Cluster Based Video Steganography Using Pattern Matching

Ritej Gaba[#1], Gaurav Deep[*2]

[#]*University College of Engineering, Punjabi University Patiala*
Jalalabad(w), Punjab, India
[1]ritejgaba@gmail.com

[*]*University College of Engineering, Punjabi University Patiala*
Patiala, Punjab, India
[2]deepgaurav48@gmail.com

Abstract— **This paper presents methodology of a new Video Steganography technique. This technique is a cluster based Video steganography using pattern matching. We will show how pattern matching and color clustering can be used compositely to create a new video steganography technique i.e how we can hide required data in video cover media, here video is media for hiding data.**

Keywords— **Video Based Steganography(VBS), Clustering, Pattern Matching.**

I. Introduction

Steganography is the technique of hiding information within any media in such a way that others cannot discern the presence of hidden message. Technically steganography means hiding one piece of data within another. The word steganography is of greek origin and means concealed writing from the greek word steganos meaning covered or protected graphei meaning writing [1].

Hiding information to media requires following elements:

- Cover media that will hold the hidden data.
- The secret message, may be plain text, cipher text or any other type of data.
- The stego function and its inverse.
- An optional stego-key or password may be used to hide and unhide the message.

The stego function operates over cover media and the message (to be hidden) along with a stego-key (optionally) to produce a stego media. Original message is being hidden within a carrier such that the changes so occurred in the carrier are not observable. Steganography is different from the cryptography in the sense that it hides the content of the message while on the other hand cryptography scrambles the message.

A. *Carriers For Steganography*

- Text
- Image
- Audio
- Video
- Network

B. *Video Based Steganography(VBS)*

Video Steganography deals with hiding secret data or information within a video. Video based steganogrpahic techniques are broadly classified into temporal domain and spatial domain. In frequency domain, images are transformed to frequency components by using FFT, DCT or DWT and then messages are embedded in some or all of the transformed coefficients. Embedding may be bit level or in block level. Moreover in spatial domain the bits of the message can be inserted in intensity pixels of the video in LSB positions[6].

The advantage in the method is that the amount of data that can be embedded is more in LSB techniques[2]. For video steganography first of all we choose a video file as cover medium then we select a frame from it which will carry the secret message then according to our proposed embedding algorithm we embed the message bit sequentially into selected frame. To extract the massage first we read the stego video (the video file that contain secret message) and apply our proposed extract algorithm and finally we get our secret message [3].

C. *Steganography vs Watermarking*

Watermarking is used to verify the identity and authenticity of the owner of a digital image. It is a process in which the information which verifies the owner is embedded into the digital image or signal. These signals could be either videos or pictures or audios. For example, famous artists watermark their pictures and images. If somebody tries to copy the image, the watermark is copied along with the image.

Steganography is changing the image in a way that only the sender and the intended recipient is able to detect the message sent through it. It is invisible, and thus the detection is not easy. It is a better way of sending secret messages than encoded messages or cryptography as it does not attract attention to itself.

II. Cluster Based Video Steganography Using Pattern Matching

In proposed methodology, we are trying to achieve steganography in which video is choosen as carrier or cover media and for hiding information in video, this video needs to be pre processed. In pre processing first of all, frames needs to be extracted with the help of frame extractor. After extracting the frames from selected video ,the system will read the frames extracted from the video and assign numbers to all the frames then we have to choose a desired frame in which we want to hide data or information. It is to be noted that assigning different sequence to the frames every time will provide more security and make harder for the attacker to attack the frame due to unknown sequence[6].

So once selected, then clustering needs to be applied which is based on the pattern matching on color basis. After creating the clusters using pattern matching based on colors, then we can embed the secret data in particular cluster using a particular embedding algorithm. On the receiver side the extraction of the data from the video file will illustrated by reading the frames, then the desired frame can be extracted by using its sequence number after identifying the frame number the extraction function can be started. But for this we should have a brief knowledge about clustering and pattern matching by using which we are going to implement this technique.

A. Clustering

Clustering is a process of creating clusters, it means the process of organizing objects into groups whose members are similar in some way. Here groups are the clusters and cluster can be defined as a collection of objects which are similar between them and are dissimilar to the objects belonging to other clusters.

B. Pattern Matching

It is used to describe patterns which are repeating or those patterns are matched which are similar or repeating in a message or image or any data file. These patterns can be simple or complex. When pattern matching is applied all similar patterns are identified[7].

III. Methodology

The objective can be achieved through these steps:

A. On The Sender Side

1) *Input Video:* A video of particular format will be taken as input.

2) *Pre-Processing:* Selected video will undergo some pre-processing such as frame extraction with the help of particular frame extractor, this extractor will extract frames and assign numbers to frames in a sequence and then a frame will be selected which will further be used for embedding secret data or message.

3) *Scanning of frame:* Selected frame will be scanned on the basis of different colors using pattern matching.

4) *Clustering:* Create clusters on the basis of color feature.

5) *Selection of cluster:* Cluster on the basis of color will be selected in which we want to embed data.

6) *Apply steganography:* On the selected cluster steganography will be applied for hiding data.

7) *Construct video:* create video by combining all the frames including the frame carrying secret information. This is stego-video.

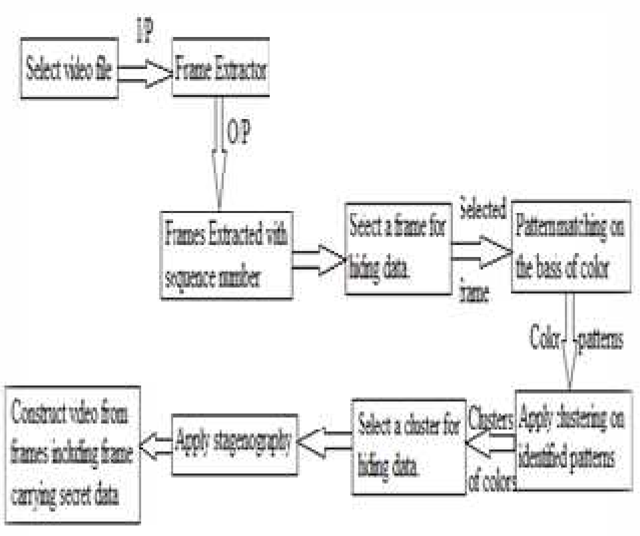
Select video file
I/P
Frame Extractor
O/P
Frames Extracted with sequence number
Seect a frame for hiding data
Selected frame
Patternmatching on the basis of color
Color patterns
Apply clustering on identified patterns
Clusters of colors
Select a cluster for hiding data
Apply stageanography
Construct video from frames including frame carrying secret data

Fig. 1 Cluster based video steganography using pattern matching

B. On The Receiver Side

1) *Extract Frames*: frames from the stego-video will be extracted using frame extractor.

2) *Scan Frame:* frame will be scanned using pattern matching.

3) *Clustering*: create cluster according to color.

4) *Identification*: identify the cluster in which information is hidden.

5) *Extract data*: extract the hidden data.

IV. Facilities Required

Facilities required to achieve this objective are as follows:

- Frame extractor is required to extract frames from a video file.(eg. Video to JPG Converter).
- Video creator from frames for creating video. (eg. Blaze media pro).
- Study of clustering algorithm which are used in color media.
- Study of pattern matching algorithms.
- Matlab software with the help of which this technique can be developed.
- Study of data structures which will be used to store data of video during processing.

V. Conclusion

In this proposed technique, the main objective of this technique is to embed data in a particular color cluster which is obtained from the frame, extracted from a particular video with the help of a frame extractor. A cluster is created by applying a clustering algorithm, which consists of pixels having same color and this color clustering is achieved by applying pattern matching based on the color. After getting the cluster of particular color secret message or data is embedded in this cluster by using a particular embedding algorithm. This technique can be applied to all the frames for hiding more data.

As we are embedding the secret message on the color cluster using pattern matching, so it becomes very difficult for the third party or the intruder to intrude in the conversation of two authorized parties and extract the secret message from the video cover carrier. Only the two interacting parties can extract the secret message by sharing some secret information and this could either be a secret key or some other data which is only known to the interacting parties not only the security can be enhanced by this technique but also the more data we can hide in the video cover media.

REFERENCES

[1] Soumyendu Das, Subhendu Das, Bijoy Bandyopadhyay and Sugata Sanyal, “Steganography and Steganalysis: Different Approaches”

[2] Arvind Kumar and KM Pooja, “Steganography- A Data Hiding Technique”, *International Journal of Computer Applications (0975 – 8887),* Volume 9– No.7, November 2010.

[3] Md. Golam Rabiul Alam, Md. Monirul Islam, Tahmina Naznen, Tasnim Niger and Shanjida Sharmin, “A Steganographic Approach In Video With Attack Detection”, *Daffodil International university journal of science and technology*, Volume 5, Issue 2, July 2010.

[4] Kousik Dasgupta, J.K. Mandal and Paramartha Dutta, “Hash Based Least Significant Bit Technique For Video Stagenography(HLSB)”, *International Journal of Security, Privacy and Trust Management (IJSPTM),* Vol. 1, No 2, April 2012.

[5] Ozdemir Cetin and Ahmet Turan Ozcerit, “ A Blind Video-Steganography Technique Based on Visible Light Wavelength for Raw Video Streams”, *1st International Syposium on Sustainable Development*, June 9-10 2009, Sarajevo.

[6] A.K Al-Frajat, H.A Jalab,Z.M Kasirun, A.A Zaidan and B.B Zaidan, “Hiding Data In Video File: An Overview”, *Journal Of Applied Sciences 10(15):* 1644-1649,2010.

[7] P. Scheunders, “Comparison Of Clustering Algorithms Applied To Color Image Quantization”, Vision Lab, Dept. of Physics, RUCA University of Antwerp.

[8] R.C. Gonzalez, and R.E. woods, “Digital Image Processing”, 2nd edition, 2002.

[9] S. Annadurai and R. Shanmugalkshmi, “Fundamentals of Digital Image Processing”, Pearson.

[10]http://software.intel.com/sites/products/documentation/hpc/ipp/ippi/ippi_ch6/ch6_color_models.html

[11] http://zone.ni.com/reference/en-XX/help/372916j-01/nvisionconcepts/color _pattern_matching/