Volume 5, Issue 7, July 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Hybridization of Motion Detection Technique in Video Steganography

Parwinder Singh, Navpreet Kaur
Department of Computer Science, Punjabi University,
Patiala, Punjab, India

Abstract- Steganography is an art of hiding information in plain sight. It relies on hiding a message in unsuspected data during a secret communication between two acknowledged clients. This paper proposes a hybrid motion detection and least significant bit technique to hide the data in moving objects which enhances the security and makes the algorithm more robust. The PSNR value is calculated on several videos and the results show there is no perceptual difference between the cover video and the stego video.

Keywords - decryption, encryption, LSB, motion vector, Steganography.

I. INTRODUCTION

Steganography is derived from two Greek words, *steganos*, which means covered or secret and, *graphia*, which means writing. In simple terms, steganography is an art of hiding information in plain form [3]. It relies on hiding a message in unsuspected data during a secret communication between two acknowledged clients. This is the most common technique used to hide information in digital images.

Technological advances in last two decades have given rise to multimedia steganography. Audio, video or image files provide an ideal gateway for hidden communication and are good medium of hiding data. Secret information can be concealed by making modifications to bits that do not cause a noticeable difference to image or audio file when it is viewed or played back [15]. Steganography is performed on video file and message is concealed in an encrypted format. The most common technique is least significant Bit steganography (LSB) [11].Motion detection technique is one of the most important tasks in the video processing systems. It helps to extract top secret information from scenes which is using automatic video surveillance like object tracking etc.

A lot of work has been done in this field and many techniques introduced but still these all technique has some drawbacks and facing challenging like sudden change in scene, quality of video. Motion from continuous video can be detected through optical flow and background subtraction [12]. In optical flow, motion in video is evaluated by using point based analysis. It is vector based method. In background subtraction, to find motion in video estimated background is compared with current frames. It is a comparison based method. Background estimation is technique in which from initial video frames background model is estimated on basis of this model it performs the detection of moving objects when a new frames arrives model is compared with the frames than threshold to be set to segment the foreground objects. Most of the background modeling techniques expects background will be available to initialize their model but in real life background may not be always available. For example if visual surveillance system is installed at traffic lights which is most of the time crowded with people and vehicles with goal of counting vehicles or to detect any material which may be considered as threat than on must initialize their model with background this is called Bootstrapping object which are detected in motion it will lead to ghosts which are the object that are detected in motion.

II. RELATED WORK

Various video steganography and motion detection techniques have been proposed. A few of them have been discussed below.

The most commonly used technique is temporal differencing [1]. It compares the current frames with the previous frames then the current image is threshold to segment out foreground object. This technique has some drawbacks if object stays in still mode than a frames period i.e. (1/fps) and if objects have uniformly distributed intensity values then it fails. One more similar approach in which current frames is compared with first frame it also fails if any structural changes occur.The authors of [2] developed a technique for video steganography through LSB hybrid approach in which 1LSB, 2LSB, 3LSB substitutions and AES (advanced encryption standard) algorithm is applied. AES is one of the most secure algorithms and secures classified information up to the top secret level. The proposed method is used for replacing 1, 2 or 3 LSB of each pixel in video frame and applies AES. The PSNR was observed to be greater for 1 bit LSB substitution as compared to 3 bit LSB so that with the increase in the number of bits the security level also increases.In [3] author has used computer forensics and steganalysis. In this paper, video is used as cover media to hide the secret message and computer forensics as a tool for authentication. For hiding information in image 4LSB is used as it can hide more data than 1LSB, 2LSB, 3LSB. It is the best suited algorithm in which is data can be hidden more than 50% and any change in data in the LSB does not change the value of data significantly which enhances the security, hence it is very difficult to find in which part of video data is hidden. This paper focuses on video steganography, cryptography and the use of computer forensics to investigate and improve the security.In [4] author proposed a technique to hide data inside moving object by using motion vector. In order to enhance the security of the data, AES algorithm is used for data encryption and then hidden. Moving objects hide the data in horizontal and vertical components. To evaluate the quality of the video after hiding the data, PSNR is calculated. It is calculated to show that the frame is transmitted without any loss or distortion. As a result, this technique is found to be a better solution and enhances the security of the data being transmitted.Codebook algorithm [5] this is a specific background subtraction algorithm in which from long training sequences without making parametric assumptions a codebook is constructed. In this, each pixel is clustered in form of code words which are based on a brightness bound and color distortion metric. In this non-parametric model based on kernel density estimation (KDE) [6] to mode the background. In the proposed method, the advantage is that it can handle situation where background of the scene is not completely static and cluttered.Self-organizing background subtraction (SOBS) algorithm [7] in this method by learning motion pattern in self-organizing method neural network structure for background model is used. This method is more secure and robust to moving background, cast shadows, camouflage and gradual illumination. One another method spatial coherence into the background update procedure proposed in [8] which lead to spatially coherent self-organizing background subtraction (SC-SOBS) algorithm. It requires 75-200 frames for initialization of model on downside of SOBS algorithm.SampleCONsensus (SACON) technique proposed by [9] this method is used for detecting foreground objects in both static and dynamic scene. from the last observed background values a pixel based model is constructed and depending upon matching of model value to pixel value a new pixel is classified as the background or foreground .to handle illumination two update mechanism are proposed to handle entire objects first is on pixel level and second on blob level. According to first in first out update policy the value of pixels models arereplaced.A robust spatial-temporal -kernel density estimation method (ST-KDE) [10] has been described in which dynamic background, moving shadows and camera jitter can be handled. It has ability to detect temporally stopped object such as vehicles standing for toll tax.

III. PROPOSED MODEL

In this paper a hybrid approach is designed with the motion detection technique and least significant bit. Motion detection is used to extract the moving object from a video sequence. Least significant bit is used to place the object by using these hybrid approach security of data and robustness increases.

The purposed model consists of two steps:

a. Encryption b. Decryption

a. Encryption

In this phase, moving and non-moving objects are analyzed by applying motion detection technique. The motion detection technique is applied to select the moving objects. In parallel to the above step, the input text is converted into ASCII code and further converted into binary code. Then, moving and non-moving objects are analyzed and hide the data in moving objects by embedding the data in video frame using least significant bit. The encrypted video sequence is thus generated as shown in Figure 1.

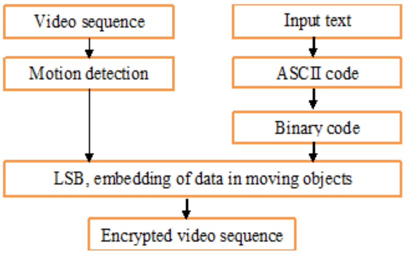

Figure 1: Encryption flowchart

b. Decryption

In Decryption phase, encrypted video sequence which obtained from the encryption phase motion detection technique is applied to select moving objects. Further the data is extracted from moving objects using least significant bit. Then, extracted data is converted into ASCII code further it convert from ASCII code into plain text.

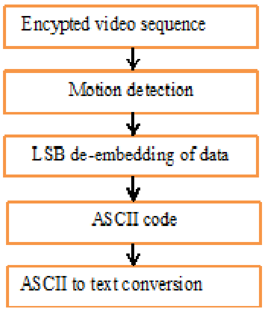

Fig.2 Decryption flowchart

IV. EXPERIMENTS AND RESULTS

The proposed methodology was implemented with image processing toolbox present in MATLAB® 2010. The tests are performed on ten video files- '.avi' as the cover video and 'exp.text' as the secret message file. The quality of cover video frame and the stego video frame has been evaluated using peak signal to noise ratio (PSNRPeak signal noise ratio (PSNR)

Visual quality is measured by PSNR. PSNR stands for Peak-to-signal noise ratio. It is used to determine how much similar the cover video frame and corresponding stego video frame is. It works between two images. PSNR is very popular in image processing. The result is calculated in decibels (db).

The PSNR is defined as:

PSNR =10.LOG$_{10}$(R^2/MSE)

Where R is the maximum possible value of luminance for an 8- bit image value of R will be 255.

Table 1. Result of quality evaluation of cover video frames and stego video frames

Cover video	Stego video	PSNR
1.mpg	1.avi	54.02
2.mpg	2.avi	57.88
3.mpg	3.avi	57.07
4.mpg	4.avi	59.35
5.mpg	5.avi	56.56
6.mpg	6.avi	60.66
7.mpg	7.avi	59.40
8.mpg	8.avi	57.81
9.mpg	9.avi	58.54
10.mpg	10.avi	62.90

Considering the size of message which is embedded in the video, the calculated performance measure i.e. PSNR, gives satisfactory results. The original video and the video with embedded message cannot be distinguished in this range of PSNR values. So, considering the PSNR ratio as acceptable, the proposed method can be used for practical implementation.

V. CONCLUSION

In this paper, the proposed technique hides data using the motion vector technique. In the previous works, still images are used to hide the data which causes the issue of data capacity and security as discussed in related work. The motion detection technique is a new and more efficient technique as compared to the existing techniques. By embedding the data in moving objects the robustness of the algorithm is increased. The PSNR value is calculated to show that results are acceptable and data is transmitted completely. Hence, the technique of data hiding using motion vector is found to be better so as to make the system more robust and secure.

REFERENCES

[1] R. Jain and H.H Nagel, "On the analysis of accumulative difference pictures from image sequences of real world scenes," IEEE Trans. Pattern analysis and Machine Intelligence, vol. PAMI-1, pp:206-214, April 1979.

[2] H. Gupta, “Video Steganography through LSB Based Hybrid Approach,” International Journal of Computer Science Network Security, vol. 14, no. 3, pp. 99–106, 2014.

[3] S. K. Moon, “Analysis of Secured Video Steganography Using Computer Forensics Technique for Enhance Data Security” proceeding of the 2013 IEEE second international conference on image information processing, pp. 660–665, 2013.

[4] R. Paul, A. K. Acharya, V. K. Yadav, and S. Batham,2014 “Hiding Large Amount of Data using a New Approach of Video Steganography,” in long island systems, application and technology conference, 2014, pp. 337–343,2014.

[5] K. Kim, T. Chalidabhongse, D. Harwood and L. Davis, "Background modeling and subtraction by codebook construction, "in IEEE International conference on image processing (ICIP), vol. 5, (Singapore), pp. 3061-3064, October 2004.

[6] A. Elgammal, d. Harwood, "Non-Parametric Model for background subtraction ", in proceeding of European Conference on computer vision, pp: 751-767, 2000.

[7] L. Maddalena and A. Petrosino, "A self –organizing approach to background subtraction for visual surveillance applications, "IEEE. Transaction on Image Processing, vol .17, No. 7, pp: 1168-1177, 2008.

[8] L. Maddalena and A.Petrosino, "A fuzzy spatial coherence based approach to background /foreground separation for moving object detection," Neutral Computing and applications, vol 19, pp: 179-186, March 2010.

[9] H. Wang and D. sutter, "Background subtraction based on a robust consensus method," in IEEE International Conference On Pattern Recognition (ICPR), (Washington, USA), pp: 223-226, August 2006.

[10] J.Y. Hao, C. Li, Z. Kim and Z. Xiong," spatio-temporal Traffic Scene Modelling for Object Motion Detection," IEEE Transaction on Intelligent Transportation Systems, vol .14, No. 1, pp: 295-302, March 2013.

[11] R. Paul, A. K. Acharya, V. K. Yadav, and S. Batham,2014 "Hiding Large Amount of Data using a New Approach of Video Steganography," in long island systems, application and technology conference, 2014, pp: 337–343,2014.

[12] Singh B., Singh D., Singh G. and Sharma N., "Motion detection for video surveillance" in IEEE International Conference on Signal propagation and Computer technology, pp: 578-584, 2014.

[13] H. Gupta, "Video Steganography through LSB Based Hybrid Approach," International Journal of Computer Science Network Security, vol. 14, no. 3, pp: 99–106, 2014.

[14] Arijit Sur, SistaVenkat, Madhav Krishna, NilkantaSahu, ShuvenduRana, "Detection of motion vector based video steganography, International journal of Multimedia tools and applications 23-nov-2013.

[15] R. J. Mstafa and K. M. Elleithy, "A highly secure video steganography using Hamming code (7, 4)," IEEE Long Island Systems, Applications and Technology Conference, 2014.

[16] Islam, M. R., Siddiqa, A., Uddin, M. P., Mandal, A. K., &Hossain, M. D, " An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography," *International Conference on Informatics, Electronics and Vision, ICIEV 2014*.

[17] Jue, W., Min-qing, Z., & Juan-li, S,"Video steganography using motion vector components." *IEEE 3rd International Conference on Communication Software and Networks*, pp: 500–503, 2011.

[18] "KasimTasdemir , FatihKurugollu , SakirSezer ," Video Steganalysis Of LSB Based Motion Vector Steganography," The Institute of Electronics, Communications and Information Technology Queen ' s University Belfast Belfast , United Kingdom, pp: 260–264,2013.

[19] Wang, K., Zhao, H., & Wang, H,"Videosteganalysis against motion vector-based steganography by adding or subtracting one motion vector value," *IEEE Transactions on Information Forensics and Security*, *9*(5), pp: 741–751, 2014.

[20] Yadav, P., Mishra, N., & Sharma, S," A Secure Video Steganography with Encryption Based on LSB Technique," 2013.

[21] Zhang, C. Su, Y. & Zhang, C,"A new video steganalysis algorithm against motion vector steganography," in *International Conference on Wireless Communications, Networking and Mobile Computing, WiCOM 2008*, (1), pp: 4–7,2008.

[22] Zhang, M, "Video Steganography Algorithm with Motion Search Cost Minimized", pp: 940–943, 2014.