ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 19, April 2017

Analysis on Steganographed Media content to determine the existence of embedded data

Abishek Udayashankar
Computer Science Engineering
SRM University

M.SEnthil, A.P(O.G)
Computer Science Engineering
SRM University

Joselin S
Computer Science Engineering
SRM University

***Abstract*—Video Steganography enables to hide a larger number of data into the cover video file compared to other media formats. Most of the current Steganalysis techniques to determine the steganographed video content include analyzing the video for End of File Injection methods or Empty pixel in the video file or Least Significant Bit. These techniques are less reliable for the steganalyst to determine the stego content for a video file steganographed based on content adaptive technique, in which the complex region of the video file is manipulated. The proposed system tries to analyze the video content for presence of data using analysis of the residual noise and by doing so makes it more reliable in determining the steganographed video content.**

Keywords*—Steganography, Least Significant Bit, EOF file Injection, Residual Noise.

I. INTRODUCTION

Steganography is the technique in which a message or secret data is hidden inside a cover media. Steganography is an ancient technique and the term was coined based on Greek word ”Steganos” meaning to hide in plain sight.

Steganalysis is the detection or analysis of these cover media or content to detect the presence of hidden messages. Steganography is used in various places such as printers, original media content, watermarking and video streaming services. There are several ways in which steganography is achieved and a variety of cover media formats are available. Video steganography is one such steganography method in which the hidden text is placed inside a cover video file.

Video files contain a variety of data streams for image, audio and other informational streams or meta information. hence a video based system for steganography can provide a variety of ways to hide the sensitive data. The video applications have made a big leap in the current generation and are very pervasive providing a robust and valuable opportunity for steganography based on video. The video stegangraphy paves the way for increased capacity of data hiding compared to other media formats such as Image or Audio. Steganographers have noticed the applications of video steganography and are constantly evolving the techniques used in video steganography. one such advanced steganographic technique is to hide the secret data while recording the video through DCT algorithms. Such video steganographed medias are content adaptive and achieve the encoding of data through motion coding technique rather than placing the secret data into a blank space of the pixel. This encoding technique manipulates the meta information of the video. These meta information are called atoms or boxes in a video file and they contain the motion and other video related information.

Such steganographed content prove to be a greater challenge for the steganalyst in detecting the presence of the hidden content. currently there steganalaysis techniques which check for data hidden through end of file injection techniques or data hidden in null space. such stegnalysis algorithm are less efficient in detecting information hidden through motion encoding. hence the proposed algorithm uses noise residual patterns which help in detecting the presence of hidden content. There are several such noise residual algorithms used for JPEG steganalysis, these algorithms such as UNIWARD (Universal Distortion Function) can be further extended to detect the presence of hidden content in the video formats.

A. Notations and Basic concepts

The algorithm used for Steganographing the hidden message onto the media content are through using the DCT Discrete Cosine Transformations.

DCT based encoding technique is content independent, in the sense that the media content can be of any type, the encoding can be done effectively and with less computing complexity. The DCT computation can also be easily implemented on parallel running algorithmns which highly increase its performance.

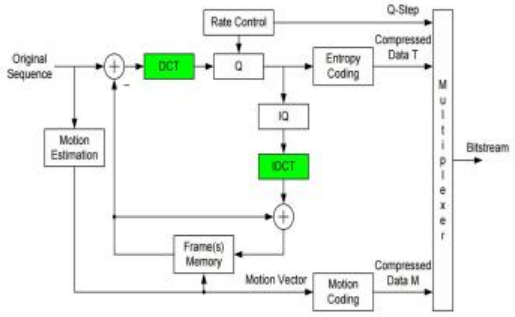


Fig:1 DCT Encoding Technique

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 19, April 2017

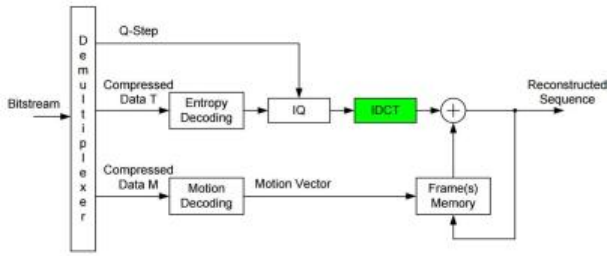


Fig. 2. DCT Decoding technique

Based on the DCT methods the hidden messages are encoded into the media content. The technique used to detect the presence of hidden message in such media content is through analyzing the media content for noise residuals. this is achieved by using a variation of the UNIWARD, a Universal Distortion functions to generate noise residual pattern graphs and determine the presence of hidden message. [7] proposed a system in which the cross-diamond search algorithm employs two diamond search patterns (a large and small) and a halfway-stop technique. It finds small motion vectors with fewer search points than the DS algorithm while maintaining similar or even better search quality. The efficient Three Step Search (E3SS) algorithm requires less computation and performs better in terms of PSNR.

2-D forward transforms

$$T(u,v)=\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} g(x,y)f(x,y,u,v)$$

2-D inverse transforms

$$g(x,y)=\sum_{u=0}^{N-1}\sum_{v=0}^{N-1} T(u,v)i(x,y,u,v)$$

The noise residual algorithm for the first order is

Rij=Xi,jXi,j+1,i1,,n1,j1,,n21.

We reduce the residual's range and to allow a compact statistical representation, R ij is truncated to the range [- T,T], R ij trunc T (R ij), where T is a positive integer, and truncT(x)=łłxTTwhenTxTwhenx¡TwhenT¡x. Since this resid- ual involves two adjacent pixels, we divide adjacent pixels in the media into several classes and compute the histogram for each class. Letpij(X,) be the embedding change probability obtained from media X while embedding payload of bpp. Given two thresholds 0¡ts¡tL¡1, we define the following four sets of residuals:

Rss=Rij—pij(X,)¡tspi,j+1(X,)¡ts

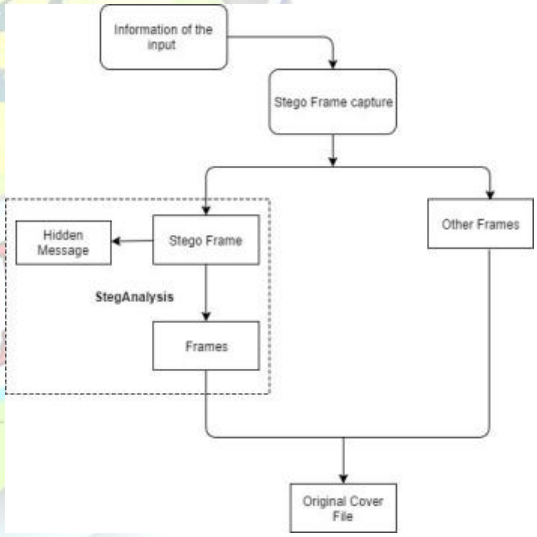
RsL=Rij—pij(X,)¡tspi,j+1(X,)¿tL

RLs=Rij—pij(X,)¿tLpi,j+1(X,)¡ts

RLL=Rij—pij(X,)¿tLpi,j+1(X,)¿tL

B. Input Video and Modules Involved

The video file is considered to be as the input. This video file can either be an original cover file or a Steganographed video file in which there is data content hidden. The goal of the system would be to analyze the input video file and determine based on the noise residual functions whether a secret data is present. The input video can be Steganographed with



secret content using the DCT technique to achieve motion encoding.

C. Media Analysis and Classification

The Analyzer and classifier is responsible for deciphering the input content. It classifies the input based on the format and applies respective noise residual algorithm to stegAnalyse the input file. It further contains two of the following modules which are the Frame capturing unit and the unit for stegana- lyzing the frame.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 19, April 2017

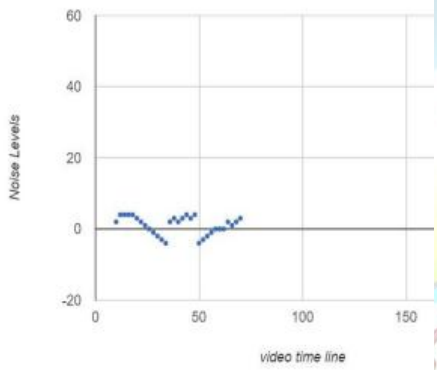
Fig. 5. Video File Information

D. Frame Capturing and StegAnalysis

The input video file is broken into several frames. These frames are analyzed to separate the hidden message from them. This is the actual part where the stegAnalysis happens. The Hidden message is separated from the Stego frame based on the noise residual patterns obtained by applying UED (Uniform Embedding Distortion) or UNIWARD histograms.These individual frames are then analyzed to determine the presence of any secret data content within it.

II. RESULT ANALYSIS

The steganographed video file and the original video file without any secret data present is analyzed and the following graphs are obtained, based on the flags or atoms in the video files. When a original



video file is analyzed the noise patterns are present in a familiar pattern without any drastic variations.

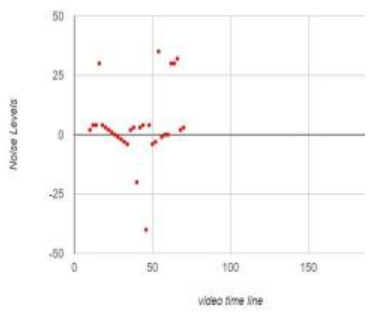
Fig. 6. Noise Pattern for Original Video File

But there can be found a large discrepancy in the noise patterns, since there are data present in the atoms, which should otherwise contain null values.

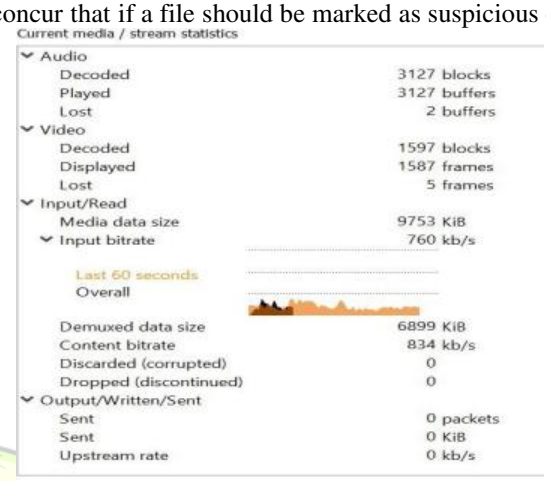
Fig. 7. Noise Pattern for Videos

Based on the flags from the graphs obtained, the system is able to analyze the content and determine the presence of secret data. The values in the flags are not consistent enough to create a fixed

signature. But by adding the positive or negative results from the flag space, it becomes possible to



concur that if a file should be marked as suspicious or



not. With a video file reader or parser, the modifications were analyzed across several video files altered by the motion encoding techniques.This identified the presence of modified flags throughout all videos. The results illustrates how hidden or secretly encoded data can be detected within an video file with high accuracy. By thoroughly examining the reserved space and analyzing for appropriate null values, it is possible to develop a very efficient video steganalysis system.

The basis of this being that, if some data is present in a field or pixel or atom in which there should have been only null values, we infer that those files are needed to be analyzed further, thus potentially detecting a steganographed media content to be analyzed further. Based on the frame loss and noise residual pattern algorithms the steganalyst can determine the presence of hidden message in a steganographed content with greater reliability. the reliability factor of the detection would increase based on the file size of the cover media. if the file size of the cover media is small the rate of detection would be higher and the rate of detection would gradually decrease as the file size increases. though there is a variation in detection rates, it is still a more reliable way to detect the presence of hidden message based on a motion encoded techinque

III. CONCLUSION

There are several renowned steganography tools, not only for video but also for other media formats such as images and audio files. Efficient techniques have been handled to ascertain embedded contents are immune to statistical steganalysis. Thus steganography especially video steganography has become a popular choice to keep their data secured. But, even such sophisticated and highly regarded

tools, it is becomes possible todetect subtle variations. presented here is one such technique to detect and exploit in such a way to detect the presence of video steganography with higher degree of accuracy. Efficient steganalysis can provide a way to not only detect the presence of steganography but also link the algorithm to the respective tool. The method presented provides nuances to the existing technique by analyzing the reserved space of multiple atoms within a video file. This technique was applied on couple of video files and found that the rate of discovery of the steganographed content was considerably higher

REFERENCES

[1] Tom Denemark, Mehdi Boroumand and Jessica Fridrich, *Steganalysis Features for Content-Adaptive JPEG Steganography*, 3rd ed. IEEE Transactions on Information Forensics and Security, 2016.

[2] Sabyasachi Samanta, Saurabh Dutta and Goutam Sanyal, *A Real Time Text Steganalysis by using Statistical Method*. 2nd IEEE International Conference on Engineering and Technology (ICETECH), March 2016, Coimbatore, India.

[3] Songtao Wu, Sheng-hua Zhong1 and Yan Liu, *Steganalysis via Deep Residual Network*. 2016 IEEE 22nd International Conference on Parallel and Distributed Systems.

[4] P.R.Vignesh Kumar, *StegAnalyzer-An Efficient Spatial Domain Steganal- ysis Tool*. 2016 International Conference on Advanced Communication Control and Computing Technologies (ICACCCT).

[5] Thomas Sloan and Julio Hernandez-Castro, *Steganalysis of OpenPuff through atomic concatenation of MP4 flags*. 2015 University of Kent, School of Computing, Canterbury, CT2 7NF, UK

[6] Aditya K and Kameswari S, *Embedding of data in motion vectors by using steganography concept.* IJRCCT 2013;2(11):1117e22.

[7] Christo Ananth, A.Sujitha Nandhini, A.Subha Shree, S.V.Ramyaa, J.Princess, "Fobe Algorithm for Video Processing", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (IJAREEIE), Vol. 3, Issue 3,March 2014 , pp 7569-7574

[8] W. Tang, H. Li, W. Luo, and J. Huang, Adaptive steganalysis against WOW embedding algorithm. in 2nd ACM IHMMSec. Workshop 2014.

[9] V. Holub, J. Fridrich, and T. Denemark, Universal distortion design for steganography in an arbitrary domain. in EURASIP Journal on Information Security, Special Issue on Revised Selected Papers of the 1st ACM IH and MMS Workshop, 2014

[10] Balaji R, Naveen G, Secure data transmission using video steganogra- phy. in 2011 IEEE International Conference on Electro/Information Technology; 2011.

[11] V. Holub and J. Fridrich, Designing steganographic distortion using di- rectional filters. in Fourth IEEE International Workshop on Information Forensics and Security, (Tenerife, Spain), December 25, 2012.