International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 09, September 2015
Available at http://internationaljournalofresearch.org

A motion vector based efficient parity LSB technique and Huffman coding for efficient video Steganography

Monika
M.Tech Scholar Computer Science and Engineering Dept of CSA Ch. Devi Lal University, Sirsa(Haryana)
deswal1810@yahoo.com
Dr. Kapil Kaswan
Asst. Professor Dept of CSA Ch. Devi Lal University, Sirsa(Haryana)
kapilkaswan@gmail.com

Abstract
Steganography is the art of covert communication, referring to the process of embedding secret messages into cover objects, the embedded data is invisible or inaudible to a human observer. In recent years, video steganography techniques are closely connected with existing video compressing standards. Information Attacks are showing the weaknesses of Information security due to the rapid growth of the globalisation. The main aim of these attacks is to retrieve the information by illegal that shows the faults in the security services. In this research, we introduce a novel secure steganography approach for defending against these information attacks. In this approach, instead of original message an encrypted message by Huffman Coding Algorithm is hidden into an Image (Stego Image) which is represent using motion vectors and by using a new approach named Parity Least significant bit technique which is a combination of LSB technique and parity coding which provides more security than conventional approaches. The computational complexity will comparatively low with other methods since our feature vector space is limited interference is not objectionable.

Keywords: steganography; motion vector; LSB technique; motion vectors, parity coding; Video data.

Introduction:
The word steganography is derived from the Greek words stages meaning cover and graphic meaning writing [1] defining it as covered writing. Steganography is the art and science of secret communication. It is the practice of encoding/embedding secret information in a manner such that the existence of the information is invisible. The original files can be referred to as cover text, cover image, or cover audio. After inserting the secret message it is referred to as stego-medium. A stego-key is used for hiding/encoding process to restrict detection or extraction of the embedded data [2].

Video files are usually consists of images and audios, so many of the existing techniques on images and audio can be applied to video files too. The great advantages of video are the large amount of data that can be hidden inside and the fact that it is a moving stream of images and sounds. Therefore, any small but perceptible distortions might go by unobserved by person because of the continuous flow of data [3].

Exact necessities whether imposed by itself or planned by an external association or client, are all designed to address the three fundamental

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 09, September 2015
Available at http://internationaljournalofresearch.org

objectives of computer security: confidentiality, integrity and authentication [4].

Related Work:

REDUCES THE EMBEDDING NOICE

J. Mielikainenet al. (2006) have suggested that the embedding is performed using a pair of pixelsas a unit, where the LSB of the first pixel carries one bit of information, and a function of the two pixel values carries another bit of information. It has been shown that embedding in this fashion reduces the embedding noise introduced in the cover signal [5].

ADAPTIVE K-LSB SUBSTITUTION

C.-H. Yang et al. (2008) proposed a method which hides large and adaptive k-LSB substitution at edge area of image and pixel value differencing (PVD) for smooth region of image. So in this way the technique provide both larger capacity and high visual quality according to experimental results. This method is complex due to adaptive k generation for substitution of LSB [6].

INDEX

Balaji et al. (2011)proposed a method to creates an index for the secret information and the index is placed in a frame of the video itself. With the help of this index, the frames containing the secret information are located[7].

ENCRYPTED USING XOR

Yadavet al. (2013) proposed a method in which each frame of secret video will be broken into individual components then converted into 8-bit binary values, and encrypted using XOR with secret key and encrypted frames will be hidden in the least significant bit of each frames using sequential encoding of Cover video[8].

STEGANALYSIS

Han-Tian Wu (2014)proposes an improved steganalysis algorithm to detect the secret message hidden in the compressed video. It shows that significant improvement in detection accuracy can be made by using the joint distribution of MV differences instead of the statistics calculated from two neighboring MVs as features [9].

Research Objective:

The implementation of the proposed work will be achieved with following objectives:

i. To calculate motion vectors of selected video signal based on H.264 compression.

ii. To apply Efficient Huffman coding efficiently on the selected secrete text message.

iii. To embed secrete message into the motion vectors using parity based LSB technique.

iv. Use of most suitable parameters such as Peak Signal-to-Noise Ratio (PSNR), Mean Square Error(MSE) and embedding capacity in performance evaluation of present research work as compared to existing noteworthy contribution.

Methodology:

The implementation of the proposed work will be achieved by using following methods:

H.264 ADVANCED VIDEO CODING

H.264 is an open, licensed standard that supports the most efficient video compression techniques available today. A digital video signal consists of periodic sequences of images called frame. A block based coding approach divides the frame into macro blocks. Each macro blocks consist 16 x 16 pixels. Each pixel consists of three color

component called YUV. Here Y represents the luminance component and U &V represents the chrominance component. In 4:2:0 format, each MB consists of 16 x 16 = 256 Y components and 2, 8 x 8 =64 U and V components.

HUFFMAN CODING FOR MESSAGE ENCRYPTION

Huffman coding is an entropy encoding algorithm used for lossless data compression. Huffman coding is such a widespread method for creating prefix codes that the term "Huffman code" is widely used as a synonym for "prefix code" even when such a code is not produced by Huffman's algorithm.

MOTION VECTOR

In video editing motion vectors are used to compress video by storing the changes to an image from one frame to the next.

LSB AND PARITY CODING

In Least Significant Bit (LSB) insertion method the LSB of every pixel is replaced by every message bit. Parity coding is used to identify the odd or even parity of bits.

Conclusion:

In order to increase the security of video steganography we can use an encrypted message by Huffman Coding Algorithm is hidden into an Image (Stego Image) which is represent using motion vectors and by using a new approach named Parity Least significant bit technique which is a combination of LSB technique and parity coding which provides more security than conventional approaches.

References:

[1] R.Anderson and F. Petitcolas, "On the limits of steganography" IEEE Journal of Selected Areas in Communications, Vol. 16, No. 4, May 1998.

[2] Niels Provos, Peter Honeyman, "Hide and Seek: An Introduction to Steganography," IEEE computer society, 2003.

[3] Yadav, P., “A secure video steganography with encryption based on LSB technique”, IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), 2013.

[4] NedeljkoCvejic, TapioSeppben: Increasing the capacity of LSB-based video steganography, IEEE 2002.

[5] J. Mielikainen, “LSB Matching Revisited”, IEEE Signal Processing Letters, vol. 13, no. 5, May 2006, pp. 285 - 287.

[6] C.-H. Yang, C.-Y. Weng, S.-J. Wang, Member, IEEE and H.-M. Sun, “Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems”, IEEE Transactions on Information Forensics and Security, vol. 3, no. (2008) September 3, pp. 488-497.

[7] Balaji, R., “Secure data transmission using video Steganography”, IEEE International Conference on Electro/Information Technology (EIT), 2011.

[8] Yadav, P, “A secure video steganography with encryption based on LSB technique”, IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), 2013.

[9] Hao-Tian Wu, “Improved steganalysis algorithm against motion vector based video steganography”, IEEE International Conference on Image Processing (ICIP), 2014.