ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 10, April 2016

A Study on Security Issues in Video Watermarking

Shravya Jain, Venugopala P S, Dr. Sarojadevi H, Dr. Niranjan.N.Chiplunkar
PG Scholar, Dept of CSE, NMAMIT, Nitte
Associate Professor, Dept of CSE, NMAMIT, Nitte
HOD, Dept of CSE, NMAMIT, Nitte
Principal, NMAMIT, Nitte

Abstract*—Video is a visual multimedia source which forms moving pictures by combining a sequence of images. This is an era where the video plays major role in multimedia exchange. A lot of videos are transmitted over the internet which is accessible to the users with their compatible devices. The spate of the video files over the internet makes it difficult for the users to oversee the threats that inhabit within the multimedia file. Moreover the video files are affected by various attacks that either are intentional or unintentional. The hiding of malicious links with executable file is one of the intentional attacks that either causes severe damage to the host computer or extracts the users profile information. Protecting the video files and its copyright has been a major concern over years. Video watermarking is a process of hiding information within the video frames to achieve authentication. The attacks on the watermarks lead to proneness of watermarking. This paper is a survey on methods of video watermarking and the attacks that affect the watermark.

***Index Terms*—Attacks, DCT, DWT, DWT-PCA, LSB, Video.**

I. INTRODUCTION

Digital Watermarking is the key concept in copyright ownership protection of electronic data. The process involves embedding a special pattern called watermark into the electronic data. Multimedia watermarking includes image watermarking, video watermarking, audio watermarking, text watermarking and graphics watermarking. The watermarking techniques vary based on the host to be watermarked. There are various approaches discussed to watermark images. Video watermarking is a trending approach in order to protect the video authenticity. Video marketing discusses the use of video for marketing brands and services [1]. Due to the compatible characteristics of video, it is easy to convey right information to the customers via video. Video provides more user understandability of information no matter how complex the product is.

Internet technologies are improving along with the multimedia and its features. Internet users will look for more videos for accessing necessary information than the text data. A survey shows that majority online visitors are more willing to watch the videos than spend time reading contents. Valuable information can be shared effectively using video. The videos are optimized to be made use in mobile devices. With such rapid development of the video, the attacks over them are also increasing. The attacks on video differ from that of images. The attacks like frame averaging, frame swapping and frame dropping are precise on videos. The watermarks that are embedded should be robust enough to withstand the attacks. There are enumerable approaches that explain video watermarking.

Watermarking comprises of three steps which involves embed, attack and extract as shown in Fig. 1. The host is watermarked in embedding phase using a unique watermarking algorithm. In the intermediate phase the attacks on the watermarked host is attempted either intentionally or unintentionally. The extraction phase extracts the watermark. Similar to image watermark, video watermark can be either visible or invisible. The visible watermarks can not only provide authenticity but is also used to advertise the brands and other information in the video. They are more susceptible to attacks since the position of the watermark is known, it makes the attacker's job easy. The invisible watermark is robust than visible watermarks. Video watermarking techniques include spatial domain watermarking, frequency domain watermarking and MPEG coding structure based watermarking [2]. Video watermarking comprise various application like copyright protection, source tracking to track the product originality, broadcast monitoring, Fingerprinting to avoid producing replicas of original, authentication and security of the digital information. This paper is a survey on the video watermarking techniques and the discussion of attacks over the watermarks.

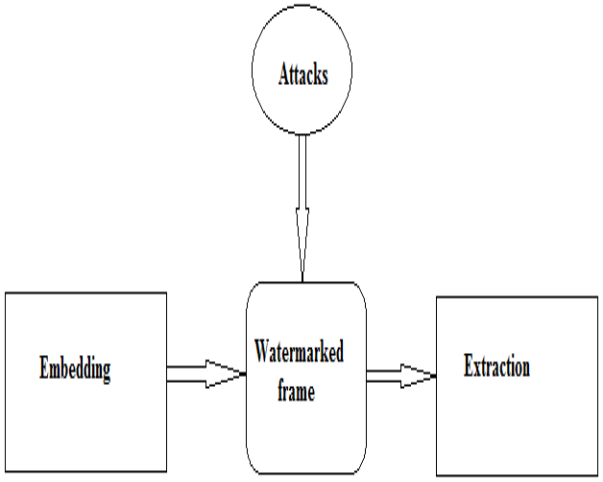

Fig. 1. Basic concept of watermarking

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 10, April 2016

II. METHODOLOGY

A. *Video Watermarking in Spatial Domain*

Spatial domain watermarking alters the pixel values of the image or frame for watermarking. Watermarking in spatial domain is easier to implement but less robust than watermarking with transformation. Spatial methods are sensible to attacks like geometric attacks and synchronization attacks [3]. Least Significant Bit (LSB) watermarking is considered to be easiest method in spatial domain method. Video frames are the still images of the video. The frames are generated depending on the frames per second of the video signal. Video frame pixels of grey level are 8-bit data value representation [2]. Once video frames are divided into 8 bit planes the LSB bits of the frame can be replaced with the watermark bit values.

The LSB method of video watermarking is not constant. There are varying methods to implement the idea. One of the methods proposed [4] enumerates that the number of frames extracted should be same as the number of watermark string character. Based on the condition if the number of frames and characters are equal the watermarking process is carried out. Binary string of watermark bits is appended to the length of the watermark string. Dividing the frames into alpha, red, green and blue components and inserting single character into every single frame is the technique used here. As shown in Fig. 2. the watermark bits are embedded into the frames. Extracting characters from every frame generates the watermark.

B. *Video Watermarking in Frequency Domain*

Watermarking in frequency domain is robust than spatial method. The transformation is applied on the frames. There are several methods of frequency domain watermarking which includes Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), Principal Component Analysis (PCA), and Singular Value Decomposition (SVD). The watermarking can be done but combining the features of different methods.

In DCT method [2], the images are decomposed into high, middle and low frequency bands. Since the middle band does not contain more important visual information, it is chosen for watermarking. It is more robust against attacks like frame averaging and dropping. In vandana et.al work [5], they consider DCT method of watermarking on an AVI file. Each frame is decomposed into RGB channel, DCT is performed on any selected channel. Secret bits are embedded into higher coefficients. The secret image bits are converted into binary bits. By calculating the bits to be embedded in each frame the number of frames to be watermarked is determined. Here 16 bits are embedded per 8×8 higher order DCT coefficients. After performing inverse DCT on the frames, AVI is reconstructed. The DFT is a multi-bit method of watermarking.

There are several approaches given for DWT based implementation. In DWT, the single, 2D or 3D transformation is applied to the host. This generates four components representing approximate, horizontal, vertical and diagonal coefficients. In jianzhong Li et.al [6] work 2D wavelet domain is used for video watermarking. After dividing host video into GOPs the watermark is embedded into the lower frequency coefficient. The frames in GOPs are decomposed into color components. In this experiment Blue channel was chosen for watermarking. In frequency domain, the methods can be combined to generate a new technique which provides better robustness. The DWT and PCA techniques are used to watermark the host video [7]. Here the host video is decomposed into color frames. The RGB components are then converted into YUV components. Y component representing the luminance is considered for transformation.

The approximate (LL), horizontal (HL), vertical (LH) and diagonal (HH) components are formed after transformation. Since lower frequency components are less suspicious to attacks LL and HH components are chosen. The LL and HH is divided into non overlapping blocks. PCA is applied to these lower frequency bands. Watermark is converted into a vector to apply it over the host. PCA is a mathematical procedure which uses orthogonal transformation, converting a set of observation of possible correlated variables into set of uncorrelated variables called principal component. To identify patterns in data and to express the data for highlighting difference and similarity, PCA is used. Inverse PCA on principal components are applied to obtain wavelet coefficient followed by inverse DWT forming luminance component. Extraction process makes use of original and watermarked video frame. The luminance value is obtained from both frames followed by wavelet decomposition. The lower frequency components divided into non overlapping blocks. PCA is applied to the components. Watermark is extracted with the formula, Refer to (1)

$$W_x = (V\text{-}V')/\alpha \qquad (1)$$

Where V is original frame after DWT and PCA application and V' is watermark video frame after DWT and PCA application, α is watermark strength.

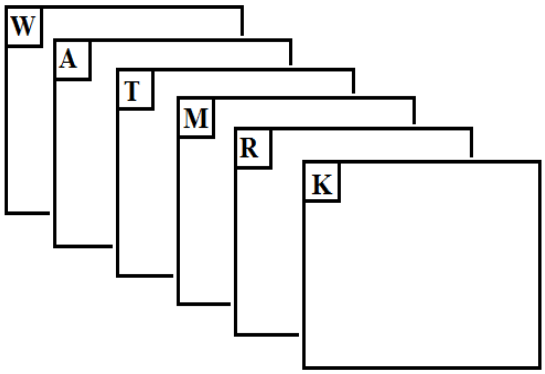

Fig. 2. Embedding string characters to the frames

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 10, April 2016

The watermarking based on MPEG coding structures [2] uses MPEG coding structures with the aim to combine watermarking and compression to reduce real-time video processing complexity.

C. Attacks on Video Watermarks

Attacks are generally defined as modification attempted by the third parties to remove the watermark or making it undetectable. The attacks on watermark differ based on the host. The major attacks concerned with video include frame averaging, frame swapping, frame dropping and statistical analysis. Averaging considers several video frames which are converted to single frame decreasing the quality of video. In swapping the sequence of the video frames are altered by swapping their positions. Dropping leads to disturbing the video sequence by removing one or more frames in between. Statistical analysis uses the videos statistical characteristics. It tries to remove the watermark, trying to obtain unwatermarked frame. Other attacks related to image watermarking is also introduced like cropping, noise, rotation and many others.

D. Evaluation Parameter

The performance of the watermarking technique is measured by the parameters used for evaluation. The PSNR (Peak Signal-to-noise ratio) and MSE (Mean Square Error) are popularly used parameters. PSNR in decibels gives the quality measurement between the host image and frames that are to be compared. The perception level is determined by PSNR, higher the value higher is the perception and video quality and vice-versa. Equation (2) gives the PSNR value of the frames to be compared.

$$PSNR = 10\log_{10}(R^2/MSE) \qquad (2)$$

where R represents Maximum fluctuation in input data type. To measure PSNR, the error metric MSE has to be calculated. MSE gives the degree of similarity or conversely the level of error between the hosts to be compared. Equation (3) gives the MSE value.

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \qquad (3)$$

where m and n are number of rows and columns in the image. I represent the noise/attack free image and K represents noisy approximation it.

III. RESULTS AND DISCUSSION

The watermark is robust if it resists attacks. Efficiency of watermarking algorithm can be determined by its behavior towards various attacks. Here the results of the video watermarking techniques are considered and based on this a discussion of techniques that are robust is conducted. In spatial domain, LSB method of implementation was considered. The watermark string is successfully embedded and extracted using LSB [4]. Discussing attacks on the watermarked frames, if frames are dropped or swapped the sequence of frames changes resulting in distortion of watermark. It also depends on the number of frames extracted. Since consecutive frames are not watermarked, averaging attacks will not cause much problem. The rotation, noise and cropping of frame changes the color pixel values. This can cause destruction of watermark.

In frequency domain DCT on AVI file was considered [5]. The robustness of the method was not discussed in the paper but based on the method of watermarking the overview on attacks can be discussed. Here if the watermark bits are inserted into sequence of frames the drop, swap or averaging frame can cause watermark bits to be manipulated. The cropping and noise changes pixel values which also causes distortion. Fig. 3 and Fig. 4 shows the method of frame dropping and frame swapping which changes the frame order.

In DWT method where the frames divided into GOPs [6] and watermark bits inserted into lower DWT components, various attacks were introduced to test for the robustness of the algorithm. The evaluation parameters PSNR (Peak Signal-to-noise Ratio) and BER (Bit Error Rate) are used to check the efficiency. The graph in Fig. 5 represents the BER exhibiting correctness of extracted video. This method does not need the host video in extraction process which is blind method of watermarking. This method provides better robustness towards attacks.

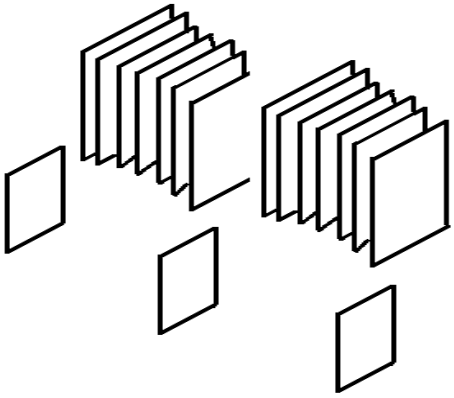

Fig. 3. Frame dropping attack

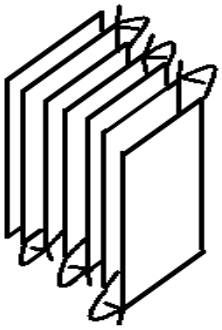

Fig. 4. Frame swapping attack

The DWT-PCA method proposed [7] considers attacks like salt & pepper, Gaussian Noise, Median Filtering, Rotation and cropping. The Normalized correlation (NC) gives the similarity and differential check between the hosts. Peak

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 10, April 2016

value one state identical and zero represents there exists differs between hosts. PSNR is used for performance evaluation. This method of watermarking is considered robust against video processing attacks as shown in the graph of Fig. 6. Since each frame can be watermarked individually, frame dropping and swapping will not alter the watermark. With the fact that watermarking each frame takes more time for computation, if only selected frame is chosen for watermarking and attacks on them are introduced then it might lead to destruction of watermark.

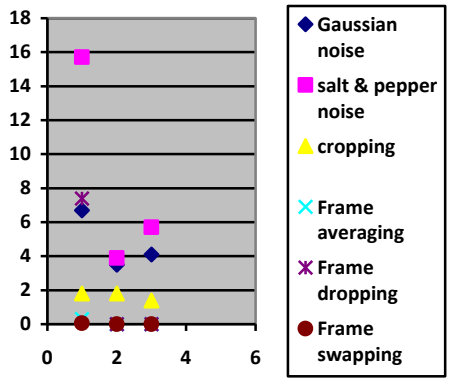

Fig. 5. Graph representing BER of videos towards various attacks.

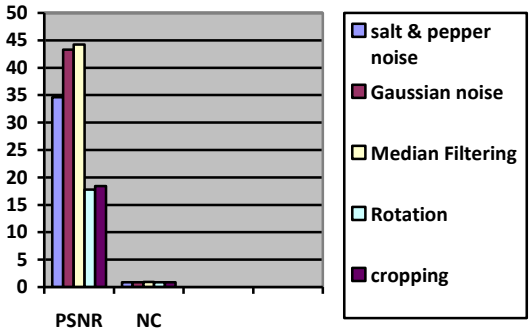

Fig. 6. Graph representation of performance of DWT-PCA towards attacks

IV. CONCLUSION

This paper describes methods of digital watermarking which provide security to the digital video. Result of attacks on watermark can help in building a robust watermarking technique that is resistant to attacks. An attack can give different results for videos with different method of watermarking.

REFERENCES

[1] http://www.business2community.com/content-marketing/16-facts-video-marketing-will-keep-night-0844491#TqZ55rbMsWFBGZXV.97

[2] Nithin A. Shelke and Dr. P.N.Chatur, "A Survey on Various Digital Video Watermarking Schemes", IJCSET, Vol. 4, No. 12, Dec 2013.

[3] Venugopala P S, Shravya jain, Sarojadevi H, Niranjan.N.Chiplunkar, " Study of Possible Attacks on Image and Video Watermark", 3rd International Conference on Computing for Sustainable Global Development, IEEE, INDIACom-2016.

[4] Venugopala P S, Ankitha.A.Nayak, Sarojadevi H, Niranjan.N.Chiplunkar, "Video Watermarking for Android Mobile Devices", 3rd International Conference on Computing for Sustainable Global Development, IEEE, INDIACom-2016.

[5] Vandana Thakur and Monjul Saikia, "Hiding Secret Image in Video," International Conference on Intelligent Systems and Signal Processing (ISSP), IEEE, 2013.

[6] Jianzhong Li, Yinghui Zhu, Ping Zhong, Cai Guo, "Robust Wavelet-Based Watermarking Scheme For Video Copyright Protection," IEEE, 7th International Conference on Image and Signal Processing, 2014.

[7] Mr Mohan A Chimanna, Prof.S.R.Khot, "Robustness of video watermarking against various attacks using wavelet Transform Techniques and Principal Component Analysis," online.