

A Survey: Secure Data Transmission on Video Embedding Using PCF Technique

K.Rajalakshmi¹ | Dr.K.Mahesh²

¹Research Scholar, Department of Computer Applications, Alagappa University, Karaikudi, Tamilnadu, India.

²Professor, Department of Computer Applications, Alagappa University, Karaikudi, Tamilnadu, India.

To Cite this Article

K.Rajalakshmi and Dr.K.Mahesh, "A Survey: Secure Data Transmission on Video Embedding Using PCF Technique", *International Journal for Modern Trends in Science and Technology*, Vol. 03, Issue 05, May 2017, pp. 279-282.

ABSTRACT

Digital Video occasionally wants to be stored and processed in an encrypted format to maintain security and privacy. Security has become the area of concern as a result of widespread use of communication medium over the internet. The Video security approach when combined with compression and embedding techniques for the efficient data transfer of the data and to maintain the secrecy of the data that is to be transmitted. Video embedding is one of the most important problems occurred on protect the data transmission in the computer world. Video Embedding based on compression is an efficient technique of video security.

From the survey results, the previous techniques do not restore the compressed video efficiently; the pixel information is lost during the transformations. Further, the existing techniques have increased time complexity and computational complexity. To avoid this problem, the proposed work using Patch wise code formation is employed. Most of the research paper has some merits and demerits using various techniques are studied and analyze in this paper. This paper presents a detailed survey of discussed video embedding method which will be helpful for future research work.

Keywords— Patch wise code formation (PCF) algorithm, Video Embedding, Video compression.

Copyright © 2017 International Journal for Modern Trends in Science and Technology
All rights reserved.

I. INTRODUCTION

Digital video represents the visual images moving in the form of digital data. Video is basically a combination of different frames and all the frames constituting a video has a fixed frame rate. These frames are vital building block for the video as well as for video encryption process. We can insert and send the text or video along with the frame by using various techniques. There are various techniques for providing security that is cryptography; Steganography and Digital Watermarking are most common techniques. Video compression is a technology used for transforming the video signals with the maintenance of the original quality under

various situations such as storage constraint, time delay constraint and power constraint.

The organization of the paper is as follows. Section II illustrates the compression techniques used for videos. Section III elaborates the various embedding techniques. Section IV describes the tables involved in the related work and Section V explains the proposed solution and Section V concludes the paper.

II. VIDEO COMPRESSION

The aim of video compression is to decrease inconsequentiality and redundancy of the video data provides capable solutions to store or transmit data in an efficient form. Video compression can be categorized as two ways such

as lossy or lossless. Lossless compression is chosen for archival purposes and frequently for medical imaging, technical drawings, clip art, or comics. Lossy compression methods are widely used, characterized by the quality of the reconstructed images and its adequacy for application. Lossy methods are especially suitable for natural videos such as imperceptible) loss of reliability is acceptable to achieve a substantial reduction in bit rate. Video Compression is the process of reducing the number of pixels in each frame by preventing the redundant information. The goal of the compression techniques is as follows,

- Reduce the color resolution and color nuances in the video
- Prevent the invisible portions of the video
- Compare the adjacent frames and remove the unchanged details between two videos.

III. VIDEO EMBEDDING

The video embedding is a process of hiding the videos with in a frame. This technique embeds the secret information/videos and the extra information within the cover video. The embedded videos are then extracted and used for various applications such as content protection, owner detection, authentication and copyright protection. The aim of the video embedding is to secure the video frames from possibly threats like as intruders can be successful is that most of the information they acquire from a system is in a form that they can read and figure out. Hackers may reveal the information to others, modify it to pretend an individual or organization, or use it to launch an attack. The embedding techniques for the video frames are classified into the following types, Digital watermarking and Data hiding algorithms.

The key advantages of the embedding techniques are:

- Robustness
- Prevention against various attacks or hackers

IV. RELATED WORK

In this section, there are several research work of some prominent authors in the same field and explained the researchers have implemented various approaches for information and data security to achieve secret communication Table.1 presents a critical study of research papers in the short description of various techniques used for video compression as well as embedding.

Title	Merits	Demerits
An Innovative Lossless compression Method for Discrete-Color Images[1]	Low complexity	This works best on mid-to-small size videos not well suited for large size Videos
Secure Data Hiding Technique Using Video Steganography and Watermarking - A Review[2]	Almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy.	The output Video by hidden data is not visually recognizable.
Analysis Of Video Steganalysis Techniques To Defend Against Statistical Attacks - A Survey[3]	The methods used in status quo are sufficiently advanced and can provide suitable defence against current attacks	The generalized 2 attack does not calculate an estimation of the message length and can be sometimes wrong if the message has a significant difference in the number of zeros compared to ones.
Data Security and Authentication Using Steganography[4]	The patchwork approach is used independent of the host Video and proves to be quite robust as the hidden message can survive conversion between lossy and lossless compression.	If the Video already contains some data you cannot add some more data for the same Video.
Analysis Of Video Steganalysis Techniques To Defend Against Statistical Attacks - A Survey[5]	Feature selection strategy implemented here gives relevant features to be used for training and thus reduces the training complexity.	It does not directly obtain the feature importance
An Extended Visual Cryptography Scheme Without Pixel Expansion	A processed Video contains white and black blocks and can be	As the new scheme does not change the share generation approach

For Halftone Videos[6]	used as an input secret Video in any visual cryptography encoding process	
Recursive Information Hiding in Visual Cryptography[8]	The idea used is to hide smaller secrets in the shares of a larger secret without an expansion in the size of the latter.	The general threshold recursive schemes are not visual cryptography schemes.
Efficient video watermarking with SWT and empirical PCA based decoding[13]	Important advantage of the SWT is the watermark need not to be strictly square in dimensions which is a mandatory condition in many transformation techniques like DCT, DWT etc.	The DWT is not a time-invariant transform. This means that, even with periodic signal extension.
Text and Video Encryption Decryption Using Advanced Encryption Standard[14]	It is suitable for mobile devices, which currently use the JPEG Video compression algorithm, due to its lower computational requirements.	An attacker can break the password in seconds by using the list of pre computed hashes .

Table: 1 Summary of Research papers

Most of the research work reviewed in this section has doing level wise compression as well as embedding. It has some drawbacks and also listed in the related work section.

V. PROPOSED SOLUTION

Most of the research work reviewed in the previous section has doing level wise compression as well as embedding. It has some drawbacks and also listed in the related work section. In order to overcome these techniques used this type of the proposed work in this research paper. At first, the input video will be split into multiple frames then each frame will be pre-processed using Fuzzy Adaptive Median Filter (FAMF). During the pre-processing process, the noises present in the

frames will be eliminated. From the idea of the proposed system we are clear with two outcomes. The outcomes will be secure transmission among receivers. These two outcomes are discussed below.

A) COMPRESSION USING PATCH CODE FORMATION:

The problem of the compression we faced there is a lack in effective decompression. If we consider compression process based on quantization using Cosine Transformations or Wavelet transformations, the results of the input Videos that is compressed may not be more effectively renovate. By using the transformations the pixel information were lost. In the encoding process the pixel information were well preserved but the compression efficiency is not improved. In order to overcome this problem lossless patch wise code formation is employed. In the patch wise based on the pixel grouping and removing the relevant and recurrent pixels. In the proposed method the videos were first reduced in size by combining the current pixel with the previous pixel. The resulting video size is nearly the half of the input video. The resulting video is then divided into small patches. In the patch recurrent pixels and their locations were identified. The identified pixel locations were placed previous to the pixel value and the process is repeated for the complete video. The result of the each patch acts as the code.

B) EMBEDDING USING LSB:

Once all the frames are compressed, the Least Significant Bit (LSB) embedding technique applied for video embedding and also it embeds the compressed frames. On the receiver end, the compressed frames are decompressed using inverse block code formation. The decompressed frames are then converted back to the videos.

VI . CONCLUSION

In this paper, based on our proposed work has introduced a method of patch based code formation for using resolved in terms of hiding information to achieve better security. compression based embedding can achieve more accuracy and reduce time complexity and provide security. Here we can use compression mainly for reduce the number of bits and also embedding process for maintain the security process. Hence, the result of our proposed work is based on simple and fast compression as well as embedding that does not degrade the video quality and security.

REFERENCES

- [1] Saif Alzhair and Arber Borici, "An Innovative Lossless compression Method for Discrete-Color Images," IEEE Transactions on Image Processing vol. 21 Issue 1 January 2015.
- [2] Shivani khosla and Paramjeet Kaur, " Secure Data Hiding Technique Using Video Steganography and Watermarking - A Review "IJCA (0975-8887)Volume 95-No 20,June 2014.
- [3] Usha B.A, N K Srinath and N K Cauvery" Analysis Of Video Steganalysis Techniques To Defend Against Statistical Attacks –A Survey", IJRET, ISSN 2319-1163.
- [4] RaviKumar and P.R.K Murti>Data Security and Authentication Using Stegnaography,"IJCSIT Vol 2(4),2011, ISSN :0975,pp. 1453-1456.
- [5] Sonali S.Ekhande Prof. S.P.Sonavane Dr. P .J .Kulkarni" UniversalSteganalysis using Feature Selection Strategy for Higher Order Video Statistics"IJCA(0975-8887) Volume 1 No-19 2013.
- [6] N. Askari, H.M. Heys, and C.R. Moloney"An Extended Visual Cryptography Scheme Without Pixel Expansion For Halftone Videos" IEEE Transactions on Image Processing 2013.
- [7] Gurpreet kaur and kamalieet kaur "Digital Watermarking and Other DataHiding Techniques" IJITEE, vol. 2, Issue 5, April 2013.
- [8] Sandeepkatta"Recursive Information Hiding in Visual Cryptography"arXiv.org>cs>arXi:1004.4914.
- [9] G. J. Garateguy, G. R. Arce and D. L. Lau" Voronoi Tessellated HalftoneMasks"IEEE Imamge processing(ICIP),2010.
- [10]R. K. Singh, D. K. Shaw, and M. J. Alam, "Experimental Studies of LSB Watermarking with Different Noise," Procedia Computer Science,vol. 54, pp. 612-620, 2015.
- [11]K. K. Gurpreet Kaur, "Image Watermarking Using LSB," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, pp. 858-861, 2013.
- [12]P. K. Shivani Khosla, "Secure Data Hiding Technique Using Video Steganography and Watermarking," International Journal of Computer Applications, vol. 95, pp. 7-12, 2014.
- [13]Teena M. Thomas "Efficient video watermarking with SWT and empirical PCA based decoding" IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-8727 Volume 16 Issue 5, 2014.
- [14]Kundankumar Rameshwar Saraf , Vishal Prakash Jagtap and Amit Kumar Mishra "Text and Video Encryption Decryption Using Advanced Encryption Standard"IJETTCS Volume 3 Issue May-June 2014.
- [15]K.Rajalakshmi,Dr.K.Mahesh 2016 "A Review on Video Compression and Embedding Techniques"International Journal of Computer Applications (0975 – 8887) Volume 141 – No.12, May 2016.
- [16]K.Rajalakshmi, Dr.K.Mahesh, "Video Embedding with Compression Based on Patchwise Code Formation", Australian Journal of Basic and Applied Sciences, Vol.10, No.13 (August), 2016, ISSN : 1991- 8178, EISSN: 2309-8414.