IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

Significance of applying K-means Clustering Technique to Video Steganography

Shree Raksha[1], Shruthi R[2], Sushma Shekar K[3], Vismaya M[4], Vidya Raj C[5]

Student, Computer Science and Engineering, The National Institute of Engineering, Mysore, India [1-4]

Professor, Computer Science and Engineering, The National Institute of Engineering, Mysore, India [5]

Abstract: The rapid growth in digitalization and usage of public domain channels has greatly facilitated transfer of data. The rapid growth in technology facilitating transfer of data through internet has a lot of security threats as these public domains are highly vulnerable. Among the techniques used for concealing the confidential data, video steganography is eminent. This paper indicates the progress in the field of video steganography, its uses and techniques based on secret media, image and video. The paper also makes a performance comparison of known video steganography techniques and identifies K-means clustering as one of the most suitable techniques for video steganography, which is applied in solving most of the real time problems.

Keywords: K-means, Random Byte Hiding, LSB, MSE, PSNR, Steganalysis.

I. INTRODUCTION

The increased use of internet has resulted in accumulation of huge amount of data. It is believed that 90% of all the data in the world today has been created in the past few years. Most of these data is generated in the fields of IT industry, educational institutions, hospitals, banking system. The data exists in various forms such as audio, video, text, images, graphics and speech. Data can also be the information which is converted into digital media from different formats. Data between the resources is transmitted over communication channels like copper wires, optical fibers, wireless channels which may or may not be secure. Due to the increased use of wireless network transmission in recent days, there are large security threats like loss of message integrity, access by unauthorized users and lack of confidentiality when compared to that of early wired internet connection. The complexity of the types of attacks to wireless systems to steal data is at its peak. There is a need for some sort of security measures to prevent the intruders from exploiting the data shared between connected resources. To overcome these issues techniques such as cryptography to encrypt the confidential information before transmitting, steganography a modus operandi to implant secret information into various multimedia files to hide the existence of information, watermarking to embed digital signature to secret information are devised. The encrypted information is prone to several attacks and also its existence is visible naked eye, but hiding the information's existence is more secure as it’s imperceptible, making steganography a robust and secure technique. Based on the type of cover medium used, steganography is classified into text, image, audio and video steganography. Video steganography is widely used as videos are series of static images accompanied by audio and can embed large amount of information than the static images alone. The intricacy of dynamic structure of the video file makes it hard for hacker to recognize by naked eye that promises security against steganalysis.

II. RELATED WORKS

Among the various secret multimedia files that are used, image and video files are chosen for analyzing the best and robust technique that can be applied for it. The main reason behind choosing only images and videos is the similarity between them as image is an array of pixels; video is a series of images. To elicit the suitable among those techniques used for video and image secret files, the following papers have been referred.

According to K. Steffy Jenifer et.al, the Least Significant Bit(LSB) approach along with masking filtering is used to hide the secret image in video steganography[1]. The bits of the image are directly embedded into least significant bit plane of the cover-frame in deterministic sequence. The embedding capacity can be increased by using two or more least significant bits.

Prabira Kumar Sethy et.al, proposed a video steganography of image using K-means clustering and direct mapping[2]. In this method the message bits are clustered and grouped together using K-means clustering algorithm. Cover video and secret image are selected, their information is collected and K-means clustering algorithm is applied for image quantization. Clustered message is embedded inside the cover medium by using direct mapping resulting in stego video.

DOI 10.17148/IJARCCE.2018.7396

Rachna Patel and Mukesh Patel proposed a method for hiding information inside another video file using random byte hiding and LSB technique[3]. The selected cover video is split into frames; the secret information is split into byte stream. Random byte allocator is used to embed the secret information inside the cover video frame at random location to obtain the stego video.

Decryptor is used to extract hidden information from these frames which are then merged to obtain the required secret data. In LSB technique, the cover video is segmented into frames and secret video is split into R × C group size . Secret messages are encrypted into data bit and embedded into the LSB of the cover video, rule list is created and stego video is generated. To obtain back the secret video, the stego video is segmented into frames, small messages are decrypted from the frame for each column, row and LSB is extracted. Then all the data are merged to generate the secret video message.

Sheng Dun Hu, KinTak U presented a video steganography system based on non-uniform rectangular partition. This technique is used for uncompressed videos[4]. The frame length of the cover video should be greater than or equal to the frame length of the secret video. Each frame of secret video is partitioned into non-uniform rectangular part which is encoded. The secret video stream is hidden in the leftmost four least significant bits of each frame of the host video stream.

III. COMPARATIVE ANALYSIS

TABLE 1 COMPARISON OF DIFFERENT VIDEO STEGANOGRAPHY TECHNIQUES

TECHNIQUE	SECRET INFORMATION	FEATURES	LIMITATIONS
K-means clustering	Image	• Lossless technique • High robustness • Spatial domain	• Difficult to predict the number of clusters
Random byte hiding	Video	• Randomness provides better security • Less encryption and decryption time • Spatial domain	• Lossy technique • Low data hiding ratio
LSB	Image Video	• Simple implementation • Spatial domain • Hides in independent frame	• Lossy technique • Image fidelity degrades • Not robust against compression
Non Uniform Rectangular Partition	Video	• All PSNR value>28dB • No visual distortion in host video • Spatial domain	• Inaccurate retrieval of secret bits leads to poor PSNR of extracted frames

To compare the performance of the above techniques with images as secret media two parameters PSNR(Peak Signal to Noise Ratio) and MSE(Mean Squared Error) are considered. Two commonly used images in video steganography, Baboon.jpg and Lena.jpg as in fig 1(a) and fig 1(b) are considered. The tabulated values are referred from [5][6][7].

Fig. 1(a) Baboon

Fig. 1(b) Lena

DOI 10.17148/IJARCCE.2018.7396

TABLE 2 COMPARISON OF PSNR AND MSE VALUES

IMAGE	TECHNIQUES	PSNR(in dB)	MSE
Baboon	LSB	44.18	2.48
	K-means clustering	65.565	2.21
Lena	LSB	44.16	2.47
	K-means clustering	61.025	2.23
	Non-Uniform Rectangular Partition	36.34	3.36

The comparative study of video steganography techniques from TABLE 1 gives glimpse of suitable method when secret information is image or video. The K-means clustering technique is more suitable when secret medium is image which has high capacity, imperceptibility when compared to LSB and Non Uniform Rectangular Partitioning techniques as described in TABLE 2. It is observed that the PSNR vale is high and MSE value is low when compared to LSB and Non-Uniform Rectangular Partition, thus making K-means a better approach. There are various other methods like DCT, TPVD, DWT for hiding video, but they are lossy techniques and can be easily identified by steganalysis. Since video is collection of images, K-means clustering method can also be applied for hiding video inside another video.

IV. K-MEANS CLUSTERING

K-means clustering is an unsupervised learning approach of data mining used for unlabelled data. The algorithm is initiated by the estimation of k centroids randomly generated from the data set. Every data points are associated with the nearest mean to obtain k clusters. The centroid of each cluster obtained is assigned as the new mean. This is repeated iteratively until the centroids obtained are as same as those of previous iteration.
In general [8], we have n data points x i, i=1...n, where n refers to maximum number of pixels in an image that have to be partitioned in k clusters. The goal is to assign a cluster to each data point. By using K-means we find the positions μ i,i=1...k of the clusters that minimize the distance from the data points to the cluster. K-means clustering solves

$$\arg\min_{c} \sum_{i=1}^{k} \sum_{x \in ci} d(X, \mu i) = \arg\min_{c} \sum_{i=1}^{k} \sum_{x \epsilon ci} ||X - \mu i||_2^2$$

Where ci is the set of points that belongs to cluster i. The K-means clustering uses the square of the Euclidean distance $d(X, \mu i) = ||X - \mu i||_2^2$

The technique is simple, easy to implement and to interpret the clustering result. Quality of the image is retained. It is fast and efficient approach in terms of computational cost. When applied to video steganography, it is imperceptible thus making it less prone to steganalysis.

V. CONCLUSION

Comparing the performance of video steganography techniques is difficult unless identical data sets and performance measures are used. Internet banking, mobile communication security, cloud security and so on are the new application areas than can make best use of steganography to maintain secrecy of information transmitted. This paper gives an overview of different video steganography techniques applied when the information to be hidden is Image and Video. It also emphasizes the significance of applying k-means clustering technique in video steganography. This technique is widely used in various applications like image segmentation, color quantization, data mining, big data.

REFRENCES

[1] K. S. Jenifer, G. Yogaraj, and K. Rajalakshmi, ‘LSB Approach for Video Steganography to Embed Images’, vol. 5, no. 1, pp. 319–322, 2014.

[2] P. K. Sethy, K. Pradhan, and S. K. Behera, ‘A security enhanced approach for video Steganography using K-Means clustering and direct mapping’, *Int. Conf. Autom. Control Dyn. Optim. Tech. ICACDOT 2016*, pp. 618–622, 2017.

[3] A. T. Bhole and R. Patel, ‘Steganography over Video File using Random Byte Hiding and LSB Technique’, pp. 5–10, 2012.

[4] S. D. Hu and K. T. U, ‘A novel video steganography based on non-uniform rectangular partition’, *Proc. - 14th IEEE Int. Conf. Comput. Sci. Eng. CSE 2011 11th Int. Symp. Pervasive Syst. Algorithms, Networks, I-SPA 2011 10th IEEE Int. Conf. IUCC 2011*, pp. 57–61, 2011.

[5] T. Kanungo, D. M. Mount, N. S. Netanyahu, C. D. Piatko, R. Silverman, and A. Y. Wu, ‘An efficient k-means clustering algorithm: analysis and implementation’, *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 24, no. 7, pp. 881–892, 2002.

[6] S. Coe, S. Coe, and S. Coe, ‘Comparison of LSB and PVD Steganography Methods’, no. Ncesc, pp. 15–17, 2015.

[7] https://www.semanticscholar.org/paper/New-Image-Steganography-Method-Based-on-K-means-Kich-Ameur/ 937481febaf9eedeae

[8] https://en.wikipedia.org/wiki/K-means_clustering.

DOI 10.17148/IJARCCE.2018.7396