steganalysis, Wiley Interdisciplinar Reviews Computational Statistics, 3(3), 2011, 251-259.

[5] M.M. Sadek, A.S. Khalifa, G. M. Mostafa, Video Steganography: A Comprehensive Review, Multimedia Tools Applications, 74, March 2014, 7063-7094.

[6] [6]. M. Jafar, K. Morteza, An adaptive scheme for compressed video steganography using temporal and spatial features of the video signal, International Journal of Imaging System and Technology,19, December 2009,306-315.

[7] E. Satir, H. Isik, A Compression-based text steganography method, Journal of System and Software, 85(10), Oct 2012, 2385-2394.

[8] A.Cheddad, J.Condell, K.Curran, P. Mckevitt, Digital image steganography: Survey and analysis of current methods, Signal Processing, 90(3), March 2010, 727-752.

[9] K.Rajalakshmi, Dr.K.Mahesh, “Video Steganography Based on Embedding the Video Using PCF Technique “Proceedings of IEEE Conference (ICICES 2017) 978-1-5090-6135-8/17 ©2017 IEEE.

[10] K.Rajalakshmi, Dr.K.Mahesh,”ZLBM:Zero Level Binary Mapping Technique for Video Security” MultimediaTools And ApplicationsSpringer, DOI 10.1007/s11042-017-4942-0, ISSN:1380-7501,Online:13 July 2017.

[11] K. Rajalakshmi, K. Mahesh, "A Review on Video Compression and Embedding Techniques", *International Journal of Computer Applications (0975–8887)*, vol. 141, no. 12, 2016.

[12] D.Mohanapriya,Dr.K.Mahesh "A novel foreground region analysis using NCP-DBP teture pattern for robust visual tracking" , Springer Multimedia Tools and Appications –An International Journal, Volume: 76 Issue No: 24, December 2017. pp:25731-25748.

[13] [D.Mohanapriya and Dr.K.Mahesh, "A video target tracking using shadow suppression and feature extraction," IEEE Xplore Digital Library.

[14] D.Mohanapriya, Dr.K.Mahesh, "Video Tracking System by suppressing shadow and Feature Extraction- A Review", International Journal of Computer Engineering and Applications(IJCEA), Vol.10, No 6 ,June , 2016

[15] K. Rajalakshmi, K. Mahesh, "Video Embedding with Compression Based on Patchwise Code Formation", *Australian Journal of Basic and Applied Sciences*, vol. 10, no. 13, pp. 2309-8414, August 2016, ISSN 1991-8178.